

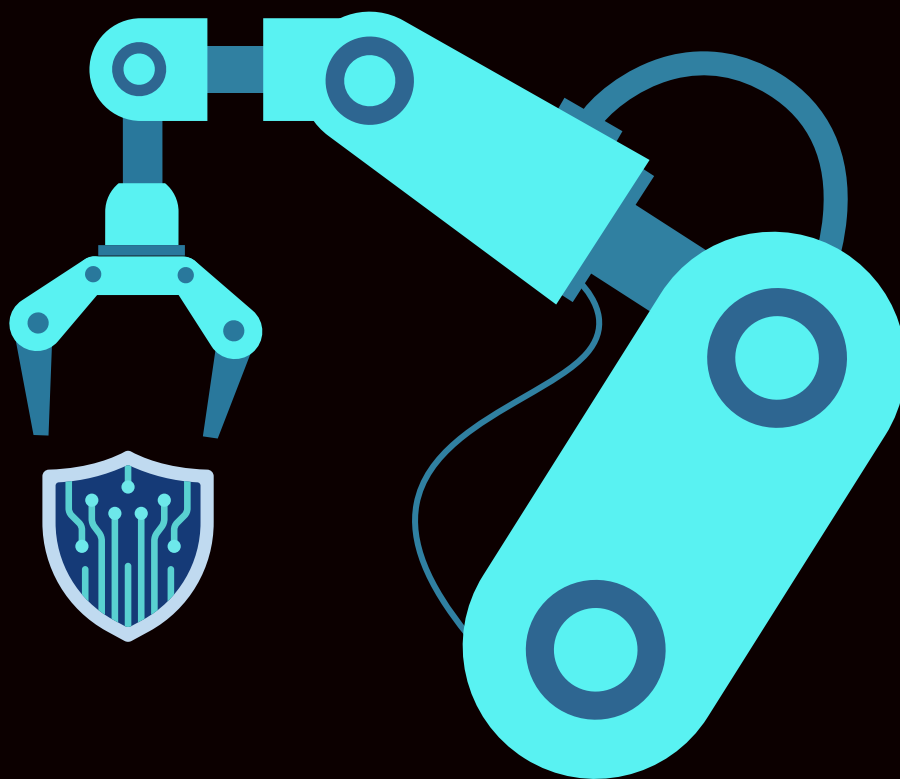
---

# INDUSTRIAL CYBERSECURITY

**Luca Durante**

Primo Ricercatore presso l'Istituto di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni del Consiglio Nazionale delle Ricerche (CNR-IEIT) di Torino

WHITEPAPER 02/2024



 **ICT  
Security**  
MAGAZINE

**ninjaOne®**

# INDICE

**06**

**Introduzione**

**09**

**Nomenclatura e differenze tra CPSs e sistemi IT tradizionali**

Nomenclatura

Differenze tra i sistemi IT tradizionali  
e i sistemi CPS

**12**

**Tipologie di CPS**

**16**

**Esempi di attacchi cyber a CPS**

**22**

**Gli attacchi più diffusi e le  
contromisure**

**25** I pilastri della sicurezza

**28** Architettura per la sicurezza

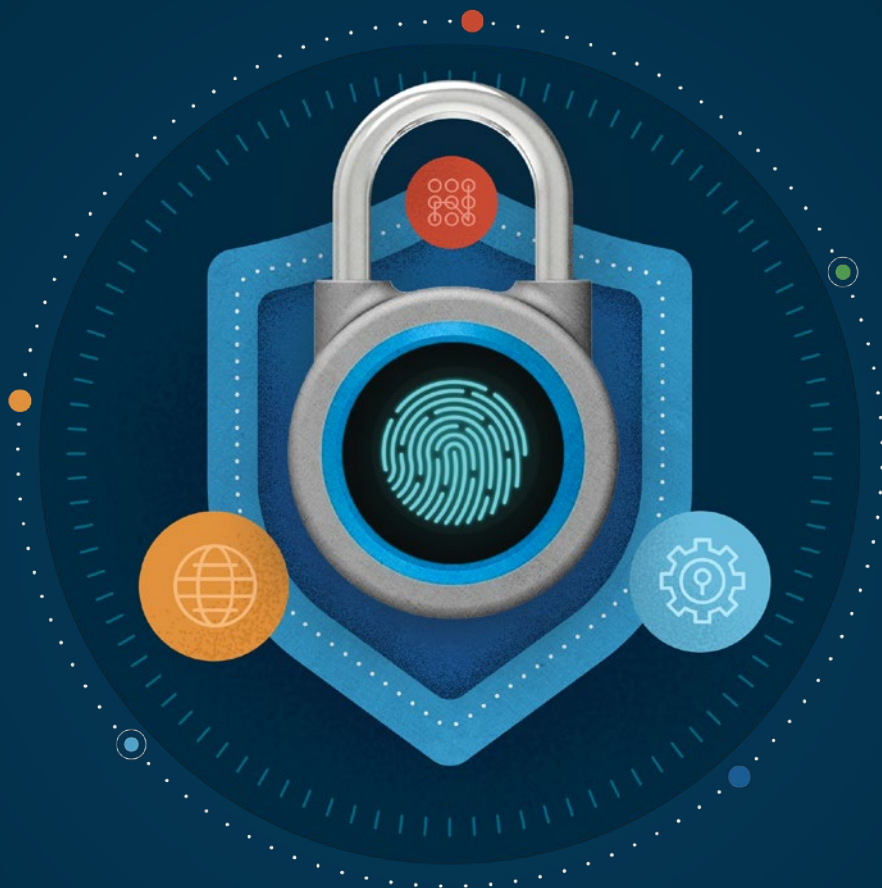
Analisi

Riconfigurazione Dinamica

Prestazioni

**37** Conclusioni

**38** Bibliografia



# Protezione da minacce informatiche a 360°

Con NinjaOne, ottieni una visibilità completa e una rapida risposta alle minacce, applicando patch, distribuendo applicazioni di sicurezza e gestendo backup da un'unica interfaccia semplice e intuitiva.

Scopri di più su NinjaOne oggi stesso! →



# ABOUT THE AUTHOR

## Luca Durante

*Primo Ricercatore presso l'Istituto di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni del Consiglio Nazionale delle Ricerche (CNR-IEIIT) di Torino*

Luca Durante è Primo Ricercatore presso l'Istituto di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni del Consiglio Nazionale delle Ricerche (CNR-IEIIT) di Torino.

Nel 1996 ha conseguito il Dottorato di Ricerca in Ingegneria Informatica presso il Politecnico di Torino, è autore di oltre 70 articoli per riviste e conferenze internazionali, ed è stato ed è tuttora Responsabile Scientifico per il CNR in Progetti Europei e in contratti di ricerca con aziende.

È stato inoltre general co-chair, program co-chair e membro del comitato di programma di conferenze internazionali, associate editor di IEEE Transactions on Industrial Informatics e revisore per riviste internazionali.

Gli interessi di ricerca vertono principalmente sulle tematiche di sicurezza informatica, attualmente declinati sulle policy di sicurezza per il controllo di accessi e la sicurezza dei sistemi cyber-fisici.

# Introduzione

Le reti industriali appartengono alla più vasta categoria dei cosiddetti *Cyber-Physical Systems* (CPS) che include, ad esempio: impianti e infrastrutture di produzione e distribuzione di energia elettrica (smart grid), acqua, gas, petrolio, raffinerie, impianti di trattamento acque e fabbriche intelligenti, infrastrutture di controllo e gestione dei trasporti terrestri, acquatici e aerei, fino al singolo veicolo (aereo, nave, treno o automobile). Quindi sistemi, mobili o immobili, con enormi differenze in termini innanzitutto di estensione, da migliaia di chilometri a qualche metro, da transnazionali a confinate in un capannone industriale.

Nonostante le differenze, vi sono sufficienti punti in comune da giustificare la classificazione unitaria in CPS.

In effetti, la dicitura *cyber-physical* racchiude la comunanza tra sistemi così eterogenei:

*“Un **sistema ciberfisico** o **ciber-fisico** (CPS, dall'inglese cyber-physical system) è un sistema informatico in grado di interagire in modo continuo con il sistema fisico in cui opera. Il sistema è composto da elementi fisici dotati ciascuno di capacità computazionale e riunisce strettamente le cosiddette “tre C”: capacità computazionale, comunicazione e capacità di controllo. Le strutture artificiali di calcolo e comunicazione, rappresentate dal prefisso “ciber”, formano un sistema distribuito che interagisce direttamente e dinamicamente con il mondo reale che le circonda. Alla base del sistema, il singolo elemento è il dispositivo embedded. Tra le possibili applicazioni: smart grid, controllo intelligente del traffico, domotica, robot cooperanti, telecomunicazioni, automobilismo, avionica, fabbriche intelligenti.”* (Fonte: [https://it.wikipedia.org/wiki/Sistema\\_ciberfisico](https://it.wikipedia.org/wiki/Sistema_ciberfisico))

In particolare, la nozione di “sistema distribuito che interagisce direttamente e dinamicamente con il mondo reale che le circonda” è il fulcro di tutto ciò che concerne la *security*<sup>1</sup>: qualsiasi alterazione, accidentale o malevola, alle strutture di computazione, comunicazione o controllo (lato cyber), ha impatti diretti sul mondo reale (lato fisico), quindi sull'ambiente e, direttamente o indirettamente, sulle persone, cioè sul piano della *safety*<sup>1</sup>.

La prima peculiarità, dunque, che i sistemi CPS hanno rispetto agli IT (*Information Technology*) tradizionali

---

1. Il termine **sicurezza**, quando inteso come **difesa**, verrà sempre utilizzato nella sua traduzione inglese *security*; mentre, quando inteso come **incolumità**, verrà sempre tradotto in *safety*.

è la connessione diretta col mondo fisico mediante la componente OT (*Operational Technology*): sensori, controllori e attuatori, che determina una connessione indissolubile tra *security* e *safety*, imponendo nuovi modelli per il calcolo del rischio e la quantificazione delle conseguenze.

La seconda peculiarità che accomuna i CPS è costituita da una serie di differenze che li distingue dai sistemi IT tradizionali. Si tratta dei loro requisiti funzionali e prestazionali, tre su tutti: determinismo, affidabilità (*reliability*) e disponibilità (*availability*), che potranno avere “scale” diverse per ciascuna tipologia di CPS ma che, con buona approssimazione, sono presenti in tutti.

In sostanza, nei CPS odierni coesistono e sono intercomunicanti le componenti IT e OT (Tabella 1): quindi la superficie di attacco è maggiore e le debolezze di una componente come le sue peculiarità, possono essere utilizzate per veicolare attacchi all'altra [1].

La restante parte del documento è organizzata come segue: un capitolo dedicato alle differenze tra i sistemi CPS e quelli tradizionali, a cui ne segue un secondo con esempi di sistemi CPS, per mostrare l'ampia varietà nel settore. A seguire, alcuni esempi di attacchi saliti alla ribalta mediatica, descritti con dovizia di particolari; poi una disamina delle tipologie di attacchi più frequenti ai CPS e relative contromisure. L'ultimo capitolo, che conclude la parte tecnica, riguarda la costruzione di un CPS sicuro da un punto di vista architetturale, con alcuni esempi mirati; seguono le conclusioni e una bibliografia tematica.

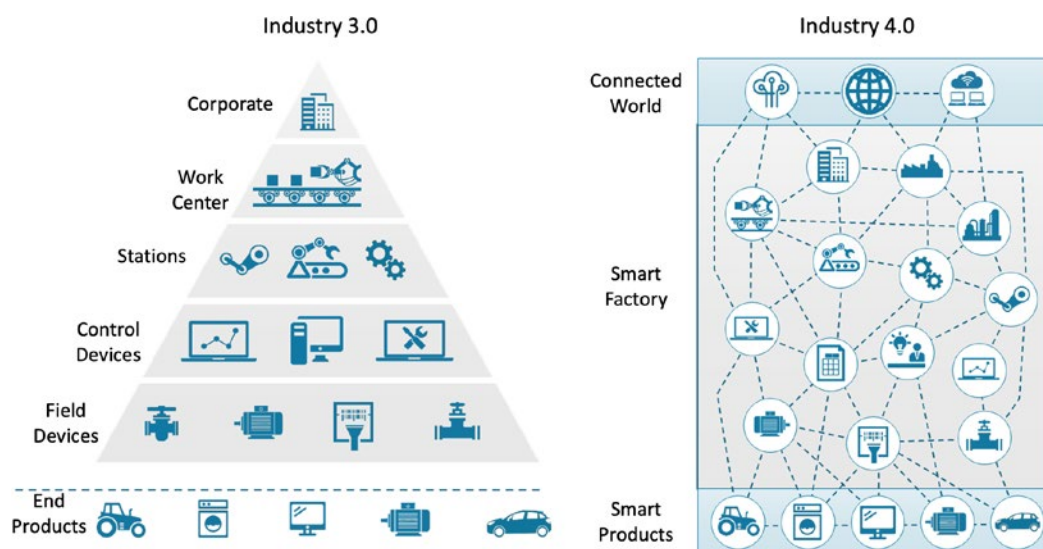


Figura 1: HIERARCHY LEVELS OF INDUSTRY 3.0 AND RAMI 4.0 (SOURCE: PLATFORM I4.0 AND ZVEI)

|                               | IT                                             | OT                                                                                                                                                                                                                  |
|-------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aggiornamenti SW e HW         | Frequenti con poca o senza pianificazione      | Pianificazione obbligatoria e su termini medio-lunghi                                                                                                                                                               |
| Protocolli di comunicazione   | TCP/IP e UDP: HTTP(S), (S) FTP, UDP, SMTP, SSH | <b><u>Wired Fieldbus</u></b> : DeviceNet, DNP3, BACnet, Modbus<br><b><u>Wired Industrial Ethernet</u></b> : Modbus-TCP, EtherCAT, Profinet, Ethernet/IP<br><b><u>Wireless</u></b> : WirelessHART, ZigBee, Bluetooth |
| Applicazioni/task             | Massimizzare il throughput                     | Real-time / determinismo                                                                                                                                                                                            |
| Vita media degli apparati     | 1-5 anni                                       | Anche oltre i 20 anni                                                                                                                                                                                               |
| Priorità di sicurezza         | Confidentiality                                | Availability                                                                                                                                                                                                        |
| Meccanismi di sicurezza       | Presenti                                       | Raramente presenti                                                                                                                                                                                                  |
| Competenze in sicurezza       | Elevate / molto elevate                        | Scarse / molto scarse                                                                                                                                                                                               |
| Danni da cyberattack          | Reputazione, informazioni, denaro              | Beni materiali, ambientali e vite umane                                                                                                                                                                             |
| Costi indotti dai cyberattack | Stimabili                                      | Difficilmente stimabili                                                                                                                                                                                             |

Tabella 1: Principali differenze tra sistemi IT e sistemi OT

# Nomenclatura e differenze tra CPSs e sistemi IT tradizionali

## Nomenclatura

Nella letteratura tecnico-scientifica coesistono moltissimi termini, acronimi e classificazioni per i sistemi CPS:

- *Industrial Cyber Physical System* (ICPS): sistema prettamente industriale. La specializzazione “industrial” non è rilevante ai fini della presente trattazione;
- *Industrial Control System* (ICS) e *Distributed Control System* (DCS) appartengono alla categoria dei CPS. In particolare, i DCS sono in stretta connessione a Internet e a servizi anche cloud;
- *Critical Infrastructure* (CI) è il sistema fisico a cui un CPS sovrintende;
- *Industrial Wireless Sensor Network* (IWSN) è un CPS dove la comunicazione wireless da/tra sensori è prevalente;
- *Industrial Internet of Things* (IIoT) è un sistema basato su *Supervisory Control And Data Acquisition* (SCADA).

## Differenze tra i sistemi IT tradizionali e i sistemi CPS

Per i CPS si considera la componente OT, peculiare rispetto alla parte IT; e queste due componenti presentano profonde differenze che non possono essere ignorate quando si tratta di sicurezza. La Tabella 1 riassume alcuni aspetti principali che devono essere presi in considerazione con attenzione.

Come mostra la tabella, i sistemi IT e OT sono molto diversi dal punto di vista dell'architettura, della gestione e della manutenzione: queste differenze sono principalmente dovute al tipo di missioni che devono supportare. I sistemi OT, infatti, pongono numerosi vincoli (ad esempio, sui tempi massimi di reazione e sulla massima indisponibilità tollerabile per il sistema) che sono, invece, assenti o marginali nei sistemi IT.

| Priorità<br>crescente  | IT              | OT              |
|---------------------------------------------------------------------------------------------------------|-----------------|-----------------|
|                                                                                                         | Confidentiality | Availability    |
|                                                                                                         | Integrity       | Integrity       |
|                                                                                                         | Availability    | Confidentiality |

Tabella 2: Priorità dei requisiti di sicurezza

|                                | IT          | OT      |
|--------------------------------|-------------|---------|
| Aggiornamenti SW e HW          | Non critico | Critico |
| Vincoli real-time              | Non critico | Critico |
| Conseguenze di attacchi/guasti | Non critico | Critico |
| Prestazioni e consumi          | Non critico | Critico |

Tabella 3: Criticità dei sistemi IT e OT

Inevitabilmente, ciò ha anche un impatto sulle alternative progettuali disponibili e influenza pesantemente le scelte per i componenti h/w e s/w. Ad esempio, i sistemi operativi e i protocolli di comunicazione su cui si basano i sistemi OT sono più interessati ad aspetti come l'elaborazione in tempo reale, la limitazione del *jitter* e la notifica degli eventi rispetto ai sistemi IT, mentre i dispositivi hanno architetture h/w più semplici e una potenza di calcolo generalmente inferiore.

Purtroppo, a causa di queste e altre peculiarità (Tabella 1), lo scenario di sicurezza è anche significativamente diverso nei due casi, come mostra la parte inferiore della tabella. Pertanto le popolari strategie e meccanismi sviluppati per proteggere i sistemi IT non sempre possono essere adottati nella maggior parte dei sistemi OT, che pongono quindi nuove sfide per la sicurezza delle informazioni.

In sintesi le più classiche proprietà di sicurezza sono contenute nell'acronimo **CIA** [2], [3]:

- **Confidentiality** (riservatezza): la garanzia che le informazioni non vengano rese disponibili o divulgate a persone, entità o processi non autorizzati.
- **Integrity** (integrità): la capacità di salvaguardare l'accuratezza e la completezza delle risorse;

- **Availability** (disponibilità): la capacità di essere accessibile e utilizzabile su richiesta da parte di altre entità;

Tali proprietà vanno soggette, nei due casi, a priorità inverse (Tabella 2) e le strategie di mitigazione devono tenere conto delle principali criticità dei sistemi OT rispetto a quelli IT (Tabella 3):

- La pratica diffusa di *patching* e aggiornamento h/w e s/w (un'attività di routine nel mondo IT che aiuta a far fronte alle nuove vulnerabilità man mano che vengono scoperte e conseguentemente sviluppate gli aggiornamenti software) di solito richiede che (parte del) sistema/impianto controllato sia temporaneamente reso inaccessibile. Nel mondo OT, sfortunatamente, questa azione deve spesso essere pianificata molto prima (anche settimane o mesi) rispetto al tempo programmato. In altre parole, il requisito di disponibilità difficilmente potrebbe essere compatibile con le attività di *patching/upgrading* tempestivo.
- I vincoli in tempo reale della maggior parte dei sistemi OT possono rendere difficile o addirittura impossibile eseguire azioni asincrone e/o sporadiche, come gli aggiornamenti dell'antivirus. Inoltre, l'adozione di firewall e filtri complessi comunemente utilizzati nei sistemi IT può introdurre ritardi imprevedibili o inaccettabili nelle reti di elaborazione e controllo.
- Le conseguenze dei fallimenti in sistemi IT sono generalmente limitate a perdite finanziarie e/o di reputazione, perché solo i dati (informazioni) necessitano di protezione. Questo aspetto è sicuramente importante anche per il mondo OT ma, in questo caso, i guasti possono anche causare danni all'ambiente gravi o catastrofici, insieme a danni alle persone e persino perdite di vite umane (Tabella 1). Ciò è dovuto principalmente alla stretta interdipendenza tra *security* e *safety* nel mondo OT. .
- Le prestazioni e la potenza sono fondamentali nel mondo OT, dove molti dispositivi di campo e di controllo hanno capacità di calcolo ridotte e/o disponibilità di energia limitata (ad esempio, dispositivi alimentati a batteria nelle reti di sensori). Ciò rende impraticabile, ad esempio, l'uso di sofisticati meccanismi di crittografia e protocolli di sicurezza che di solito richiedono ingenti risorse di calcolo e comunicazione.

A causa del complesso scenario così brevemente introdotto, il problema della messa in sicurezza di sistemi OT non può essere risolto semplicemente adottando le stesse tecniche sviluppate per il mondo IT, sebbene gli ingredienti di base che costruiscono l'intero processo possano essere gli stessi. Nella maggior parte dei casi, infatti, sono necessari adattamenti delle metodologie in uso nei sistemi IT, se non diverse soluzioni scientifiche e tecnologiche.

# Tipologie di CPS

La Figura 1 illustra le caratteristiche dell'architettura di riferimento "tradizionale" e quella "smart" di Industry 4.0: da una struttura gerarchica, con confini e interfacce ben definite, si passa ad una struttura fortemente connessa, non più gerarchica, quindi certamente più fluida e flessibile (anche per quanto riguarda gli *ingressi* e le *uscite* di nodi, anche mobili, dal sistema) ma anche maggiormente esposta: connettività, flessibilità ed esposizione agli attacchi vanno di pari passo e quindi, a fronte dei vantaggi, occorre sempre attivamente predisporre contromisure per mitigare gli svantaggi.

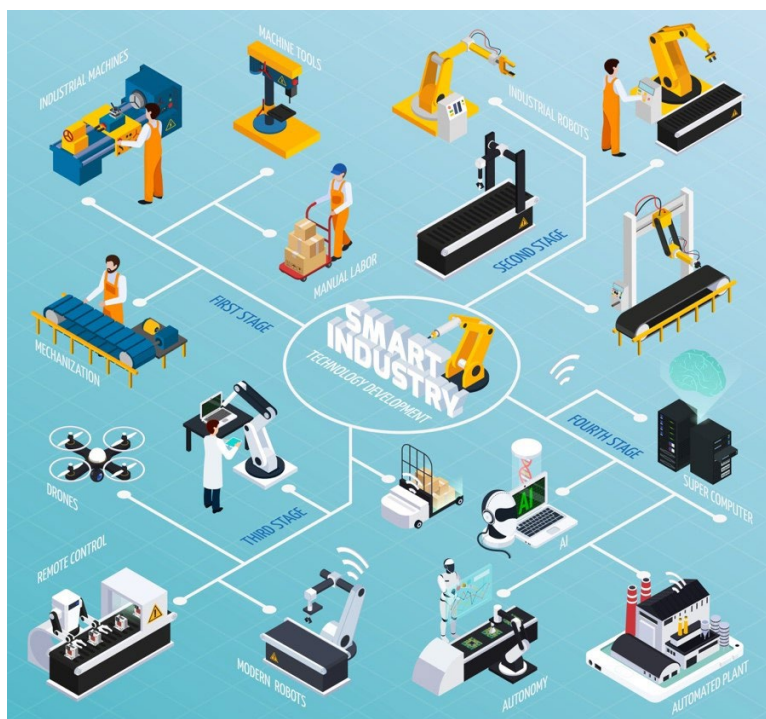


Figura 2: CPS industriale

Un elemento degno di particolare nota è che nella "visione" Industry 4.0 il cordone ombelicale tra la Smart Factory e lo Smart Product permane, ad esempio per manutenzioni programmate e non, statistiche di uso e funzionamento, ricambi, garanzia, riparazioni, aggiornamenti software e firmware dello Smart Product o dell'app che lo controlla/gestisce.



Figura 3: Smart grid

La Figura 1 riproduce lo schema astratto di un impianto industriale, ma alcuni tratti architettureali caratterizzanti saranno presenti anche in altri CPS: connessione a Internet, presenza di servizi *cloud*, elevato grado di connessione di rete tra gli elementi, sia *wired* che *wireless*, oltre ai vincoli funzionali e prestazionali già descritti.

Il medesimo grado di interconnessione si rileva anche in rappresentazioni meno astratte di CPS, come quello mostrato in Figura 2, dove è riconoscibile un ambiente industriale con le varie componenti e le loro interconnessioni funzionali e di comunicazione.

Esistono altre importanti declinazioni del concetto di CPS: ad esempio le *Smart Grid*, come schematizzato in Figura 3, dove lo scambio di informazioni tra i soggetti coinvolti riguarda sia il consumo che la produzione di energia, che oggi può avvenire in modo capillare sul territorio, dove la tradizionale figura di utente consumatore si è estesa anche a produttore. In tal caso la necessità di scambio di dati tra i vari attori è continua, non solo per consumo e produzione nei due sensi, con relativa tariffazione, ma anche per la gestione delle attività di manutenzione e degli allarmi di ciascuna installazione. Un altro esempio di CPS (utile nel prosieguo) è quello di trattamento delle acque: che lega la gestione delle acque da trattare, le risorse necessarie al trattamento, la gestione dei flussi all'interno dell'impianto e le misurazioni automatiche dei parametri di qualità durante ciascuna fase del trattamento, come mostrato in Figura 4.

La Figura 5 mostra un ulteriore CPS appartenente all'ormai molto popolata categoria dei mezzi di trasporto, un tempo soltanto fisici e oggi con una componente cyber sempre in aumento, sia per la gestione intra-veicolo che inter-veicoli, nonché da/a altre infrastrutture, quali l'assistenza alla guida autonoma e i vari allarmi.

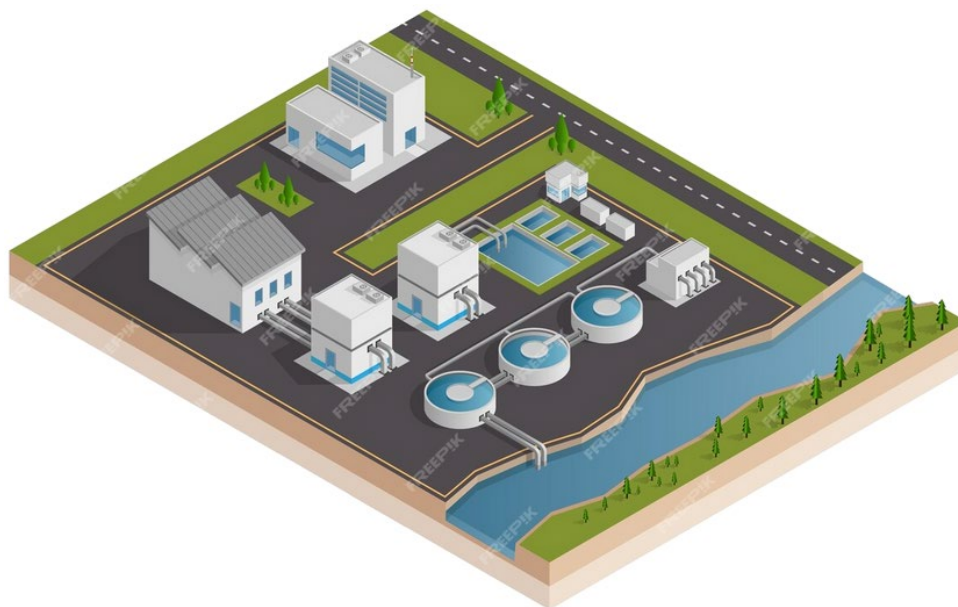


Figura 4: Trattamento delle acque

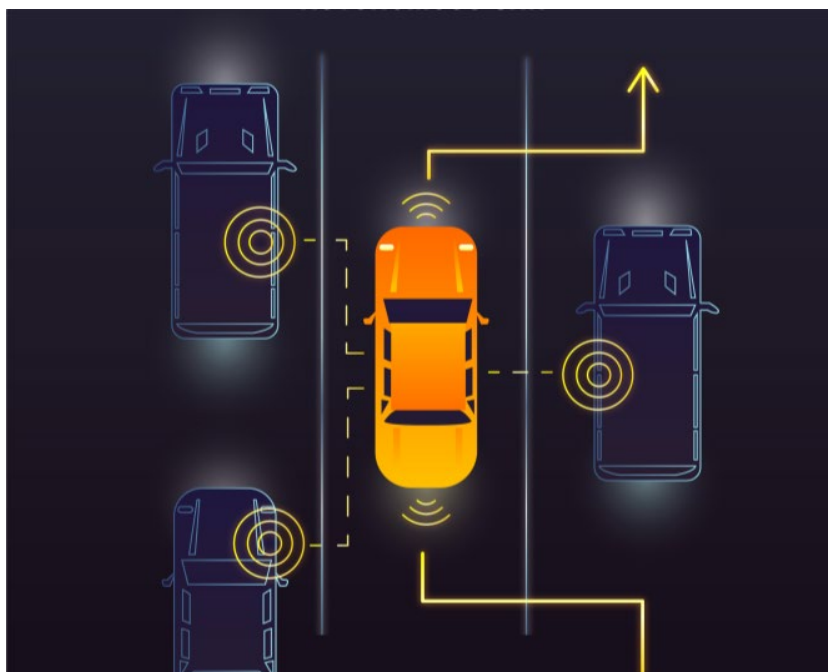
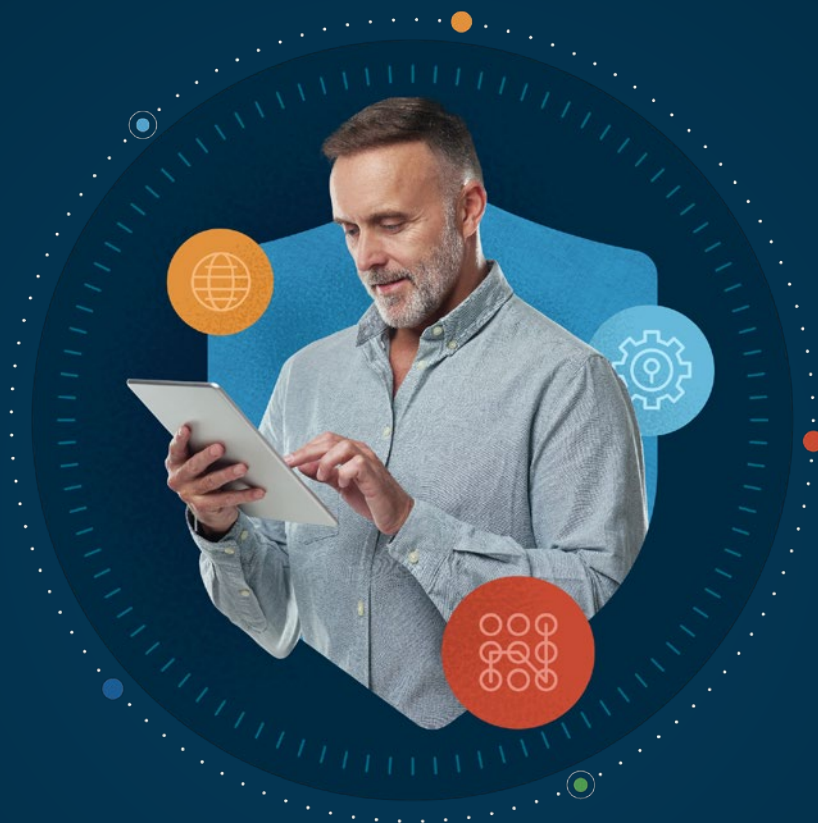


Figura 5: Smart car



# Protezione degli endpoint: Un percorso sicuro inizia con robuste fondamenta

NinjaOne ti permette di sfruttare l'automazione IT per semplificare il processo di hardening degli endpoint, ridurre notevolmente l'esposizione alle vulnerabilità e liberare il tuo team IT da lunghe operazioni manuali.

Scarica la guida gratuita →



# Esempi di attacchi cyber e guasti accidentali a CPS

Di seguito si descrivono brevemente alcuni tra i più famosi attacchi contro CPS, divenuti noti ai mezzi di informazione. Si sottolinea che, in generale, i soggetti attaccati preferiscono tacere su quanto subito, salvo che sia impossibile tacere, proprio per evitare di ammettere la propria vulnerabilità e, di conseguenza, perdere la fiducia di clienti e investitori.

1. **Maroochy Shire Sewage Spill** [4]. Nel 2000 un ex dipendente di Maroochy Water Services ha violato 142 stazioni di pompaggio delle acque reflue e ha causato la fuoriuscita di circa un milione di litri di acque reflue nei sistemi idrici locali. L'attacco è stato effettuato solo con un laptop, un PC compatto e un trasmettitore radio. L'ex dipendente vendicativo ha avuto accesso al sistema con le proprie credenziali, colpevolmente non disabilitate dall'azienda dopo il suo allontanamento, e ha agito come un *insider*, e, muovendosi tra le stazioni di pompaggio dell'infrastruttura ha manipolato le configurazioni di sistema. Questo incidente è un buon esempio per mostrare come l'utilizzo delle credenziali conosciute dagli ex dipendenti possa causare incidenti. Occorre una gestione efficace e puntuale del controllo degli accessi da parte delle organizzazioni, revocando tempestivamente le credenziali a chi smetta di averne necessità o diritto.
2. **Stuxnet** [5], [6]. Nel 2009 l'impianto nucleare dell'Iran è stato preso di mira dall'attacco più complesso conosciuto fino ad oggi. Stuxnet ha infettato più di 100.000 *host* in 25 Paesi, con il 60% degli *host* infettati in Iran. Ha preso di mira in modo specifico vulnerabilità esistenti nei sistemi operativi Microsoft e nei PLC Siemens, pur rimanendo nascosto, riuscendo a deteriorare le centrifughe per l'arricchimento dell'uranio, senza che ai sistemi di monitoraggio arrivassero indicazioni di problemi in corso. Si sostiene [6] che Stuxnet sia stato sviluppato dagli Stati Uniti e da Israele per sabotare il programma iraniano di arricchimento dell'uranio. Tuttavia, non ci sono state conferme ufficiali in tal senso. In particolare, è stato sfruttato il fatto che ai PLC Siemens non fosse stata cambiata la password di default.
3. **Saudi Aramco Attack** [7]. Nel 2012 il produttore di petrolio e gas Saudi Aramco è stato preso di mira da un *malware* successivamente denominato Shamoon. Gli aggressori hanno avuto accesso alla rete aziendale e hanno distribuito il *malware*, che ha eliminato i dati relativi alla produzione. Poiché la distribuzione di quel tipo di malware richiede l'accesso fisico ai computer interni, si ritiene che gli aggressori abbiano avuto an-

che l'aiuto di un *insider*. L'attacco, che non è riuscito ad accedere alla componente OT, è stato rivendicato dal gruppo "The Cutting Sword of Justice" per motivi politici.

4. **Fukushima Daiichi Nuclear Disaster** [8]. Nel 2011 un terremoto ha interrotto l'operatività della centrale nucleare di Fukushima Daiichi danneggiando i sistemi di alimentazione che raffreddano i reattori, provocando contaminazione radioattiva e rendendo necessaria l'evacuazione di circa 100.000 residenti. I disastri naturali sono prevedibili solo in una certa misura; di solito, i rischi che possono verificarsi a causa di questi eventi vengono ignorati durante la progettazione del CPS. L'incidente all'impianto nucleare di Fukushima Daiichi ha portato al riesame delle infrastrutture strutturali simili, per verificare quanto siano sicure contro i disastri naturali e i conseguenti guasti provocati da questi ultimi.
5. **Tridium Niagara Framework Attack** [9]. Nel 2012 gli aggressori si sono infiltrati nel sistema HVAC (*Heating, Ventilation and Air Conditioning*) di un'azienda con sede negli Stati Uniti. L'azienda utilizzava una versione non aggiornata di Tridium Niagara (software per il monitoraggio e l'individuazione di anomalie), contenente diverse vulnerabilità che consentono l'accesso *backdoor*. Queste vulnerabilità erano all'epoca già state rese note e descritte da diverse organizzazioni di sicurezza informatica. Tuttavia, la società vittima non era a conoscenza del problema, né aveva aggiornato i propri sistemi. Il CPS era connesso a Internet con protezione basata su password. Gli aggressori, che hanno ottenuto privilegi di amministrazione senza conoscere la password, sfruttando la vulnerabilità già nota, non hanno comunque avuto accesso ad alcun documento significativo e la motivazione dietro l'attacco è rimasta sconosciuta.
6. **Target Attack** [10]. Nel 2013 le anomalie nel sistema informatico di Target sono state scoperte da un team esterno all'organizzazione, specializzato in analisi per la sicurezza informatica. Gli aggressori avevano avuto accesso alle informazioni personali di oltre 1.000.000 di clienti. L'elenco dei fornitori di terze parti era accessibile nel portale di Target, e gli aggressori hanno scelto Fazio Mechanical (produttore HVAC) e inviato un'e-mail di *phishing* a uno dei dipendenti, che ha consentito l'installazione del *malware* e rubato le credenziali di accesso di Fazio Mechanical. Hanno così avuto accesso alla rete aziendale e rubato informazioni personali con la motivazione del guadagno finanziario. Questo incidente è unico per il modo in cui gli aggressori hanno avuto accesso alla rete IT, ovvero compromettendo prima la rete OT.
7. **Godzilla Attack! Turn Back!** [11]. Nel 2013 i segnali stradali elettronici a San Francisco, (Stati Uniti) sono stati violati e, invece di messaggi su viabilità e traffico, mostravano "Godzilla Attack" e "Turn Back!" I segnali erano controllati da una società esterna che utilizzava ancora le credenziali predefinite per accedere alla

rete. L'incidente non ha causato problemi significativi. La società responsabile dei segnali ha affermato che l'attacco è stato compiuto da qualcuno che già conosceva le credenziali. Si ritiene che la motivazione dietro l'attacco fosse meramente ludica.

8. **Brute Force Attacks on Internet-Facing Control Systems** [12]. Nel 2013 il proprietario di una stazione di pompaggio del gas negli Stati Uniti ha allertato ICS-CERT in merito a un aumento del numero di tentativi di attacco basati su forza bruta ai propri sistemi, eseguiti da 49 diversi indirizzi IP. Gli attori della minaccia e la motivazione dietro gli attacchi, nessuno dei quali ha avuto successo, sono ancora sconosciuti. Questo caso è un buon esempio per dimostrare come il rilevamento tempestivo dei tentativi di intrusione prevenga ulteriori danni ai sistemi industriali, aumentando la possibilità di una risposta efficace.
9. **German Steel Mill Cyberattack** [13]. Nel 2014 è stato attaccato l'altoforno di un'acciaieria tedesca. Non essendo stato possibile spegnere la fornace, l'attacco ha provocato ingenti danni fisici. Gli aggressori hanno avuto accesso alla rete aziendale tramite un'e-mail di *phishing*, quindi si sono trasferiti sulla rete industriale e hanno eseguito il codice dannoso per riprogrammare diversi PLC e compromettere le funzioni della fornace. Hanno sfruttato le vulnerabilità risultanti dalla debole protezione dei confini tra le reti a causa della mancanza di zone demilitarizzate (DMZ) che espongono la rete locale alla rete esterna. L'attacco è stato definito APT (*Advanced Persistent Threat*) e si ritiene sia stato eseguito da un gruppo con l'obiettivo del furto della proprietà intellettuale.
10. **Kemuri Water Company Attack** [14]. Nel 2016 Verizon ha pubblicato un rapporto su un attacco a una società di trattamento delle acque. L'azienda aveva memorizzato le credenziali di accesso al sistema OT sul server Web *front-end*. Gli aggressori, che hanno avuto accesso a tali credenziali tramite *SQL injection* e *phishing*, hanno riprogrammato gli attuatori di controllo ma non sono riusciti a causare alcun danno a causa della mancanza di esperienza sui sistemi SCADA. Tuttavia, si ritiene siano state rubate le informazioni personali di circa 2.500.000 utenti.
11. **Ukrainian Power Grid Attack** [15]. Nel 2015 la società di distribuzione elettrica ucraina Kyivoblenergo è stata oggetto di un attacco che ha provocato un'interruzione di corrente che ha interessato 225.000 utenti. Gli aggressori hanno avuto accesso alla rete IT tramite e-mail di *phishing*, quindi hanno acquisito le credenziali per infiltrarsi nella rete OT, ove eseguire il *malware*, denominato BlackEnergy 3; hanno poi continuato ad attaccare il sistema a intervalli di 30 minuti, per impedire l'attivazione di tecniche di mitigazione.

- 12. TRITON [16].** Nel 2017 il Safety Instrumented System (SIS) di una società di servizi petroliferi e gas del Medio Oriente è stato spento a causa dell'esecuzione riuscita di un *malware* denominato TRITON. Un *controller* SIS, realizzato da Schneider Electric e connesso a un PC Windows, è stato disattivato lasciando l'intera *utility* vulnerabile agli incidenti OT. Gli aggressori si sono prima infiltrati nella rete IT, quindi sono passati all'OT sfruttando la debole protezione del confine tra queste reti.
- 13. Cryptocurrency Malware Attack on SCADA [17].** Nel 2018 è stato scoperto un *malware* sul sistema OT di un'azienda europea di servizi idrici. Il malware, progettato per estrarre la criptovaluta Monero utilizzando i server HMI e SCADA della vittima, era in grado di funzionare in modalità invisibile, ma l'IDS ha rilevato un aumento dell'utilizzo della CPU e della larghezza di banda. L'aggiornamento dei sistemi OT richiede pianificazioni a lungo termine e quindi la maggior parte dei sistemi non può ricevere tempestivamente gli aggiornamenti più recenti. In questo caso, le applicazioni HMI non aggiornate, collegate a Internet per consentire la gestione remota, sono state violate dagli aggressori per accedere al sistema.
- 14. Norsk Hydro Ransomware Attack [18].** Nel 2019 la società produttrice di alluminio Norsk Hydro ha subito un attacco *ransomware* successivamente denominato LockerGoga. Gli aggressori hanno effettuato l'accesso e crittografato i dati critici, provocando l'arresto della rete aziendale e l'interruzione di molte operazioni, inclusa l'elaborazione degli ordini. Poiché gli avversari, dopo aver ottenuto l'accesso al sistema, hanno scelto di eseguire un ransomware precedentemente noto, si stima che l'attacco mirasse a interrompere la produzione per colpire la reputazione dell'azienda piuttosto che a un guadagno finanziario.
- 15. Riviera Beach Ransomware Attack [19].** Nel 2019, i servizi idrici di Riviera Beach (una piccola città situata in Florida, USA) sono stati oggetto di un attacco *ransomware*. Gli aggressori hanno inviato un'e-mail di *phishing* e il destinatario ha consentito all'attacco di raggiungere tutte le reti cittadine, compresi i sistemi di utenza idrica, a causa dell'interconnessione alla rete informatica senza alcun meccanismo di protezione specifico. Il consiglio comunale ha accettato di pagare il riscatto di 65 Bitcoin (circa \$ 600.000 entro quella data); tuttavia, gli aggressori non hanno inviato la chiave di decrittazione. Quindi il consiglio comunale ha deciso di rinnovare i sistemi oggetto dell'attacco.
- 16. Florida Water Treatment Poisoning Attack [20].** L'8 febbraio 2021 un attaccante ha tentato di avvelenare Oldsmar, una città della Florida negli Stati Uniti. L'attaccante ha avuto accesso al computer che ospita il software di controllo del trattamento dell'acqua tramite un programma di accesso remoto (TeamViewer), quindi ha aumentato la quantità di idrossido di sodio al di sopra del livello normale. Il cambiamento di

concentrazione dell'acqua è stato rilevato da un operatore e immediatamente annullato e l'accesso remoto è stato disabilitato. L'avversario non ha infatti falsificato le letture del sensore per ingannare l'operatore, contrariamente a quanto avvenuto per Stuxnet, quindi il cambiamento inaspettato è stato rilevato tempestivamente. Il modo in cui sono state acquisite le credenziali del computer è ancora sconosciuto. In questo incidente, avere personale IT operativo 24 ore su 24, 7 giorni su 7 (che non è il caso della maggior parte dei sistemi industriali) per supervisionare il sistema ha impedito che si verificasse un disastro dalle gravi conseguenze.

**17. Colonial Pipeline Ransomware Attack [21].** Il 7 maggio 2021 Colonial Pipeline, una compagnia con sede a Houston (Texas) che trasporta benzina e carburante per aerei mediante un sistema di oleodotti, principalmente negli Stati Uniti sudorientali, ha subito un attacco informatico *ransomware* che ha avuto un impatto sulle apparecchiature computerizzate che gestiscono l'oleodotto. La Colonial Pipeline Company ha interrotto tutte le attività dell'oleodotto per contenere l'attacco. Sotto la supervisione dell'FBI, la società ha pagato l'importo richiesto dal gruppo DarkSide (75 bitcoin o \$ 4,4 milioni di dollari.) Al ricevimento del riscatto gli attaccanti hanno fornito alla compagnia uno strumento informatico per ripristinare il sistema, che tuttavia ha richiesto un tempo di esecuzione assai lungo per giungere al completo ripristino. La Federal Motor Carrier Safety Administration ha emesso una dichiarazione di emergenza regionale per 17 Stati e Washington DC per mantenere aperte le linee di rifornimento di carburante nei giorni successivi all'attacco. È stato il più grande attacco informatico su un obiettivo di infrastrutture petrolifere nella storia degli Stati Uniti. L'FBI e varie fonti dei media hanno identificato il gruppo criminale DarkSide come parte responsabile, ritenendo che lo stesso gruppo avesse rubato 100 gigabyte di dati dai server aziendali nei giorni precedenti. Il 7 giugno, il Dipartimento di Giustizia ha annunciato di aver recuperato 63,7 bitcoin (circa 2,3 milioni di dollari) del pagamento del riscatto. Questo è stato uno dei primi attacchi informatici aziendali di alto profilo che ha avuto inizio da una password personale di un dipendente violata, e probabilmente trovata nel dark web, piuttosto che da un attacco diretto ai sistemi dell'azienda.

Gli attacchi contro i CPS si articolano generalmente in più fasi, e quelli avanzati possono eseguire l'intera *Cyber Kill Chain* (CKC). L'integrazione di reti IT e OT senza che ci sia una protezione dei confini solida e sicura è l'elemento che si riscontra sia usato più frequentemente negli attacchi.

Gli aggressori prendono di mira principalmente le aziende prive di personale di sicurezza con esperienza nella sicurezza industriale tramite e-mail di *phishing*; altre (con) cause negli esempi analizzati sono sempre legate al fattore umano, ad esempio il mancato aggiornamento di sistemi e applicativi software o una ge-

stione carente delle credenziali, dal non modificare le password di fabbrica dei dispositivi a non disabilitare tempestivamente le credenziali di chi non ne abbia più diritto o necessità. Anche carenze progettuali e/o implementative, talvolta volute per comodità di accesso remoto semplificato, che rendono debole o inesistente la separazione tra le parti IT e OT di un sistema – eventualmente in concomitanza con le “disattenzioni” di cui sopra – possono consentire a un attaccante di accedere facilmente alla parte OT, ove poter causare ingenti danni.

Quando gli effetti degli attacchi si manifestano a livello OT, a causa degli eventuali danni inferti a cose e/o persone, per l'azienda vittima può essere più difficile occultare l'evento. D'altro canto, la maggior parte delle aziende soggette a violazione dei dati rifiuta di pubblicare un rapporto pubblico sugli incidenti per non intaccare la propria reputazione. Le informazioni sugli incidenti sono per lo più disponibili tramite agenzie di stampa o blogger di sicurezza informatica che affermano di ottenere informazioni tramite informatori (ad esempio, ex o attuali dipendenti sotto pseudonimo), rendendo più difficili ulteriori esami.

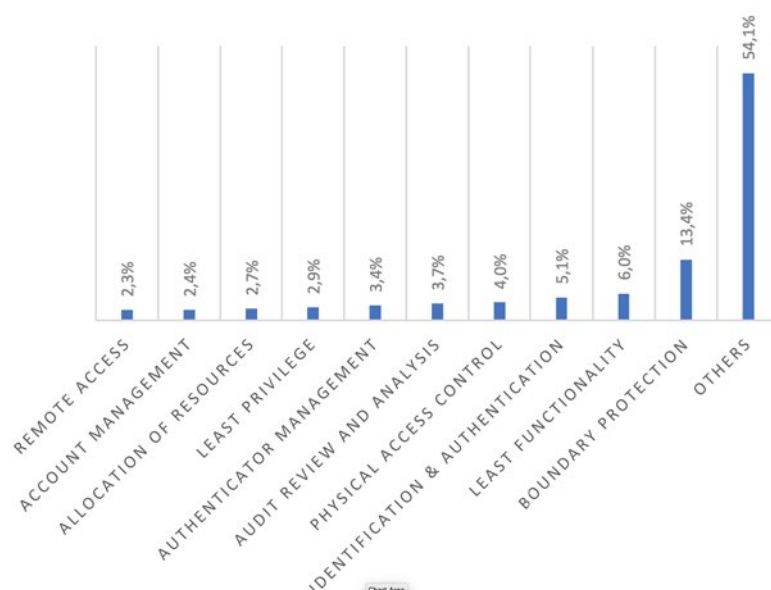


Figura 6: le 10 vulnerabilità più sfruttate nei CPS

# Gli attacchi più diffusi e le contromisure

Le vulnerabilità non sono isolate ma correlate tra di loro; ed esistono tipiche sequenze del loro sfruttamento per portare a compimento degli attacchi. Certamente avere barriere al confine tra parte IT e parte OT, così come adeguate policy di sicurezza, sono sfide ancora da vincere.

*Boundary Protection:* il confine tra le reti IT e OT in CPS sta svanendo a causa della maggiore connettività. I confini deboli rappresentano un grande rischio, come si è visto negli incidenti informatici del passato [13] [14] [19]. Stabilire una DMZ che contenga meccanismi di protezione, incluso un firewall, è il primo passo per rafforzare questi confini. Tuttavia, anche la stessa DMZ può essere soggetta ad attacchi e deve essere attentamente progettata e implementata.

*Least Functionality:* la rete industriale eterogenea interconnessa contiene una varietà di potenziali punti di accesso (ad es. porta, protocollo, servizi) e non è necessario mantenerli tutti attivi. La *Least Functionality* si riferisce al divieto e alla limitazione dell'uso di questi per prevenire potenziali abusi: tenere "aperti" solo i punti di accesso strettamente necessari. Le aziende tendono a sottovalutare o addirittura ignorare la sicurezza perché si concentrano sulla riduzione dei costi, con conseguente presenza di vulnerabilità legate alla mancata implementazione di tale policy, che effettivamente ha un costo: ridurre al minimo necessario le funzionalità di un sistema, spegnendo quelle non necessarie, richiede un'analisi attenta e costante delle sue necessità, funzionalità e prestazioni. Costa meno lasciare i dispositivi configurati così come vengono forniti dal venditore, anziché entrare nel merito dell'uso che se ne farà una volta installati.

*Identification & Authentication:* l'applicazione di adeguati meccanismi di autenticazione in un ambiente industriale impedisce l'accesso non autorizzato a dispositivi e informazioni. L'autenticazione delle comunicazioni uomo-macchina o macchina-macchina (M2M) richiede l'identificazione preventiva. Alle entità non identificate in tali ambienti dev'essere proibito di agire. Un avversario che riesca a inserirsi in una comunicazione non autenticata può danneggiare il CPS modificando, da un lato, i valori comunicati dai sensori e/o agli attuatori nonché, al contempo, impedire il rilevamento dell'intrusione stessa.

*Physical Access Control:* l'accesso alle strutture industriali avviene tramite chiavi, schede elettroniche e tec-

nologie mobili. Mentre le chiavi fisiche sono soggette a furto, le carte elettroniche e le tecnologie mobili non sono inviolabili. Disporre quindi di sistemi di verifica continua degli accessi a tutti i livelli consente di prevenire eventuali abusi.

*Audit Review and Analysis:* le organizzazioni dovrebbero adottare il sistema ISM (*Information Security Management*) come meccanismo operativo di monitoraggio e analisi degli eventi in tempo reale, nonché tracciamento e registrazione dei dati di sicurezza per scopi di conformità o di *auditing*. Naturalmente il sistema ISM stesso dev'essere protetto perché, se manipolato da un attaccante, costui potrebbe renderlo inefficace, e non consentire l'individuazione degli abusi commessi.

*Authentication Management:* tre principi essenziali che devono essere regolati dai criteri di applicazione della password sono la modifica, la rimozione e la crittografia delle password.

1. *Password Change:* i dispositivi COTS (**C**ommercial **O**ff-**t**he-**S**helf ) per CPS, come i PLC, vengono forniti con una password predefinita assegnata dal fornitore. Ciò (vedi Stuxnet) rappresenta un grande rischio, pertanto dovrebbe essere impostata una nuova password prima della messa in funzione del dispositivo, cambiandola con frequenza regolare.
2. *Password Removal:* questo è, più in generale, il tema delle credenziali che devono essere rimosse dal sistema e rese inattive per tutti quei soggetti che, a vario titolo, non hanno più necessità od obbligo di usarle. Anche questa attività richiede un'attenzione continua al controllo degli accessi. Anche gli eventuali *repository* di credenziali devono essere protetti.
3. *Password Encryption:* è necessario applicare meccanismi di crittografia avanzata per proteggere le password a partire dalla fase di autenticazione. Se la password viene trasmessa o conservata come testo in chiaro, un malintenzionato può accedervi in caso di intrusione.

*Least Privilege:* il NIST [22] suggerisce di applicare il principio del privilegio minimo come parte della strategia di difesa in profondità per il CPS. In base a tale principio, si fornisce un accesso minimo a un software/utente per attività essenziali e solo quando necessario, mentre il numero di attività viene mantenuto al minimo. Ciò determina sistemi facili da analizzare, con una maggiore sicurezza complessiva. Il privilegio minimo può essere fornito tramite l'applicazione del controllo degli accessi in base al ruolo (RBAC) [23] che assegna ben precisi diritti di accesso a specifici ruoli.

*Allocation of Resources:* a causa della crescente interconnettività, fornire un ambiente sicuro per i CPS richie-

de sempre più risorse. Questo problema dev'essere affrontato anche a livello di *management*, per orientare anche verso la sicurezza gli investimenti da effettuare.

*Account Management*: gli account aggiuntivi nelle reti dei CPS vengono utilizzati in situazioni eccezionali (ad esempio, prima messa in funzione da parte del venditore/installatore). Questi account temporanei/di emergenza hanno in genere elevati privilegi di accesso. Pertanto, devono essere rimossi/disabilitati una volta completato il loro utilizzo. Tale azione dovrebbe essere regolata da una rigorosa politica di controllo degli accessi.

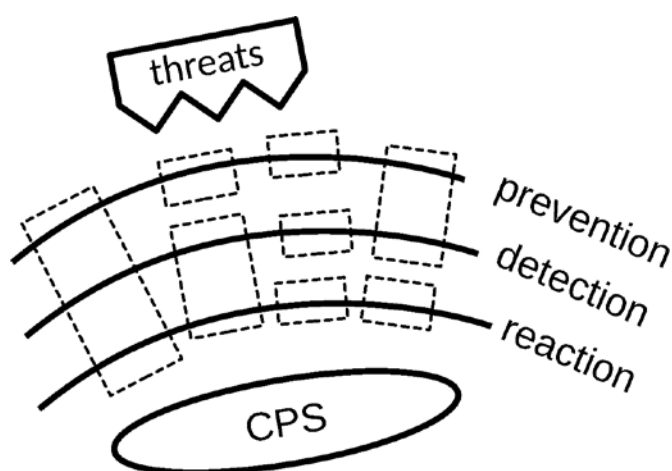


Figura 7: Linee di difesa

*Remote Access*: la possibilità di accedere remotamente ai CPS ne aumenta indubbiamente la superficie di attacco; anche perché ormai l'accesso remoto non solo è utilizzato in modo passivo per scopi di monitoraggio, ma si vuole che consenta di operare sul sistema e i suoi dispositivi esattamente come se si fosse fisicamente presenti nell'impianto. A fronte di un'indubbia comodità in tal senso, una politica forte di controllo degli accessi a tutti i livelli, compreso quello remoto, è allora necessaria. I principali modelli di controllo degli accessi implementati negli ambienti industriali sono il DAC (*Discretionary Access Control*) [24], MAC (*Mandatory Access Control*) [24] [22], RBAC (*Role Based Access Control*) [23] e ABAC (*Attribute Based Access Control*) [25]. Ulteriori modelli sono stati sviluppati per l'IloT e il Cloud.

# I pilastri della sicurezza

Gli attacchi informatici più sofisticati della storia (ad es. Stuxnet, TRITON) prendono di mira i sistemi di controllo gestiti da CPS. Pertanto, il concetto di difesa in profondità deve essere applicato a tutti gli elementi del CPS. La difesa in profondità può essere fornita stabilendo diversi livelli di difesa in cui ogni livello ha un determinato scopo, mentre l'obiettivo comune è fornire un ambiente sicuro. Questi livelli possono differire per le risorse tecniche (ad es. hardware, software) pur mostrando somiglianze in termini di personale e procedure. Un ambiente industriale sicuro, progettato sulla base di un approccio di difesa in profondità, dovrebbe contenere le tre linee di difesa schematizzate in Figura 7.

In particolare, la *prevention* si basa su meccanismi capaci di impedire il successo di eventuali attacchi, quindi renderli inoffensivi. D'altro canto non è possibile poter sempre prevenire tutto ciò che è indesiderato, compreso ciò che ancora non si conosce; inoltre, in ambito cyber, la ricerca e lo sviluppo di nuove tecniche di attacco corrono persino più velocemente dell'attività opposta, sul fronte della difesa. Quindi, accanto alla *prevention*, occorre disporre di sistemi di *detection* che, utilizzando informazioni fornite dal *monitoring*, identifichi con la maggiore tempestività possibile i potenziali attacchi.

In che modo? Ad esempio riconoscendo deviazioni rispetto al comportamento atteso o agli standard del sistema. A quale livello? Tutti: dall'analisi del traffico di rete a livello di singolo pacchetto, ad anomalie nel consumo di energia da parte di attuatori in tempo reale, ma anche offline, ad esempio con la verifica di corretta implementazione nel sistema di determinate policy di sicurezza, o con l'analisi di prestazioni dei dispositivi impiegati per la sicurezza per accertare che siano compatibili coi requisiti prestazionali del sistema. La *detection* dunque prevede di disporre di una sorta di riferimento, che può anche essere un modello, rispetto al quale valutare il comportamento e/o la configurazione effettiva del sistema. In questo tipo di attività, oggi trovano largo impiego tecniche basate sull'intelligenza artificiale. La *reaction* rappresenta l'applicazione dei correttivi necessari a contrastare e possibilmente inibire quanto di (potenzialmente) malevolo o rischioso è stato individuato dalla *detection*, parallelamente all'eventuale ripristino delle funzionalità e prestazioni eventualmente già affette dall'attacco stesso. Chiaramente, *detection* e *reaction* sono attività che si possono sviluppare su tempi anche lunghi: ad esempio sequenze storiche che vanno molto indietro nel tempo per la *detection*, mentre la *reaction*, soprattutto quando non può essere totalmente automatica e richiede quindi un intervento umano, può portare a tempi assai lunghi per il recupero totale delle funzionalità e prestazioni del

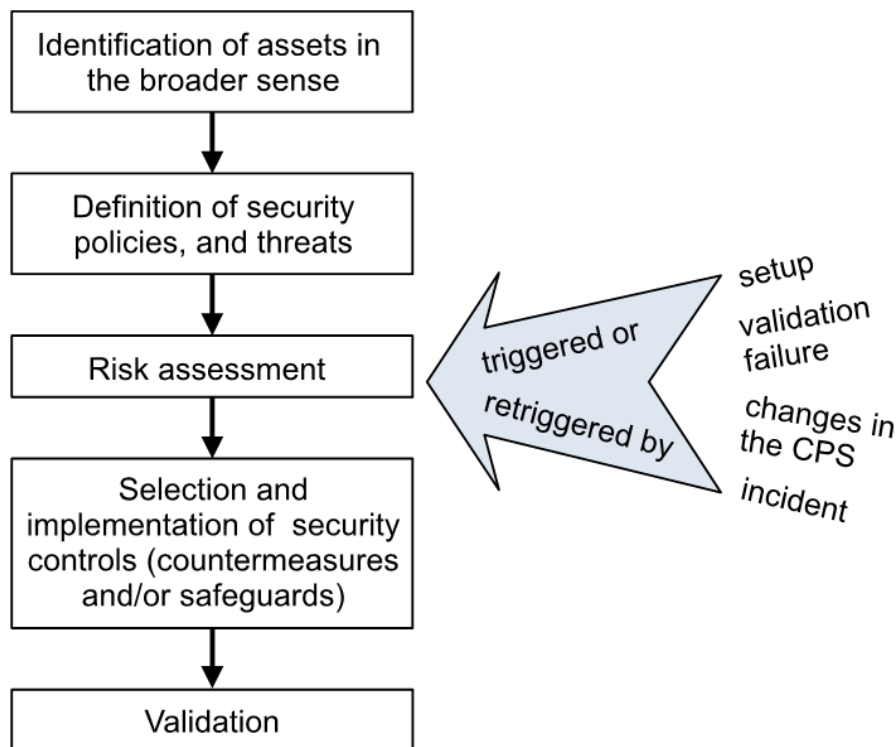


Figura 8: Information Security Management (ISM)

sistema attaccato, oltre al suo irrobustimento nei confronti delle criticità identificate.

Come appare quindi evidente, la sicurezza dei sistemi in generale è un processo sempre attivo, in continua esecuzione ed evoluzione, che può essere schematizzato come ISM (*Information Security Management*) in Figura 8, secondo i principali documenti sul tema, come [3] e [26] che adottano modelli concettuali simili basati sui passaggi logici e temporali rappresentati nella parte sinistra della figura. Gli eventi che compaiono nella parte destra dell'immagine, invece, sono i responsabili del (ri)avvio e dell'iterazione del processo ISM fino al raggiungimento di una situazione soddisfacente e confermata dalla fase di validazione. La convalida ha lo scopo di dimostrare che il rischio complessivo è stato abbassato al di sotto di una soglia accettabile e di solito comporta sia attività *offline* (ovvero nuove sessioni di valutazione del rischio) che *run-time* (ovvero monitoraggio e misurazioni).

L'intera sequenza di passaggi viene quindi ripetuta ogni volta che:

1. i risultati verificati in fase di validazione non corrispondono alle aspettative (riduzione del rischio inadeguata);
2. vengono introdotte modifiche in qualsiasi parte/componente del sistema generale, comprese apparecchiature, policy, livelli di rischio, requisiti aziendali, normativi o legali, minacce o vulnerabilità scoperte di recente e così via;
3. le attività di monitoring e detection in fase di esecuzione rilevano un incidente di sicurezza con conseguenze superiori alla soglia di gravità accettabile (le conseguenze stimate fanno parte dei risultati prodotti durante la valutazione del rischio).

In sostanza, dunque, l'ISM riguarda l'intera organizzazione di una società, includendo i seguenti elementi:

- formazione e impegno dei dipendenti e dei dirigenti;
- rapporti con partner, fornitori e clienti;
- *business continuity*;
- requisiti legali e contrattuali;
- rispetto delle politiche e degli standard di sicurezza;
- conformità tecnica;
- gestione delle risorse;
- *access control*;
- gestione delle comunicazioni e delle operazioni;
- sicurezza fisica e ambientale.

Si noti che tutti gli aspetti sopra elencati sono strettamente correlati: ad esempio, l'impegno del *management* garantisce le risorse e gli investimenti necessari (formazione, attrezzature e *audit*), mentre la formazione dei dipendenti consente la comprensione di meccanismi e tecniche di sicurezza, così come la corretta attuazione delle policy e delle procedure.

# Architettura per la sicurezza

I concetti introdotti in precedenza trovano la naturale e conseguente collocazione nello schema concettuale di Figura 9, dove il *Target System* è appunto il CPS in questione e i blocchi all'esterno, con le loro interdipendenze logiche, relazionano tra loro e con il sistema quanto evidenziato in Figura 7 e nella sua descrizione.

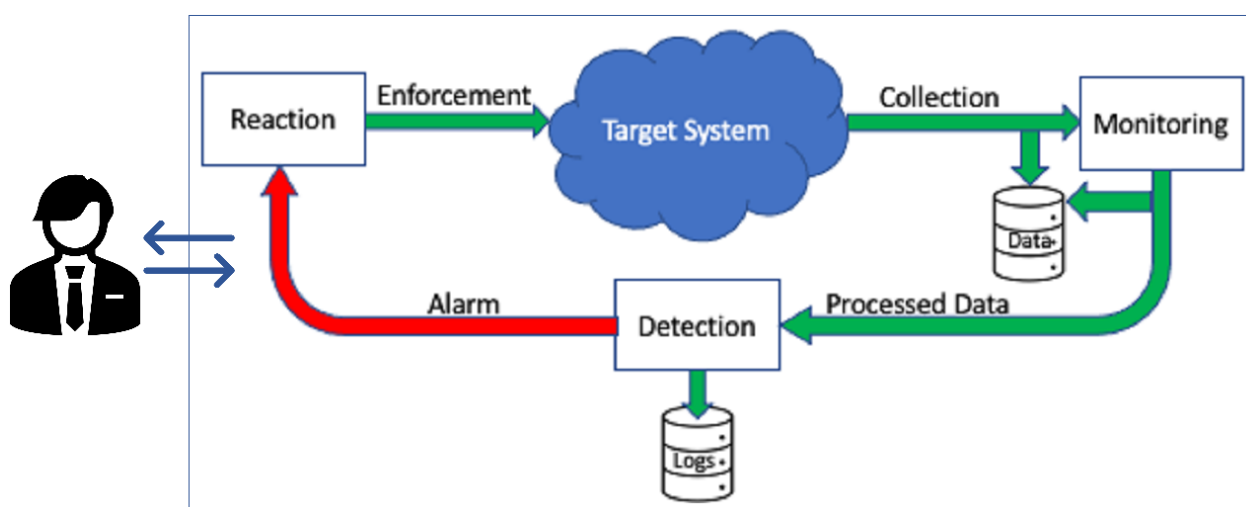


Figura 9: Architettura concettuale di un CPS sicuro

Il *monitoring* prevede l'acquisizione di informazioni dal/nel *target system* circa il suo stato e il suo funzionamento. Tali informazioni, in formato grezzo e/o preventivamente elaborato e/o aggregato, vengono rese disponibili all'attività di *detection* che, in caso di errore, criticità o anomalia, coinvolge l'attività di *reaction* per l'attuazione delle necessarie contromisure, il tutto sotto la supervisione di personale dedicato.

Si noti che lo schema di Figura 9 si riferisce ad attività che possono essere svolte sia totalmente dentro al sistema in esecuzione, ad esempio quanto legato ad attacchi di tipo DoS (Denial of Service) sia, parzialmente, all'esterno, come la verifica di corretta implementazione di policy di sicurezza quando (un caso tipico sono gli Industrial Control Systems) non siano disponibili meccanismi automatici (*enforcement*) di applicazione delle policy stesse. In tal caso, a fronte di una descrizione dettagliata del sistema, comprensiva dei meccanismi di sicurezza, fornita possibilmente in modo (semi) automatico dal *monitoring*, si costruisce un modello

del sistema stesso, su cui si verifica, tramite opportune tecniche di analisi, che le policy di sicurezza previste per il sistema siano soddisfatte dalla sua implementazione: ad esempio verificando che chi esercita il ruolo di "operatore" su di una certa macchina non possa modificarne i "parametri di configurazione" e che a farlo possa essere soltanto il "responsabile della produzione". Per fare ciò, occorre verificare che l'assegnazione delle credenziali agli utenti dei singoli dispositivi e la loro configurazione consenta appunto di garantire tali desiderata.

Nel caso in cui la verifica fallisca, le necessarie correzioni vengono apportate sul modello del sistema e, in caso di successiva verifica positiva, ribaltate sul sistema reale.

Per ciò che concerne le attività di *monitoring*, *detection* e *reaction* effettuate sul sistema reale, sono evidentemente necessari sensori o sonde di acquisizione, risorse di computazione e comunicazione e quanto altro necessario alla riconfigurazione, quindi componenti hardware e software che devono trovarsi distribuiti nel sistema stesso per assolvere alle suddette funzioni.

Questa sovrastruttura per la sicurezza dev'essere progettata indissolubilmente dal sistema nel caso di nuovi CPS, oppure aggiunta in caso di CPS esistenti, privi o non sufficientemente dotati di risorse per la sicurezza.

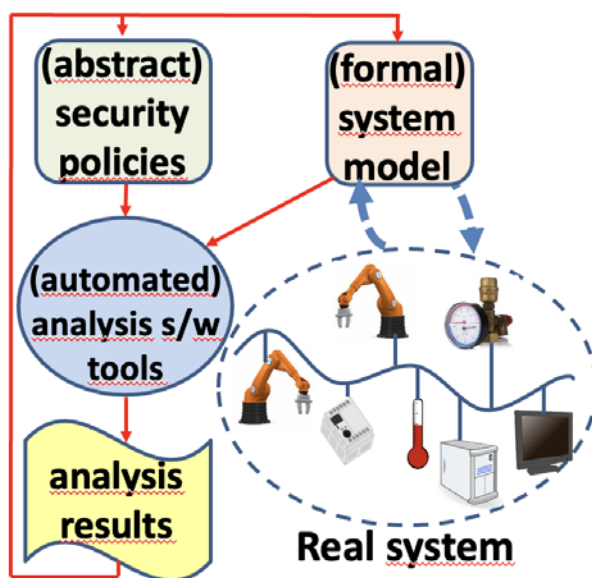


Figura 10: Analisi di sicurezza

## Esempi

Esempi di quanto sopra descritto possono provenire da recenti attività di ricerca nel settore. In particolare, verranno introdotti:

strumenti di **analisi** che operano su modelli di sistema, costruiti mediante informazioni acquisite dall'attività di *monitoring* sul sistema in esecuzione;

strumenti di **riconfigurazione automatica** dell'infrastruttura di sicurezza a seguito di intervenute situazioni di rischio, causate da azioni malevole o semplicemente da impreviste situazioni fisiologiche;

analisi delle **prestazioni** di software e dispositivi per la sicurezza, al fine di garantire che la loro introduzione non influisca negativamente sulle prestazioni del sistema.

## Analisi

Lo schema di Figura 10 illustra il modo di operare delle metodologie di analisi di sicurezza su modelli del sistema, eventualmente acquisiti dal sistema stesso mediante il supporto del *monitoring*. In sostanza, l'attività di verifica svolta da un *tool* software determina se il modello del sistema soddisfa i requisiti di sicurezza espressi come policy. Dal risultato ottenuto si possono effettuare, sul modello e/o le policy, le opportune correzioni, da applicare infine sul sistema reale quando i risultati dell'analisi diano esito positivo.

L'esempio specifico descritto qui concerne la verifica di implementazione di policy di access control [27]: da un lato ci sono le policy descritte mediante il formalismo RBAC [23] e, dall'altro, il modello del sistema comprensivo di descrizione della geografia dei luoghi, locali, armadi, quadri elettrici, della configurazione di rete atta a determinare la raggiungibilità di un dispositivo da un altro, la configurazione di ciascun dispositivo con il software installato, gli account e appunto la connettività; infine gli utenti del sistema, quindi tutte le unità di personale, ciascuna con le credenziali assegnate e il ruolo (o i ruoli) di competenza. Le policy di access control di fatto definiscono direttamente chi può fare cosa e dove nel sistema: per ciascun soggetto (chi), quale azione (cosa) e su quale oggetto (dove), senza che debba essere specificato il come. A partire dalla descrizione dettagliata del sistema, si computano le medesime informazioni attraverso il come e si confrontano i due insiemi. Eventuali discrepanze possono significare che il sistema non implementa correttamente le policy e che, quindi, occorre apportare le necessarie correzioni. In ciò, l'analisi stessa è di aiuto: in quanto è in

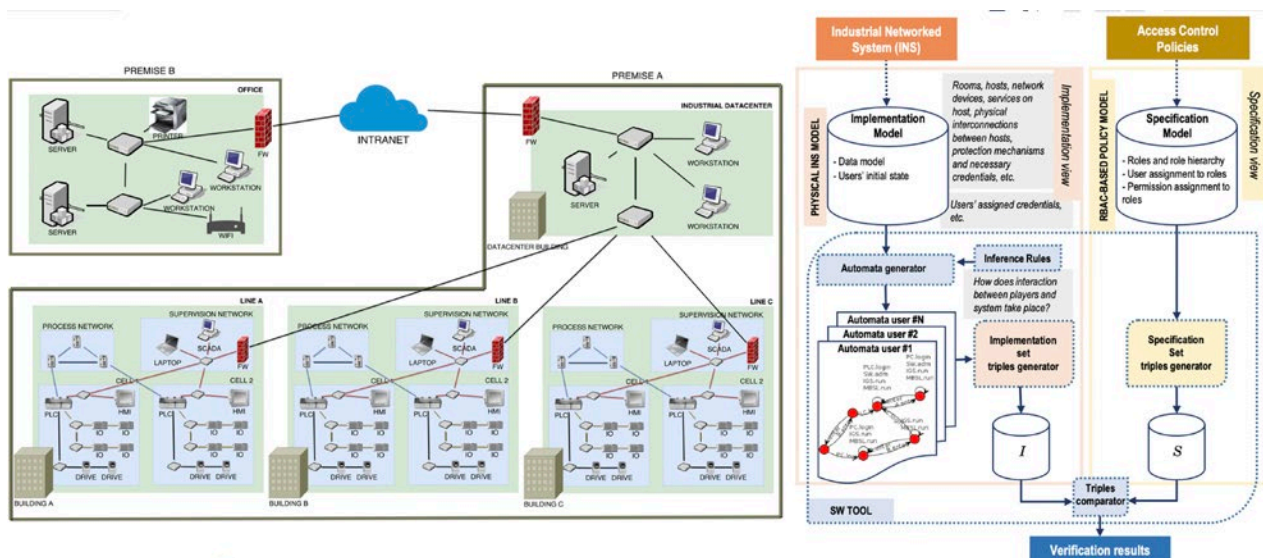


Figura 11: Verifica di implementazione di policy di access control

grado di fornire, per ogni azione da parte di un soggetto su di un certo oggetto, la sequenza di operazioni necessarie al compimento di quella che determina la discrepanza nel confronto di cui sopra (il come). In altre parole, l'analisi fornisce il controesempio. La computazione di ciò può essere decisamente onerosa, quindi particolare attenzione è stata dedicata alle ottimizzazioni, ottenute mediante la composizione degli automi a stati finiti che descrivono rispettivamente le azioni fisiche (ad es. accesso a un locale o a un cabinet attraverso una porta) e quelle cyber (ad es. accesso a server web, ssh a nodo remoto) da parte di ciascun soggetto. La Figura 11 fornisce un esempio specifico, costituito, sul lato sinistro, da una infrastruttura geograficamente dislocata in due siti, dove uno dei due è costituito da più edifici (capannoni) ognuno dei quali contiene più celle di lavoro, ciascuna con le proprie connessioni all'interno e verso l'esterno. I collegamenti di rete tra edifici e verso l'esterno sono protetti da firewall. Per tutti i dispositivi e i locali descritti si conoscono le azioni che è possibile effettuare su ciascuno, nonché le eventuali credenziali necessarie e le configurazioni (server software installati, ad esempio). Non rappresentati in figura ci sono poi i soggetti che popolano la struttura, ad esempio i manutentori, l'ingegnere di produzione, gli operatori di linea ecc., ciascuno con le credenziali che gli sono state fornite.

La parte destra della Figura 11 descrive come vengono elaborate la suddetta descrizione – chiamata *Implementation Model* – e l'insieme delle policy di access control, chiamato *Specification Model*: da ciascuno

si determinano i due rispettivi set  $I$  e  $S$  di triple **chi agisce dove** (soggetto, azione e oggetto) che vengono confrontati. Alla luce del risultato del confronto vengono attuate le eventuali correzioni, modificando opportunamente il modello del sistema o le policy. Si noti che in questo modo di procedere si riconoscono i passi dell'ISM descritti in Figura 8: *Identification of Assets in the Broader Sense* è il sistema con la sua geografia, geometria e dispositivi che lo occupano e relative interconnessioni, *Definition of Security Policies and Threats* sono le policy di *access control*, mentre il *Risk Assessment* non compare in maniera esplicita ma il suo effetto è la determinazione della configurazione del sistema, anch'essa parte della sua descrizione per ciò che concerne i meccanismi di sicurezza.

La fase di *Validation* è qui costituita dall'analisi vera e propria.

## Riconfigurazione Dinamica

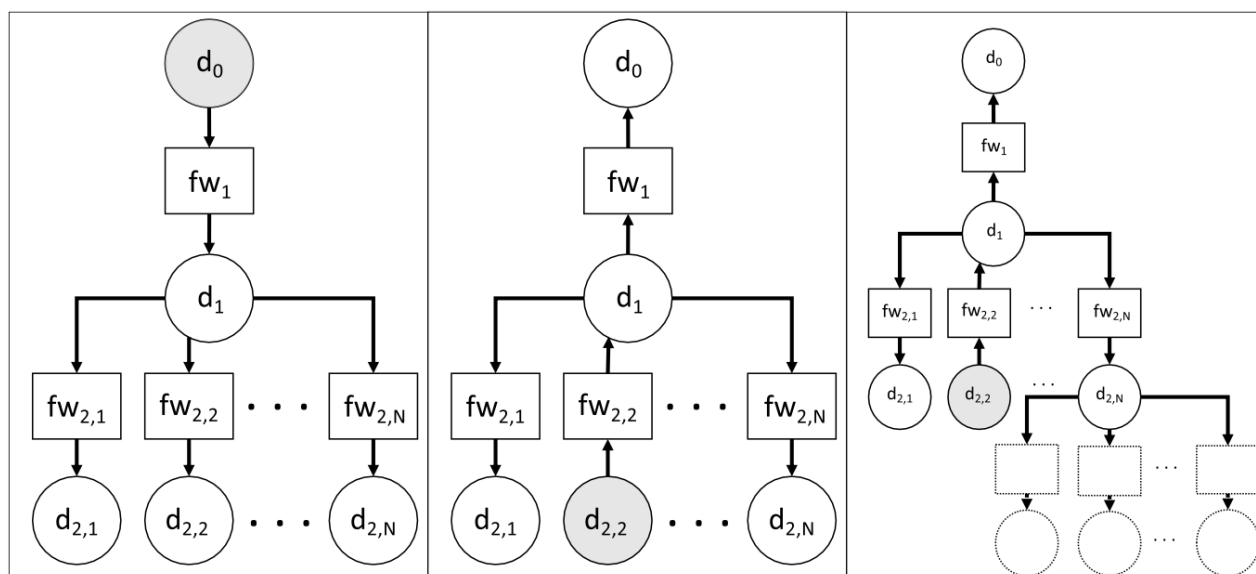


Figura 12: Topologia di riferimento

La ridistribuzione dinamica delle regole di filtraggio, tra firewall che risiedono nella stessa rete, è una soluzione tecnica in grado di far fronte a variazioni temporanee del carico di traffico elaborato dai firewall stessi [28]. Nelle reti che includono più firewall in cascata, questi possono essere sfruttati per consentire il trasferimento di un insieme di regole da un firewall ai suoi vicini "a valle", quando i cambiamenti nel profilo del traffico di

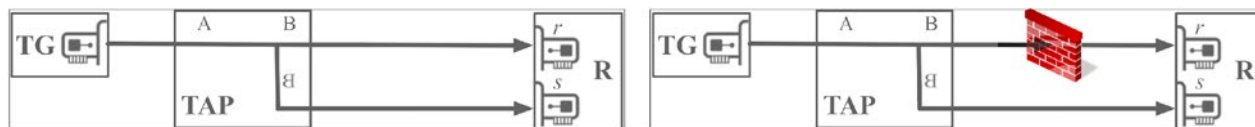


Figura 13: Sistema di misura di latenza

input lo suggeriscono. Il meccanismo su cui si basa questa tecnica è la riduzione del numero medio di regole controllate per pacchetto, al fine di aumentare la velocità di elaborazione dei pacchetti. Il modello di rete tiene conto sia della topologia del sistema che delle caratteristiche del firewall. Un opportuno algoritmo di trasformazione sposta le regole tra i firewall in cascata, consentendo miglioramenti tangibili delle prestazioni in termini di velocità di elaborazione dei pacchetti per un dato profilo di traffico e garantendo l'integrità di sicurezza della rete. Lo scotto da pagare è un maggior consumo di banda, dato che anche ai pacchetti che verranno scartati è consentito effettuare un percorso più lungo nella rete del sistema. Per questa ragione, tale metodologia è utile durante le fasi di aumento del traffico, ma conviene tornare alla configurazione iniziale nel momento in cui la situazione di sofferenza abbia termine. La Figura 12 illustra parte di quanto descritto: data la topologia della rete, che può essere fisica o virtuale, con i dispositivi di rete fisici o virtualizzati, eventualmente basati su SDN (Software Defined Networks) e NFV (Network Function Virtualization), il flusso del traffico critico, indicato dal verso delle frecce che descrivono i collegamenti di rete, muove dal nodo sorgente, in grigio, verso le destinazioni. Ad esempio,  $fw_1$  è il firewall sovraccarico nello schema di sinistra della figura, mentre lo stesso ruolo è recitato da  $fw_{2,2}$  nello schema centrale. Lo schema di destra illustra invece la modularità e la scalabilità dell'approccio: se, per motivi diversi, una parte di rete non può o non deve essere considerata in dettaglio, può venire assimilata ad un singolo nodo a cui vengono associati tutti gli indirizzi della sottorete che rappresenta.

Riferendosi alla Figura 9, la situazione di criticità deve venire identificata dall'attività di detection che attinge dal monitoring, che quindi deve poter acquisire in tempo reale informazioni circa le prestazioni dei singoli firewall: ad esempio dai firewall stessi se possono rendere disponibili informazioni sul loro stato, quali il numero di pacchetti in coda, oppure da misure indirette quali la latenza dei pacchetti, cioè quanto tempo impiegano ad attraversare ciascun firewall. In quest'ultimo caso occorre disporre di un sofisticato sistema di acquisizione e misurazione, basato ad esempio su TAP (Test Access Point). Lo stesso monitoring può essere di aiuto nel determinare la topologia della rete, necessaria all'attività di reaction per il calcolo della nuova configurazione a partire dalla configurazione corrente dei firewall, da iniettare poi nei firewall coinvolti dalla trasformazione.

Tutto ciò per dire che in questo caso, come in moltissimi altri, la gestione efficace – e quindi ampiamente automatizzata – della sicurezza richiede una sovrastruttura non banale, la cui attività non deve inficiare le prestazioni richieste al CPS e che deve a sua volta essere sicura.

## Prestazioni

La disponibilità di studi prestazionali e modelli semplici per firewall in grado di gestire protocolli di comunicazione a livello di applicazione industriale, come Modbus/TCP, è cruciale quando l'impatto di questi dispositivi deve essere stimato, anche approssimativamente, prima della loro effettiva messa in funzione nel sistema destinazione. Sfortunatamente, la maggior parte dei produttori non fornisce questo tipo di informazioni per i prodotti disponibili in commercio. Pertanto, una soluzione praticabile è lo sviluppo e la convalida sperimentale di modelli semplici che possono essere utilizzati dai progettisti per prevedere quelle caratteristiche del firewall non esplicitamente correlate alle loro capacità di sicurezza. Ad esempio, la latenza introdotta sull'itinerario dei messaggi è un aspetto di notevole interesse in molti sistemi di controllo industriale, dove ritardi e oscillazioni nei tempi di gestione dei pacchetti possono avere un forte impatto sull'efficacia del controllo e dell'automazione. È pertanto necessario disporre di modelli prestazionali per dispositivi commerciali per la sicurezza nei CPS. In particolare, qui si riporta brevemente l'esperienza [29] che ha portato a caratterizzare un dispositivo commerciale [30] in grado di eseguire filtraggio avanzato a livello di applicazione del traffico Modbus/TCP. Una serie di esperimenti progettati *ad hoc*, eseguiti per mezzo di un *testbed* di laboratorio appositamente sviluppato, ha consentito sia lo sviluppo che la validazione del modello, confermando una buona corrispondenza delle prestazioni stimate con il comportamento effettivo del dispositivo.

La Figura 13 illustra lo schema concettuale del sistema di misura: a sinistra senza dispositivo, per la caratterizzazione del sistema stesso, a destra con il dispositivo da caratterizzare. In sostanza, il nodo TG genera e spedisce pacchetti con cadenza costante programmabile e lunghezza costante programmabile, il TAP duplica il messaggio e il ricevitore R riceve le due istanze sulle porte *r* e *s*, salvando, per ciascun pacchetto ricevuto su ciascuna porta, il tempo di arrivo. Nel caso dello schema di sinistra i due tempi, che dovrebbero teoricamente coincidere, differiscono di pochi microsecondi per il fatto che vengono gestiti in sequenza dalla routine di *interrupt* di R, che impiega appunto qualche microsecondo. Questa differenza non inficia le misure effettuate con l'inserimento del dispositivo da caratterizzare, nello schema di destra, perché quest'ultimo introduce una latenza sempre superiore ai 100 microsecondi, rendendo marginale, quindi trascurabile, la latenza introdotta dal sistema di misura: infatti la differenza tra i tempi di arrivo a R delle due istanze di

ciascun pacchetto trasmesso da TG è, al netto della marginale latenza del sistema di misura, la latenza che il dispositivo introduce.

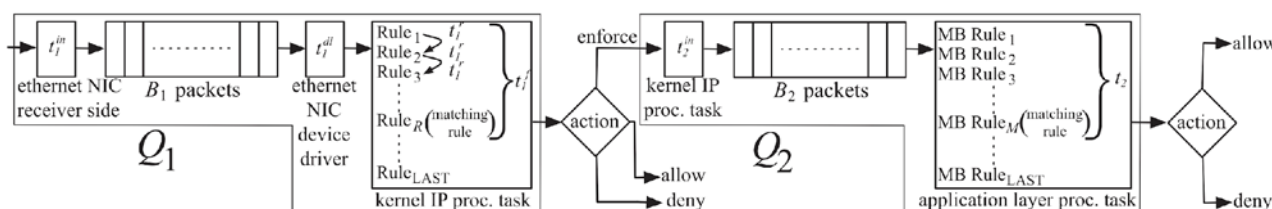


Figura 14: Schema architetturale del firewall oggetto di indagine

Il dispositivo è in grado di filtrare traffico TCP e UDP standard e traffico Modbus/TCP, cioè pacchetti TCP il cui payload è costituito da un pacchetto Modbus. Mentre il traffico “standard” viene filtrato in base al contenuto dell’header del pacchetto, quindi il test rispetto alle regole di filtraggio è veloce, il traffico Modbus/TCP per essere filtrato richiede l’analisi del payload del pacchetto, quindi è certamente più oneroso da un punto di vista computazionale. Ciò comporta un rischio: da un lato si vuole filtrare traffico potenzialmente affetto da vincoli temporali anche stringenti e, dall’altro, questo filtraggio è computazionalmente oneroso, quindi rischia di introdurre latenze incompatibili con gli eventuali vincoli temporali che il controllo impone alla comunicazione. Questo giustifica un’indagine approfondita per determinare l’esatto comportamento del dispositivo e la latenza introdotta dall’attività di filtraggio. Dai dati forniti dal produttore, non è possibile inferire alcunché circa la struttura funzionale del dispositivo, né il ritardo introdotto dal filtraggio; ma grazie a una serie di campagne di misura, dapprima per il solo traffico “standard” e poi per il traffico Modbus/TCP, è stato possibile determinare lo schema funzionale del firewall con estrema precisione, riuscendo anche a determinare i tempi di attraversamento di ciascun blocco da parte del pacchetto sotto esame, come illustrato in Figura 14. In particolare, è risultato che il dispositivo è di fatto costituito da due firewall in sequenza,  $Q_1$  e  $Q_2$ , dove  $Q_1$  è un tradizionale firewall IP mentre il secondo riceve dal primo solo i pacchetti Modbus/TCP, non gestiti da  $Q_1$ . In base a ciò, risulta che il traffico “standard” ha la priorità sul traffico Modbus/TCP; inoltre il filtraggio dei pacchetti Modbus/TCP, accumulati eventualmente nel *buffer*  $B_2$ , avviene soltanto quando  $Q_1$  è inattivo, riducendo ulteriormente la priorità del filtraggio di tale traffico.

Le misure effettuate con *data rate* 100 Mb/s hanno consentito di determinare la lunghezza dei due *buffer*  $B_1$  e  $B_2$ : 256 elementi ciascuno, e sono rispettivamente circa 31.95, 138.87 e 0.745 microsecondi e rappresentano il tempo medio di attesa del pacchetto prima di essere accodato nel *buffer*  $B_1$ , il tempo medio di attesa

prima che il pacchetto, estratto da B1, venga valutato rispetto alle regole di  $Q_1$  e il tempo medio di valutazione del pacchetto rispetto ad una singola regola: quindi se la regola soddisfatta è in posizione R, il tempo di valutazione è . Circa  $Q_2$ , invece, è in media 99.27 microsecondi, mentre il tempo di valutazione del pacchetto rispetto alle regole Modbus/TCP è in media 282.75 microsecondi e non dipende dalla posizione della regola soddisfatta.

Tale modello è stato poi validato mediante ulteriori campagne di misura dove, date le caratteristiche del traffico iniettato, la latenza prevista, determinata utilizzando il modello, è risultata coincidente con il valore misurato.

Il risultato, in sintesi, è che il dispositivo ha una latenza compresa tra 100 e 600 microsecondi (a seconda del tipo di pacchetto e della posizione della regola soddisfatta) e che il firewall non è in grado di gestire flussi superiori ai 2000 pacchetti per secondo.

L'importanza di questa esperienza non è tanto nei numeri che sono stati determinati, quanto nel fatto che nessuno di questi è reso noto dal produttore, rendendo di fatto impossibile stabilire a priori se il dispositivo sia idoneo e compatibile con le caratteristiche del traffico e del sistema che dovrebbe impegnarlo. Ciò deve quindi portare a una grande attenzione e prudenza nella scelta di dispositivi di sicurezza per i CPS: senza un'indicazione delle performance, infatti, non è possibile stabilire la compatibilità del dispositivo rispetto alle necessità del traffico da filtrare o da gestire.

# Conclusioni

Da una prospettiva storica, i requisiti di sicurezza dei CPS sono stati tradizionalmente specificati da organizzazioni attive in una serie di domini di infrastrutture critiche, tra cui, ad esempio:

- distribuzione di acqua e gas;
- trasmissione e distribuzione di energia elettrica [31];
- produzione di gas e petrolio [32], [33];
- produzione e distribuzione alimentare [34];
- sistemi di trasporto.

In tutti questi ambiti, la *security* è sempre stata tenuta in debita considerazione: quindi si sono inizialmente sviluppate linee guida e raccomandazioni specifiche, oggi certamente obsolete ma comunque importanti nell'evoluzione darwiniana delle linee guida per la *security* dei CPS.

Nel tempo, infatti, i requisiti comuni sono stati individuati, fusi e amalgamati in diversi documenti da vari organismi di normazione internazionali e nazionali. Oggi l'*Information Security Management* (ISM) è universalmente considerato come un processo, chiamato anche *Information Security Program* (ISP) dal NIST [26], che ha recentemente introdotto un importante aggiornamento alla sua linea guida [22]. Questo documento, nella sua ultima versione, sebbene ancora in forma di *draft*, è considerato tra i migliori e più completi punti di partenza per approfondire le tematiche della *security* dei CPS a 360°.

Indipendentemente dalla loro diversa struttura e grado di generalità, tutti i principali sforzi di normazione concordano, in pratica, sullo stesso concetto di base.

Ovvero:

*i rischi per la sicurezza devono essere minimizzati mediante opportuni controlli che affrontino le vulnerabilità sfruttabili da possibili minacce, il cui obiettivo è l'abuso e/o il danneggiamento dei beni.*

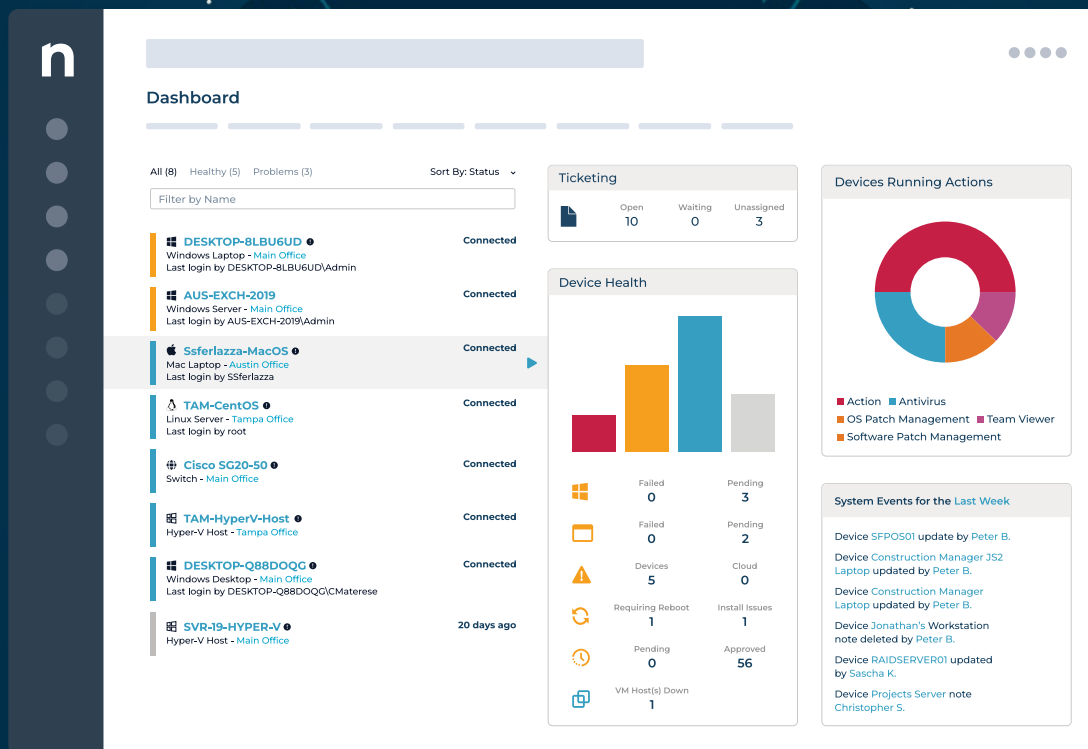
Concetto che, al termine del presente documento, dovrebbe risultare del tutto chiaro e condiviso, alla luce dell'aumentata sensibilità e consapevolezza che si spera siano progressivamente maturate con la lettura del medesimo.

# Bibliografia

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1]  | M. Cheminod, L. Durante and A. Valenzano, "Review of Security Issues in Industrial Networks," <i>IEEE Trans. Ind. Informat.</i> , vol. 9, no. 1, pp. 277-293, 2013.                                                                                                                                                                                                                                                                                                                                                                                                                |
| [2]  | D. Dzung, M. Naedele, T. P. von Hoff and M. Crevatin, "Security for Industrial Control Systems," <i>Proc. IEEE</i> , vol. 93, no. 6, pp. 1152-1177, 2005.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| [3]  | <i>ISA-62443-1-1-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [4]  | J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in <i>Int. Conf. on Critical Infrastructure Protection (ICCIP)</i> , 2007.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [5]  | R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," <i>IEEE Secur. Privacy Mag.</i> , vol. 9, no. 3, pp. 49-51, 2011.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| [6]  | T. M. Chen, "Stuxnet, the real start of cyber warfare?," <i>IEEE Netw.</i> , vol. 24, no. 6, pp. 2-3, 2010.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [7]  | C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco," <i>Survival</i> , vol. 55, no. 2, pp. 81-96, 2013.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [8]  | K. Younghwan, K. Minki and K. Wonjoon, "Effect of Fukushima Nuclear Disaster on the Global Public Acceptance of Nuclear Energy," <i>Energy Policy</i> , vol. 61, pp. 822-828, 2013.                                                                                                                                                                                                                                                                                                                                                                                                |
| [9]  | Federal Bureau of Investigations, "Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Access to a New Jersey Company's Industrial Control System," 23 July 2012. [Online]. Available: <a href="https://info.publicintelligence.net/FBI-AntisecICS.pdf">https://info.publicintelligence.net/FBI-AntisecICS.pdf</a> . [Accessed 11 May 2023].                                                                                                                                                                                                                       |
| [10] | M. Plachkinova and C. Maurer, "Security Breach at Target," <i>J. of Inf. Syst. Education</i> , vol. 29, no. 1, pp. 11-20, 2018.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| [11] | T. Thornhill and Z. Szathmary, "Godzilla Attack! Pranksters hack San Francisco road sign to warn drivers of trouble ahead," Mail Online, 23 May 2014. [Online]. Available: <a href="https://www.dailymail.co.uk/news/article-2632556/Godzilla-Attack-Turn-Pranksters-hack-San-Francisco-road-sign-warn-drivers-just-movie-makes-monster-93-2million-box-office.html">https://www.dailymail.co.uk/news/article-2632556/Godzilla-Attack-Turn-Pranksters-hack-San-Francisco-road-sign-warn-drivers-just-movie-makes-monster-93-2million-box-office.html</a> . [Accessed 11 May 2023]. |
| [12] | ICS-CERT, "Incident Response Activity: BRUTE FORCE ATTACKS ON INTERNET-FACING CONTROL SYSTEMS," U.S. Department of Homeland Security, 2013. [Online]. Available: <a href="https://www.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf">https://www.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf</a> . [Accessed 11 May 2023].                                                                                                                                                                                                     |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [13] | R. M. Lee, M. J. Assante and T. Conway, "German Steel Mill Cyber Attack," <i>Industrial Control Systems</i> , vol. 30, no. 62, pp. 1-15, 2014.                                                                                                                                                                                                                                                                                                                             |
| [14] | J. Leyden, "Water treatment plant hacked, chemical mix changed for tap supplies," <i>The Register</i> , 24 March 2016. [Online]. Available: <a href="https://www.theregister.com/2016/03/24/water_utility_hacked/">https://www.theregister.com/2016/03/24/water_utility_hacked/</a> . [Accessed 11 May 2023].                                                                                                                                                              |
| [15] | R. M. Lee, M. J. Assante and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, 18 March 2016. [Online]. Available: <a href="https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf">https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf</a> . [Accessed 11 May 2023].                                                  |
| [16] | A. Di Pinto, Y. Dragoni and A. Carcano, "TRITON: The first ICS cyber attack on safety instrument systems," in <i>Black Hat USA</i> , 2018.                                                                                                                                                                                                                                                                                                                                 |
| [17] | Radiflow Team, "Cryptocurrency Malware Attack on a SCADA Network," Radiflow, 8 February 2018. [Online]. Available: <a href="https://www.radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/">https://www.radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/</a> . [Accessed 11 May 2023].                                                                             |
| [18] | B. Briggs, "Hackers hit Norsk Hydro with ransomware. The company responded with transparency," <i>Microsoft</i> , 16 December 2019. [Online]. Available: <a href="https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/">https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/</a> . [Accessed 11 May 2023]. |
| [19] | L. O'Donnell, "Post-Ransomware Attack, Florida City Pays \$600K," 20 June 2019. [Online]. Available: <a href="https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869/">https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869/</a> . [Accessed 11 May 2023].                                                                                                                                                                               |
| [20] | E. Montalbano, "Hacker Tries to Poison Water Supply of Florida Town," <i>Threatpost</i> , 9 February 2021. [Online]. Available: <a href="https://threatpost.com/hacker-tries-to-poison-water-supply-of-florida-town/163761/">https://threatpost.com/hacker-tries-to-poison-water-supply-of-florida-town/163761/</a> . [Accessed 11 May 2023].                                                                                                                              |
| [21] | S. M. Kerner, "Colonial Pipeline hack explained: Everything you need to know," <i>Techtarget</i> , 26 April 2022. [Online]. Available: <a href="https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know">https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know</a> . [Accessed 11 May 2023].                                                                               |
| [22] | K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri and S. Lightman, "NIST SP 800-82 Rev. 3 (Draft): Guide to Operational Technology (OT) Security," National Institute of Standards and Technology, 2022.                                                                                                                                                                                                                                                         |
| [23] | ANSI, "INCITS 359-2012: Information technology - Role Based Access Control," 2012.                                                                                                                                                                                                                                                                                                                                                                                         |

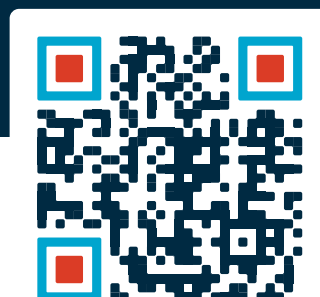
|      |                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [24] | S. Osborn, R. Sandhu and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," <i>ACM Trans. Inf. Syst. Secur.</i> , vol. 3, no. 2, pp. 85-106, 2000.                                                                                                                                                                                      |
| [25] | V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone, "NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations," National Institute of Standards and Technology, 2019.                                                                                                                                                             |
| [26] | Joint Task Force, "NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, 2022.                                                                                                                                                                                                                                |
| [27] | M. Cheminod, L. Durante, L. Seno and A. Valenzano, "Semiautomated Verification of Access Control Implementation in Industrial Networked Systems," <i>IEEE Trans. Ind. Informat.</i> , vol. 11, no. 6, pp. 1388-1399, 2015.                                                                                                                                                                               |
| [28] | L. Durante, L. Seno and A. Valenzano, "A Formal Model and Technique to Redistribute the Packet Filtering Load in Multiple Firewall Networks," <i>IEEE Trans. Inf. Forensics Security</i> , vol. 16, pp. 2637-2651, 2021.                                                                                                                                                                                 |
| [29] | M. Cheminod, L. Durante, L. Seno and A. Valenzano, "Performance Evaluation and Modeling of an Industrial Application-Layer Firewall," <i>IEEE Trans. Ind. Informat.</i> , vol. 14, no. 5, pp. 2159-2170, 2018.                                                                                                                                                                                           |
| [30] | Belden - Hirschmann, "Tofino Xenon industrial security appliance," 2016. [Online]. Available: <a href="https://www.belden.com/products/industrial-networking-cybersecurity/cybersecurity/firewalls/tofino-xenon">https://www.belden.com/products/industrial-networking-cybersecurity/cybersecurity/firewalls/tofino-xenon</a> . [Accessed 11 May 2023].                                                  |
| [31] | NERC, "Reliability Standards," North American Electric Reliability Corp., 2023. [Online]. Available: <a href="https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx">https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx</a> . [Accessed 11 May 2023].                                                                                                                                 |
| [32] | American Gas Assoc., "AGA 12, Cryptographic Protection of SCADA Communications - Part 1: Background, Policies and Test Plan," 2006. [Online]. Available: <a href="https://doku-men.tips/documents/aga-12-cryptographic-protection-of-scada-communications.html?page=1">https://doku-men.tips/documents/aga-12-cryptographic-protection-of-scada-communications.html?page=1</a> . [Accessed 11 May 2023]. |
| [33] | American Gas Assoc., "AGA 12, Cryptographic Protection of SCADA Communications - Part 2: Performance Test Results," 2006. [Online]. Available: <a href="https://www.energy.gov/ceser/articles/aga-12-part-2-performance-test-results">https://www.energy.gov/ceser/articles/aga-12-part-2-performance-test-results</a> . [Accessed 11 May 2023].                                                         |
| [34] | Food and Drug Administration, "Title 21, Volume 1, Part 11: Electronic Records, Electronic Signatures," FDA, 2011. [Online]. Available: <a href="https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.1">https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.1</a> . [Accessed 11 May 2023].                                                            |



# Prova subito NinjaOne

Prova NinjaOne gratuitamente per 14 giorni e scopri come può aiutarti a proteggere la tua azienda. Nessun impegno richiesto.

Richiedi subito una prova gratuita di NinjaOne! →



The logo for ICT Security Magazine features a stylized icon of three overlapping squares in red and yellow to the left of the text. The text 'ICT' is in a large, bold, yellow sans-serif font, while 'Security' is in a larger, bold, yellow script font. Below 'Security', the word 'MAGAZINE' is written in a smaller, bold, red sans-serif font.

# ICT Security MAGAZINE

## ISCRIVITI ALLA NEWSLETTER

per ricevere aggiornamenti sulle  
prossime iniziative. Seguici sui canali  
social: [Linkedin](#), [Facebook](#), [Twitter](#)