ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA

SCUOLA DI INGEGNERIA E ARCHITETTURA

DIPARTIMENTO

Informatica

CORSO DI LAUREA

Ingegneria Informatica

TESI DI LAUREA

in

OT CYBER SECURITY:

“DEFINIZIONE, SPECIALIZZAZIONE SETTORIALE E APPLICAZIONE DI FRAMEWORK PER LA VALUTAZIONE DELLA CYBER SECURITY IN STABILIMENTI PRODUTTIVI”

Candidato:

Alessandro Vannini

Relatore:

Prof. Marco Prandini

Matricola n°:

0001039520

Correlatore:

Dott. Alessandro Musacchio

Anno Accademico 2022/2023

OT Cyber Security:

“Definizione, specializzazione settoriale e applicazione di framework per la valutazione della Cyber Security in stabilimenti produttivi”

1. INTRODUZIONE

Questa tesi tratta tematiche di OT Security ed è costruita intorno alle attività progettuali svolte presso PwC Italy fra Febbraio 2023 e Dicembre 2023, che hanno permesso di definire due Framework di sicurezza da applicare all'ambiente industriale. Di seguito viene illustrata la struttura della tesi.

Il contesto dell'ambiente industriale odierno

In questo capitolo sarà effettuata un'introduzione sui sistemi industriali, mostrando l'evoluzione del mondo industriale nei suoi cinque paradigmi (Industria 1.0 - Industria 5.0) e sulle relative diverse esigenze rispetto ai normali sistemi informativi.

L'ecosistema industriale, il Purdue Model ed i principali vettori di attacco

In questo capitolo sarà dettagliata la struttura ed i vari componenti essenziali dei sistemi industriali. Verranno prima elencati i principali dispositivi (es.., PLC) e sistemi (es. sistemi SCADA) che compongono l'ecosistema industriale, e sarà poi mostrato come tali sistemi si integrano gerarchicamente all'interno dell'ambiente OT attraverso il *Purdue Model.* Saranno definiti tutti i livelli del *Purdue Model,* con le relative funzioni e responsabilità. Infine, verrà fatta una breve panoramica sui principali vettori di attacco all'interno del *Purdue Model.*

IEC/ISA 62443, lo Standard di riferimento per l'OT Security

In questo capitolo verrà caratterizzato l'attuale Standard di riferimento per la sicurezza dei sistemi industriali, ovvero l'IEC/ISA 62443. Partendo da brevi cenni storici, sarà poi mostrata la struttura della "famiglia" di Standard 62443 e verrà eseguito un focus sulla sezione 62443 3-3, spiegando il concetto di *System Requirements* e *Functional Requirements.*

Definizione di un Framework di sicurezza da applicare agli stabilimenti industriali

In questo capitolo sarà descritto il primo dei due Framework di sicurezza definiti durante le trascorse attività progettuali. Verranno messe in evidenza le principali tematiche di OT Security all'interno degli stabilimenti produttivi con le relative contromisure da applicare, seguendo l'ordine dei vari Domini e controlli definiti all'interno del Framework (per un totale di 78 controlli). I Domini in questione prevedono controlli di:

- Network Security
- Identificazione ed Autenticazione
- Accessi Remoti
- Third Party Security

- Backup e ripristino
- Detection & Recovery
- Data Security
- Patching & Update
- Asset Inventory & Device Hardening
- Physical Security
- Training e Awareness
- Security Governance

Restrizione del dominio di analisi ai sistemi di supervisione e controllo (SCADA) con definizione di un Framework di sicurezza specifico

In questo capitolo sarà descritto il secondo dei due Framework definiti durante le attività progettuali al fine di evidenziare le principali esigenze in termini di sicurezza dei sistemi SCADA. Saranno mostrati i vari Domini definiti, che prevedono controlli di:

- Data security
- Platform and Application Security
- Communication Security
- Personnel Security
- Configuration Management
- Detection and Recovery
- Physical Access security

Applicazione dei Framework a due realtà industriali ed illustrazione dei principali risultati ottenuti

In questo capitolo saranno illustrate le modalità con cui i due Framework definiti sono stati applicati a due importanti realtà industriali e verrano illustrati i risultati emersi da tali attività, permettendo di identificare le principali vulnerabilità dei sistemi industriali odierni.

Conclusioni

Infine, saranno definite le conclusioni emerse dalle attività svolte.

2. IL CONTESTO DELL'AMBIENTE INDUSTRIALE ODIERNO

L'ambiente industriale ha subito una trasformazione sostanziale e progressiva nel corso della storia, passando attraverso diverse fasi evolutive che hanno plasmato le modalità con le quali vengono attualmente prodotti beni ed erogati servizi. Questo processo evolutivo è comunemente rappresentato tramite in cinque paradigmi, noti come Industria 1.0, Industria 2.0, Industria 3.0, Industria 4.0 e Industria 5.0. Ognuna di queste fasi fase ha portato significative innovazioni e cambiamenti nel processo produttivo, con conseguenti impatti sostanziali sulla società.

Dall'Industria 1.0 all'Industria 5.0

L'Industria 1.0 ha avuto inizio nel XVIII secolo con la nascita dell'industria stessa attraverso la rivoluzione industriale, caratterizzata dall'introduzione della macchina a vapore e dalla meccanizzazione dei processi produttivi. Le fabbriche hanno progressivamente sostituito i laboratori artigianali, aumentando notevolmente la capacità di produzione.

Il passaggio all'Industria 2.0 è avvenuto nel tardo XIX secolo grazie all'avvento dell'elettricità e della produzione in serie. La catena di montaggio ha reso la produzione più efficiente e ha portato a una produzione su larga scala di beni di consumo. L'automazione ha inoltre iniziato a sostituire il lavoro umano in alcune fasi della produzione.

Successivamente, negli anni '70 e '80, la digitalizzazione dei processi produttivi ha avviato la transizione all'Industria 3.0 e l'utilizzo di sistemi informatici per gestire e monitorare le operazioni di produzione ha permesso di migliorare la precisione, il *throughput* e la velocità dei processi. Le tecnologie digitali (es. PLC, sistemi software) hanno quindi cominciato a svolgere un ruolo cruciale nella gestione degli stabilimenti produttivi e delle catene di produzione.

L'Industria 4.0, iniziata alla fine degli anni 2000, ha portato l'integrazione di tecnologie e paradigmi quali l'*Internet of Things* (IoT), l'intelligenza artificiale, la stampa 3D e l'analisi dei dati. Il *deployment* su larga scala di sensori, attuatori e le comunicazioni M2M (machine to machine) hanno permesso un livello di controllo, analisi e personalizzazione della produzione mai visto prima. E' inoltre emerso il concetto di *Digital Twin,* ovvero la digitalizzazione dello stabilimento produttivo e di tutte le sue componenti e processi.

Infine, l'Industria 5.0, concetto emerso solamente negli ultimi anni, mira a integrare le capacità umane con l'automazione robotica avanzata al fine di migliorare la creatività, la flessibilità e l'efficienza dei processi di produzione. Tecnologie emergenti quali la robotica collaborativa e l'intelligenza artificiale avanzata sono al centro di questa fase.

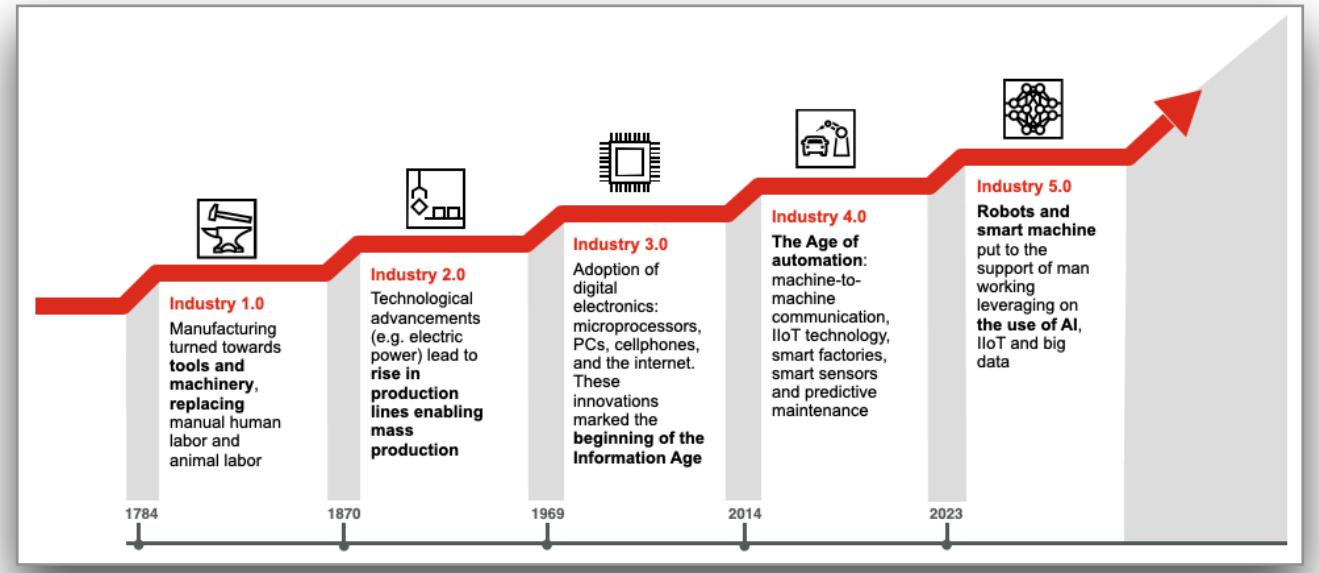


Figura 1: Evoluzione dei processi di produzione industriale

E' opportuno effettuare alcune considerazioni sul panorama industriale globale odierno, che risulta essere estremamente eterogeneo in termini di tecnologie e processi di produzione. In particolare, in Italia, molti stabilimenti produttivi risalgono ancora agli '80, e risulta quindi infrastrutturalmente difficile adeguarsi alle nuove tecnologie. È quindi evidente che non sia possibile assegnare un paradigma specifico ed univoco al panorama industriale globale.

Alcuni settori industriale sono intrinsecamente meno propensi all'adozione di soluzioni tecnologie avanzate. Infatti:

- Sebbene ci siano crescenti sforzi per introdurre tecnologie agricole avanzate, molte aree dell'agricoltura rimangono legate a pratiche tradizionali.
- In alcune aree della produzione manifatturiera, l'adozione di tecnologie avanzate come l'automazione e l'*Internet of Things* (IoT) può essere più lenta rispetto ad altri settori.
- Anche se ci sono alcune innovazioni nel settore minerario, molte operazioni continuano a seguire modelli tradizionali.
- Nonostante gli evidenti progressi nell'edilizia sostenibile e nell'uso di tecnologie innovative, in alcuni casi il settore edile può essere meno tecnologicamente avanzato.

In questi casi, l'Industria 3.0 risulta essere il paradigma ancora maggiormente adottato.

Altri settori industriali invece spesso sono i precursori dei nuovi paradigmi precedentemente definiti:

- L'industria biometrica e farmaceutica, anche a causa di stringenti normative e regolamentazione, è tecnologicamente altamente avanzata e sfrutta ampiamente la robotica e l'IoT.
- Il settore Automotive e l'industria aerospaziale sono spesso all'avanguardia in termini di automazione e monitoraggio dei processi produttivi.

Tali settori industriali hanno ampiamente integrato le innovazioni tecnologiche introdotte dall'Industria 4.0 o, in alcuni casi, dall'industria 5.0.

Le differenze fra l'ambiente IT e l'ambiente OT

Per dimostrare il particolare livello di attenzione che deve essere dedicato alla sicurezza dei sistemi industriale (OT), è necessario mettere prima in evidenza le sostanziali differenze che caratterizzano l'ambiente OT rispetto all'ambiente IT tradizionale.

Se la IT Cyber Security è fortemente basata sul cosiddetto *CIA Trident (Confidentiality, integrity, Availability),* tale modello risulta non essere più interamente applicabile alla OT Cyber Security. Il mondo OT è caratterizzato dalla prioritizzazione della continuità operativa e dalla continuità di processo. Ogni singola interruzione non programmata nel processo produttivo o di erogazione di servizio si traduce in una consistente perdita economica per l'azienda, oltre che introdurre importanti rischi di Safety. Analizzando quindi il *CIA Trident* a seguito di questa premessa è quindi osservabile che, mentre l'integrità e la disponibilità del dato restano fondamentali anche nel contesto OT, la confidenzialità dei dati diventa invece un caratteristica non più essenziale, se non controproducente. L'*overhead* computazionale introdotto dai principali meccanismi di crittografia, identificazione ed autenticazione è infatti spesso mal visto all'interno degli stabilimenti industriali.

Di seguito, vengono inoltre riportate altre sostanziali differenze fra i sistemi IT ed i sistemi OT:

	Sistemi IT	**Sistemi OT**
Tipologia di dati trattati	Ogni tipo (es. transazioni, dati personali, voce e multimedia, etc.).	Prevalentemente dati per il monitoraggio, controllo e supervisione dei sistemi e del processo produttivo.
Accesso ad internet	Accesso frequente ad internet e connessioni con Cloud Data Center.	Idealmente, accesso ad internet solo quando strettamente necessario (es. update dei sistemi, etc.) e presenza di sistemi *Air-Gapped.*
Conseguenze dei fallimenti	Perdita di dati.	Rischi di Safety.
Frequenza di aggiornamento	Sistemi frequentemente aggiornati e modificati. Architettura in continua espansione e cambiamento.	Sistemi raramente aggiornati per ragioni di operatività. Architetture stabili.
Replica dei sistemi	Sistemi facilmente replicabili con meccanismi di Disaster Ricovery per garantire *Business Continuity* e *Operational Resilience.*	Linee produttive difficilmente replicabili. Difficoltà nel garantire l'interoperabilità dei sistemi.

Un'altra caratteristica peculiare dei sistemi OT è la complessità ed eterogeneità dell'ecosistema di dispositivi hardware e software di cui sono composti. All'interno dei sistemi industriali infatti, come meglio dettagliato nel capitolo seguente, è possibile trovare una vasta gamma di dispositivi prodotti da vendor differenti, sui quali sono installati software e sistemi operativi differenti e spesso considerati *legacy* (tipo di software che, a causa di cambiamenti nel contesto tecnologico o delle esigenze aziendali, viene considerato obsoleto o superato e non più ufficialmente supportato dal vendor), e che comunicano attraverso protocolli differenti e solitamente proprietari (es. Siemens

S7, Rockwell DeviceNet, etc.). Risulta di conseguenza evidente che una tale eterogeneità di dispositivi e sistemi espanda enormemente la superficie di attacco, introducendo numerose vulnerabilità e relativi vettori di attacco, sfruttabili da utenti malevoli.

3. L'ECOSISTEMA INDUSTRIALE, Il PURDUE MODEL ED I PRINCIPALI VETTORI DI ATTACCO

Con l'evoluzione dell'industria in quella che oggi definiamo "Industry 4.0", si è potuto assistere ad una sempre maggiore integrazione fra il mondo IT ed il mondo OT. Qualsiasi sistema industriale, al giorno d'oggi è infatti descrivibile come un ecosistema composto da diversi sistemi e dispositivi eterogenei, interconnessi fra loro tramite varie reti e sotto-reti, ed in cui il confine netto fra "OT" ed "IT" si va molto ad assottigliare.

Questa evoluzione dell'industria ha portato ad un notevole aumento nell'efficienza e nella produttività degli sistemi industriali, ma ha anche esposto i tali sistemi, precedentemente "isolati" ed "autonomi", a nuove minacce e vettori di attacco ereditati direttamente dal mondo IT.

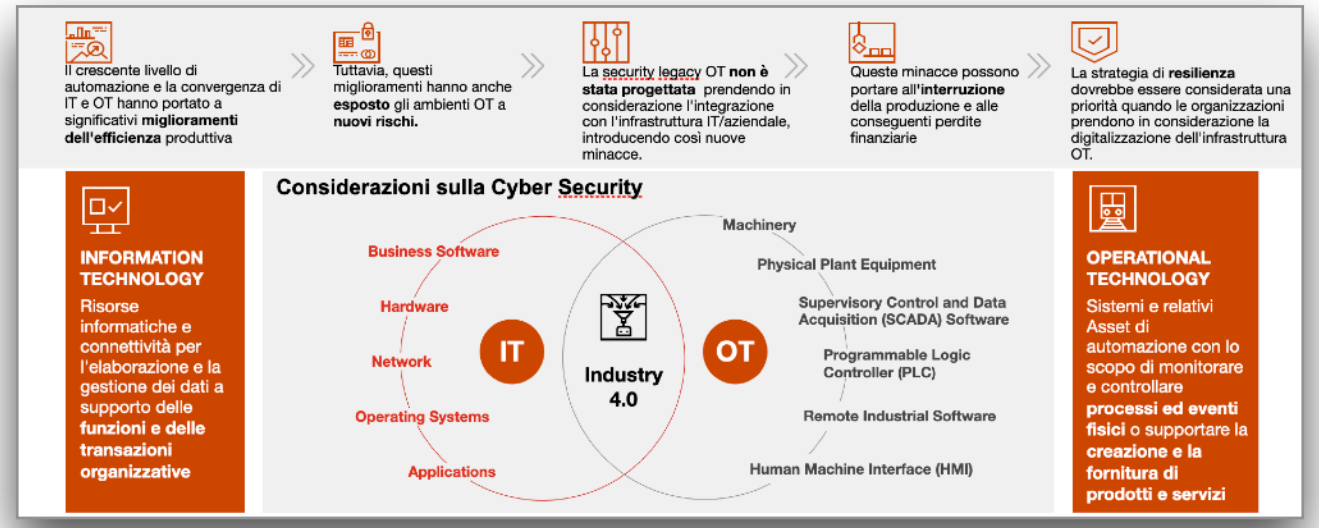


Figura 2: L'ambiente industriale odierno

Prima di approfondire le tematiche di sicurezza relative ai sistemi industriali, è opportuno dettagliare meglio quali sono gli elementi fondamentali che compongono i sistemi industriali e la loro posizione all'interno dell'architettura di riferimento.

I componenti essenziali dei sistemi industriali

Di seguito, viene dettagliato un elenco, non esaustivo, dei dispositivi e sistemi chiave che compongono l'ecosistema industriale.

PLC

I *Programmable logic Controller*, o PLC, sono il cuore di quasi tutti i sistemi di controllo industriale. Sono i dispositivi che ricevono i dati dai sensori di campo attraverso i canali di input e controllano gli attuatori attraverso i canali di output. Un tipico PLC è costituito da un microcontrollore e da una serie di canali I/O, che possono essere analogici, digitali o valori esposti in rete. Questi canali di I/O sono spesso disponibili come schede aggiuntive da collegare modularmente al *backplane* di un PLC, in modo tale da adattare il PLC alle esigenze e funzioni necessarie.

La programmazione di un PLC può avvenire tramite un'interfaccia USB o seriale dedicata sul dispositivo, o tramite il bus di comunicazione di rete integrato (o fornito come scheda aggiuntiva). I protocolli di rete solitamente utilizzati nelle comunicazioni con i PLC sono Modbus, Ethernet, e PROFINET.

I PLC possono essere utilizzati come dispositivi autonomi, per il controllo di una determinata parte del processo produttivo, ad esempio una singola macchina, oppure come sistemi distribuiti, che si estendono su più impianti in località dislocate con migliaia di interfacce I/O.

In figura 3, è possibile osservare un PLC completo, composto dal microcontrollore sulla sinistra e dalle numerose interfacce I/O che si estendono sulla destra.

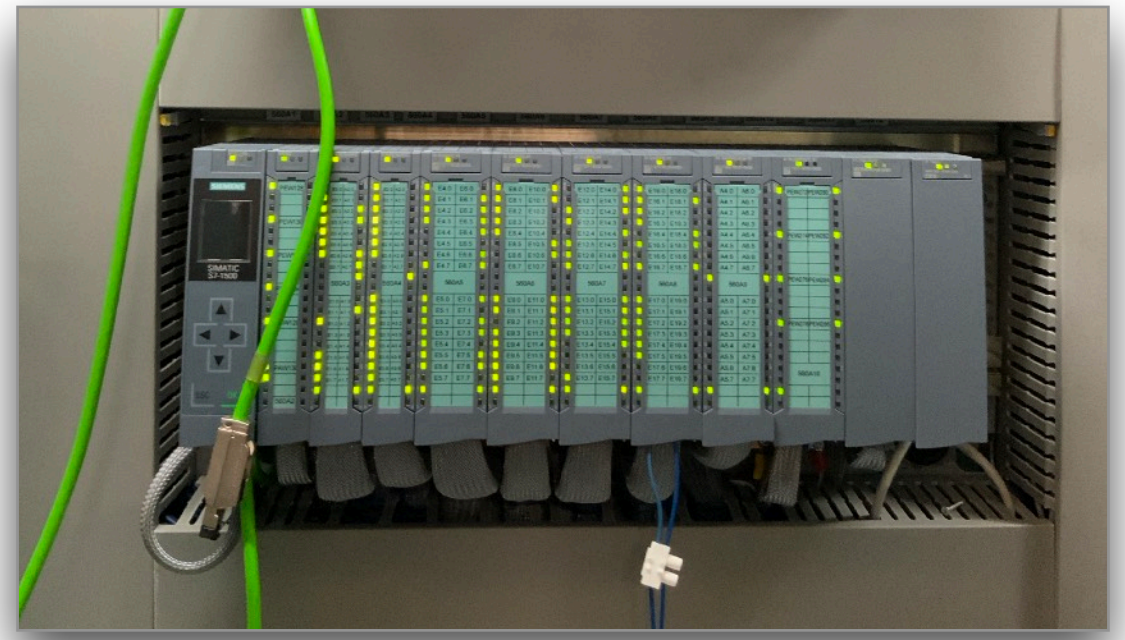


Figura 3: Fotografia di un PLC

HMI

L' *Human Machine Interface,* o HMI, è l'interfaccia tramite il cui l'operatore può avere visibilità sul sistema di controllo, visualizzando il processo in corso, consentendo di ispezionare e manipolare i valori di processo e visualizzando gli allarmi e l'andamento dei valori di controllo.

Nella sua forma più semplice, un HMI è un dispositivo *standalone touch-enabled* , mentre i sistemi HMI più avanzati possono utilizzare server distribuiti per la replicazione e ridondanza delle interfacce.

SCADA

Il sistema SCADA (Supervisory Control And Data Acquisition) ha la funzione di effettuare telemetria e telecontrollo, ovvero la raccolta, supervisione e modifica dei dati e parametri operativi provenienti dai dispositivi di campo. Solitamente un Sistema SCADA prevede diverse componenti:

- Una o più workstation che permettono all'operatore di supervisionare e controllare i parametri di produzione;
- Una serie di unità periferiche (es. PLC, RTU, etc.) che si interfacciano direttamente con il processo di produzione (es. macchinari, impianto, etc.) tramite sensori e attuatori;
- Una rete di comunicazione, caratterizzata da una molteplicità di mezzi trasmissivi e di protocolli di comunicazione, in grado di assicurare il corretto scambio di informazioni fra computer di supervisione e unità periferiche;
- Un server, solitamente chiamato *Historian DB,* per la raccolta dello storico dei dati di produzione.

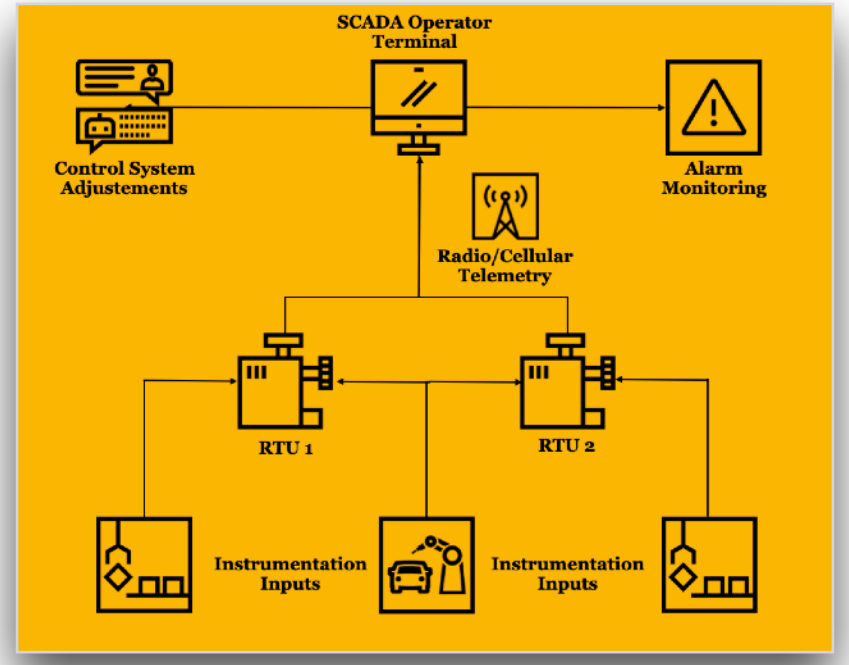


Figura 4: Architettura di un sistema SCADA

Sistemi di Safety

I sistemi di Safety, o SIS, sono sistemi di monitoraggio della sicurezza dedicati. Hanno il compito di arrestare in modo sicuro e graduale il sistema monitorato o di portarlo a uno stato di sicurezza predefinito (fail-safe) in caso di malfunzionamento dell'hardware. Un SIS utilizza una serie di parametri per determinare se un sistema funziona normalmente e, solitamente, i sistemi SIS all’interno degli impianti sono contraddistinti da un colore giallo.

Il Purdue Model

Tutti i sistemi precedentemente elencati sono integrati all’interno dell’ecosistema industriale secondo un modello ben definito, denominato Purdue Enterprise Reference Architecture (PERA), ma attualmente riconosciuto come *Purdue Model*. Tale modello, definito negli anni ’90 dalla Purdue University per far fronte alla crescente complessità degli stabilimenti industriali, mostra come si interconnettono gli elementi tipici di un'architettura ICS, dividendoli in sei/sette livelli che contengono sistemi informatici (IT) e OT. In particolare, sono definiti:

- *Enterprise Zone:*
  - Livello 5: *Enterprise*
  - Livello 4: *Corporate IT Network*
  - Livello 3.5: IT/OT IDMZ
- *Manufactoring Zone:*
  - Livello 3: *Operations*
- *Cell/Area Zone:*
  - Livello 2: *Process Network*
  - Livello 1: *Control Network*
  - Livello 0: *Field Devices*

Se implementato correttamente, il *Purdue Model* aiuta a segregare i vari sistemi, isolandoli in modo che l'organizzazione possa applicare un efficace controllo degli accessi senza ostacolare l’operatività.

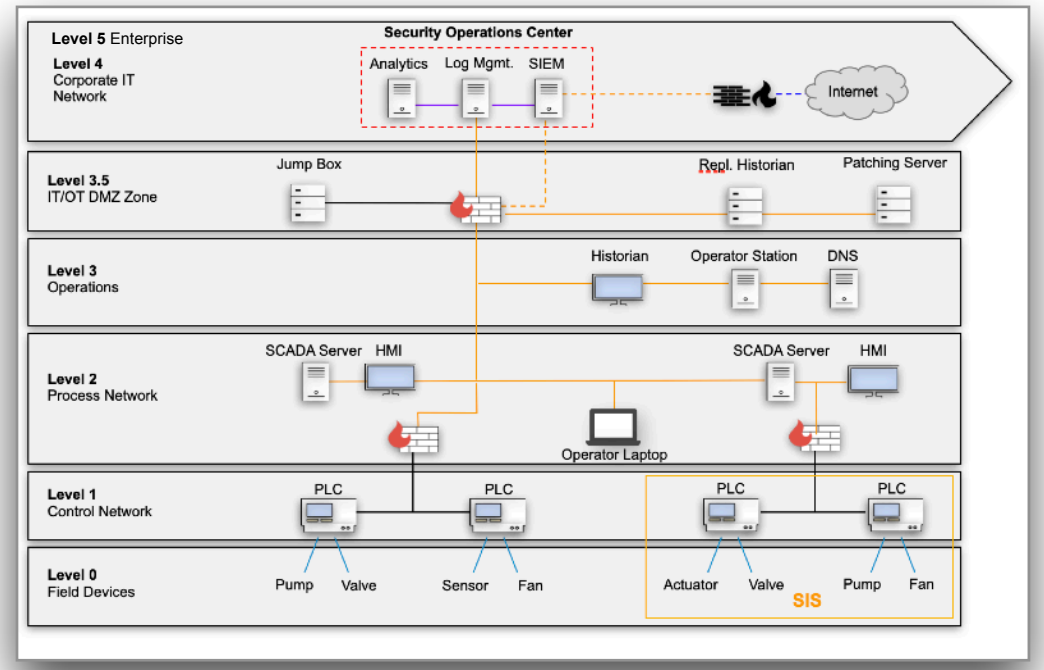


Figura 5: Architettura del *Purdue Model*

Di seguito, vengono meglio dettagliati i livelli che compongono il *Purdue Model*.

Livello 5 - Enterprise

Il livello 5 è quello in cui sono collocati sistemi e funzioni IT centralizzati. La gestione delle risorse aziendali, i servizi *business-to-business* e *business-to-customer* risiedono tipicamente a questo livello e, spesso, i sistemi di accesso delle terze parti o degli ospiti si trovano qui, anche se non è raro trovarli a livelli inferiori (ad esempio, il livello 3).

Il sistema industriale comunica con le applicazioni aziendali per scambiare dati sulla produzione e, in genere, non è richiesto l'accesso diretto ai livelli inferiori del *Purdue Model*. Un'eccezione è rappresentata dall'accesso remoto per la gestione dei macchinari da parte di terze parti e manutentori.

Livello 4 - Corporate IT Network

Il livello 4 è quello in cui risiedono le funzioni e i sistemi che necessitano l’accesso ai servizi forniti dalla rete aziendale. Questo livello è solitamente considerato un'estensione della rete aziendale, poiché qui si svolgono le attività di amministrazione aziendale e si fa affidamento sui servizi IT. Queste funzioni e sistemi includono l'accesso via cavo e wireless ai servizi della rete aziendale, come, ad esempio:

- Accesso a Internet;
- Accesso alla posta elettronica (ospitata nei Data Center);
- Sistemi non critici dell'impianto, come i sistemi di esecuzione della produzione e la reportistica generale dell’impianto;

- Accesso alle applicazioni aziendali, come SAP;
- *Landing Point* per le soluzioni Remote Desktop Gateway (RD Gateway) nei livelli inferiori.

Gli utenti e i sistemi del livello 4 spesso richiedono dati e informazioni sintetiche dai livelli inferiori della rete di Plant, e essendo questo livello maggiormente esposto ad internet, viene spesso considerato come il livello più sensibile ad eventuali minacce. La sicurezza dell'interazione tra il livello 4 e i livelli inferiori si ottiene implementando una zona industriale demilitarizzata (IDMZ o DMZ).

Livello 3.5 - IT/OT IDMZ (DMZ)

La zona demilitarizzata industriale (DMZ) è definibile come un *buffer* che applica le politiche di sicurezza e filtraggio dei dati tra una rete fidata (zona industriale) e una rete non fidata (zona aziendale). Per fare ciò, la DMZ contiene solitamente asset che fungono da servizi di intermediazione tra la zona industriale e la zona aziendale, come ad esempio:

- Mirror applicativi, come la replica SQL per gli storici dei dati;
- Servizi di gateway Microsoft Remote Desktop (RD) per le sessioni interattive remote;
- Server proxy inverso per il traffico web.

Tali servizi contribuiscono a nascondere e proteggere l'esistenza e le caratteristiche dei server e delle applicazioni della zona industriale dai client e dai server della zona aziendale.

Una DMZ implementata correttamente prevede che:

- Tutto il traffico di rete da entrambi i lati della DMZ termini nella DMZ stessa. Nessun tipo di traffico attraversi direttamente la DMZ;
- Il traffico di rete OT sensibile, come i pacchetti EtherNet/IP, non entri nella DMZ e rimanga all'interno della zona industriale;
- I servizi primari non siano memorizzati in modo permanente nella DMZ;
- Tutti i dati siano transitori. La DMZ non memorizza i dati in modo permanente;
- Le sotto-reti funzionali all'interno della DMZ siano configurate per segmentare l'accesso ai dati e ai servizi di rete OT (ad esempio, zone IT, operative e terze parti);
- La DMZ supporti la capacità di essere scollegata in caso di compromissione, pur consentendo alla zona industriale di mantenere la continuità operativa.

Livello 3 - Operations

Il livello 3 rappresenta il livello più alto della zona di produzione. I sistemi e le applicazioni presenti a questo livello supportano e gestiscono le funzioni OT a livello di Plant e solitamente prevedono:

- Funzioni di rete OT, come l'instradamento inter-VLAN e l'ispezione del traffico;
- Reportistica di processo (es. tempi di ciclo, indice di qualità, etc.);
- Storico dei dati dell'impianto;
- Pianificazione dettagliata della produzione;
- Infrastruttura virtuale per l'accesso a workstation e sessioni desktop remote;
- Server per il patching di sistemi operativi ed applicazioni;
- Servizi di rete e di dominio, come Active Directory (AD), Dynamic Host Configuration Protocol (DHCP), Dynamic Naming Services (DNS), Windows Internet Naming Service (WINS), Network Time Protocol (NTP), ecc.

I sistemi e le applicazioni di livello 3 possono comunicare con i dispositivi dei livelli 0 e 1 e possono funzionare come *landing zone* per l'accesso alla zona di produzione dai livelli superiori, permettendo di condividere i dati con i sistemi e le applicazioni dell'Enterprise Zone ai livelli 4 e 5. I sistemi e le applicazioni del livello 3 utilizzano principalmente dispositivi e sistemi operativi standard (sistemi informatici basati su Unix o Windows) e solitamente comunicano tramite protocolli di rete Ethernet e IP standard.

Il livello 3, è il livello all'interno della zona di produzione in cui avvengono la maggior parte delle interazioni. È l'area in cui gli operatori delle sale di controllo centrali accedono ai sistemi informatici condivisi, osservando e interagendo con i sistemi e le applicazioni dell'impianto.

Livello 2 - Process Network

Il livello 2 rappresenta le applicazioni e le funzioni associate alla supervisione e al funzionamento della cella/zona. Alcuni esempi di applicazioni e sistemi di livello 2 possono essere:

- Interfacce operatore o HMI;
- Allarmi o sistemi di allerta;
- Postazioni di lavoro in sala controllo.

Le applicazioni e i sistemi di livello 2 comunicano con i controllori di livello 1 e si interfacciano o condividono i dati con i sistemi e le applicazioni a livello di Plant (livello 3) o di azienda (livello 4/5) attraverso la DMZ.

Solitamente, le applicazioni di livello 2 comunichino con protocolli di rete Ethernet e IP standard e non con protocolli proprietari. Inoltre, sono tipicamente collegate internamente e direttamente alla rete di celle/aree per le quali svolgono funzioni di supervisione.

Livello 1 - Control Network

Il livello 1 è costituito da controllori (es. PLC, RTU) che regolano il processo di produzione attraverso l'interfacciamento con i dispositivi del livello 0 (es. sensori e attuatori).

I dispositivi presenti a questo livello utilizzano sistemi operativi in tempo reale specifici del settore, programmati e configurati da postazioni di lavoro di progettazione. Solitamente, i controllori sono gestiti da un'applicativo installato su una workstation, situata a un livello superiore della rete OT. Da questa workstation, l'operatore può modificare ad aggiornare il programma installato sui controllori.

Dato che i controllori hanno una funzione particolarmente critica all'interno di un ambiente OT, l'accesso ad essi deve essere strettamente controllato. L'accesso diretto a un PLC potrebbe, infatti, dare ad un utente malevolo la possibilità di interrompere il corretto funzionamento del controllore, ad esempio attraverso un attacco di tipo Denial Of Service (DOS) o manipolando i valori dei registri e dei tag.

Livello 0 - Field Devices

Il livello 0 è costituito da un'ampia gamma di sensori e attuatori coinvolti nel processo produttivo di base. Questi dispositivi eseguono le funzioni primarie del processo produttivo, come l'azionamento di un motore, la misurazione di variabili e l'esecuzione di funzioni chiave. Tali funzioni possono essere azioni relativamente semplici (es. indicatore di temperatura) o molto complesse (es. movimento di un robot). I protocolli di comunicazione utilizzati in questo livello sono molto eterogenei e variano da protocolli proprietari dei produttori dei dispositivi, a protocollo più comuni.

Vettori di attacco dei sistemi industriali

E' molto importante osservare che, nonostante il *Purdue Model* rappresenti un modello architetturale per i sistemi industriali, una sua corretta implementazione non garantisce necessariamente un buon livello di Security. Mentre infatti vi è una segregazione orizzontale dei sistemi, non è presente una segregazione orizzontale, che permetta di creare zone e canali di comunicazione specifici all'interno di ogni livello del *Purdue Motel*. Tali tematiche saranno trattate nel seguente capitolo.

Vediamo invece ora quali sono i principali vettori di attacco tramite i quali un hacker o utente malevolo potrebbe ottenere accesso al sistema industriale. Va specificato che la quasi totalità di questi vettori, fatta esclusione per quelli che prevedono l'accesso fisico ai sistemi, sono stati introdotti con l'integrazione con il mondo IT e la connessione dei sistemi ad Internet.

- Accesso remoto non protetto: La maggioranza delle attività di manutenzione sulle linee di produzione avviene tramite accesso remoto delle terze parti esterne allo stabilimento. Se la procedura per gli accessi remoti non è sufficientemente robusta, una compromissione delle

utenze dei fornitori potrebbe fornire ad un utente malevolo l'accesso a buona parte delle linee di produzione;

- Phishing: Nei livelli 4 e 5 del *Purdue Model* è spesso possibile trovare workstation esposte ad internet. Gli operatori di tali workstation possono essere soggetti a campagne di *Phishing* e *Spear Phishing*, finalizzati ad ottenere accesso ai dati di produzione o, nel peggiore dei casi, all'interno stabilimento;
- Assenza/*misconfiguration* di Firewall: La segregazione orizzontale proposta dal *Purdue Model* deve essere implementata anche attraverso vari strati di Firewall, correttamente configurati per abilitare solo il traffico consentito. Idealmente, tutti i Firewall dovrebbero essere configurati secondo il modello *Deny-all-Allow-by-exception.* Una configurazione troppo permissiva delle regole di Firewall potrebbe permettere agli attaccanti di ottenere accesso sistemi con i quali non dovrebbero essere in grado di comunicare;
- Reti Wireless insicure: Le reti Wireless non sono solitamente il sistema primario di comunicazione all'interno degli impianti industriali. Se sono presenti reti Wi-Fi, sono spesso utilizzate per gestire i dispositivi mobili utilizzati all'interno degli impianti (es. laptop di manutenzione, pistole laser per lettura di codici a barre, etc.). Spesso, tali reti Wi-Fi risultano essere configurate con lo Standard WPA2 Pre-Shared Key (PSK), o altri Standard ormai deprecati e soggetti a possibili attacchi di cattura dell'Handshake.
- Best Practice e principi di *Least Functionality* non rispettati: All'interno dei sistemi industriali è spesso possibile trovare vulnerabilità legate a:
  - Utilizzo di credenziali di default o deboli;
  - Salvataggio delle Password su fogli di carta o sotto le tastiere;
  - Porte di rete accessibili e non protette;
  - Porte USB abilitate;
  - Servizi ed applicativi non necessari installati sulle workstation.
- *Disgruntled Employees, insider* o dipendenti corrotti: Spesso, gli attacchi più pericolosi vengono proprio svolti da insider malevoli che riescono ad accedere fisicamente ai sistemi delle rete OT.

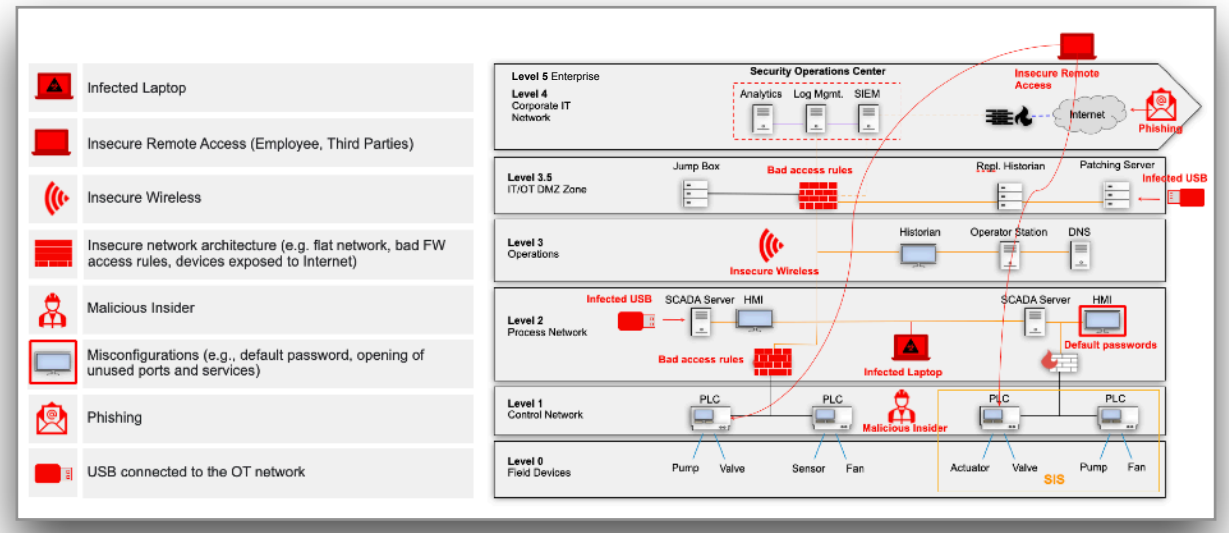


Figura 6: Vettori di attacco per i sistemi industriali

4. IEC/ISA 62443: LO STANDARD DI RIFERIMENTO PER L'OT SECURITY

Lo stato dell'arte dell'OT Security è caratterizzato da un ambiente ancora relativamente povero in termini di linee guida, Sandard e Best Practice. Ciò è sintomo di un settore in cui la Cyber Security è ancora erroneamente vista non come una necessità, ma piuttosto come un o*verhead* che comporta più svantaggi in termini di operatività che vantaggi in termine di protezione dei sistemi. Attualmente, il principale Standard di riferimento per le tematiche dell'OT Security è rappresentato dall'IEC/ISA 62443, la quale sarà trattata nel seguente capitolo.

Overview

La famiglia di Standard 62443 inizia ad essere sviluppata ne 2002, quando l'ISA (International Society of Automation) definisce uno Standard per la Cyber Security nei sistemi industriali (ISA99). Nel 2010, tale Standard viene rinominato ANSI/ISA 62443 e viene successivamente preso come riferimento dell'IEC (International Electrotechnical Commission) per sviluppare quella che poi diviene la famiglia di Standard IEC/ISA 62443.

Nel 2021 l'IEC approva la famiglia di Standard IEC/ISA 62443 come 'Standard Orizzontale' di settore, ovvero come Standard da prendere come riferimento per lo sviluppo di eventuali nuovi Standard relativi alla Cyber Security nel mondo OT.

Struttura della famiglia di Standard IEC/ISA 62443

La famiglia IEC/ISA 62443, composta da 13 sezioni, definisce una serie di requisiti e metodologia per far fronte a criticità di Cyber Security nel mondo industriale. Questa specificità sull'ambiente OT è proprio ciò che differenzia la 62443 da altri importanti standard di Cyber Security quali la ISO 2700x od il NIST CSF. Le 13 sezioni dell'IEC/ISA sono raggruppate in una struttura a quattro livelli che, partendo da tematiche più generali ed *high level,* approfondiscono in maniera sempre maggiormente tecnica i requisiti di sicurezza legati agli ambienti OT.

Più nello specifico, la gerarchia della 62443 prevede un primo livello in cui sono presenti documenti di stampo generale:

- 62443-1-1: Introduce i concetti e i modelli utilizzati nella famiglia di Standard;
- 62443-1-2: E' un glossario generale dei termini e delle abbreviazioni utilizzati nelle varie sezioni della famiglia;
- 62443-1-3: Descrive una serie di metriche quantitative derivate da *Functional Requirements* e *System Requirements;*
- 62443-1-4: fornisce una descrizione più dettagliata del ciclo di vita dell'OT Security, oltre a diversi casi d'uso.

Un secondo livello in cui sono definite Policy e procedure relative all'OT Security:

- 62443-2-1: descrive i requisiti necessari per definire e implementare un sistema di gestione della sicurezza informatica in un contesto OT;
- 62443-2-2: fornisce una metodologia per valutare il livello di protezione fornito da un sistema OT contro eventuali minacce di sicurezza e come applicare quanto richiesto dal 62443-2-1;
- 62443-2-3: fornisce indicazioni sulla gestione delle patch per i sistemi OT;
- 62443-2-4: specifica i requisiti per i fornitori relativi ai sistemi OT;
- 62443-2-5: fornisce una guida su ciò che è necessario per operare un efficace sistema di gestione dell'OT Security.

Un terzo livello in cui vengono definiti i requisiti di sicurezza dei sistemi OT:

- 62443-3-1: descrive l'applicazione di varie tecnologie di sicurezza in un ambiente OT;
- 62443-3-2: tratta la valutazione del rischio di sicurezza e la progettazione dei sistemi OT;
- 62443-3-3: fornisce le basi per la valutazione dei livelli di sicurezza forniti da un sistema OT.

Un quarto livello che fornisce informazioni maggiormente dettagliate relative allo sviluppo di componenti OT:

- 62443-4-1: descrive i requisiti applicabili allo sviluppo dei prodotti;
- 62443-4-2: contiene una serie di requisiti derivati che forniscono una mappatura dettagliata dei *System Requirements* ai sottosistemi e ai componenti del sistema OT.

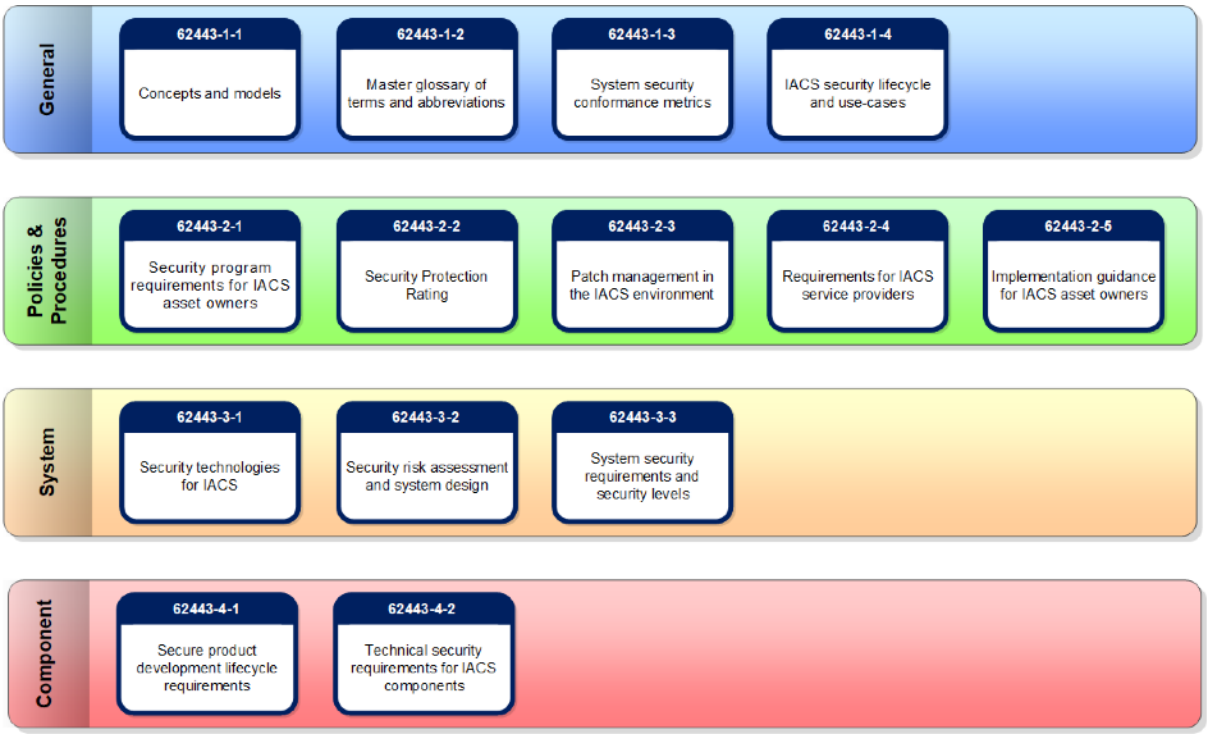


Figura 7: Famiglia di Standard 62443

Modello a “Zones & Conduits”

Il modello *Zones & Conduits* è un concetto chiave definito dallo Standard IEC/ISA 62443. Tale modello mira a suddividere l'architettura di un sistema di controllo industriale in diverse zone di sicurezza, separate da percorsi di comunicazione chiamati *Conduits,* aiutando a organizzare e proteggere il sistema in modo più efficace. Più nel dettaglio, le zone rappresentano le diverse parti del sistema OT che richiedono una protezione specifica. Ogni zona è caratterizzata da un livello di sicurezza associato, determinato dalla sensibilità delle informazioni e dalla criticità del processo che gestisce. Le zone possono includere, ad esempio, la zona di produzione, la zona di controllo e la zona di monitoraggio. I *Conduits* sono invece i percorsi di comunicazione tra le diverse zone. Questi percorsi consentono il flusso di informazioni tra le zone, e devono essere progettati e gestiti in modo sicuro per impedire intrusioni, accessi non autorizzati o qualsiasi altra minaccia. Possono essere utilizzati meccanismi di sicurezza quali crittografia e gestione degli accessi per garantire la protezione di tali *Conduits.*

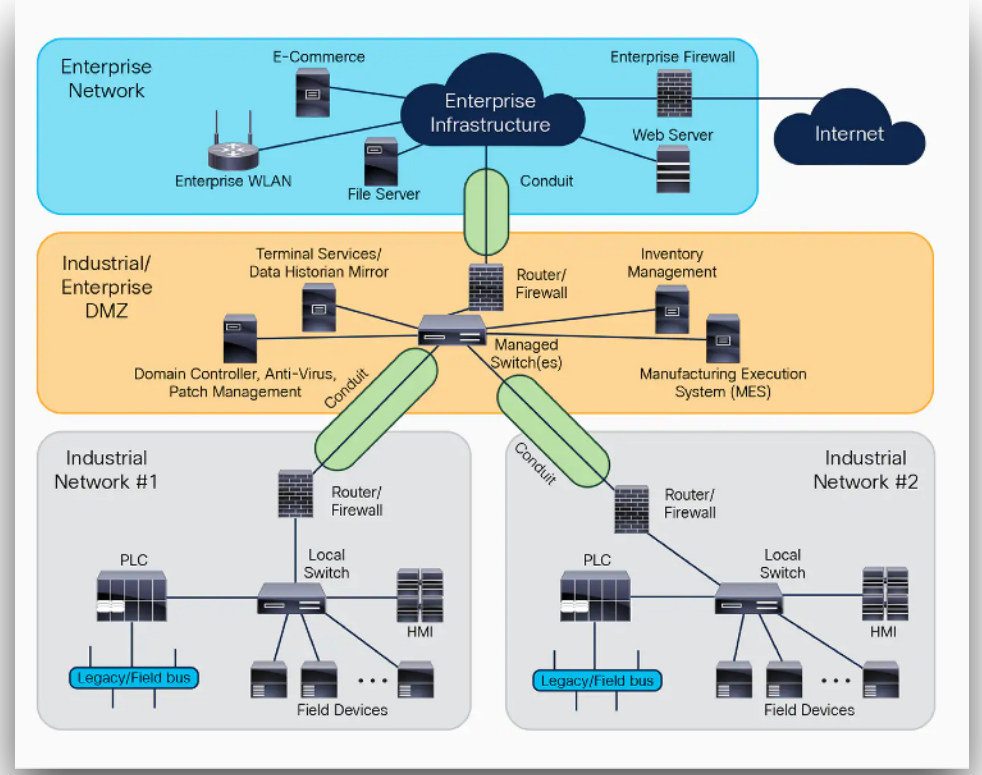


Figura 8: Esempio di modello a *Zones & Conduits*

Ora che è stato definito il concetto di *Zones & Conduits*, è necessario riprendere in considerazione il *Purdue Model* precedentemente definito. La sicurezza dei sistemi OT deve essere garantita sia sfruttando la struttura gerarchica definita dal *Purdue Model,* sia attraverso la “zonizzazione” proposta dal modello *Zones & Conduits* della 62443. Mentre, infatti, il *Purdue Model* implementa la segregazione orizzontale dei sistemi, il modello *Zones & Conduits* aiuta nella segregazione orizzontale, definendo varie zone all’interno dei livelli del *Purdue Model* ed i relativi canali di comunicazione.

IEC/ISA 62443 : analisi delle sezione 3-3

Fra le varie sezioni dell'IEC/ISA 62443 elencate nel capitolo precedente, quella che sicuramente è stata maggiormente utile per lo sviluppo dei Framework illustrati in questa tesi è la sezione 3-3. Tale sezione definisce una struttura gerarchica di requisiti di sicurezza da applicare ai sistemi OT. Inoltre, vengono definiti dei livelli di sicurezza che, applicati ad ogni requisito, permettono di valutare lo stato complessivo di sicurezza dei sistemi. Di seguito, vengono meglio dettagliate le principali tematiche trattate dall'IEC/ISA 62443 3-3.

Functional Requirements

La 62443 3-3 definisce sette *Functional Requirements (FR),* osservabili nella seguente tabella, i quali rappresentano le principali aree di interesse relativamente allOT Security.

ID	Functional Requirment
1	Identificazione ed Autenticazione
2	Autorizzazione e Controllo dell'utilizzo
3	Integrità di sistema
4	Confidenzialità dei dati
5	Limitazione del flusso di dati
6	Monitoraggio e tempestività di risposta
7	Disponibilità delle risorse

Partendo dalle tematiche di gestione ed *enforcement* degli accessi, si passa poi all'integrità dei sistemi OT, alla confidenzialità dei dati in transito e *At-Rest* e alla limitazione e monitoraggio del flusso di dati nel sistema, per trattare infine la disponibilità delle risorse.

System Requirements

Un volta definiti gli FR, vengono poi definiti numerosi *System Requirements (SR),* che rappresentano degli effettivi requisiti di sicurezza da associare ai sistemi OT. Ad ogni FR definito, vengono associati diversi SR in base alla tematica trattata. Nella tabella seguente è illustrato un esempio, non esaustivo, della associazione fra *Functional Requirements* e *System Requirements.*

ID	Functional Requirment	SR ID	System Requirement
1	Identificazione ed Autenticazione	1	Identificazione ed Autenticazione di utenti umani
		2	Identificazione ed Autenticazione di processi software e dispostivi
		3	Gestione degli Account
		4	Gestione degli Autenticatori
		5	Gestione degli accessi wireless
		6	…
2	Autorizzazione e Controllo dell'utilizzo	1	Applicazione dell'Autorizzazione
		2	…
3	…	1	…

Requirement Enhancement

Spesso, ad ogni *System Requirements* definito vengono associati ulteriori requisiti aggiuntivi, chiamati *Requirement Enhancement (RE),* che permettono di aumentare il livello di sicurezza complessivo associato al requisito. Di seguito viene mostrato un esempio di gestione degli RE. Partendo dall'SR base 2.1 che prevede l'*enforcement* dei meccanismi di autenticazione solo per alcuni utenti, vengono poi definiti RE aggiuntivi che prevedono, rispettivamente:

- L'*enforcement* dell'autenticazione su tutti gli utenti
- Il mapping dei vari permessi sui ruoli di sistema (RBAC)
- L'override manuale dei permessi da parte di una utenza amministrativa autorizzata
- Una doppia approvazione delle operazioni da parte di più utente amministrative

SR ID	System Requirment	RE ID	Requirement Enhancement
2.1	Applicazione dell'Autorizzazione	1	Applicazione dell'Autorizzazione per tutti gli utenti
		2	Mapping dei permessi sui ruoli
		3	Override manuale dei permessi
		4	Doppia approvazione

Security Levels

Una volta definiti i requisiti di sicurezza dei sistemi OT, la 62443 3-3 propone quindi la definizione di quattro (o cinque, considerando anche l'SL0) livelli di sicurezza che permettono di rappresentare la *Security Posture* dei sistemi. Tali livelli di sicurezza sono strettamente connessi ai requisiti introdotti dai SR e dagli RE, e possono essere descritti come di seguito:

- Security Level 0 (SL0): Non sono richiesti requisiti o protezioni particolari.
- Security Level 1 (SL1): Protezione da un uso improprio non intenzionale o accidentale.
- Security Level 2 (SL2): Protezione contro l'uso improprio intenzionale attraverso strumentazione *high level,* poche risorse, competenze superficiali e scarsa motivazione.
- Security Level 3 (SL3): Protezione contro l'uso improprio intenzionale attraverso strumentazione sofisticata, con risorse moderate, conoscenze specifiche in ambito OT e buona motivazione.
- Security Level 4 (SL4): Protezione contro l'uso improprio intenzionale attraverso strumentazione sofisticata e non comunemente reperibile, con risorse estese, conoscenze specifiche in ambito OT e motivazione elevata.

L'implementazione di ogni *System Requirements* permette di soddisfare almeno uno dei *Security Level* definiti. Nel caso in cui il SR non soddisfi tutti gli SL, e nel caso in cui tutti gli SL siano disponibili per tale SR, il raggiungimento dei *Security Level* mancanti può essere ottenuto attraverso la progressiva l'implementazione dei vari *Requirement Enhancement* definiti per il SR in questione. In questo modo, una volta definito un *Security Level* target per una zona (definita secondo il modello *Zones & Conduits*), è possibile decidere dinamicamente e modularmente quali RE implementare per raggiungere il S*ecurity Level* desiderato. Di seguito, con riferimento al SR 2.1 ed ai relativi RE definiti nella tabella precedente, viene illustrata una matrice che permette di mappare i SR e RE sui vari *Security Level.*

SR ID/ RE ID	SL 1	SL 2	SL 3	SL 4
SR 2.1	✓	✓	✓	✓
SR 2.1 RE 1		✓	✓	✓
SR 2.1 RE 2		✓	✓	✓
SR 2.1 RE 3			✓	✓
SR 2.1 RE 4				✓

IEC/ISA 62443 4-2: caratteristiche principali

Infine, è opportuno soffermarsi brevemente sulla sezione 4-2 dell'IEC/ISA 62443, in quanto strettamente connessa alle tematiche trattate nella sezione 3-3. La 62443 4-2 precede a concretizzare i *System Requirements* definiti nella sezione 3-3 attraverso la definizione di *Component Requirements* (CR), con l'obbiettivo di definire dei requisiti di sicurezza per ogni tipo di

componente presente all'interno dei sistemi OT. I CR sono infatti definiti per quattro diversi tipi di componenti: applicativi software, dispositivi embedded, dispositivi host e dispositivi di rete. Pertanto, i CR sono a loro volta suddivisi nelle seguenti tipologie di requisiti:

- Software application requirements (SAR)
- Embedded device requirements (EDR)
- Host device requirements (HDR)
- Network device requirements (NDR)

E' importante osservare che i CR sono coincidenti, nella maggior parte dei casi, con i requisiti definiti negli SR della sezione 3-3. Per questo motivo, per la definizione dei Framework di sicurezza trattati in questa tesi, sono stati presi maggiormente in considerazione i *System Requirements* della sezione 3-3.

Avendo ora descritto in questo capitolo la struttura e le caratteristiche principali dello Standard orizzontale per l'OT Security, è possibile introdurre i due Framework relativi all'OT Security trattati in questa tesi, in quanto strettamente connessi ai System Requirements definiti dall'IEC/ISA 62443 3-3.

5. DEFINIZIONE DI UN FRAMEWORK DI SICUREZZA DA APPLICARE AGLI STABILIMENTI INDUSTRIALI

L'attuale carenza di Standard e Best Practice di sicurezza specifiche per l'ambiente OT è stata la motivazione principale che ha portato alla creazione dell'OT Security Framework. Lo scopo di questo Framework è proprio quello di fornire una check-list di controlli che permetta di valutare a 360 gradi la Cyber Security di uno stabilimento.

Il Framework è suddiviso in 78 controlli di sicurezza, raggruppati in 12 Domini, dove ogni Dominio rappresenta una macro-area relativa alla sicurezza dei sistemi OT. I Domini definiti prevedono tematiche di:

- Network Security
- Identificazione ed Autenticazione
- Accessi Remoti
- Third Party Security
- Backup e ripristino
- Detection & Recovery
- Data Security
- Patching & Update
- Asset Inventory & Device Hardening
- Physical Security
- Training e awareness
- Security Governance

Processo di definizione dell'OT Security Framework

I Domini sono stati disposti in un ordine tale da permettere una buona continuità logica in fase di intervista e di applicazione dell'OT Security Framework in contesti *real-life.* Vengono infatti inizialmente trattate tematiche di architettura, segmentazione e segregazione della rete OT, fondamentali per identificare in maniera chiara la tipologia di stabilimento sotto analisi. Una volta identificata la rete che connette i dispositivi OT, vengono poi trattate tematiche di identificazione ed autenticazione a tali sistemi, prima per gli accessi locali, e poi per gli accessi remoti. Dal momento che la maggior parte degli accessi remoti agli stabilimenti viene effettuato da manutentori e terze parti, il Dominio seguente è proprio quello riguardante la Third Party Security e la gestione sicura dei fornitori. Successivamente, passando a tematiche di software a dati, vengono prima discusse le tematiche di gestione dei backup, dei log e di Detection, fondamentali per introdurre poi i temi di

Disaster Ricovery. Vengono poi discussi i controlli relativi alla protezione del dato e alla gestione sicura degli aggiornamenti. Passando alla gestione degli Asset dello stabilimento, vengono trattate tematiche di Asset Inventory, Hardening logico (es. Antivirus, EDR, configurazione sicura, etc.) e fisico dei dispositivi. Restando nell'area di interesse della sicurezza fisica, vengono poi discusse tutte le tematiche di protezione fisica dello stabilimento e di gestione sicura degli accessi fisici. Infine, vengono trattate tematiche di *People* e *Process,* con controlli relativi al Training & Awareness dei dipendenti e alla gestione della Security Governance (es. Framework documentale, ruoli e responsabilità, etc.).

I controlli del Framework sono stati definiti partendo dallo stato dell'arte dei requisiti di sicurezza in ambito OT Cyber Security. Per fare ciò, sono state prese in considerazioni tutti i *System Requirements* definiti dall'IEC/ISA 62443 3-3 e alcuni controlli di sicurezza provenienti dall'IEC/ISA 62443 4-2. Tali controlli di sicurezza prevedono un focus sulle principali tematiche tecniche di Cyber Security, come mostrato nel capitolo precedente. Tuttavia, per valutare a pieno non solo le tematiche di *Technologies,* ma anche quelle di *People* e *Process,* sono stati presi in considerazione ulteriori Standard in ambito Cyber Security, ovvero l'ISO 27001 e il NIST Cyber Security Framework (CSF), al fine di inserire controlli sulla formazione del personale e sulla Governance.

I controlli definiti non sono fra loro equipollenti. Alcuni controlli hanno infatti maggiore importanza e richiedono maggiore *effort* per essere correttamente implementati. Per tale motivo, ad ogni controllo è stato assegnato un peso specifico in percentuale relativo al proprio dominio di appartenenza.

Struttura dell'OT Security Framework

L'OT Security Framework è stato implementato attraverso un foglio di calcolo, utilizzando il software Microsoft Excel. In questo modo, è stato possibile sfruttare al meglio la struttura tabellare di questo Framework, sia in fase di definizione, che in fase di applicazione in contesti *real-life.* Il Framework prevede un controllo per ogni riga, e presenta nelle colonne i seguenti campi:

- ID Dominio: Codice identificativo del Dominio del Framework. Tale valore va da 1 a 12.
- Dominio: Dominio di appartenenza del controllo.
- ID Controllo: Codice identificativo del controllo. Tale valore è utilizzato nella forma 1.1, 1.2, 2.1, 2.2, etc.
- Controllo: Nominativo del controllo.
- Domanda: Domanda associata al controllo. Tale domanda può essere utilizzata come riferimento durante l'analisi di casi di studio *real-life,* o può essere direttamente posta agli interlocutori in fase di intervista o Audit presso uno stabilimento.

- Riferimento: Riferimento all'identificativo del *System Requirement* dello Standard ISA/IEC 62443 preso come riferimento per la definizione del controllo. Nel caso siano stato preso come riferimento un altro Standard, sarà esplicitato nel nome dell'identificativo.
- ISA 62443 Requirement/Enhancement: Descrizione del *System Requirement* preso come riferimento per la definizione del controllo. Nel caso siano stato preso come riferimento un altro Standard, sarà esplicitato nel nome dell'identificativo.
- Descrizione razionali maturità: questi campi definiscono le condizioni tramite le quali è possibile determinare il livello di implementazione del controllo. I Razionale di implementazione variano per ogni controllo ma, generalmente, il loro significato è esplicitato nella seguente tabella:

Razionale Non implementato	Descrizione maturità "Non implementato". Tale maturità indica che il controllo non è soddisfatto. **Il controllo è KO**.
Razionale Implementato Ad-Hoc	Descrizione maturità "Implementato Ad-hoc". Tale maturità indica che vengono effettuate alcune attività in merito ma non sono sufficenti al soddisfacimento del controllo. **Il controllo è KO**.
Razionale Implementato	Descrizione maturità "Implementato". Tale maturità indica che le attività in merito sono sufficenti al soddisfacimento del controllo. **Il controllo è OK**.
Razionale Ottimizzato	Descrizione maturità "Ottimizzato". Tale maturità indica che le attività in merito sono superiori ai requisiti del controllo. **Il controllo è OK**.

- Maturità: Campo compilabile. In tale campo è possibile inserire, selezionandolo da una lista di valori, il livello di maturità identificato a seguito delle attività di analisi o intervista. Nel caso in cui, per qualche motivazione, il controllo non sia applicabile al contesto in analisi, è possibile selezionare il valore "Non Applicabile".
- Note: Campo compilabile. E' possibile utilizzare questo campo per inserire i risultati emersi dalle analisi o interviste.
- Azioni di miglioramento: Campo compilabile. E' possibile usare tale campo per identificare eventuali azioni di miglioramento consigliate, nel caso in cui il controllo non sia pienamente soddisfatto.
- Documentazione in ambito: Campo compilabile. Tale campo può essere utilizzato per associare al controllo eventuale documentazione già presente in ambito.
- Ownership controllo: Campi comparabili. Tali campi permettono di identificare quale funzione/i aziendale abbia la responsabilità di gestire il controllo in questione. E' importante osservare che le le funzioni aziendali possono variare da caso di studio in caso di studio ma, solitamente, le principali funzioni responsabili della Cyber Security di uno stabilimento sono:
  - Corporate IT
  - Corporate OT
  - Amministrazione locale del Plant
  - Altre funzioni aziendali (es. Physical Security)

- Calcolo Maturità: Questi campi associano ad ogni controllo un peso specifico rispetto al proprio Dominio di appartenenza e, in base al livello di maturità assegnato, permettono di calcolare automaticamente il punteggio ponderato che contribuirà ad influire sulla livello di maturità globale dello stabilimento analizzato.

Vengono di seguito dettagliati i vari Domini e controlli dell'OT Security Framework.

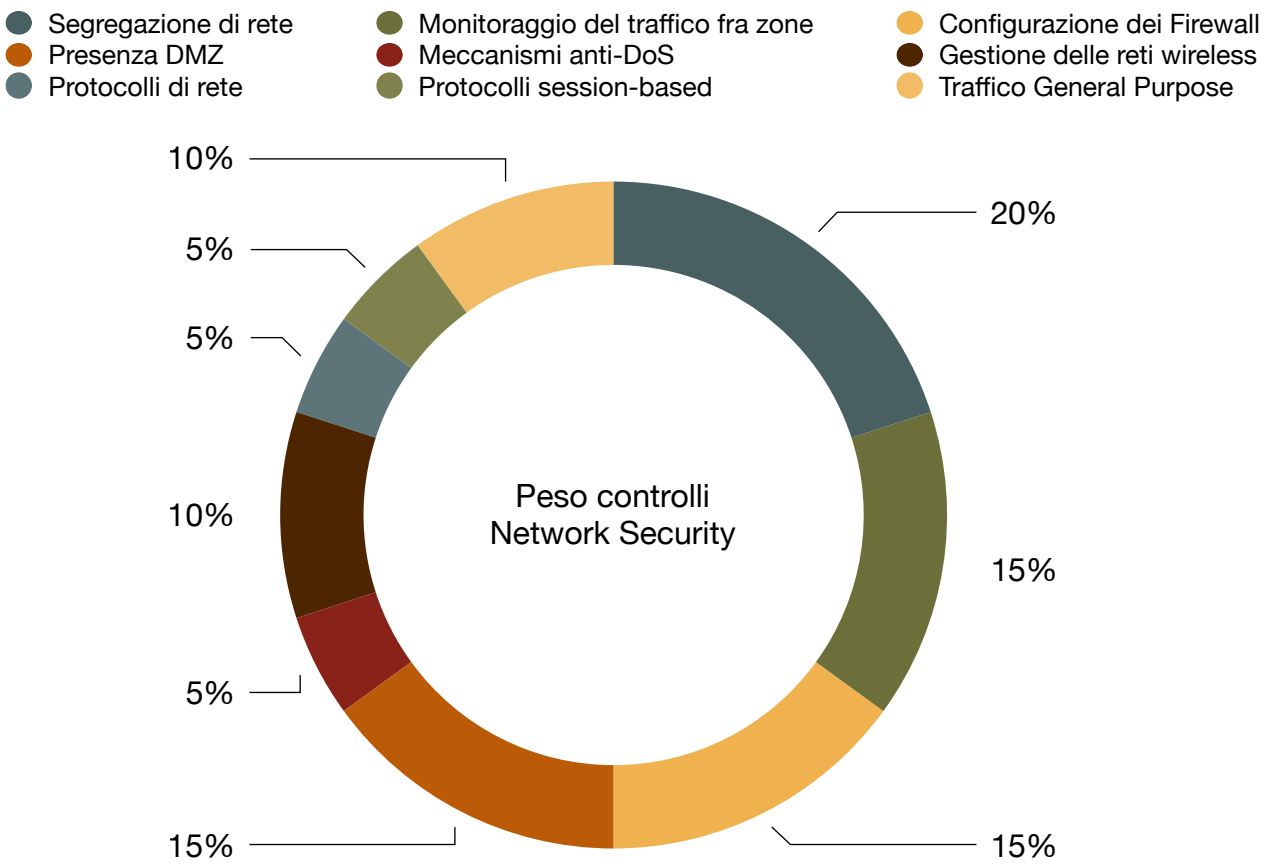
Network Security

La gestione della sicurezza delle reti OT è cruciale poiché tali reti supportano processi industriali critici. La compromissione della loro sicurezza potrebbe causare danni gravi, con conseguenza sulla produzione e sulla Safety. La protezione delle reti OT è essenziale per evitare accessi non autorizzati, *sniffing* e manipolazione del traffico di rete e garantire la continuità operativa.

Tale Dominio prevede 9 controlli relativi a:

1. Segregazione di rete
2. Monitoraggio del traffico fra zone
3. Configurazione dei Firewall
4. Presenza DMZ
5. Meccanismi anti-DoS
6. Gestione delle reti wireless
7. Protocolli di rete
8. Protocolli session-based
9. Traffico General Purpose

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Segregazione di rete

Una rete correttamente segregata permette di controllare meglio il traffico e limitare eventuali *lateral movement* di un utente malevolo che ha ottenuto accesso al sistema. La rete può essere segregata secondo diversi criteri e con diversi livelli di granularità.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente nessuna segregazione di rete.
Razionale Implementato Ad-Hoc	È presente una segregazione high-level tra ambienti IT e OT.
Razionale Implementato	La rete è segregata secondo il modello "Zones & Conduits".
Razionale Ottimizzato	La rete è segregata secondo modelli di architettura di sicurezza avanzata per gli ambienti OT (Zero Trust Architecture).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.1	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

Monitoraggio del traffico fra zone

Se la rete è segregata, le comunicazioni tra le varie zone devono essere monitorate e controllate, per permettere di filtrate il traffico in linea con quanto definito dagli schemi di rete. Ciò può essere fatto attraverso l'utilizzo di Firewall, IDS/IPS o Data Diodes/Unidirectional Gateways.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente nessun dispositivo di filtraggio del traffico di rete.
Razionale Implementato Ad-Hoc	È presente un sistema di sicurezza perimetrale per il flusso North/South.
Razionale Implementato	Sono presenti più sistemi di sicurezza di campo dedicati ad ogni cella/zona.
Razionale Ottimizzato	Sono presenti più Firewall di campo dedicati ad ogni cella/zona, con funzionalità Deep Packet Inspection OT-aware e/o IDS/IPS.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.1	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

Configurazione dei Firewall

Se le comunicazioni sono controllate tramite Firewall, essi devono essere configurati in modo tale da bloccare tutto il traffico di default e permetterlo solo in caso di eccezioni (*modello deny-all, permit by exception*).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vi è alcuna restrizione sul traffico passante per i Firewall.
Razionale Implementato Ad-Hoc	Non vi è alcuna restrizione sul traffico passante per i Firewall.
Razionale Implementato	Il traffico è configurato secondo la modalità "deny all-permit by exception" e le regole vengono revisionate periodicamente in linea con un processo definito.
Razionale Ottimizzato	Sono state definite delle regole di traffico specifiche non solo in base a "source", "destination" e "port", ma anche per determinati tipi di applicativi (es. browser) ed utenti.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.2 RE 1	The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

Presenza DMZ

Come già illustrato nel Capitolo 2, l'utilizzo di una zone demilitarizzata (DMZ) che funga da *broker* per il traffico è fondamentale per segregare correttamente l'ambiente IT da quello OT, in modo tale che nessuno dei due ambienti abbia visibilità diretta e scambio di informazioni con l'altro.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene utilizzata una DMZ.
Razionale Implementato Ad-Hoc	E' presente una DMZ generica di rete.
Razionale Implementato	Viene utilizzata una DMZ (VLAN dedicata) per i sistemi OT utilizzati da IT.
Razionale Ottimizzato	È presente una DMZ con replica dei sistemi accessibili da IT (es. replica historian).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.1 RE 2	The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks

Meccanismi anti-DoS

Gli attacchi di tipo DoS e DDoS rappresentano una grande minaccia per tutti i sistemi informatici, inclusi quelli appartenenti al contesto industriale. Un attacco DoS/DDoS lanciato esternamente o internamente allo stabilimento può facilmente sovraccaricare controllori con potenza di calcolo e banda già abbastanza limitati. Per tale motivo è fondamentale che nella rete OT siano presenti meccanismi per prevenire tale tipo di attacchi (es., Rate Limiter, Load Balancing, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente alcun tipo di meccanismo di difesa da attacchi DDoS/DoS.
Razionale Implementato Ad-Hoc	Sono presenti alcuni meccanismi elementari di difesa da attacchi DDoS/DoS (es. IP whitelisting).
Razionale Implementato	Sono presenti uno o più meccanismi anti DDoS/DoS attivabili sui Firewall (es. Rate Limiter, Load Balancing e Blackholing/Sinkholing).
Razionale Ottimizzato	Sono adottate soluzioni dedicate per la mitigazione di attacchi DDoS/DoS (es. Akamai, CloudFlare, etc.)

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.1 RE 2	The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks

Gestione delle reti wireless

Nel caso vengono utilizzate reti Wireless all'interno dello stabilimento, queste devono essere configurate tenendo conto di Standard e Best Practice di settore (es. WPA2/3 Enterprise).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Vengono utilizzate reti Wireless senza autenticazione.
Razionale Implementato Ad-Hoc	Vengono utilizzate reti WPA 2/3 con PSK o standard obsoleti (es. WEP, WPA).
Razionale Implementato	Vengono utilizzate reti WPA 2/3 Enterprise (con certificati/radius)
Razionale Ottimizzato	Vengono utilizzate reti WPA 3 Enterprise (con certificati/radius), con il monitoraggio dello spettro wireless.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.2	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices

Protocolli di rete

Solitamente, all'interno dei sistemi OT vengono utilizzati numerosi protocolli di comunicazione. Tali protocolli, tuttavia, spesso non prevedono la cifratura dei pacchetti o l'autenticazione del mittente per motivi di operatività (es. Modbus). Attualmente, sono disponibili diversi protocolli di comunicazione (es. OPC UA, Secure Modbus, etc.) che garantiscono la confidenzialità dei dati, senza compromettere l'operatività.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi OT utilizzano protocolli che non garantiscono la confidenzialità e integrità dei dati in-transit (es. Modbus TCP, etc.).
Razionale Implementato Ad-Hoc	In alcuni casi vengono utilizzati protocolli che garantiscono la confidenzialità e integrità dei dati in-transit (es. OPC UA, Secure Modbus, Profinet, etc.).
Razionale Implementato	N/A

Razionale Ottimizzato	Vengono utilizzati esclusivamente protocolli che garantiscono la confidenzialità e integrità dei dati in-transit (es. OPC UA, Secure Modbus, Profinet, etc.).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.1	The control system shall provide the capability to protect the integrity of transmitted information.

Protocolli session-based

Solitamente, i PLC ed altri dispositivi OT possono essere configurati attraverso un'interfaccia web (es. TIA Portal) accessibile inserendo l'indirizzo IP del PLC nel Browser di ricerca. Se tale pagine di configurazione è abilitata, è necessario assicurarsi che utilizzi protocolli *session-based* (es. HTTPS).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Vengono utilizzati protocolli che non garantiscono la confidenzialità e l'integrità delle sessioni (es. HTTP).
Razionale Implementato Ad-Hoc	In alcuni casi vengono utilizzati protocolli che garantiscono la confidenzialità e l'integrità delle sessioni (es. HTTPS).
Razionale Implementato	Vengono esclusivamente utilizzati protocolli che garantiscono la confidenzialità e l'integrità delle sessioni (es. HTTPS).
Razionale Ottimizzato	Vengono esclusivamente utilizzati protocolli che garantiscono la confidenzialità e l'integrità delle sessioni (es. HTTPS) e le sessioni sono monitorate.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.8	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.

Traffico General Purpose

Il traffico *General Purpose* (navigazione web, mail, messaggistica istantanea, etc.) non dovrebbe essere consentito di default (fatta eccezione per rare occasioni) all'interno della rete OT, in quanto non conforme al tipo di traffico presente all'interno della rete.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Il traffico general purpose è consentito.
Razionale Implementato Ad-Hoc	Il traffico general purpose è parzialmente consentito, utilizzando delle blacklist.

Razionale Implementato	Il traffico general purpose non è consentito, fatta eccezione per alcune deroghe, le quali sono comunque monitorate e tracciate.
Razionale Ottimizzato	Il traffico general purpose non è consentito.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 5.3	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.

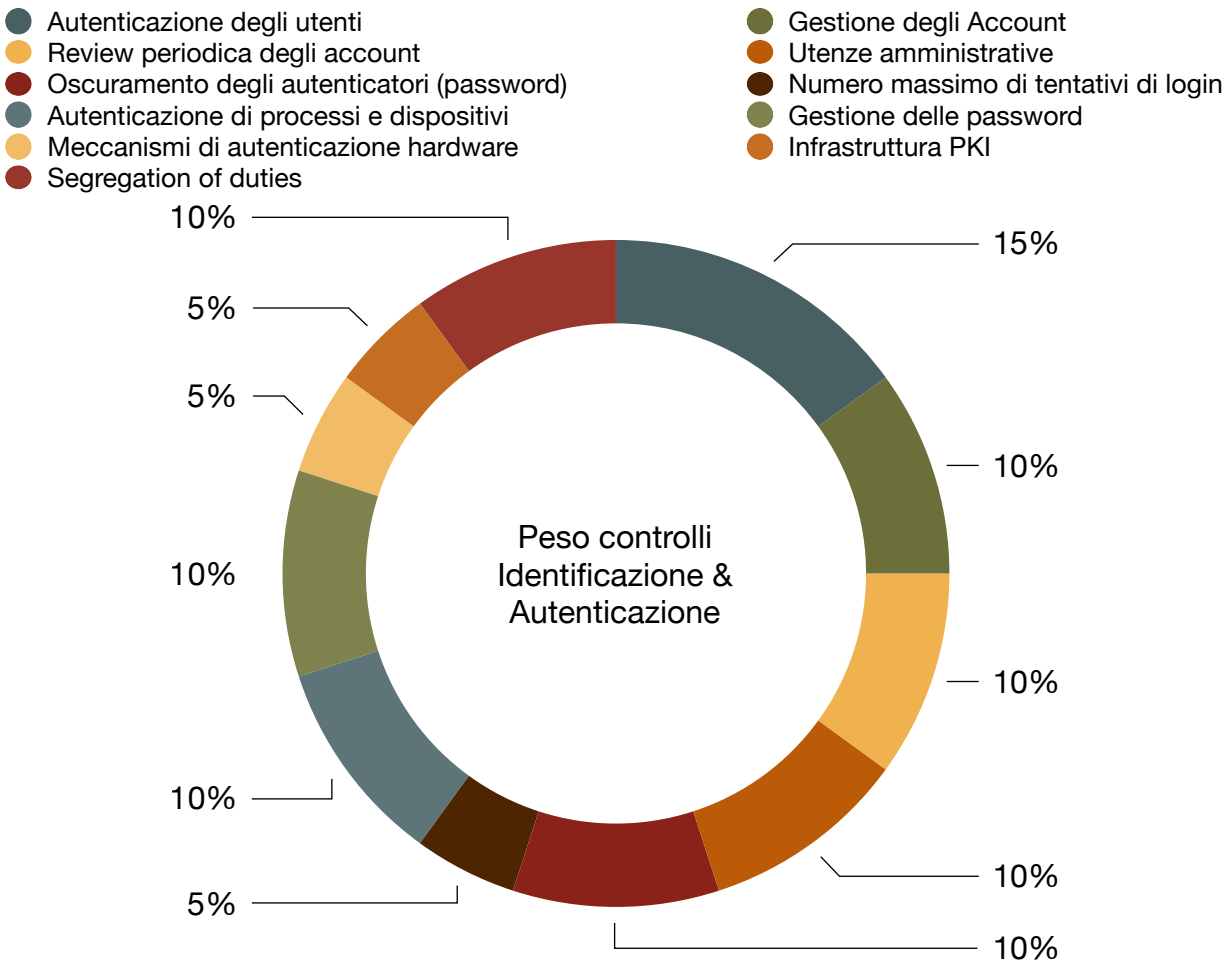
Identificazione ed Autenticazione

La gestione delle utenze e dei meccanismi di identificazione ed autenticazioni ai sistemi OT è fondamentale per impedire ad un utente malevolo l'accesso ai dati sensibili di produzione o a alle variabili di processo.

Tale Dominio prevede 11 controlli relativi a:

1. Autenticazione degli utenti
2. Gestione degli Account
3. Review periodica degli account
4. Utenze amministrative
5. Oscuramento degli autenticatori (password)
6. Numero massimo di tentativi di login
7. Autenticazione di processi e dispositivi
8. Gestione delle password
9. Meccanismi di autenticazione hardware
10. Infrastruttura PKI
11. Segregation of duties

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Autenticazione degli utenti

La grande eterogeneità dei dispositivi e delle utenze presenti all'interno di uno stabilimento industriale rende molto complicato gestire in maniera sicura gli accessi ai sistemi. E' strettamente consigliato l'utilizzo di utenze nominali all'interno dei sistemi OT, nonostante ciò introduca grande complessità e richieda molto *effort.*

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono adottati meccanismi di autenticazione (es. Auto-logon).
Razionale Implementato Ad-Hoc	Sono presenti meccanismi di autenticazione che prevedono l'uso di account generici (non nominali).
Razionale Implementato	Sono presenti meccanismi di autenticazione che prevedono l'uso di account nominali per ogni human account.
Razionale Ottimizzato	Sono utilizzati esclusivamente account nominali, protetti da meccanismi di autenticazione avanzata, quali MFA.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.1	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures

Gestione degli Account

Un sistema di gestione centralizzata degli account (es. MS Active Directory) può aiutare a ridurre la complessità derivante dall'eterogeneità e quantità di utenze e dispositivi all'interno dei sistemi OT. Idealmente, dovrebbe essere presente un sistema di gestione centralizzata degli account specifico per l'ambiente OT ed indipendente da quello già presente per l'ambiente IT.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente una soluzione centralizzata di gestione utenze.
Razionale Implementato Ad-Hoc	È presente una soluzione centralizzata di gestione utenze condivisa tra IT e OT.
Razionale Implementato	È presente una soluzione centralizzata di gestione utenze dedicata all'ambiente OT, adeguatamente isolata dal resto della rete.
Razionale Ottimizzato	Oltre ad una soluzione centralizzata di gestione utenze, viene utilizzata una soluzione PAM per gli accessi privilegiati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.3	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

Review periodica degli account

Un processo di review periodica delle utenze può permettere la loro corretta abilitazione, disabilitazione e autorizzazione.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vengono effettuate review periodiche delle utenze.
Razionale Implementato Ad-Hoc	Vengono effettuate alcuni controlli ad-hoc in merito alle utenze.
Razionale Implementato	Vengono effettuare delle review periodiche delle utenze e relativi privilegi.
Razionale Ottimizzato	Le review delle utenze sono supportate da strumenti automatici.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.3	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

Utenze amministrative

Fra le numerose utenze presenti all'interno dei sistemi OT, particolare attenzione deve essere ovviamente fornita alle utenze amministrative. Gli admin possono assegnare, modificare e revocare i privilegi assegnati alle utenze e, di conseguenza, una compromissione di tale account rappresenta una grave minaccia di sicurezza. Idealmente, devono essere presenti più utenze amministrative, al fine di garantire che chi assegna le autorizzazioni non sia la stessa persona che le conferma.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene adottata una separazione dei privilegi delle utenze.
Razionale Implementato Ad-Hoc	È presente un'unica utenza amministrativa che gestisce le autorizzazioni ed i permessi delle altre utenze.
Razionale Implementato	Sono presenti diverse utenze amministrative suddivise in base al ruolo al fine di garantire che chi assegna le autorizzazioni non sia la stessa persona che le conferma.

Razionale Ottimizzato	Sono presenti diverse utenze amministrative, al fine di garantire che chi assegna le autorizzazioni non sia la stessa persona che le conferma. Gli amministratori vengono sottoposti a corsi di formazione e Awareness specifici per sottolineare l'importanza del proprio ruolo.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.1 RE 2	The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.

Oscuramento degli autenticatori (password)

Per evitare tecniche di *Shoulder surfing,* è opportuno che i sistemi OT a cui accedono gli operatori tramite password permettano di oscurare l'inserimento degli autenticatori (oscuramento della password durante il suo inserimento).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente alcun tipo di oscuramento degli autenticatori.
Razionale Implementato Ad-Hoc	Gli autenticatori vengono oscurati, ma è consentito effettuare operazioni copia-incolla degli autenticatori.
Razionale Implementato	Durante l'inserimento, gli autenticatori vengono oscurati e ove possibile sono state impedite operazioni copia-incolla degli autenticatori.
Razionale Ottimizzato	Durante l'inserimento gli autenticatori non vengono mostrati in modo da nascondere la lunghezza dei caratteri.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.10	The control system shall provide the capability to obscure feedback of authentication information during the authentication process.

Numero massimo di tentativi di login

Al fine di evitare attacchi di *Brute Force,* per le interfacce di accesso ai sistemi OT dovrebbe essere configurato un numero massimo di tentativi di login falliti (in linea con Standard e Best Practice di settore e/o esigenze operative e di Safety) dopo il quale l'utente deve aspettare un periodo di tempo configurabile prima di effettuare un nuovo tentativo.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è stato configurato un numero massimo di tentativi di login falliti.
Razionale Implementato Ad-Hoc	Sono stati configurati un numero massimo di tentativi di login falliti e tempistiche di lock-out ma non sono stati implementati in linea con Standard e Best Practice di settore e/o esigenze operative e di Safety.

Razionale Implementato	Sono stati configurati un numero massimo di tentativi di login falliti e tempistiche di lock-out in linea con Standard e Best Practice di settore e/o esigenze operative e di Safety.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.11	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

Autenticazione di processi e dispositivi

Molto frequentemente, le comunicazioni M2M (*machine-to-machine*) fra i dispositivi OT situati nei livelli più bassi del *Purdue Model* (es. HMI-PLC, PLC-SCADA, etc.) avvengono attraverso protocolli di comunicazione che non permettono di autenticare e/o identificare il dispositivo con cui si stanno scambiando informazioni (es. Modbus). Per rendere più complicato eseguire attacchi di *spoofing,* dovrebbero essere utilizzati protocolli che permettano ai dispositivi OT di identificare ed autenticare le comunicazioni tra di loro.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I dispositivi OT non sono in alcun modo in grado di identificare ed autenticare le comunicazioni fra di loro.
Razionale Implementato Ad-Hoc	I dispositivi OT sono in grado di identificarsi a vicenda (ma non autenticarsi).
Razionale Implementato	I dispositivi OT sono in grado di identificarsi ed autenticare le comunicazioni fra di loro.
Razionale Ottimizzato	I dispositivi OT sono in grado di identificarsi ed autenticare le comunicazioni fra di loro tramite certificati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.2	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.

Gestione delle password

La gestione sicura delle password rappresenta la modalità fondamentale con cui garantire che le utenze definite vengono effettivamente accedute ed utilizzate da i relativi intestatari e non da utenti indesiderati. Le politiche di gestione delle password dovrebbero essere definite all'interno di una Password Policy che definisca, ad esempio:

- Requisiti di cambio password di default
- Modifica periodica delle password
- Salvataggio delle password
- Requisiti di complessità
- Profondità dello storico delle password

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vi sono requisiti di complessità e lifetime delle password.
Razionale Implementato Ad-Hoc	Vi sono requisiti di complessità in fase di creazione delle Password.
Razionale Implementato	Vi sono requisiti di complessità e di lifetime in fase di creazione delle Password (almeno per human account).
Razionale Ottimizzato	Vi sono requisiti di complessità e di lifetime in fase di generazione delle Password.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.5	The control system shall provide the capability to: h) initialize authenticator content; i) change all default authenticators upon control system installation; j) change/refresh all authenticators; and k) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.

Meccanismi di autenticazione hardware

Il processo di autenticazione ai sistemi potrebbe essere reso maggiormente sicuro attraverso l'utilizzo di un meccanismo di autenticazione hardware (es. badge). In questo modo, l'acceso ad un dispositivo da parte di un utente malevolo può risultare più complicato, anche in caso di furto di credenziali.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono previsti dispositivi di autenticazione hardware.
Razionale Implementato Ad-Hoc	Il processo di autenticazione hardware prevede l'utilizzo di dispositivi hardware non sicuri (es. protocolli Low Frequency).

Razionale Implementato	Il processo di autenticazione hardware prevede l'utilizzo di dispositivi hardware sicuri (es. protocolli High Frequency).
Razionale Ottimizzato	Il processo di autenticazione prevede l'utilizzo di un dispositivo hardware con protocolli sicuri (MIFARE DESFire, iCLASS Elite con Custom Keys/EMV) in combinazione con una password o altro meccanismo di autenticazione.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.5 RE 1	For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms

Infrastruttura PKI

L'utilizzo di una Public Key Infrastructure, seppur non strettamente necessario, può essere utile per la gestione delle chiavi crittografiche all'interno dello stabilimento.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non esiste un'infrastruttura PKI.
Razionale Implementato Ad-Hoc	Esiste un'infrastruttura PKI ma non gestita in linea con Standard e Best Practice di settore.
Razionale Implementato	L'infrastruttura PKI e il ciclo di vita dei certificati sono gestiti in linea con Standard e Best Practice di settore.
Razionale Ottimizzato	Utilizzo di meccanismi hardware per la protezione delle chiavi private.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.8	Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

Segregation of duties

Durante la fase di assegnazione dei privilegi delle utenze possono essere seguiti alcuni principi di progettazione per limitare le potenziali superfici di attacco. In particolare, devono essere presi in considerazione:

- Segregation of Duties (SoD): Principio di progettazione che mira a distribuire le responsabilità e le autorizzazioni in modo tale che nessuna singola utenza o abbia il controllo completo su un processo o un sistema critico.
- Principle of Least Privilege (PoLP): Principio secondo cui un utente o un sistema dovrebbe avere solo i permessi e gli accessi strettamente necessari per svolgere le sue funzioni o compiti specifici.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vengono rispettati i principi di PoLP e "segregation of duties".
Razionale Implementato Ad-Hoc	I principi di PoLP e "segregation of duties" sono adottati in maniera non granulare.
Razionale Implementato	I principi di PoLP e "segregation of duties" vengono applicati in maniera granulare su tutte le uteanze.
Razionale Ottimizzato	Viene applicato il principio di Zero Privilege, secondo cui gli utenti non hanno alcun accesso di default e gli accessi vengono concessi solo dopo l'autenticazione e la verifica della necessità.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.1	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

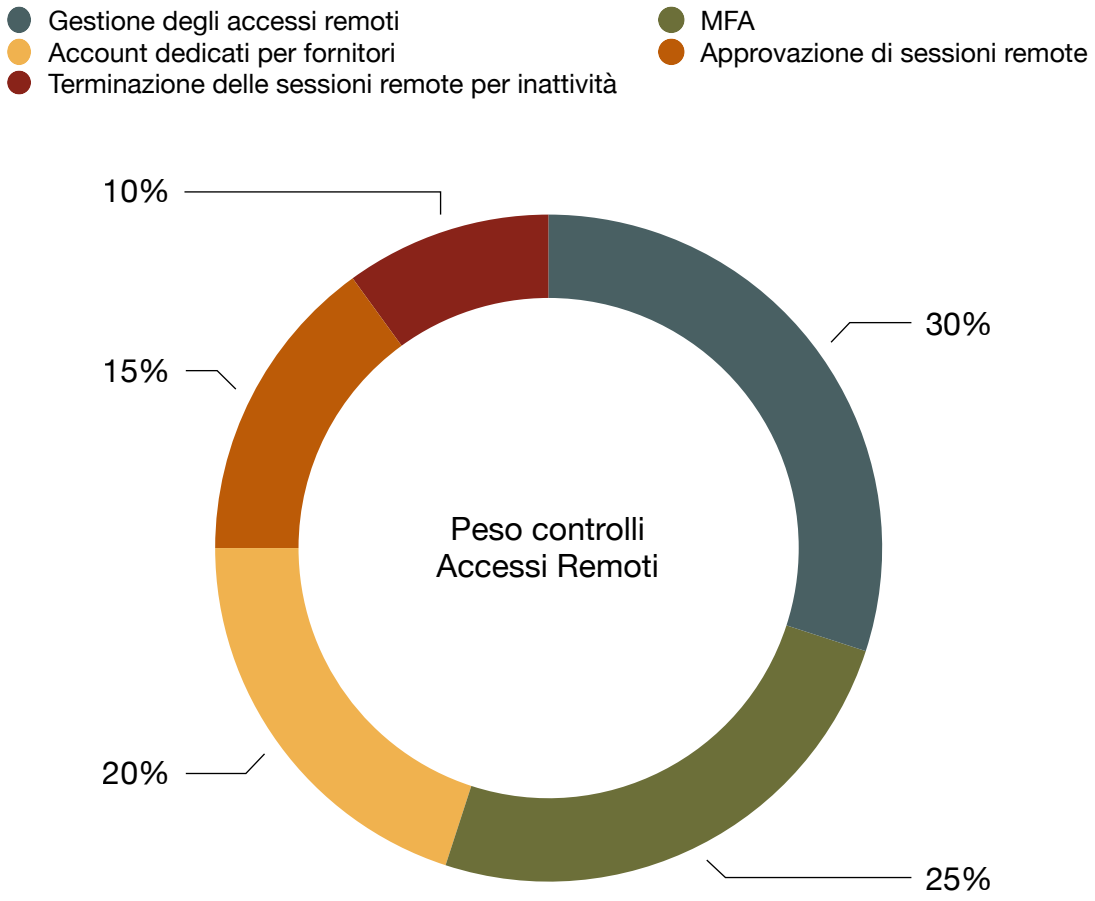
Accessi remoti

Gli accessi remoti allo stabilimento, spesso utilizzati dai manutentori, rappresentano una grande minaccia per la sicurezza, poiché possono dare ad utenti malevoli accesso diretto ai macchinare e dispositivi OT di basso livello, permettendogli di sabotare il processo di produzione. Gli accessi remoti devono quindi essere gestiti in maniera sicura attraverso la definizione di una Policy specifica, che ne dettagli modalità e procedure di esecuzione.

Tale Dominio prevede 5 controlli relativi a:

1. Gestione degli accessi remoti
2. MFA
3. Account dedicati per fornitori
4. Approvazione di sessioni remote
5. Terminazione delle sessioni remote per inattività

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Gestione degli accessi remoti

Gli accessi remoti devono essere gestiti in maniera sicura attraverso la definizione di una Policy specifica, che prevedano l'utilizzo di una connessione tramite VPN. Inoltre, le connessioni VPN dovrebbero "atterrare" su dei Server che fungono da Jump Host e che permettono poi di accedere tramite RDP solamente alla macchina/linea di produzione interessata.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Gli accessi remoti non utilizzano protocolli sicuri (VPN) e non prevedono l'utilizzo di Jump Host.
Razionale Implementato Ad-Hoc	Gli accessi remoti richiedono l'utilizzo di una VPN ma non prevedono l'utilizzo di Jump Host.
Razionale Implementato	Gli accessi remoti richiedono l'utilizzo di una VPN e prevedono l'utilizzo di Jump Host configurati in linea con Standard e Best Practice di settore.
Razionale Ottimizzato	Sono presenti meccanismi per il trasferimento sicuro di file tra host remoto e target (es. sandbox). Le operatzioni eseguite sono adeguatamente registrate (es. registrazione video). Le sessioni remote su asset critici sono monitorate e prontamente interrotte in caso di attività anomale.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.13	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

MFA

Per garantire un maggior livello di sicurezza, gli accessi remoti dovrebbero prevedere un meccanismo di autenticazione multifattoriale (MFA). Inoltre, è importante che il secondo/terzo fattore di autenticazione vengano trasmessi su un canale di comunicazione differente rispetto al fattore primario, come ad esempio:

- token fisico
- SMS
- Applicativo per smartphone
- Chiamata cellulare

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è revisto un meccanismo di MFA per gli accessi remoti.
Razionale Implementato Ad-Hoc	Il meccanismo di MFA è richiesto solo in fase di registrazione e/o invia il secondo fattore sullo stesso canale del primo.
Razionale Implementato	Il meccanismo di MFA viene richiesto in fase di registrazione e per ogni accesso. Il secondo fattore viene trasmesso su un canale differente (chiamata, app mobile, sms).

Razionale Ottimizzato	Vi è un meccanismo di Adaptive MFA.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.1 RE 2	The control system shall provide the capability to employ multifactor authentication for human user to access to the control system via an untrusted network

Account dedicati per fornitori

Come già osservato in precedenza, gli accessi remoti ai macchinare dello stabilimento vengono spesso utilizzati dai fornitori per eseguire attività di manutenzione e controllo periodico. E' opportuno che vengano create utenze nominali per ogni fornitore e non solamente utenze generiche per tutti i dipendenti dell'azienda terza parte.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti utenze dedicate alle terze parti.
Razionale Implementato Ad-Hoc	Sono presenti utenze generiche dedicate alle terze parti, che permettono l'accesso completo ai sistemi.
Razionale Implementato	Sono presenti utenze nominali dedicate alle terze parti, che permettono di accedere solo ai sistemi/aree necessarie tramite autenticazione MFA rivisti periodicamente.
Razionale Ottimizzato	Sono presenti utenze nominali dedicate alle terze parti, che permettono di accedere solo ai sistemi/aree necessarie. Vengono svolti Risk Assessment periodici su tali utenze e sui relativi permessi, al fine di identificare eventuali criticità.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
N/A	N/A

Approvazione di sessioni remote

Per garantire un ancor maggiore livello di sicurezza delle sessioni remote, dovrebbero essere necessaria un'esplicita approvazione interna (da parte, ad esempio, di un amministratore) per ogni sessione remota.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è necessaria un'approvazione interna per le sessioni remote.
Razionale Implementato Ad-Hoc	Per le sessioni remote è richiesta solo un'approvazione interna iniziale, durante la fase di creazione delle utenze.

Razionale Implementato	Per le sessioni remote è richiesta un'approvazione interna per ogni sessione.
Razionale Ottimizzato	Per le sessioni remote è richiesta una approvazione interna per ogni sessione tramite PAM.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.13 RE 1	The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role

Terminazione delle sessioni remote per inattività

Le sessioni remote dovrebbero essere terminate in maniera automatica dopo un determinato periodo di inattività dell'utente. Tale periodo di inattività deve ovviamente essere stabilito tenendo in considerazioni eventuali esigenze operative.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Le sessioni remote non vengono terminate in maniera automatica a seguito di un periodo di inattività.
Razionale Implementato Ad-Hoc	Le sessioni remote vengono terminate in maniera automatica dopo un periodo non linea con Standard e Best Practice di settore.
Razionale Implementato	Le sessioni remote vengono terminate in maniera automatica dopo un periodo di inattività implementato in linea con Standard e Best Practice di settore e/o esigenze operative e di Safety.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.5	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.

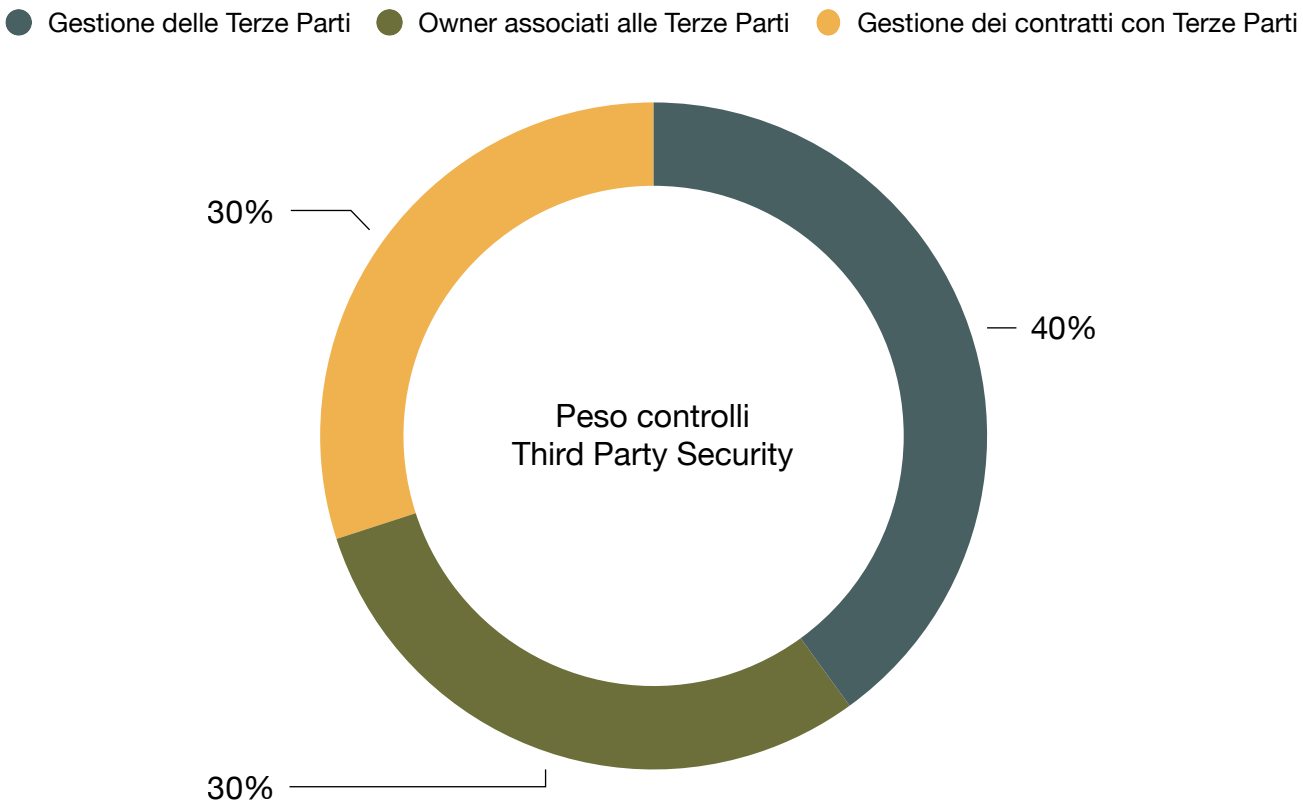
Third Party Security

Gli attacchi tramite *Supply Chain* sono largamente diffusi al giorno d'oggi. Ogni stabilimento può avere un elenco di fornitori IT e non IT nell'ordine di grandezza delle centinaia, se non migliaia. Considerando che, spesso, le Terze Parti hanno accessi privilegiati allo stabilimento, è evidente che la gestione della Third Party Security è fondamentale per evitare compromissioni.

Tale Dominio prevede 3 controlli relativi a:

1. Gestione delle Terze Parti
2. Owner associati alle Terze Parti
3. Gestione dei contratti con Terze Parti

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Gestione delle Terze Parti

Per gestire al meglio la sicurezza legata alle Terze Parti, dovrebbe essere mantenuta un lista accurata ed aggiornata contenente i principali fornitori/Terze Parti che offrono servizi e forniture OT al Plant (es. infrastrutture network, manutenzione, etc.), con le relative funzioni ed informazioni rilevanti.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente una lista dei fornitori/terze parti.
Razionale Implementato Ad-Hoc	È presente una lista approssimativa dei fornitori/terze parti suddivisa per cluster di appartenenza, non aggiornata e revisionata periodicamente.
Razionale Implementato	È presente una lista dettagliata ed accurata dei fornitori/terze parti divisa per cluster, aggiornata e revisionata periodicamente. Vengono richiesti dei Self Assessment in ambito IT/OT Cyber Security.
Razionale Ottimizzato	È presente una lista dettagliata ed accurata dei fornitori/terze parti divisa per cluster, aggiornata e revisionata periodicamente. Vengono richiesti dei Self Assessment in ambito IT/OT Cyber Security.

Il controllo si basa sul seguente *System Requirement* definito dal NIST CSF:

ID Riferimento NIST	Riferimento NIST
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Owner associati alle Terze Parti

Al fine di gestire al meglio la lista dei fornitori, dovrebbero essere associati degli owner interni all'azienda a ciascun fornitore con il ruolo di gestire le comunicazioni e/o monitorare eventuali SLA (Service Level Agreement) definiti.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono stati definiti degli owner da associare ai fornitori.
Razionale Implementato Ad-Hoc	È stato definito un unico owner associato a tutti i fornitori/terze parti.
Razionale Implementato	È definita una mappatura puntuale fra i fornitori/terze parti e i relativi owner associati.
Razionale Ottimizzato	È definita una mappatura puntuale fra i fornitori/terze parti e i relativi owner associati. Tale mappatura viene revisionata periodicamente. Vengono inoltre erogate attività di Awareness sull'importanza degli owner associati ai fornitori.

Il controllo si basa sul seguente *System Requirement* definito dal NIST CSF:

ID Riferimento NIST	Riferimento NIST
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's Cyber Security program and Cyber Supply Chain Risk Management Plan.

Gestione dei contratti con Terze Parti

In caso di nuove forniture, dovrebbero essere inseriti all'interno dei contratti delle clausole e/o requisiti in ambito IT/OT Cyber Security, in modo tale da ridurre la superficie di attacco rafforzando la sicurezza delle Terze Parti coinvolte.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	All'interno dei contratti non vengono inseriti requisiti di IT/OT Cyber Security.
Razionale Implementato Ad-Hoc	All'interno dei contratti sono stati inseriti requisiti minimi di IT/OT Cyber Security.
Razionale Implementato	All'interno dei contratti sono inseriti requisiti puntuali di IT/OT Cyber Security, ed è stato definito un workflow che prevede il coinvolgimento della Cyber Security per le nuove forniture.
Razionale Ottimizzato	I contratti vengono aggiornati in base alle nuove direttive nazionali ed internazionali (es. NIS2, PNSC)

Il controllo si basa sul seguente *System Requirement* definito dal NIST CSF:

ID Riferimento NIST	Riferimento NIST
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s Cyber Security program and Cyber Supply Chain Risk Management Plan.

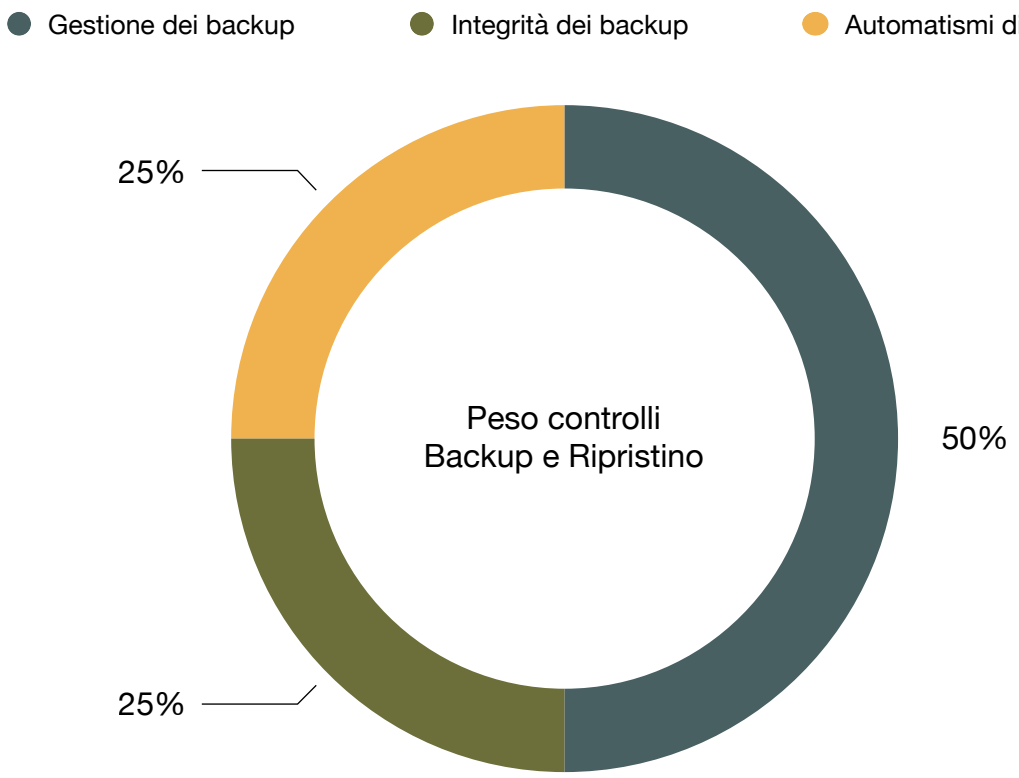
Backup e Ripristino

Così come per l'ambiente IT, l'esecuzione di attività di backup e restore all'interno dell'ambiente OT è fondamentale per garantire la resilienza e la continuità operativa degli impianti industriali. Gli ambienti OT gestiscono processi critici, e la perdita o la compromissione dei dati può avere conseguenze gravi, inclusi malfunzionamenti operativi, arresti della produzione e rischi di Safety. I backup regolari consentono di ripristinare rapidamente i sistemi in caso di incidenti, come attacchi informatici o guasti tecnici, riducendo i tempi di inattività e minimizzando l'impatto negativo sulle operazioni industriali e sulla sicurezza.

Tale Dominio prevede 3 controlli relativi a:

1. Gestione dei backup
2. Integrità dei backup
3. Automatismi di backup

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Gestione dei backup

Per gestire al meglio i backup, la definizione di una Backup Policy permette di definire formalmente:

- Quali sistemi sono sottoposti a backup

- Quali sono le tempistiche definite per il backup ed il restore completo
- Quante copie e dove vengono effettuati i backup (es. su supporti read-only)

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene effettuato alcun tipo di backup dei sistemi.
Razionale Implementato Ad-Hoc	Viene effettuato un backup sporadico e non completo di alcuni sistemi.
Razionale Implementato	Vengono effettuati backup completi e programmati di tutti i sistemi, con tempistiche definite in linea con RTO e RPO.
Razionale Ottimizzato	Vengono effettuati backup completi e programmati di tutti i sistemi, con tempistiche definite in linea con RTO e RPO. I backup vengono effettuati seguendo la regola "3-2-1" (3 copie, 2 supporti diversi, almeno 1 location geograficamente distante).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.3	The identity and location of critical files and the ability to conduct backup of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.

Integrità dei backup

Il processo di backup deve essere correttamente accompagnato dall'esecuzione di una serie di controlli (es. test sul restore) atti a verificare l'integrità dei backup effettuati.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene effettuato alcun tipo di test di integrità sui backup.
Razionale Implementato Ad-Hoc	Vengono effettuati test senza tempistiche prestabilite sull'integrità dei backup.
Razionale Implementato	Vengono effettuati test programmati e frequenti, supportati da una policy che regola le modalità e le tempistiche di esecuzione.
Razionale Ottimizzato	Vengono effettuati test programmati e frequenti in maniera automatica tramite tool dedicati. Tali test sono supportati da una policy che regola le modalità e le tempistiche di esecuzione.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.3 RE 1	The control system shall provide the capability to verify the reliability of backup mechanisms

Automatismi di backup

L’esecuzione di backup in modalità Ad-Hoc e manuale è altamente sconsigliata, in quanto può introdurre grossa confusione ed imprecisione nelle procedure. E’ invece consigliabile l'implementazione di automatismi implementati in ambito Backup & Restore (es. esecuzione automatica dei backup, test automatici dell'integrità, restore automatico, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I backup non sono automatizzati.
Razionale Implementato Ad-Hoc	La maggioranza dei backup sono automatizzati.
Razionale Implementato	Tutti i backup sono automatizzati e ne viene verificata l'integrità.
Razionale Ottimizzato	Tutti i backup sono automatizzati, inoltre ne viene verificata l'integrità e il restore.

Il controllo si basa sul seguente *System Requirement* definito dall’IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.3 RE 2	The control system shall provide the capability to automate the backup function based on a configurable frequency.

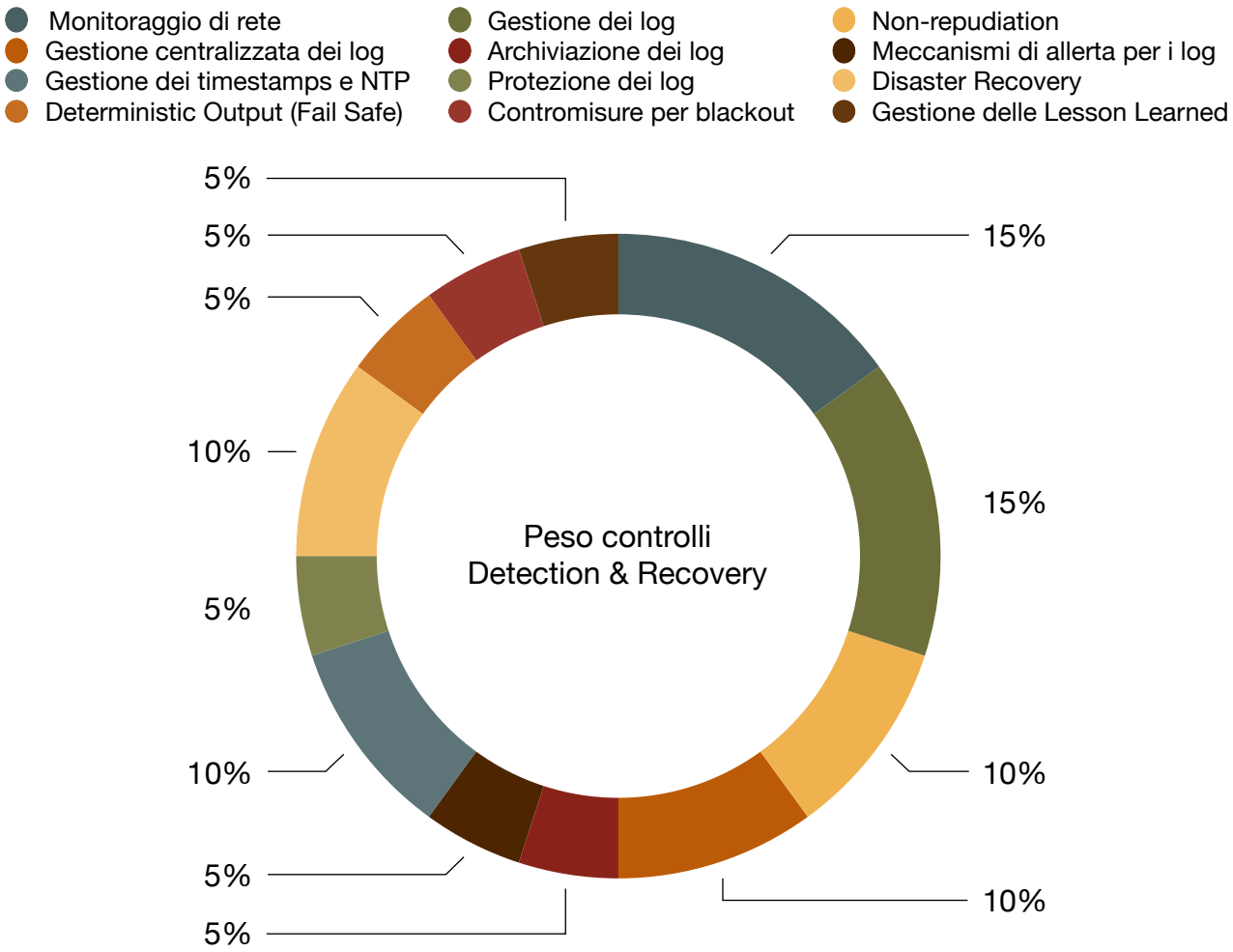
Detection e Recovery

L’analisi del traffico di rete e delle varie tipologie di log generate dai sistemi OT è fondamentale per effettuare al meglio la Detection di incidenti ed attacchi informatici. Ovviamente, il rilevamento di un attacco deve essere accompagnato da un piano strutturato di Disaster Recovery che permetta, ove possibile, la continuità operativa ed il tempestivo ripristino dei sistemi compromessi.

Tale Dominio prevede 12 controlli relativi a:

1. Monitoraggio di rete
2. Gestione dei log
3. Non-repudiation
4. Gestione centralizzata dei log
5. Archiviazione dei log
6. Meccanismi di allerta per i log
7. Gestione dei timestamps e NTP
8. Protezione dei log
9. Disaster Recovery
10. Deterministic Output (Fail Safe)
11. Contromisure per blackout
12. Gestione delle Lesson Learned

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Monitoraggio di rete

Il traffico di rete OT è il *backbone* fondamentale al fine di garantire l'operatività dell'impianto. Per tale motivo, tutto il traffico di rete dovrebbe essere raccolto ed analizzato tramite una soluzione specifica di Deep Packet Inspection (es. Claroty, Nozomi, Defender for IoT), al fine di individuare potenziali incidenti o traffico sospetto. Solitamente, tali soluzioni prevedono una serie di sonde, collegate agli switch di rete OT, che eseguono il *mirroring* del traffico e lo trasmettono ad un *collector* centralizzato (*on-premise* o in Cloud) al fine di eseguire analisi del traffico.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Il traffico di rete non è monitorato.
Razionale Implementato Ad-Hoc	Il traffico di rete viene analizzato attraverso soluzioni generiche (es. tool open source come Snort, Suricata, Zeek, Security Onion, etc.)
Razionale Implementato	Il traffico di rete viene analizzato attraverso soluzioni dedicate in ambito OT (es. Nozomi, Claroty, etc.) e gli alert sono constantemente monitorati.

Razionale Ottimizzato	Il traffico di rete viene analizzato attraverso soluzioni dedicate per l'analisi di traffico OT (es. Nozomi, Claroty, etc.) e gli alert vengono gestiti da personale con know-how in ambito OT.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 6.2	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

Gestione dei log

I log generati dai sistemi OT sono il secondo elemento chiave per il processo di Detection. Attraverso l'analisi dei log è infatti possibile determinare la *timeline* di un attacco o incidente e risalire al dispositivo sorgente. Di conseguenza, la raccolta dei log è fondamentale e dovrebbe essere dettagliata in una log Policy che preveda:

- Quali sistemi sono sottoposti a raccolta dei log
- Quali tipologie di log vengono raccolti (es. di sistema, di produzione, applicativi, etc.)
- Vengono raccolti log in ambito security (es. tentativi di accesso falliti, eventi del sistema di controllo, cambi alle configurazioni, operazioni degli amministratori, etc.)
- Dove vengono salvati i log

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene effettuata una raccolta dei log.
Razionale Implementato Ad-Hoc	Vengono raccolti i log previsti di default previsti dai sistemi OT (es. log default Windows, log default PLC, etc.).
Razionale Implementato	Vengono raccolti log applicativi e di sistema con configurazioni in linea con Standard e Best Practice di Settore.
Razionale Ottimizzato	Vengono raccolti log applicativi e di sistema, inclusi log in ambito security, con configurazioni in linea con Standard e Best Practice di Settore.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.8	The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

Non-repudiation

Con il termine *non-repudiation* si intende la capacità di identificare univocamente il responsabile di un azione e garantire che tale utente/dispositivo non possa successivamente negare di aver partecipato o di aver effettuato la specifica azione. All'interno dei sistemi OT, la *non-repudiation* è ottenibile attraverso tre componenti chiave:

- Raccolta di varie tipologie di log
- Utilizzo di utenze nominali
- Sincronizzazione dei *clock* dei dispositivi

Sfruttando la combinazione di questi elementi, è possibile risalire in maniera univoca al dispositivo e/o utente responsabile di una certa operazione.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi OT non sono in alcun modo in grado di tracciare le operazioni effettuate dagli utenti.
Razionale Implementato Ad-Hoc	I log di sistema vengono raccolti, ma l'utilizzo di utenze generiche in ambito OT non permette di tracciare accuratamente le azioni compiute dagli utenti.
Razionale Implementato	I log di sistema ed applicativi vengono raccolti e l'utilizzo di utenze nominali in ambito OT permette di tracciare accuratamente le azioni compiute dagli utenti.
Razionale Ottimizzato	I log di sistema ed applicativi vengono raccolti e l'utilizzo di utenze nominali in ambito OT permette di tracciare accuratamente le azioni compiute dagli utenti.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.12	The control system shall provide the capability to determine whether a given human user took a particular action

Gestione centralizzata dei log

La grossa mole di log generati dai sistemi OT, può rendere difficile, se non impossibile, l'analisi manuale al fine di identificare eventuali segnali di allarme. Di conseguenza, un SIEM dovrebbe essere utilizzato per la raccolta ed analisi centralizzata dei log. Idealmente, il SIEM dovrebbe essere presidiato da personale con *know-how* in ambito OT Security ed in grado, quindi, di identificare eventuali minacce.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I log non vengono raccolti e analizzati in maniera centralizzata.
Razionale Implementato Ad-Hoc	I log provenienti da alcune sorgenti (es. Server, workstation a dominio, etc.) vengono raccolti ed analizzati in maniera centralizzata (es. tramite SIEM).

Razionale Implementato	I log provenienti da tutti i dispositivi OT (es. PLC, HMI, SCADA, Eng. Workstation, etc.) vengono raccolti ed analizzati in maniera centralizzata (es. tramite SIEM).
Razionale Ottimizzato	I log provenienti da tutte le sorgenti, incluse quelle OT, vengono raccolti ed analizzati in maniera centralizzata (es. tramite SIEM) da personale con know-how in ambito OT Security.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.8 RE 1	The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a systemwide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management(SIEM)

Archiviazione dei log

In caso di raccolta centralizzata dei log, dovrebbe essere dedicato loro sufficiente spazio di archiviazione, stabilito tramite un'opportuna analisi. Per evitare la saturazione di tale spazio di archiviazione, possono essere introdotti meccanismi di *log retention* per la sovrascrittura periodica dei log.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono state fatte analisi sullo spazio di archiviazione dedicato ai log.
Razionale Implementato Ad-Hoc	Sono state fatte analisi generiche ed approssimative sullo spazio di archiviazione dedicato ai log.
Razionale Implementato	Lo spazio di archiviazione dedicato ai log è stato definito tramite analisi puntuale.
Razionale Ottimizzato	Lo spazio di archiviazione dedicato ai log è stato definito tramite analisi puntuale. È stato definito un periodo di rotazione dei log per evitare la saturazione dello spazio di archiviazione. Su base periodica viene effettuata una review dello spazio di archiviazione dedicato ai log.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.9	The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

Meccanismi di allerta per i log

Idealmente, dovrebbero essere predisposti meccanismi di allarme per segnalare un problema al processo di logging (es. saturazione dello spazio, interruzione della raccolta dei log, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono stati predisposti meccanismi di allarme.
Razionale Implementato Ad-Hoc	Vi sono meccanismi base per notificare problemi di spazio al processo di logging.
Razionale Implementato	Sono stati predisposti meccanismi di allarme avanzati per notificare in merito a problemi di spazio e perdita delle sorgenti dei log.
Razionale Ottimizzato	Tali meccanismi vengono periodicamente testati e verificati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.10	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

Gestione dei timestamps e NTP

La presenza di un timestamp è fondamentale all'interno dei log. Come già citato in precedenza, la sincronizzazione dei clock di sistema è fondamentale per permettere la *non-repudiation.* Ciò può essere ottenuto attraverso l'utilizzo di un server Network Time Protocol (es. Inrim).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un timestamp all'interno dei log, oppure non è stato configurato tramite server NTP.
Razionale Implementato Ad-Hoc	È presente un timestamp all'interno dei log con clock interno alla macchina.
Razionale Implementato	È presente un timestamp all'interno dei log ed è stato configurato tramite NTP centralizzato.
Razionale Ottimizzato	È presente un timestamp all'interno dei log ed è stato configurato tramite NTP centralizzato.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.11	The control system shall provide timestamps for use in audit record generation.

Protezione dei log

I file di log dovrebbero essere adeguatamente protetti da accessi non autorizzati, modifiche o eliminazione, attraverso l'accesso *read-only* e la loro cifratura.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Il file di log è accessibile e modificabile senza restrizione.
Razionale Implementato Ad-Hoc	I file di log sono accessibili in modalità read-only, ma non sono protetti da accessi non autorizzati.
Razionale Implementato	I file di log sono accessibili solo in modalità read-only, sono cifrati e sono protetti da accessi non autorizzati.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.9	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.

Disaster Recovery

In un contesto in cui l'operatività è fondamentale, un'infrastruttura di Disaster Recovery (DR) permette di garantire la continuità operativa all'interno dello stabilimento. Nel caso ciò non sia realizzabile, è comunque opportuno definire un piano di Disaster Recovery che preveda ruoli e procedure di ripristino chiare da seguire in caso di incidente.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un'infrastruttura di Disaster Recovery.
Razionale Implementato Ad-Hoc	È presente un'infrastruttura di Disaster Recovery.
Razionale Implementato	È presente un'infrastruttura avanzata di Disaster Recovery con failover automatizzato, supportato da policy dedicate ed un Disaster Recovery in cui vengono definiti RPO ed RTO, definito a seguito di un'attività di BIA.
Razionale Ottimizzato	È presente un'infrastruttura avanzata di Disaster Recovery con failover automatizzato, supportato da policy dedicate ed un Disaster Recovery in cui vengono definiti RPO ed RTO, definito a seguito di un'attività di BIA. L'infrastruttura di DR viene definita secondo il modello IaC (Infrastructure as a Code).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.4	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

Deterministic Output (Fail Safe)

Per questioni di Safety, i sistemi OT dovrebbero essere in grado di impostare uno stato sicuro (deterministico) a seguito di malfunzionamenti, attacchi informatici o altre cause che impattino la normale operatività del sistema.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi non sono in grado di impostare uno stato sicuro a seguito di un disastro.
Razionale Implementato Ad-Hoc	Solo i sistemi più critici sono in grado di impostare uno stato sicuro.
Razionale Implementato	I sistemi sono in grado di impostare uno stato sicuro a seguito di un disastro.
Razionale Ottimizzato	I sistemi vengono periodicamente testati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.6	The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.

Contromisure per blackout

Un'altro meccanismo di Disaster Recovery prevede l'utilizzo di misure per contrastare blackout o cali di tensione (es. tramite UPS, gruppi elettrogeni, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti misure per contrastare cali di corrente e/o blackout.
Razionale Implementato Ad-Hoc	Sono presenti UPS per permettere ai sistemi di impostare uno stato sicuro e avviare la procedura di shutdown a seguito di cali di corrente.
Razionale Implementato	È presente un'infrastruttura composta da UPS e gruppi elettrogeni collocati in-line per prevenire cali di corrente e balckout prolungati.
Razionale Ottimizzato	È presente un'infrastruttura composta da UPS e gruppi elettrogeni collocati in-line per prevenire cali di corrente e blackout prolungati. Sono presenti sistemi di monitoraggio della qualità e continuità della corrente, protezione da sovratensioni, isolatori di linea, sistemi di raffreddamento d'emergenza e ridondanza nella distribuzione elettrica. Vengono effetuati test per verificare l'efficacia dei sistemi installati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.5	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.

Gestione delle Lesson Learned

Nonostante il ripristino dell'operatività resti la priorità, al termine di eventuali incidenti di sicurezza è importare che sia stato definito un processo di *follow-up* al fine di individuare le *lesson-learned* dall'incidente e ridurre la probabilità futura di accadimento di incidenti analoghi.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è stato definito un processo per l'identificazione di "lesson learned" a seguito di un incidente.
Razionale Implementato Ad-Hoc	Vengono effettuate delle attività generiche di post-incident.
Razionale Implementato	È stato definito un processo per l'identificazione di "lesson learned" a seguito di un incidente che prevede la relazione e condivisione di un report post incident.
Razionale Ottimizzato	È stato definito un processo per l'identificazione di "lesson learned" a seguito di un incidente che prevede la relazione e condivisione di un report post incident che include KPI e KRI.

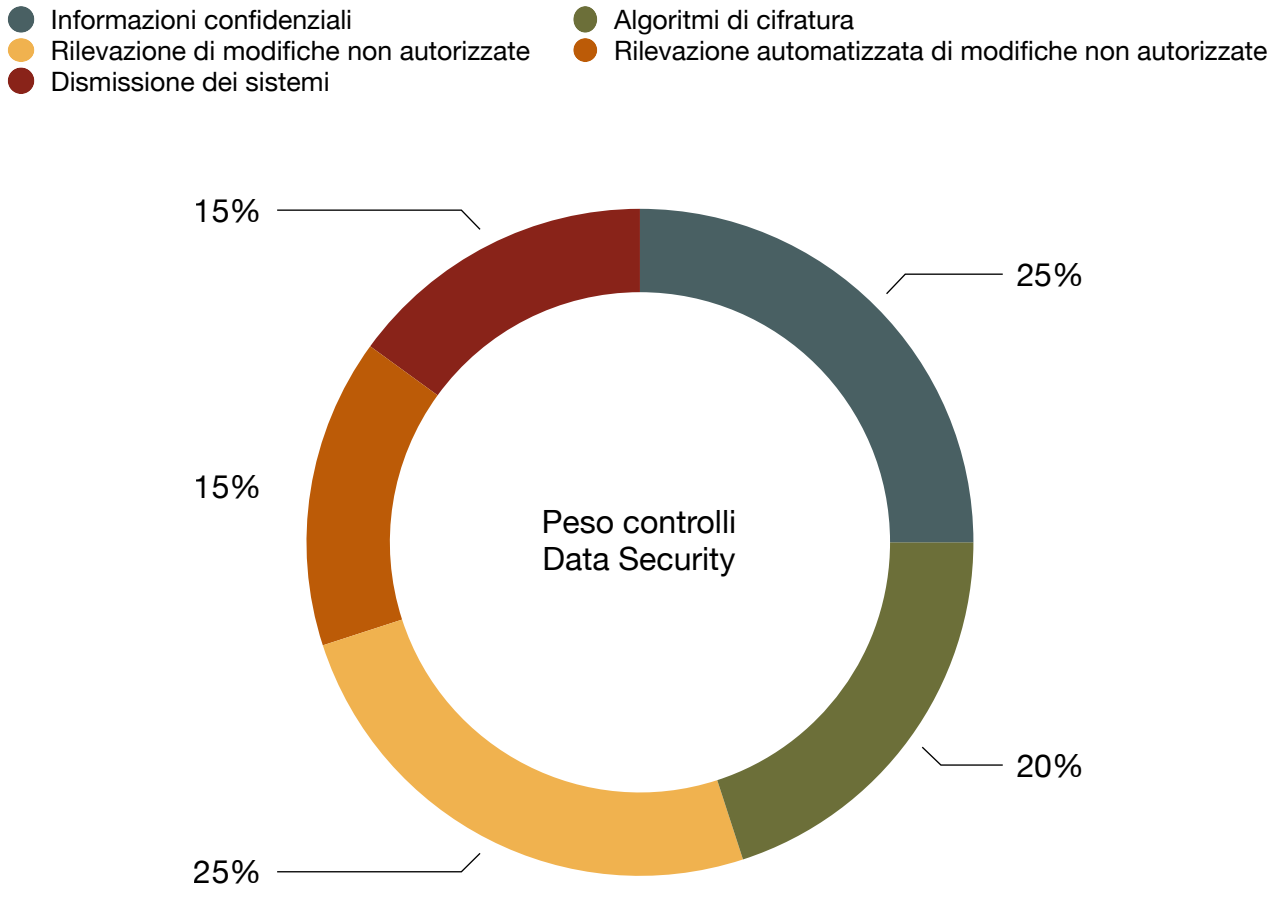
Data Security

Nonostante l'ambiente OT sia incentrato sulla produzione di beni e sull'erogazione di servizi, la protezione del dato resta comunque una tematiche rilevante.

Tale Dominio prevede 5 controlli relativi a:

1. Informazioni confidenziali
2. Algoritmi di cifratura
3. Rilevazione di modifiche non autorizzate
4. Rilevazione automatizzata di modifiche non autorizzate
5. Dismissione dei sistemi

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Informazioni confidenziali

Il primo passo per la protezione dei dati all'interno dei sistemi OT è l'identificazione di eventuali informazioni confidenziali che debbano essere protette. Tali informazioni possono includere, ad esempio:

- Dati di produzione
- Ricette, valori di variabili di produzione ed altre IP
- Credenziali di accesso nei sistemi

Le informazioni sensibili all'interno dei sistemi devono essere identificate attraverso una Policy specifica e possono essere protette attraverso soluzioni di Data Loss Prevention che permettano di catalogare, monitorare e prevenire la perdita di tali dati.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un processo per classificare le informazioni all'interno dei sistemi OT.
Razionale Implementato Ad-Hoc	Esiste un processo implementato ad-hoc eseguito caso per caso.
Razionale Implementato	Le eventuali informazioni confidenziali sono identificate e protette attraverso un processo strutturato e definito da policy.
Razionale Ottimizzato	E' stata adottata una soluzione di DLP. Inoltre vengono effettuate delle review periodiche sulla tipologia dei dati trattati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 4.1	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit

Algoritmi di cifratura

Una volta identificate, le informazioni possono essere protette attraverso l'utilizzo di algoritmi di cifratura comunemente riconosciuti come sicuri (es. AES 256, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vengono utilizzati algoritmi di cifratura per proteggere le informazioni confidenziali.
Razionale Implementato Ad-Hoc	Una parte delle informazioni confidenziali sono protette tramite algoritmi di cifratura deboli (es. chiave <256 bit).
Razionale Implementato	Tutte le informazioni confidenziali sono protette tramite algoritmi di cifratura robusti.
Razionale Ottimizzato	Viene effettuata una review degli algoritimi di cifratura utilizzati al fine di sostituire quelli che risultano deprecati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 4.3	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.

Rilevazione di modifiche non autorizzate

Per meglio proteggere le informazioni all'interno dei sistemi OT possono essere utilizzati dei meccanismi che permettono di rilevare modifiche non autorizzate alle informazioni at-rest ed al software (es. attraverso hash/checksum).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti meccanismi che permettono di rilevare modifiche non autorizzate alle informazioni at-rest ed al software.
Razionale Implementato Ad-Hoc	Vengono utilizzati meccanismi che permettono di rilevare modifiche non autorizzate alle informazioni at-rest ed al software.
Razionale Implementato	Vengono utilizzati meccanismi che permettono di rilevare e notificare modifiche non autorizzate alle informazioni at-rest ed al software.
Razionale Ottimizzato	Vengono utilizzati meccanismi che permettono di rilevare, notificare e proteggere le informazioni at-rest ed il software da modifiche non autorizzate.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.4	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

Rilevazione automatizzata di modifiche non autorizzate

Se sono presenti meccanismi di rilevamento di modifiche apportate alle informazioni ed al software, tali meccanismi dovrebbero essere automatizzati e dovrebbero essere in grado di notificare le modifiche rilevate (es. cambi alle configurazioni dei PLC, modifica di valori limite/ setpoint, etc.).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I meccanismi di rilevamento di modifiche apportate alle informazioni non sono automatizzati.
Razionale Implementato Ad-Hoc	I meccanismi di rilevamento di modifiche apportate alle informazioni sono automatizzati.
Razionale Implementato	I meccanismi di rilevamento di modifiche apportate alle informazioni sono automatizzati e sono in grado di notificare le modifiche rilevate.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.4 RE 1	The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification

Dismissione dei sistemi

Le informazioni dovrebbero essere protette durante tutto il loro ciclo di vita. Ciò include anche la loro rimozione sicura in fase di dismissione dei sistemi. La dismissione dei sistemi deve essere dettagliata attraverso una procedura specifica, che preveda le modalità di rimozione sicura delle delle informazione, come ad esempio:

- formattazione multipla dei supporti di memoria
- Distruzione fisica dei supporti di memoria
- *Degaussing* (demagnetizzazione) dei supporti di memoria

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Le informazioni non vengono eliminate in maniera sicura dai supporti di memoria in fase di decommissioning.
Razionale Implementato Ad-Hoc	In fase di decommissioning le informazioni vengono eliminate con metodi standard (es. formattazione semplice dei drive).
Razionale Implementato	In fase di decommissioning le informazioni vengono eliminate in maniera sicura (es. formattazione multipla, distruzione fisica dei drive, demagnetizzazione, etc.).
Razionale Ottimizzato	Verifica della effettiva rimozione delle informazioni in maniera irrecuperabile dai supporti dismessi.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 4.2	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.

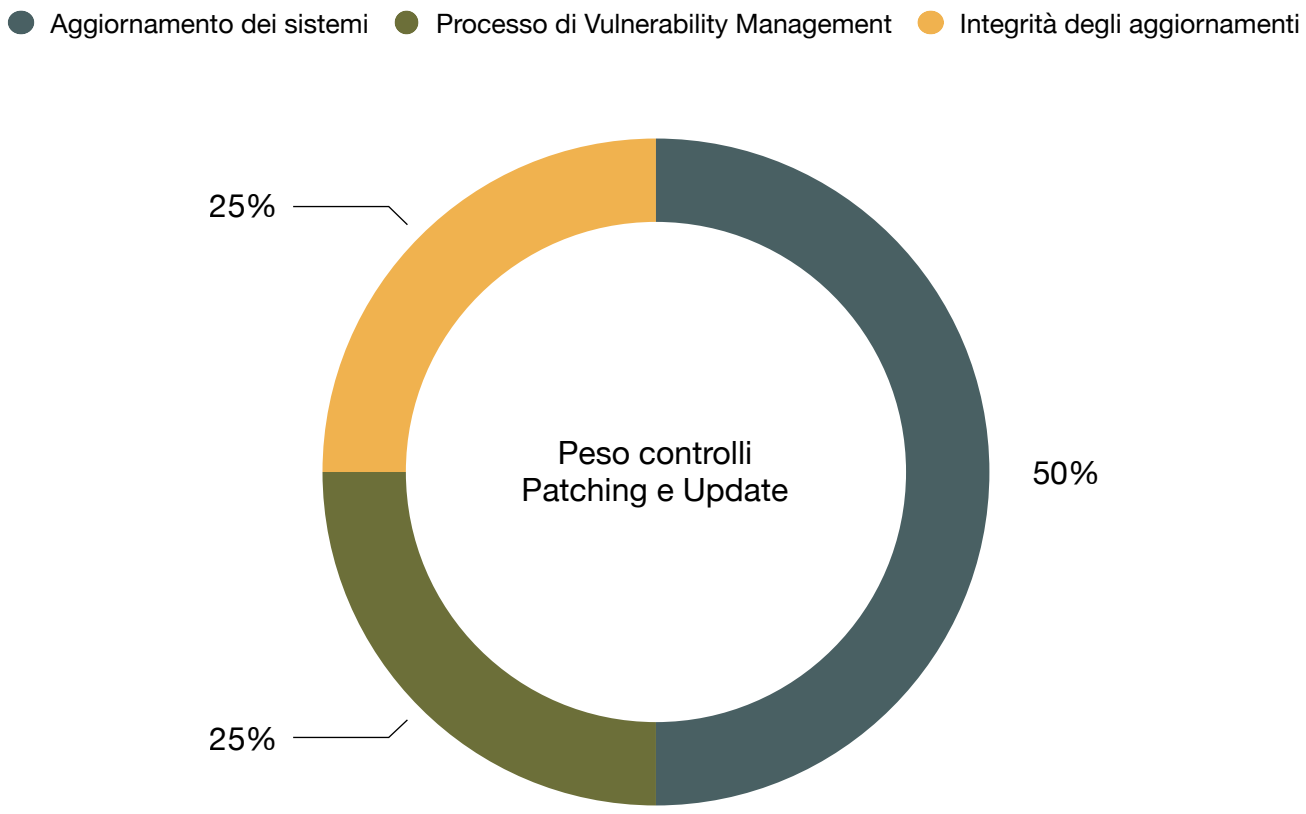
Patching e Update

Il tema del Patching e Update è particolarmente delicato quando ci si sposta dall'ambiente IT più tradizionale a quello OT. Mantenere i dispositivi *up-to-date* non è più infatti una priorità per i sistemi. Ciò che si cerca di ottenere è invece il mantenimento di una versione del software stabile e che non provochi incompatibilità con i numerosi sistemi *Legacy* presenti all'interno dello stabilimento. Proprio relativamente a questi dispositivi *Legacy,* l'impossibilità di ottenere nuove versioni di sistema, con le relative patch, introduce grandi vulnerabilità di sicurezza. Negli stabilimenti non è infatti raro trovare versioni di software e sistemi operativi considerati in *End of Life*(EoL), o addirittura *End of Support*(EoS).

Tale Dominio prevede 3 controlli relativi a:

1. Aggiornamento dei sistemi
2. Processo di Vulnerability Management
3. Integrità degli aggiornamenti

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Aggiornamento dei sistemi

Come già detto in precedenza, la procedura di aggiornamento dei sistemi OT è particolarmente sensibile, e deve prevedere il continuo monitoraggio dei siti dei produttori del software, al fine di verificare che le nuove release non creino incompatibilità con i sistemi OT presenti nello stabilimento.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi OT non vengono aggiornati.
Razionale Implementato Ad-Hoc	I sistemi OT vengono sporadicamente aggiornati e non vi è un processo che definisce il processo di selezione e distribuzione degli aggiornamenti.
Razionale Implementato	I sistemi OT vengono frequentemente aggiornati automaticamente.
Razionale Ottimizzato	I siti dei produttori vengono costantemente monitorati per tracciare la disponibilità di nuove patch. È presente un sistema centralizzato di Patch Management.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.5	Host devices shall support the ability to be updated and upgraded.

Processo di Vulnerability Management

Per gestire al meglio le vulnerabilità di sicurezza dovrebbe essere introdotto una processo di Vulnerability e Patch Management che preveda:

- Continuo monitoraggio ed identificazione delle vulnerabilità
- Analisi e prioritizzazione delle vulnerabilità
- Definizione ed implementazione di Patch correttive per risolvere le vulnerabilità identificate

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Le vulnerabilità non vengono identificate e gestite.
Razionale Implementato Ad-Hoc	Le vulnerabilità vengono identificate saltuariamente e non è presente un processo strutturato di Vulnerability Management.
Razionale Implementato	Le vulnerabilità identificate vengono gestite attraverso un processo strutturato di Vulnerability Management.
Razionale Ottimizzato	Le vulnerabilità identificate vengono gestite attraverso un processo strutturato di Vulnerability Management. Il processo viene rivisto su base annuale e/o in base a modifiche rilevanti all'interno dell'ambiente OT.

Il controllo si basa su di un controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.12.6	Gestione delle vulnerabilità tecniche

Integrità degli aggiornamenti

Prima di effettuare un update, è opportuno che venga verificata l'autenticità ed integrità dell'aggiornamento (es. attraverso la verifica tramite hash/checksum).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Prima di verificare un update non ne viene verificata l'autenticità ed integrità.
Razionale Implementato Ad-Hoc	L'autenticità e integrità degli aggiornamenti viene verificata manualmente prima dell'installazione.
Razionale Implementato	L'autenticità e integrità degli aggiornamenti viene verificata automaticamente prima dell'installazione.
Razionale Ottimizzato	Gli aggiornamenti vengono installati su ambienti di test dedicati per identificare eventuali problemi di compatibilità, performance e/o security.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.5 RE 1	Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation

Asset Inventory & Device Hardening

Con il termine Asset, viene fatto riferimento a:

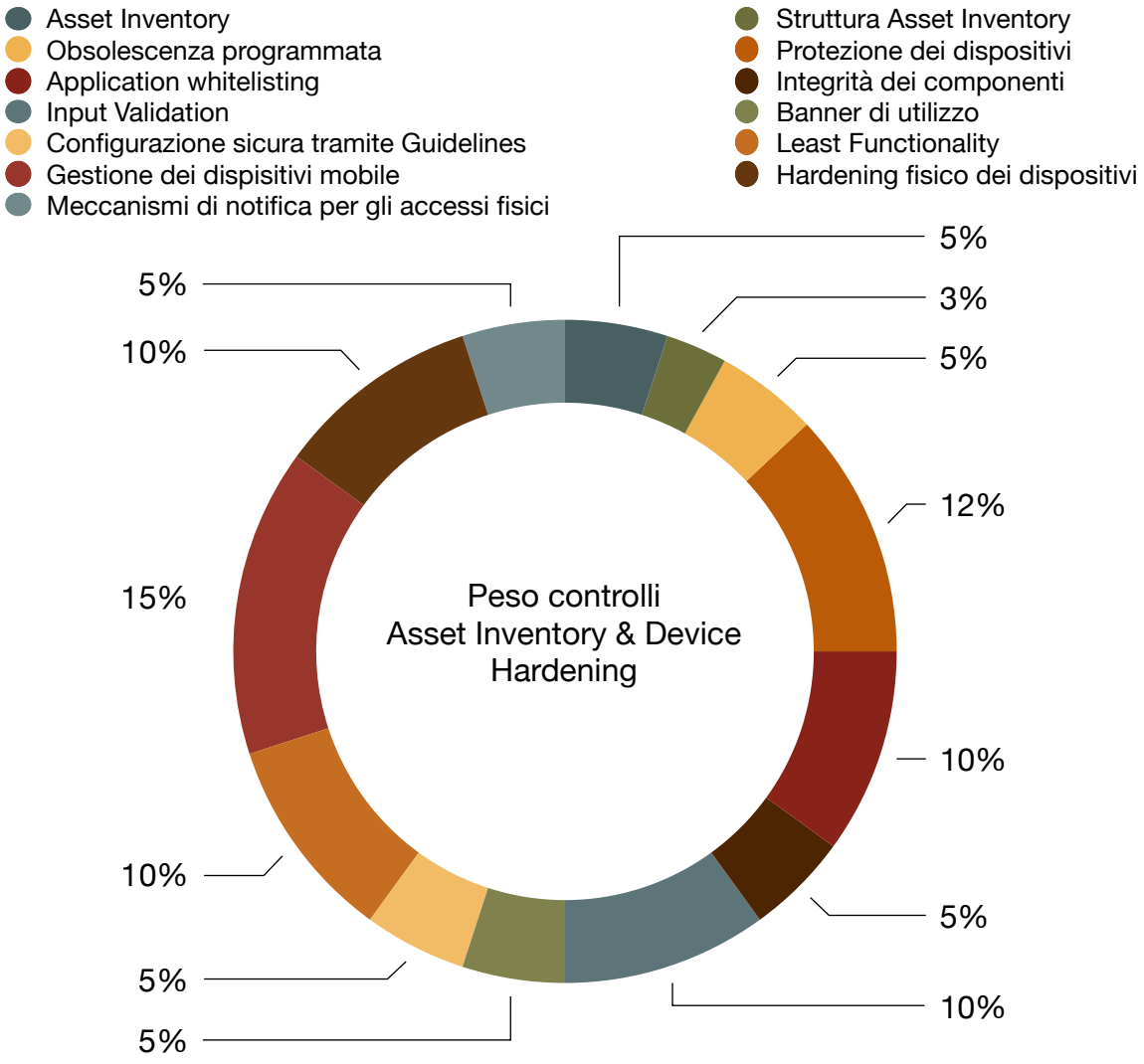
- Dispositivi Hardware (es. Workstation, PLC, etc.)
- Macchine Virtuali
- Software

Uno stabilimento industriale può contenere un numero di Asset quantificabile nell'ordine di grandezza delle migliaia o decine di migliaia. Risulta quindi evidente che la corretta gestione di tali Asset sia fondamentale in termini di sicurezza, sia da un punto di vista di inventario, sia a un punto di vista di *hardening* sia logico che fisico.

Tale Dominio prevede 13 controlli relativi a:

1. Asset Inventory
2. Struttura Asset Inventory
3. Obsolescenza programmata
4. Protezione dei dispositivi
5. Application whitelisting
6. Integrità dei componenti
7. Input Validation
8. Banner di utilizzo
9. Configurazione sicura tramite Guidelines
10. Least Functionality
11. Gestione dei dispositivi mobile
12. Hardening fisico dei dispositivi
13. Meccanismi di notifica per gli accessi fisici

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Asset Inventory

Un Asset Inventory sia dei dispositivi/componenti (Hardware) sia dei programmi installati (Software) e dei relativi flussi di comunicazione sul sistema permette di tenere traccia di tutti gli Asset posseduti dallo stabilimento. La definizione dell'Asset Inventory può essere eseguita manualmente, anche se, data la grande mole di Asset, è più consigliato l'utilizzo di soluzioni automatizzate.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente alcun tipo di Asset Inventory.
Razionale Implementato Ad-Hoc	È presente un Asset Inventory aggiornato manualmente contenente le informazioni essenziali dei dispositivi.
Razionale Implementato	È presente un Asset Inventory completo di tutti i dispositivi (inclusi eventuali Software installati, flussi di comunicazione e ownership) aggiornato automaticamente.
Razionale Ottimizzato	L'Asset Inventory viene aggiornato anche sulla base di soluzioni dedicate al monitoraggio del traffico OT (es. Nozomi, Claroty, etc.)

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.8	The control system shall provide the capability to report the current list of installed components and their associated properties.

Struttura Asset Inventory

Gli standard e Best Practice (ISA/IEC 62443) suggeriscono di definire i seguenti campi all'interno dell'Asset Inventory:

- Per i dispositivi hardware (es. PLC, HMI, Eng. Workstation, SCADA, etc.): Nome del dispositivo o sistema; Asset ID; Tipologia di dispositivo; Funzione; Network interface(s); Network address(es); Serial Number; Sistema operativo e versione (se applicabile); Versione del firmware (se applicabile); Locazione del dispositivo.
- Per le macchine virtuali: Nome della VM; Tipologia di VM; Funzione; Network interface(s); Network address(es); Nome/ID dell'Host; Tipologia dell'Host; Sistema operativo e versione; Responsabile/i della VM; Admin; Note.
- Per i software utilizzati: Nome del Software; Tipologia del Software (es. OS, applicativo, database, firmware, etc.); Funzione; Nome dell'Host; Tipologia dell'Host (physical or virtual, server or workstation, network device, controller, etc.); Vendor; Versione; Responsabile/i del software; Informazioni di Licenza (es. # di Licenza, Scadenza della Licenza); Processo di Update/Patch.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente alcun tipo di Asset Inventory.
Razionale Implementato Ad-Hoc	Alcuni campi generici (es. prodotto, brand, modello, linea, etc.)
Razionale Implementato	Sono tracciati tutti i campi specificati da Standard e Best Practice di settore.
Razionale Ottimizzato	Tutti i campi sono aggiornati automaticamente.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.8	The control system shall provide the capability to report the current list of installed components and their associated properties.

Obsolescenza programmata

Oltre che per motivazioni di Cyber Security, l'Asset Inventory permette anche di indirizzare tematiche di obsolescenza programmata, tenendo traccia del ciclo di vita dell'Asset e delle eventuali date di *End of Life* ed *End of Support.*

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Nessuna attività in ambito di obsolescenza programmata.
Razionale Implementato Ad-Hoc	Esecuzione di attività di planning in ambito di obsolescenza programmata in maniera non strutturata.
Razionale Implementato	E' presente un processo strutturato che disciplina le attività in ambito di obsolescenza programmata.
Razionale Ottimizzato	Sono presenti tool automatici di previsione a supporto delle attività.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.8	The control system shall provide the capability to report the current list of installed components and their associated properties.

Protezione dei dispositivi

Relativamente *all' hardening* dei dispositivi, l'utilizzo, ove possibile, di una soluzione di Antivirus o EDR permette di rafforzare la *Security posture overall* delle workstation, attraverso l'introduzione di determinati meccanismi di identificazione e protezione dalle minacce.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti meccanismi di protezione quali EDR ed Antivirus.
Razionale Implementato Ad-Hoc	Sono implementati meccanismi di protezione quali EDR ed Antivirus solo su parte dei dispositivi che ne supportano l'esecuzione.
Razionale Implementato	Sono implementati meccanismi di protezione quali EDR ed Antivirus su tutti i dispositivi che ne supportano l'esecuzione. Tali soluzioni sono configurate in linea con Standard e Best Practice di settore e in modo da non impattare sull'operatività della macchina.
Razionale Ottimizzato	Sono state implementate funzionalità avanzate (es. analisi comportamentale dei processi) oltre all'analisi delle firme.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.2	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms

Application whitelisting

Relativamente all'utilizzo di una soluzione di Antivirus/EDR, dovrebbero essere definite delle liste (es. whitelisting, blacklist, etc.) per limitare l'esecuzione di applicativi sui sistemi OT.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Nessuna limitazione in merito agli applicativi eseguibili sui sistemi OT.
Razionale Implementato Ad-Hoc	Definizione di una blacklist contenente gli applicativi che non possono essere installati sui sistemi OT.
Razionale Implementato	Definizione di una whitelist contenente gli unici applicativi che possono essere installati sui sistemi OT.
Razionale Ottimizzato	La whitelist è costantemente aggiornata per consentire la sola installazione delle ultime release.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.2	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms

Integrità dei componenti

L'integrità dei componenti dovrebbe essere verificata prima dell'avvio del sistema operativo, ad esempio attraverso l'utilizzo di Secure Boot.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non viene verificata l'integrità dei componenti.
Razionale Implementato Ad-Hoc	Attività di verifica delle componenti eseguite con logiche di default.
Razionale Implementato	Viene verificata l'integrità dei componenti prima dell'avvio del sistema operativo (es. uso del Secure Boot).
Razionale Ottimizzato	Viene verificata l'integrità dei componenti prima dell'avvio del sistema operativo attraverso la verifica delle Root of Trust per verificare l'autenticità di firmware, software e configurazioni necessarie all'avvio.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.9	Host devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

Input Validation

L'operatività dei sistemi OT si basa sull'inserimento da parte dell'operatore di parametri di produzione all'interno dei sistemi OT. Per evitare rischi di compromissione dell'operatività e di Safety, dovrebbero essere eseguiti controlli sugli input inseriti nei sistemi OT (input validation), tenendo conto, ad esempio, di:

- Range sicuro di valori
- Sintassi errata degli input
- Tentativi di *Code Injection*

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Gli input inseriti nei sistemi OT non vengono validati.
Razionale Implementato Ad-Hoc	Vengono effettuati dei controlli superficiali per confermare che i parametri inseriti siano all'interno di range prestabiliti.
Razionale Implementato	Vengono effettuati controlli anche sulla sintassi degli input per mitigare il rischio collegato ad attacchi come SQL Injection, Malformed Packets, cross-site scripting, etc.
Razionale Ottimizzato	I controlli implementati sono in linea con Standard e Best Practice di settore (es. Open Web Application Security Project (OWASP) Code Review Guide).

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 3.5	The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.

Banner di utilizzo

Nonostante a livello Europeo non siano attualmente presenti particolari normative a riguardo, è opportuno che sui sistemi OT siano presenti messaggi/banner (es. MOTD) che notifichino l'utente in merito al corretto uso del sistema (es. durante l'accesso tramite SSH/terminale oppure prima del login su Windows).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono mostrati banner/MOTD durante l'accesso al sistema.
Razionale Implementato Ad-Hoc	Sono presenti direttive in merito al corretto uso dei sistemi all'interno di Policy e procedure interne.
Razionale Implementato	Ove possibile, sono presenti banner/MOTD che notificano l'utente in merito al corretto utilizzo del sistema. Tali messaggi possono essere configurati solo dal personale autorizzato.
Razionale Ottimizzato	Il contenuto dei banner/MOTD è in linea con Regulation applicabili al contesto.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 1.12	The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

Configurazione sicura tramite Guidelines

Durante la fase di configurazione dei sistemi OT, dovrebbero essere seguite guidelines di security fornite dai *vendor* o da Best Practice di settore. In particolare:

- Il CIS Benchmark definisce linee guida di sicurezza per le principali tipologie di sistemi operativi (es. Windows, Android, etc.) e dispositivi (es. Workstation, dispositivi di rete, etc.)
- Per i dispositivi di più basso livello (es. PLC, HMI, etc.), spesso i fornitori definiscono linee guida per la configurazione sicura.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi vengono configurati senza seguire le linee guida di security definite dal vendor
Razionale Implementato Ad-Hoc	Sono specificati requisiti di configurazione generici in ambito IT/OT Cyber Security.
Razionale Implementato	I sistemi vengono configurati seguendo le linee guida di security definite dal vendor e le best practice di settore
Razionale Ottimizzato	Esiste un processo di miglioramento continuo relativo alla definizione dei requisiti di sicurezza da applicare.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.6	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.

Least Functionality

I sistemi OT dovrebbero essere configurati seguendo il principio di "least-functionality", secondo cui i sistemi o applicativi dovrebbero fornire solo le funzionalità necessarie per svolgere le attività specifiche per le quali sono stati progettati (es. abilitando solo le porte, protocolli e servizi strettamente necessari). Ogni funzionalità aggiuntiva rappresenta una potenziale vulnerabilità di sicurezza.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	I sistemi non sono stati configurati seguendo il principio di "least-functionality"
Razionale Implementato Ad-Hoc	Sono stati disabilitati alcuni servizi comunemente noti come vulnerabili (es. Telnet, FTP, etc.)
Razionale Implementato	I sistemi sono stati configurati seguendo il principio di "least-functionality"
Razionale Ottimizzato	I sistemi sono stati configurati seguendo il principio di "least-functionality" e sono periodicamente testati.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 7.7	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

Gestione dei dispositivi mobile

L'uso di dispositivi portatili e mobili (es. laptop, tablet, smartphone, dispositivi rimovibili, etc.), se richiesto per lo svolgimento delle attività lavorative, dovrebbe essere gestito in maniera centralizzata attraverso soluzioni di Mobile Device Management (MDM).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non vi sono particolari limitazioni per utilizzo di dispositivi mobile all'interno del Plant ed i dispositivi mobile non vengono tracciati e gestiti.
Razionale Implementato Ad-Hoc	L'utilizzo di dispositivi mobili è soggetto a restrizioni e tali dispositivi vengono gestiti in maniera non centralizzata.
Razionale Implementato	L'utilizzo di dispositivi mobili è soggetto a restrizioni e tali dispositivi vengono gestiti tramite una soluzione centralizzata (es. MDM).
Razionale Ottimizzato	L'utilizzo di dispositivi mobile è soggetto a restrizioni e tali dispositivi vengono gestiti tramite una soluzione centralizzata (es. MDM). È presente una soluzione di Mobile Application Management in caso di dispositivi BYOD. All'interno dei dispositivi mobile è presente una containerizzazione per sperare dati ed applicazioni personali da quelli aziendali.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 3-3:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
SR 2.3	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.

Hardening fisico dei dispositivi

Oltre alle misure di *hardening* logico sopra citate, dovrebbero essere adottate anche contromisure per prevenire l'accesso fisico alle macchine e relative interfacce fisiche (es. porte USB) al personale non autorizzato.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Le macchine e le relative interfacce I/O sono liberamente accessibili.
Razionale Implementato Ad-Hoc	Le interfacce I/O sono disabilitate o l'accesso è consentito solo al personale autorizzato.
Razionale Implementato	Le interfacce I/O sono disabilitate o l'accesso è consentito solo al personale autorizzato. Le workstation più sensibili non sono fisicamente accessibili (es. tramite utilizzo di KVM).
Razionale Ottimizzato	Tentativi di accesso alle interfacce fisiche vengono automaticamente rilevati e notificati al personale dedicato.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.6	Host devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

Meccanismi di notifica per gli accessi fisici

Idealmente, dovrebbero essere presenti meccanismi per notificare in caso di accessi fisici ai sistemi non autorizzati.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti meccanismi di notifica in caso di accessi non autorizzati.
Razionale Implementato Ad-Hoc	Sono presenti misure come CCTV e/o allarme antintrusione per rilevare accessi fisici non autorizzati.
Razionale Implementato	Sono presenti meccanismi di notifica in caso di accessi non autorizzati (es. sensori dedicati negli armadi e nei case delle workstation, etc.)
Razionale Ottimizzato	Le notifiche sono monitorate e prontamente indagate.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.6 RE 1	Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

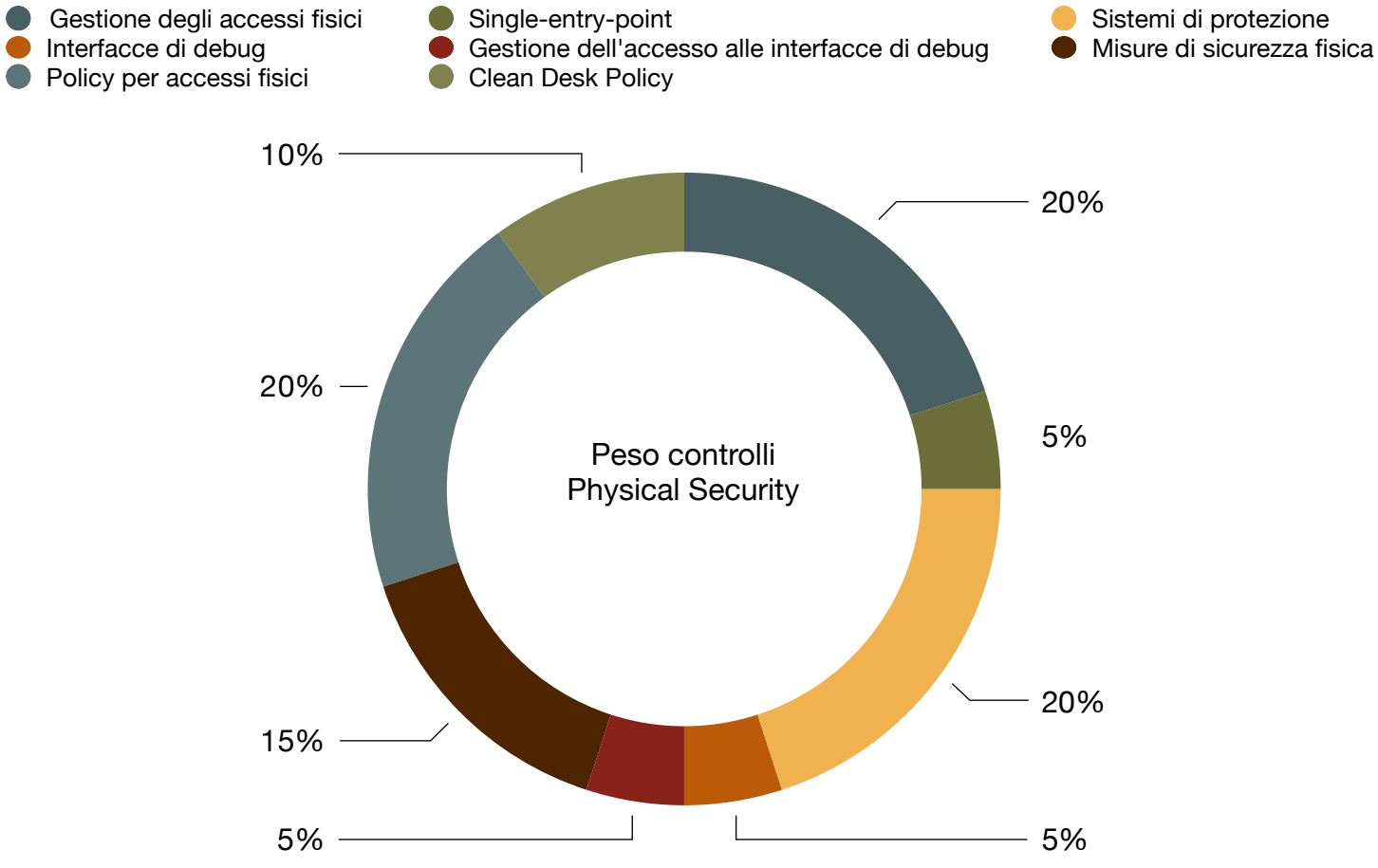
Physical Security

Pur essendo le tematiche di Network, Software e Data Security fondamentali per i sistemi OT, resta indiscutibile la “fisicità” degli stabilimenti industriali. Di conseguenza, la sicurezza degli accessi fisici ai Plant è una tematica molto sensibile. Per proteggere gli stabilimenti da accessi non autorizzati, è quindi possibile predisporre una serie di misure di sicurezza.

Tale Dominio prevede 8 controlli relativi a:

1. Gestione degli accessi fisici
2. Single-entry-point
3. Sistemi di protezione
4. Interfacce di *debug*
5. Gestione dell'accesso alle interfacce di *debug*
6. Misure di sicurezza fisica
7. Policy per accessi fisici
8. Clean Desk Policy

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Gestione degli accessi fisici

La gestione degli accessi fisici allo stabilimento è la prima misura di sicurezza da considerare in ambito di Physical Security. Ciò prevede la segregazione dei vari ambienti dello stabilimento (es. sala server, control room, area di produzione o altre aree sensibili), oltre che meccanismi per limitare e registrare gli accessi (es. tramite badge o registro cartaceo).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	L'accesso fisico ai locali non è regolato.
Razionale Implementato Ad-Hoc	L'accesso fisico ai sistemi è regolato e limitato tramite l'utilizzo di dispositivi di identificazione (es. badge).
Razionale Implementato	L'accesso fisico ai sistemi è regolato e limitato tramite l'utilizzo di dispositivi di identificazione (es. badge). Gli accessi sono registrati e tracciati tramite soluzione digitale.
Razionale Ottimizzato	L'accesso fisico ai sistemi è regolato e limitato tramite l'utilizzo di dispositivi di identificazione (es. badge). Gli accessi sono registrati e tracciati tramite soluzione digitale. Gli accessi ai locali più sensibili (es. sala server, sala controlli, etc.) sono regolamentati da MFA (es badge + pin/biometria).

Il controllo si basa sul seguente controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.11	Physical & Environmental Security

Single-entry-point

Le modalità con cui i dipendenti, fornitori e *visitor* accedono allo stabilimento rappresentano una tematica critica di sicurezza. La possibilità di accedere al Plant attraverso più ingressi separati rende molto più difficile il monitoraggio ed il controllo degli accessi. Di conseguenza, è preferibile la definizione di un *single-entry-point* per effettuare l'accesso al Plant (es. ingresso obbligato tramite reception).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un single-entry-point per accedere al Plant-
Razionale Implementato Ad-Hoc	L'accesso del personale è convogliato attraverso un canale unico principale (es. cancello principale). Resta comunque possibile accedere al Plant tramite ingressi secondari.
Razionale Implementato	L'accesso del personale è possibile esclusivamente attraverso un single-entry-point.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.11	Physical & Environmental Security

Sistemi di protezione

Il perimetro dello stabilimento dovrebbe essere monitorato e protetto attraverso sistemi di protezione come videosorveglianza e/o allarme anti-intrusione. Idealmente, dovrebbero essere presenti anche percorsi di ronda monitorati da personale di vigilanza.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti sistemi di allarme e videosorveglianza.
Razionale Implementato Ad-Hoc	Sono presenti sistemi di allarme e videosorveglianza che coprono il perimetro del Plant.
Razionale Implementato	Sono presenti sistemi di allarme e videosorveglianza gestiti centralmente che coprono l'intero perimetro dello stabilimento, con sensori/videocamere dedicati alle aree più sensibili (es. sala server, sala controllo, etc.).
Razionale Ottimizzato	Presenza di vigilanza H24-7/7 con ronde esterne/interne.

Il controllo si basa sul seguente controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.11	Physical & Environmental Security

Interfacce di debug

Spesso, i sistemi OT nei livelli più bassi del *Purdue Model* presentano interfacce I/O fisiche dedicate per finalità di *debug* o testing (es. JTAG debugging). Nel caso siano presenti, dovrebbero essere adottate contromisure per prevenire utilizzi non autorizzati di tali interfacce.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	L'accesso alle interfacce di debug non è regolato.
Razionale Implementato Ad-Hoc	Sono presenti misure ad-hoc per prevenire l'accesso non autorizzato alle interfacce di debug.
Razionale Implementato	L'accesso alle interfacce di debug è regolamentato per prevenire accessi non autorizzati.
Razionale Ottimizzato	L'accesso alle interfacce di debug è regolato per prevenire accessi fisici non autorizzati e monitorato.

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.3	Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (es. JTAG debugging).

Gestione dell'accesso alle interfacce di debug

Nel caso siano presenti interfacce di *debug* o JTAG, l'accesso a tali interfacce dovrebbe essere registrato all'interno dei log e/o notificato al personale di riferimento.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	L'accesso alle interfacce di debug non viene registrato e notificato.
Razionale Implementato Ad-Hoc	L'accesso alle interfacce di debug viene registrato nei log.
Razionale Implementato	L'accesso alle interfacce di debug viene registrato nei log e notificato automaticamente.
Razionale Ottimizzato	N/A

Il controllo si basa sul seguente *System Requirement* definito dall'IEC/ISA 62443 4-2:

ID Riferimento IEC/ ISA 62443	Riferimento IEC/ISA 62443
HDR 14.3 RE 1	Host devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

Misure di sicurezza fisica

Oltre ai sistemi di protezioni, dovrebbero essere presenti misure e dispositivi per la sicurezza fisica all'interno dello stabilimento e nel relativo perimetro (es. recinzioni, segregazione fisica degli ambienti, guardie di sicurezza).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono presenti particolari misure per la sicurezza fisica.
Razionale Implementato Ad-Hoc	Sono presenti misure di sicurezza fisica perimetrale (es. recinsioni, mura, etc.).
Razionale Implementato	Le aree sensibili (es. sala server, sala controllo) sono fisicamente isolate dal resto del Plant (es. con serrature elettroniche, doppia porta, etc.).
Razionale Ottimizzato	Sono presenti misure avanzate per la sicurezza fisica quali reti sensibili, barriere ad infrarossi, accessi veicolari controllati, zone tampone.

Il controllo si basa sul seguente controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.11	Physical & Environmental Security

Policy per accessi fisici

Nonostante le misure di sicurezza fisica siano fondamentali, esse possono essere sfruttate al meglio solo se accompagnate da un processo per gestire gli accessi fisici ai diversi ambienti del Plant (es. reception, sala di controllo, etc.) da parte sia dei dipendenti che degli ospiti.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	L'accesso agli ambienti del Plant non è regolato tramite una Policy dedicata.
Razionale Implementato Ad-Hoc	L'accesso ambienti più sensibili del Plant è regolato tramite Policy dedicata e gli accessi monitorati.
Razionale Implementato	Il personale esterno è tenuto a indossare badge di riconoscimento ed è scortato per l'intero periodo della visita.
Razionale Ottimizzato	L'accesso a tutti gli ambienti del Plant è regolato tramite Policy dedicate. L'enforcement di tali Policy viene periodicamente verificato.

Il controllo si basa sul seguente controllo dell'ISO 27k:

ID Riferimento ISO 27k	Riferimento ISO 27k
A.11	Physical & Environmental Security

Clean Desk Policy

Una tematica spesso sottovalutata all'interno degli stabilimenti è l'*enforcement* di una Clean Desk Policy. Le postazioni di lavoro non dovrebbero presentare documenti sensibili esposti liberamente e, le relative workstation dovrebbero sempre essere "bloccate" in caso di abbandono della postazione da parte dell'operatore. In tale modo, è possibile contrastare il furto di informazioni sensibili come parte di campagne di spionaggio industriale, oltre che evitare i più comuni tipi di attacchi informatici.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è stata definita una "Clean Desk Policy".
Razionale Implementato Ad-Hoc	È stata definita una "Clean Desk Policy".
Razionale Implementato	È stata definita una "Clean Desk Policy" e ne viene periodicamente verificato l'enforcement.

Razionale Ottimizzato	È stata definita una "Clean Desk Policy" e ne viene periodicamente verificato l'enforcement. Per tale Policy vengono erogate campagne di Awareness verso i dipendenti.

Training e Awareness

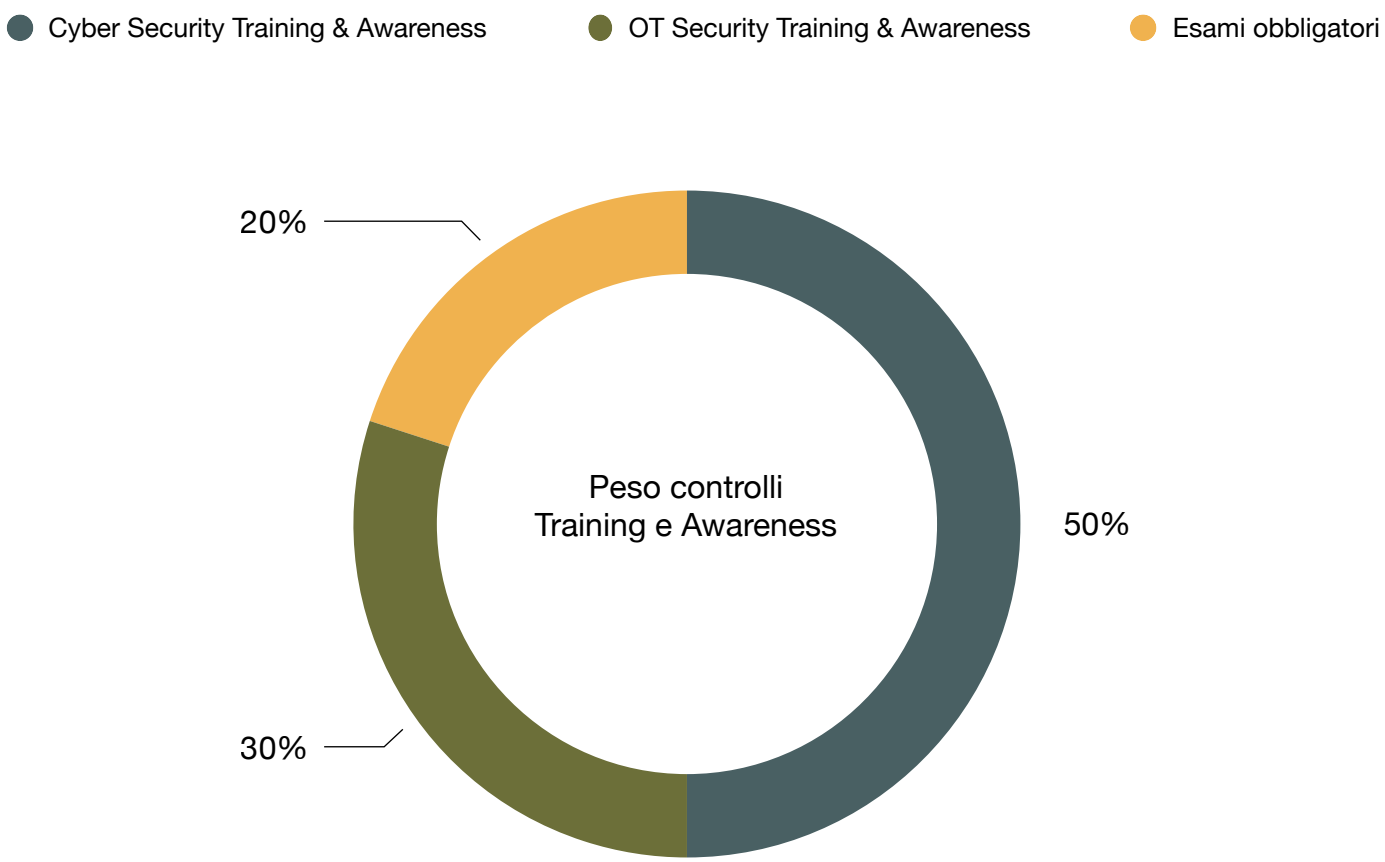
Le misure tecniche (*Technologies*) di Cyber Security non possono essere sfruttate a pieno, se non sono accompagnate da una corretta formazione dei dipendenti (*People)* e dalla gestione della Governance e di ruoli e responsabilità (*Process*) in ambito di sicurezza.

In particolare, la formazione del personale permette di aumentare *l'awareness* dei dipendenti relativa alle tematiche di Cyber Security e ridurre quindi la probabilità di attacchi di *Phishing* e *Spear Phishing*, tipologia di attacchi assai diffusa al giorno d'oggi.

Tale Dominio prevede 3 controlli relativi a:

1. Cyber Security Training & Awareness
2. OT Security Training & Awareness
3. Esami obbligatori

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Cyber Security Training & Awareness

È importante che sia stato definito un piano di Training ed Awareness aziendale che copra almeno le tematiche più generali relative alla Cyber Security, come ad esempio:

- Gestione sicura delle credenziali
- Identificazione dei tentativi di *Phishing*
- Identificazione di eventuali attività anomale

Tali campagne di Training & Awareness devono essere erogate non solo al personale amministrativo e manageriale (*White Collar*), ma anche al personale OT che opera i macchinari (*Blue Collar*).

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un piano di Training & Awareness relativo alla Cyber Security dedicato ai dipendendti OT.
Razionale Implementato Ad-Hoc	È presente un piano non strutturato di Training & Awareness.
Razionale Implementato	È presente un piano di Training & Awareness, sia teorico che pratico, relativo alla Cyber Security svolto anche dai dipendendti OT.
Razionale Ottimizzato	Piano svolto tramite sessioni in aula con programma determinato in base al livello di conoscenza dei temi OT recepiti nelle precedenti wave.

OT Security Training & Awareness

Se presente, il piano di Training & Awareness dovrebbe idealmente includere anche un modulo dedicato a tematiche specifiche di OT Cyber Security.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Il piano di Training & Awareness non include tematiche di OT Security.
Razionale Implementato Ad-Hoc	Il piano di Training & Awareness include anche tematiche di OT Security.
Razionale Implementato	Il piano di Training & Awareness include un modulo dedicato, sia teorico che pratico, alle tematiche di OT Security.
Razionale Ottimizzato	N/A

Esami obbligatori

Infine, al termine dello svolgimento dei corsi previsti dal programma di Training e Awareness dovrebbero essere previsti degli esami obbligatori per verificare l'apprendimento delle nozioni insegnate durante l’erogazione dei corsi.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono previsti esami obbligatori.

Razionale Implementato Ad-Hoc	Sono previsti quiz non obbligatori.
Razionale Implementato	Sono previsti esami obbligatori al termine del programma di Training & Awareness.
Razionale Ottimizzato	N/A

Security Governance

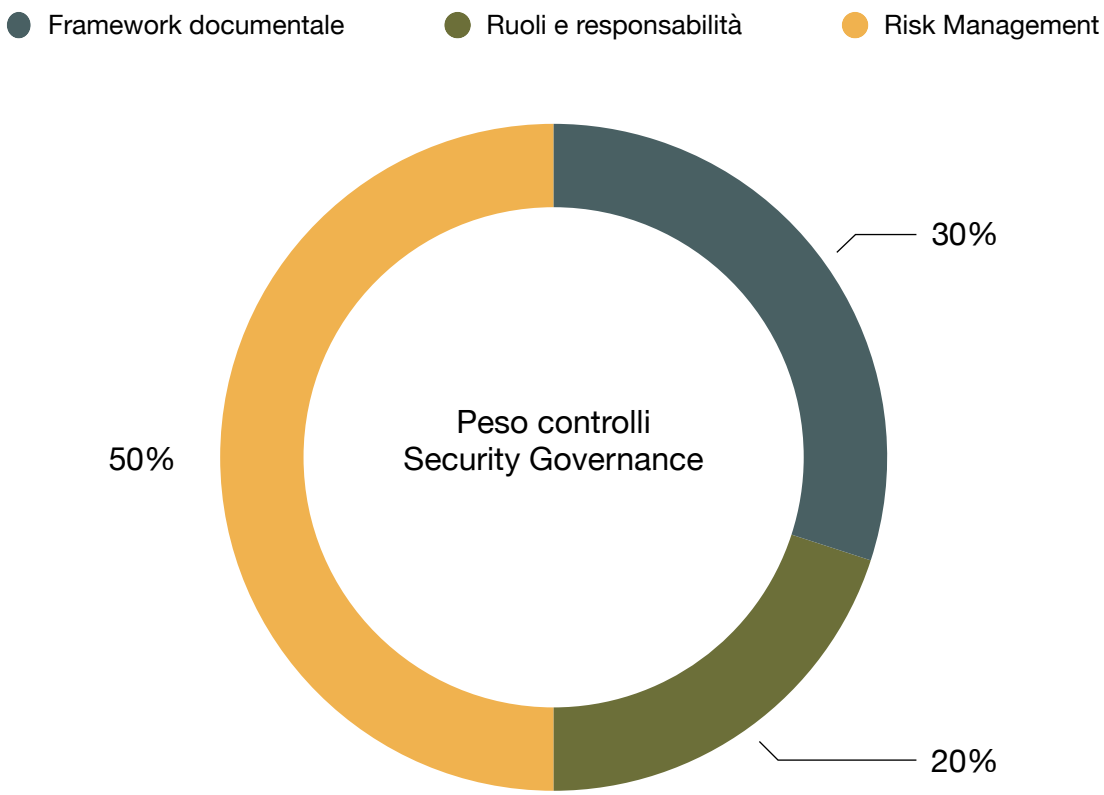
Le misure tecniche (*Technologies*) di Cyber Security non possono essere sfruttate a pieno, se non sono accompagnate da una corretta formazione dei dipendenti (*People)* e dalla gestione della Governance e di ruoli e responsabilità (*Process*) in ambito di sicurezza.

In particolare, una corretta definizione della Security Governance permette di gestire al meglio le numerose Policy, procedure operative, linee guida e processi che dovrebbero essere stati definiti relativamente alla OT Cyber Security.

Tale Dominio prevede 3 controlli relativi a:

1. Framework documentale
2. Ruoli e responsabilità
3. Risk Management

Nel seguente grafico è possibile osservare la distribuzione dei pesi dei controlli in questione:



Framework documentale

La definizione di un Framework documentale in ambito OT, in linea con Standard e Best Practice di settore (es. ISO27001) permette di gestire al meglio, da un punto di vista di processo, la maggior

parte delle tematiche di OT Cyber Security trattate in questo Framework. Alcuni esempi di Policy che possono essere adattate al contesto OT includono:

- Scope of the Information Security Management System
- Information security policy and objectives
- Risk assessment and risk treatment methodology
- Statement of applicability
- Definition of security roles and responsibilities
- Acceptable use of assets
- Access control policy
- Secure system engineering principles
- Supplier security policy
- Risk treatment plan
- Operating procedures for IT management
- Incident management procedure
- Business continuity procedures
- Inventory of assets
- Risk assessment report
- Vulnerability & Patch management policy
- Information classification policy
- Password policy
- Disposal and destruction policy
- Clear desk and clear screen policy
- Change management policy
- Backup policy
- Business continuity & Disaster recovery strategy

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non è presente un framework documentale in ambito OT.
Razionale Implementato Ad-Hoc	Sono presenti alcune Policy o procedure che coprono parte degli argomenti indicati in Standard e Best Practice.
Razionale Implementato	E' presente un framework documentale completo e periodicamente aggiornato che indirizza tutti gli aspetti presenti in Standard e Best Practice.
Razionale Ottimizzato	Il framework è frequentemente aggiornato in linea con le ultime indicazioni.

Ruoli e responsabilità

La definizione di ruoli e responsabilità (ad esempio, attraverso una matrice RACI) delle varie figure coinvolte in ambito OT Cyber Security permette di ottimizzare la gestione delle tematiche di sicurezza, associando ad ogni tematica e processo dei relativi responsabili.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Non sono stati definiti ruoli e responsabilità.
Razionale Implementato Ad-Hoc	I ruoli e le attività svolte sono note ma non formalizzate in documentazione specifica.
Razionale Implementato	Esiste un documento formale periodicamente aggiornato che dettaglia ruoli e responsabilità con un dettaglio delle mansioni svolte.
Razionale Ottimizzato	Le figure sono adeguatamente formate in modo da essere interscambiabili.

Risk Management

Lo svolgimento di attività di Risk Management permette di identificare in modo sistematico le minacce e le vulnerabilità nei sistemi OT. Questo processo fornisce una panoramica chiara delle potenziali debolezze che possono essere sfruttate dagli utenti malevoli. Il Risk Management consente inoltre di valutare il rischio associato a ciascuna minaccia e vulnerabilità identificata. Questa valutazione aiuta a determinare la priorità delle azioni di sicurezza e a concentrare le risorse dove sono maggiormente necessarie.

I livelli di implementazione del controllo prevedono:

Razionale Non Implementato	Nessuna attività di Risk Assessment.
Razionale Implementato Ad-Hoc	Esecuzione di attività di analisi superficiali in maniera ad-hoc.
Razionale Implementato	Esisste un processo formalizzato di Risk Management dedicato all'area OT che prevede attività periodiche di Risk Assessment su tutto il perimetro.
Razionale Ottimizzato	Il processo è supportato dall'esecuzione di verifiche tecniche (es. VAPT) e da tool automatizzati.

6. RESTRIZIONE DEL DOMINIO DI ANALISI AI SISTEMI DI SUPERVISIONE E CONTROLLO (SCADA) CON DEFINIZIONE DI UN FRAMEWORK DI SICUREZZA SPECIFICO

Mentre l'obbiettivo dell'OT Security Framework, descritto nel procedente capitolo, mirava a valutare lo stato complessivo di Cyber Security di uno stabilimento analizzandone tutte le varie componenti e processi critici, è stato ritenuto opportuno, anche a causa delle esigenze legate alle progettualità, definire un Framework di sicurezza focalizzato esclusivamente sulla protezione dei sistemi SCADA (Supervisory Control And Data Acquisition). Per fare ciò è stato ovviamente necessario prendere in considerazione requisiti di sicurezza relativi a tutte le principali componenti dai sistemi SCADA, partendo dalla sicurezza dei dati di produzione e passando per la sicurezza delle Workstation e la gestione degli accessi ai sistemi. E' opportuno osservare che, essendo il contesto dei sistemi SCADA strettamente legato all'OT Cyber Security dei sistemi industriali, è possibile notare numerose similitudini fra i controlli dell'OT Security Framework e i requisiti dello SCADA Security Framework. Tuttavia, quest'ultimo è stato ottimizzato a livello di definizione di Domini e Sotto-Domini e specificità dei requisiti e delle domande.

Il Framework è suddiviso in 63 requisiti di sicurezza, raggruppati in 7 Domini e 17 Sotto-Domini, dove ogni Dominio rappresenta una macro-area relativa alla sicurezza dei sistemi SCADA ed ogni Sotto-Dominio ne specifica i principali punti di interesse chiave.

Dominio	Sotto Dominio	Numero Controlli
Data security	Data Backup	2
	Data Integrity and Destruction	4
	Malicious Software Protection	1
Platform and Application Security	Client/Server Protection	6
	SCADA Application Protection	2
Communication Security	Network Perimeter Protection	5
	Remote and External Access	2
	Wired and Wireless Connectivity	3
Personnel Security	Training	3
Configuration Management	Account Configuration	2
	Identification and Authentication	8
	Secure Configuration	5
	Update Security	2

Dominio	Sotto Dominio	Numero Controlli
Detection and Recovery	Continuous Monitoring	3
	log Configuration	6
	Recovery Capability	3
Physical Access security	SCADA Asset Protection	6

Processo di definizione dello SCADA Security Framework

Il processo che ha portato alla definizione dello SCADA Security Framework è stato relativamente differente rispetto al processo di definizione dell'OT Security Framework. Le fondamenta per la definizione di tale Framework provengono infatti dal modello proposto nel 2005 dai Sandia National Laboratories nel "Framework for SCADA Security Policy". Il modello proposto, osservabile nell'immagine sottostante, definisce attraverso una struttura a Domini e Sotto-Domini quelle che sono le principali sezioni di interesse quando si prende in considerazione la sicurezza dei sistemi SCADA.

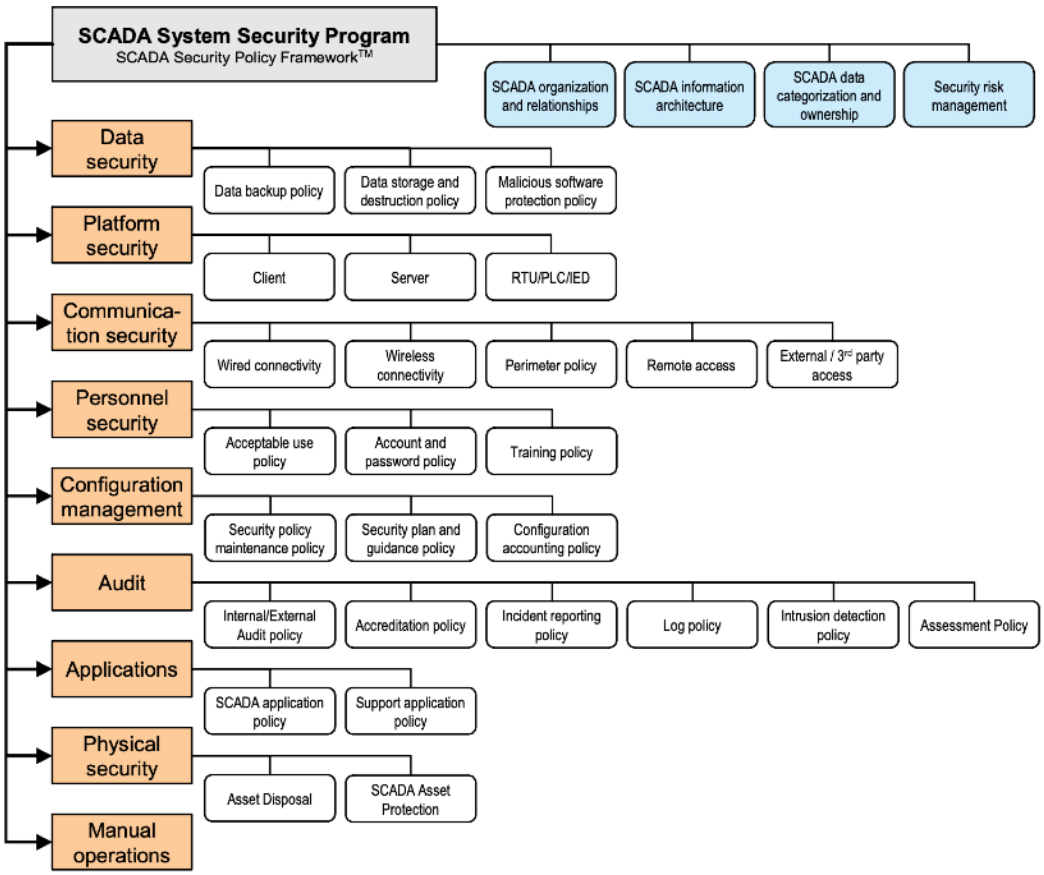


Figura 9: "Framework for SCADA Security Policy"

Tali sezioni e sotto-sezioni sono state analizzate e riorganizzate (attraverso la modifica, aggiunta o rimozione) per permettere di definire la struttura organizzative dello SCADA Security Framework. Ciò è stato fatto prendendo anche in considerazione i *Functional Requirements* e *System Requirements* proposti dell'IEC/ISA 62443. Il modello proposto nel "Framework for SCADA Security Policy" non procede nella definizione di effettivi controlli e requisiti di sicurezza da associare alle varie sezioni e sotto-sezioni, mantenendo invece un livello di approfondimento abbastanza generale ed *high-level.* Il passo successivo nella definizione dello SCADA Security Framework è stato quindi quello di andare ad analizzare tutti i *System Requirements* definiti dall'IEC/ISA 62443 3-3 e 4-2, valutandone la rilevanza all'interno del contesto dei sistemi SCADA. Una prima fase è quindi consistita nel filtraggio di tali *System Requirements,* escludendo quelli che richiedessero un livello di sicurezza troppo stringente per i sistemi SCADA o che non fossero proprio rilevanti o applicabili a tale contesto. La fase successiva ha poi previsto di andare ad inserire la lista di *System Requirements* ritenuti rilevanti all'interno della struttura a Domini e Sotto-Domini definita in precedenza, associando ogni *System Requirement* alla categoria di appartenenza più opportuna. Unica eccezione è rappresentata dai requisiti relativi al Dominio *Personnel Security* ed alcuni requisiti relativi al Dominio *Physical Access Security,* le quali tematiche non vengono trattate all'interno dell'IEC/ISA 62443, ma che sono tuttavia rilevanti quando si considera la sicurezza dei sistemi SCADA. La gestione degli accessi fisici ai sistemi SCADA e la formazione degli operatori che utilizzano tali sistemi sono infatti tematiche che non possono essere trascurate e, di conseguenza, sono stati definiti dei requisiti *Ad-Hoc* tenendo in considerazione Standard e Best Practice di settore. Infine, ad ogni *System Requirement* identificato è stata associata una o un set di domande da effettuare in fase di analisi o Audit al fine di valutare lo stato di sicurezza dei sistemi.

I requisiti definiti non sono fra loro equipollenti. Alcuni requisiti hanno infatti maggiore importanza e richiedono maggiore *effort* per essere correttamente implementati. Per tale motivo, ad ogni requisito è stato assegnato un peso specifico in percentuale relativo al proprio Dominio di appartenenza.

Struttura dello SCADA Security Framework

Lo SCADA Security Framework è stato implementato attraverso un foglio di calcolo, utilizzando il software Microsoft Excel. In questo modo, è stato possibile sfruttare al meglio la struttura tabellare di questo Framework, sia in fase di definizione, che in fase di applicazione in contesti *real-life.* Il Framework prevede un controllo per ogni riga, e presenta nelle colonne i seguenti campi:

- ID Dominio: Codice identificativo del Dominio del Framework. Tale valore va da 1 a 7.
- Dominio: Dominio di appartenenza del controllo.
- ID Sotto-Dominio: Codice identificativo del sotto-Dominio del Framework. Tale valore è utilizzato nella forma 1.1, 1.2, 2.1, 2.2, etc.
- Sotto-Dominio: Nominativo del sotto-Dominio.

- Rif. ISA 62443: Riferimento all'identificativo del *System Requirement* dello Standard ISA/IEC 62443 preso come riferimento per la definizione del controllo.
- ISA 62443 Requirement/Enhancement: Descrizione del *System Requirement* preso come riferimento per la definizione del controllo.
- ID Domanda: Codice identificativo della domanda/e associata al sotto-Dominio. Tale valore è utilizzato nella forma 1.1.1, 1.1.2 1.2.1, 2.1.2, 2.2.1, etc.
- Domanda: Domanda associata/e associata al sotto-Dominio e . Tale domanda può essere utilizzata come riferimento durante l'analisi di casi di studio *real-life,* o può essere direttamente posta agli interlocutori in fase di intervista o Audit presso uno stabilimento.
- Maturità: Campo compilabile. In tale campo è possibile inserire, selezionandolo da una lista di valori, il livello di maturità identificato a seguito delle attività di analisi o intervista. Nel caso in cui, per qualche motivazione, il controllo non sia applicabile al contesto in analisi, è possibile selezionare il valore "Non Applicabile". Il significato dei Razionale di implementazione è esplicitato nella seguente tabella:

Razionale Non implementato	Descrizione maturità "Non implementato". Tale maturità indica che il controllo non è soddisfatto. **Il controllo è KO**.
Razionale Parzialmente Implementato	Descrizione maturità "Implementato Ad-hoc". Tale maturità indica che vengono effettuate alcune attività in merito ma non sono sufficenti al soddisfacimento del controllo. **Il controllo è KO**.
Razionale Implementato	Descrizione maturità "Implementato". Tale maturità indica che le attività in merito sono sufficenti al soddisfacimento del controllo. **Il controllo è OK**.

- Note: Campo compilabile. E' possibile utilizzare questo campo per inserire i risultati emersi dalle analisi o interviste.
- Azioni di miglioramento: Campo compilabile. E' possibile usare tale campo per identificare eventuali azioni di miglioramento consigliate, nel caso in cui ii requisiti associati alle domande non siano pienamente soddisfatti.
- Calcolo Maturità: Questi campi associano ad ogni requisito un peso specifico rispetto al proprio Dominio di appartenenza e, in base al livello di maturità assegnato, permettono di calcolare automaticamente il punteggio ponderato che contribuirà ad influire sulla livello di maturità globale dello stabilimento analizzato.

E' evidente che lo SCADA Security Framework, focalizzandosi esclusivamente sui sistemi SCADA, può essere visto come un Framework "satellite" del più generale e ricco OT Security Framework. Di conseguenza, non verranno trattati i singoli requisiti del Framework, ma saranno presi in considerazione, di seguito, esclusivamente i Domini e Sotto-Domini.

Data Security

I sistemi SCADA trattano una vasta gamma di dati per monitorare e controllare i processi industriali, tra cui:

- Dati di processo: Informazioni riguardanti le variabili fisiche e chimiche associate al processo industriale monitorato. Ciò può includere temperature, pressioni, livelli di liquidi, flussi di gas, e altre grandezze fisiche specifiche del processo.
- Dati di controllo: Informazioni relative ai comandi e alle istruzioni inviate al sistema di controllo per regolare o controllare i dispositivi all'interno del processo. Questi dati sono essenziali per garantire che il processo si mantenga entro i limiti desiderati.
- Dati di stato: Informazioni sullo stato operativo dei dispositivi e delle apparecchiature all'interno del sistema. Ciò può includere informazioni su allarmi, segnalazioni di guasti, disponibilità di apparecchiature e altri indicatori di stato.
- Dati di allarme: Notifiche generate quando il sistema rileva condizioni anomale o pericolose. Gli allarmi aiutano gli operatori a rispondere a situazioni critiche e ad adottare le misure necessarie.
- Dati storici: Registrazioni storiche delle variabili di processo nel tempo. Questi dati sono spesso utilizzati per analizzare le prestazioni passate, identificare tendenze e supportare la pianificazione delle attività di manutenzione.
- Dati di sicurezza: Informazioni relative alla sicurezza del sistema SCADA stesso, inclusi dati di autenticazione, autorizzazione e monitoraggio degli accessi per garantire la sicurezza e l'integrità delle informazioni.
- Dati di comunicazione: Informazioni scambiate tra i diversi componenti del sistema SCADA attraverso reti di comunicazione. Questi dati sono fondamentali per garantire la trasmissione affidabile delle informazioni tra i dispositivi di campo, i terminali remoti e il centro di controllo.

La gestione efficace di questi tipi di dati è cruciale per il corretto funzionamento e la sicurezza dei sistemi SCADA.

Data Backup

I dati conservati all’interno dei sistemi SCADA dovrebbero essere sottoposti a backup periodici per evitarne la perdita in caso di guasti, incidenti e attacchi.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
1.1.1	Gestione dei backup	Vengono effettuati i backup dei sistemi? Se si: - Quali sistemi sono sottoposti a backup? - Quali sono le tempistiche definite? - Quante copie e dove vengono effettuati i backup? - Il processo di backup avviene automaticamente?	SR 7.3	75
1.1.2	Controlli sui backup	Vengono effetuati controlli sui backup e sulla relativa integrità?	SR 7.3 RE 1	25

Data Integrity and Destruction

I dati conservati all'interno dei sistemi SCADA dovrebbero essere protetti attraverso adeguati meccanismi sia *At-Rest* che *In-Transit.* Inoltre, è necessario garantire che i dati siano rimossi in maniera sicura dai sistemi quando questi vengono dismessi.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
1.2.1	Rilevamento di modifiche non autorizzate alle informazioni	Sono presenti meccanismi che permettono di rilevare modifiche non autorizzate alle informazioni at-rest ed al software (es. attraverso hash/ checksum)?	SR 3.4	15
1.2.2	Automatizzazione dei meccanismi di rilevamento di modifiche	Se sono presenti mecccanismi di rilevamento di modifiche apportate alle informazioni ed al software, sono automatizzati? Segnalano eventuali modifiche rilevate all'utente/ amministratore?	SR 3.4 RE 1	15
1.2.3	Informazioni confidenziali	Ci sono informazioni confidenziali nei sistemi, sia in transito che at-rest? Se si, sono adeguatamente protette (es. attraverso l'utilizzo di meccanismi di cifratura)?	SR 4.1	50
1.2.4	Dismissione sicura dei sistemi	È possibile eliminare tutte le informazioni in maniera sicura e definitiva dai sistemi dismessi?	SR 4.2	20

Malicious Software Protection

I dati conservati all'interno dei sistemi SCADA dovrebbero essere protetti da eventuale codice malevolo.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
1.3.1	Hardening logico dei sistemi	Sono stati implementati meccanismi di protezione come Antivirus o EDR? Se si, su quali sistemi/device? Come sono configurati?	SR 3.2	100

Platform and Application Security

I sistemi SCADA sono composti da diversi componenti e applicativi che collaborano per monitorare e controllare processi industriali. Tali componenti solitamente includono:

- PLC ed RTU: Questi dispositivi raccolgono dati dai sensori e dagli attuatori, li elaborano e li inviano al sistema SCADA centrale.
- Human-Machine Interface (HMI): Interfaccia utente che consente agli operatori di interagire con il sistema SCADA attraverso una visualizzazione intuitiva dello stato del processo e delle informazioni di controllo.
- Server SCADA: Componente centrale che gestisce la raccolta, l'elaborazione e l'archiviazione dei dati provenienti dai dispositivi di campo. Esso facilita la comunicazione tra gli elementi di campo e il sistema di supervisione.
- SCADA Database (Historian DB): I sistemi SCADA spesso utilizzano database per archiviare dati storici, informazioni di configurazione e altri dati critici per l'analisi e la gestione del sistema.
- Applicativi di monitoraggio e reporting: Strumenti software che consentono agli utenti di monitorare le prestazioni del processo nel tempo, generare report e analizzare dati storici per migliorare l'efficienza operativa.

Tali componenti ed applicativi devono essere protetti per garantire la sicurezza dei sistemi SCADA.

Client/Server Protection

E’ opportuno abilitare meccanismi di protezione logica su tutti gli *endpoint* sui quali si distribuisce il sistema SCADA. Ciò prevede la protezione dei PLC, delle Workstation sulle quali sono installate le interfacce HMI e degli SCADA Server e Database.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
2.1.1	Asset Inventory	È presente un asset inventory sia dei dispositivi/componenti (Hardware) sia dei programmi installati (Software), e dei relativi flussi di comunicazione sul sistema?	HDR 14.9	30
2.1.2	Integrità dei componenti all’avvio dei sistemi	Viene verificata l'integrità dei componenti prima dell'avvio del sistema operativo (viene effettuata una verifica dell'integrità del BIOS prima dell'avvio della macchina)?	HDR 14.9	10

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
2.1.3	Gestione dei dispositivi mobili	L'uso di dispositivi portatili e mobili (laptop, tablet, smartphone, dispositivi rimuovibili) è consentito per la gestione di determinate funzioni o attività? Se sì, essa viene implementata attraverso una soluzione di MDM?	SR 2.3	20
2.1.4	Terminazione delle sessioni per inattività	È possibile terminare o bloccare le sessioni, sia remote che locali, dopo un certo periodo di inattività dell'utente sia manualmente che automaticamente per prevenire accessi indesiderati alle postazioni di lavoro? (e.g Uso di auto-lock)	SR 2.5	15
2.1.5	Algoritmi di cifratura	In caso di utilizzo di algoritmi di cifratura, vengono utilizzati cifrari/algoritmi comunemente riconosciuti come sicuri (es. AES 256, etc.)?	SR 4.3	15
2.1.6	Meccanismi di Load balancing	Vengono utilizzati meccanismi di load balancing al fine di mitigare il rischio di saturazione delle risorse?	SR 7.1 RE 1	10

SCADA Application Protection

Oltre alla protezione dei dispositivi che compongono i sistemi SCADA, è necessario garantire la sicurezza degli applicativi software che permettono il funzionamento del sistema.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
2.2.1	Input Validation	Vengono effettuati dei controlli sugli input inseriti nel sistema (i.e input validation?) Se si, come sono stati configurati i criteri di validazione (es. sono state seguite linee guida OWASP o altre best practice)?	SR 3.5	50
2.2.2	Segregazione logica delle risorse	Il sistema permette la collocazione delle risorse (es. applicativi, sistemi, etc.) in ambienti separati e segregati tra di loro al fine di poter implementare il concetto di "Zones & Conduits"?	SR 5.4	50

Communication Security

I vari *endpoint* che compongono il sistema SCADA devono essere correttamente connessi attraverso un architettura di rete che definisca la topologia delle connessioni e i protocolli utilizzati, sia per le connessioni cablate per le comunicazioni Wireless.

Network Perimeter Protection

La rete dei sistemi SCADA deve essere correttamente segregata secondo il modello *Zones & Conduit* proposto dall'IEC/ISA 62443. L'interazione fra i dati di produzione conservati nell'*Hisotrian* DB e la rete IT aziendale deve avvenire esclusivamente passando attraverso una *Demilitarized Zone*. Inoltre, tutte le comunicazioni devono essere filtrate attraverso Firewall accuratamente configurati.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
3.1.1	Segregazione di rete	La rete del sistema è segregata? Se si, su quali criteri è stata effettuata la segregazione?	SR 5.1	50
3.1.2	Demilitarized Zone	Esiste una DMZ al fine di evitare lo scambio diretto di informazioni tra sistemi OT e IT?	SR 5.1 RE 2	15
3.1.3	Monitoraggio di rete	Se la rete è segregata, le comunicazioni tra le varie zone sono monitorate e controllate (es. tramite IDS/IPS, Firewall, data diodes, etc.)?	SR 5.2	15
3.1.4	Configurazione dei Firewall	Se le comunicazioni sono controllate, i FW sono configurati in modo da bloccare il traffico di default e permetterlo su "base exception" (deny all, permit by exception)?	SR 5.2 RE 1	10
3.1.5	Meccanismi anti DoS/DDoS	Sono presenti meccanismi di difesa da attacchi DoS/DDoS? Il sistema è in grado di funzionare durante un attacco di questa tipologia?	SR 7.1	10

Remote and External Access

Nel caso in cui l'accesso alle HMI ed i Server possa avvenire tramite modalità remota, tali accessi remoti dovrebbero essere opportunamente gestiti.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
3.2.1	Gestione degli accessi remoti	Come vengono gestiti gli accessi remoti ai sistemi (es. uso di VPN, Jump Host, RDP, etc.)?	SR 1.13	70
3.2.2	Approvazione delle sessioni remote	Le sessioni remote avvengono soltanto dopo esplicita approvazione interna?	SR 1.13 RE 1	30

Wired and Wireless Connectivity

Tutte le connessioni cablate e wireless dei sistemi SCADA dovrebbero essere configurate attraverso l'utilizzo di protocolli di rete che permettano di garantire la confidenzialità del dato.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
3.3.1	Configurazione delle reti Wireless	In caso di utilizzo di reti wireless, esse sono state configurate tenendo conto di standard e best practice di settore?	SR 2.2	55
3.3.2	Protocolli di rete	Il sistema di controllo utilizza protocolli che garantiscono l'integrità delle informazioni che vengono trasmesse? (es. OPC UA, Secure Modbus)	SR 3.1	35
3.3.3	Utilizzo di protocolli session-based	Il sistema di controllo utilizza protocolli session-based (es. HTTPS, etc.)? Se sì, sono previsti meccanismi per proteggere l'integrità degli ID di sessione?	SR 3.8	10

Personnel Security

Essendo i sistemi SCADA gestiti direttamente da operatori interni all'azienda, è opportuno che tali operatori siano correttamente formati, attraverso campagne di Training & Awareness, per avere una discreta conoscenza dei principali di rischi legati alla Cyber Security e per essere in grado di eseguire il proprio lavoro seguendo Best Practice e linee guida di sicurezza.

Training

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
4.1.1	Cyber Security Training	E' presente un piano di Training ed Awarness aziendale relativo alle tematiche di Cyber Security svolto anche dai dipendenti OT?	-	25
4.1.2	OT Cyber Security Training	E' presente un piano di Training ed Awarness aziendale relativo alle tematiche di Cyber Security in ambiente OT?	-	50
4.1.3	Esami obbligatori	Il piano di Training e Awarness è seguito da una esaminzione obbligatoria alla quale i dipendenti devono partecipare?	-	25

Configuration Management

I sistemi SCADA dovrebbero essere correttamente configurati, fornendo meccanismi sicuri di identificazione ed autenticazione e configurando le funzionalità di sistema in accordo a Standard e Best Practice di settore.

I sistemi SCADA coinvolgono diverse utenze con ruoli specifici, ognuna delle quali deve avere accesso alle informazioni e alle funzionalità necessarie per svolgere il proprio compito. Le principali utenze che accedono ai sistemi SCADA includono:

- Operatori di sistema: Gli operatori di sistema sono responsabili del monitoraggio in tempo reale delle operazioni del processo industriale. Utilizzano le interfacce utente (HMI) per visualizzare lo stato del sistema, ricevere notifiche sugli allarmi e intervenire manualmente se necessario. Gli operatori possono anche eseguire azioni di controllo e regolazione del processo.
- Ingegneri di controllo e manutenzione: Possono accedere al sistema SCADA per configurare parametri, regolare la logica di controllo, eseguire aggiornamenti del software e pianificare attività di manutenzione preventiva. Hanno spesso accesso più avanzato e possono apportare modifiche al sistema per ottimizzarne le prestazioni.
- Supervisori di produzione: I supervisori di produzione utilizzano il sistema SCADA per monitorare le prestazioni del processo e generare report sull'efficienza operativa. Possono analizzare i dati storici, identificare tendenze e prendere decisioni strategiche per migliorare le prestazioni complessive del sistema.
- Amministratori di sistema: Gli amministratori di sistema sono responsabili della gestione e della manutenzione del sistema SCADA. Possono configurare utenti, applicare patch di sicurezza, gestire la sicurezza e garantire la disponibilità continua del sistema.

È fondamentale che l'accesso a un sistema SCADA sia gestito in modo sicuro e che vengano adottate misure adeguate per proteggere i dati e prevenire l'accesso non autorizzato. La gestione degli account, le politiche di sicurezza e le procedure di autenticazione sono componenti chiave per garantire un utilizzo sicuro e efficace dei sistemi SCADA.

Account Configuration

Le utenze che possono accedere ai sistemi SCADA devono essere correttamente definite da amministratori di sistema e gestite attraverso soluzioni specifiche per la gestione centralizzata delle utenze.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
5.1.1	Gestione centralizzata degli account	È presente un sistema, dedicato all'ambiente OT, che permetta la gestione degli account (es. Active Directory dedicata per rete OT)?	SR 1.3	70
5.1.2	Utenze amministrative	Chi può assegnare, modificare o revocare i privilegi assegnati alle utenze?	SR 2.1 RE 2	30

Identification and Authentication

L'autenticazione ai sistemi da parte degli operatori dovrebbe avvenire attraverso meccanismi di accesso sicuri e strutturati e le password di accesso dovrebbero essere gestire attraverso Policy dedicate e sistemi di gestione centralizzata.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
5.2.1	Autenticazione ai sistemi	Come funziona l'autenticazione degli utenti sul sistema? Vengono utilizzati account univoci e nominali?	SR 1.1	20
5.2.2	MFA	Per gli accessi remoti viene utilizzata l'autenticazione multifattoriale (MFA)? Se si, che tipologia (es. token, SMS, etc.)?	SR 1.1 RE 2	15
5.2.3	Oscuramento degli autenticatori	I sistemi a cui si accede tramite password permettono il mascheramento degli autenticatori (oscuramento della password durante il suo inserimento)?	SR 1.10	10
5.2.4	Numero massimo di tentativi di login	Per le interfacce di accesso al sistema è possibile configurare un numero massimo di tentativi di login falliti (es. fino a 5 tentativi) dopo il quale l'utente deve aspettare un periodi di tempo configurabile prima di effettuare un nuovo tentativo?	SR 1.11	10
5.2.5	Identificazione ed autenticazione M2M (machine to machine)	Il sistema permette di identificare e autenticare i diversi processi e dispositivi che operano e/o scambiano dati con il sistema?	SR 1.2	10
5.2.6	Gestione delle password	Come vengono gestite le password o altri metodi di autenticazione per accedere ai sistemi (es. cambio password di default, modifica periodica delle password, salvataggio delle password, requisiti di complessità)?	SR 1.5	20
5.2.7	Meccanismi di autenticazione hardware	Il processo di autenticazione avviene anche attraverso dispositivi hardware (es. badge)?	SR 1.5 RE 1	10

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
5.2.8	Infrastruttura PKI	Sono utilizzati certificati a chiave pubblica (PKI)? (es. per autenticare i dispositivi, crittografare file) Se sì, come vengono gestiti?	SR 1.8	5

Secure Configuration

Le funzionalità dei dispositivi necessari per il funzionamento del sistema SCADA devono essere configurati tenendo conto di Best Practice e principi di sicurezza, quali:

- Message Of The Day (MOTD)
- Segregation of Duties (SoD)
- Principle of Least Privilege (PoLP)
- Least Functionality

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
5.3.1	MOTD (Message Of The Day)	Sono presenti messaggi/banner che notificano l'utente in merito al corretto uso del sistema (es. durante l'accesso tramite SSH/terminale oppure prima del login su Windows)? Se sì, chi può impostare e modificare tali banner?	SR 1.12	10
5.3.2	SoD (Segregation of Duties) e PoLP (Principle of Least Privilege)	Vengono rispettati i principi di "segregation of duties" e "least priviledge" in fase di assegnazione dei privilegi delle utenze?	SR 2.1	30
5.3.3	Traffico General Purpose	Sono implementati meccanismi per bloccare il traffico general-purpose?	SR 5.3	20
5.3.4	Configurazione sicura dei sistemi	Sono seguite le guidelines di security fornite dai vendor durante la configurazione dei sistemi?	SR 7.6	20
5.3.5	Principio di “Least Functionality”	I sistemi sono stati configurati seguendo il principio di "least-functionality" (es. abilitando solo le porte, protocolli e servizi strettamente necessari)?	SR 7.7	20

Update Security

E’ inoltre necessario che i sistemi SCADA vengano correttamente aggiornamenti, seguendo un processo strutturato di Patch Management che preveda il monitoraggio attivo dei siti web dei fornitori dei software.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
5.4.1	Aggiornamento dei sistemi	Il sistema permette di essere aggiornato? Se si, come avviene il processo di aggiornamento?	HDR 14.5	70
5.4.2	Verifica dell’integrità dei sistemi	Prima di effettuare un update, vene verificata l'autenticità ed integrità dell'aggiornamento (es. attraverso la verifica tramite hash/checksum)?	HDR 14.5 RE 1	30

Detection and Recovery

L'operatività dei sistemi SCADA deve essere garantita attraverso un appropriato processo di Detection e Recovery che preveda:

- Il monitoraggio continuo del traffico all'interno dei sistemi.
- L'identificazione tempestiva di traffico di rete anomalo dovuto a malfunzionamenti, errori involontari e attacchi informatici.
- Il ripristino dei sistemi ad uno stato sicuro ed il mantenimento della continuità operativa.

Continuous Monitoring

Il traffico di rete dovrebbe essere analizzato attraverso soluzioni dedicate per l'analisi del traffico di rete OT. In tale modo è possibile tracciare eventuali attività anomale e risalire alla loro sorgente.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
6.1.1	Non repudiation	Il sistema è in grado tracciare le operazioni effettuate da una determinata utenza (rispettare i principi di "non-repudiation")?	SR 2.12	25
6.1.2	Automatizzazione dei meccanismi di rilevamento di modifiche	Se sono presenti mecccanismi di rilevamento di modifiche apportate alle informazioni ed al software? Se si, essi sono automatizzati e in grado di segnalare in caso di modifica non autorizzata?	SR 3.4 RE 1	25
6.1.3	Analisi del traffico di rete	Il traffico di rete è monitorato con soluzioni specializzate nel monitoraggio del traffico di rete OT?	SR 6.2	50

Log Configuration

I log generati dai sistemi SCADA sono fondamentali per tracciare correttamente lo storico delle attività e degli eventi all'interno dei sistemi.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
6.2.1	Meccanismi di protezione del processo di logging	Sono stati predisposti meccanismi di allarme per segnalare un problema al processo di logging (es. saturazione dello spazio, interruzione della raccolta dei log, etc.)?	SR 2.10	10

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
6.2.2	Timestamps	Ai log di sistema sono associati i corrispondenti timestamps? Se sì, come sono stati configurati? (e.g uso di server NTP)	SR 2.11	10
6.2.3	log di sistema	Vengono registrati i file di log? Se si: - Quali sistemi sono sottoposti a raccolta dei log? - Quali tipologie di log vengono raccolti (es. di sistema, di produzione, etc.)? - Vengono raccolti log in ambito security (es. tentativi di accesso falliti, eventi del sistema di controllo, cambi alle configurazioni, etc.)? - Dove vengono salvati i log?	SR 2.8	30
6.2.4	Gestione centralizzata dei log di sistema	I log di sistema vengono raccolti e analizzati in maniera centralizzata (es. attraverso un SIEM)?	SR 2.8 RE 1	30
6.2.5	Spazio di archiviazione dedicato ai log di sistema	Viene dedicato sufficiente spazio di archiviazione per i log? Vi è un meccanismo di allarme per notificare l'esaurimento dello spazio dedicato al salvataggio dei log?	SR 2.9	10
6.2.6	Protezione dei log di sistema	I file di log sono adeguatamente protetti da accessi non autorizzati, modifiche o eliminazione?	SR 3.9	10

Recovery Capability

I sistemi SCADA dovrebbero essere in grado di essere ripristinati ad uno stato sicuro a seguito di incidente o attacco, al fine di mantenere la continuità operativa.

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
6.3.1	Deterministic Output	Il sistema di controllo è in grado di impostare uno stato sicuro a seguito di malfunzionamenti, attacchi informatici o altre cause che impattino la normale operatività del sistema?	SR 3.6	20
6.3.2	Ripristino dei sistemi ad uno stato sicuro	Il sistema di controllo ha la capacità di essere ripristinato automaticamente ad uno stato sicuro in seguito ad un fallimento?	SR 7.4	50
6.3.3	Contromisure per cali di corrente e blackout	Sono presenti misure per contrastare cali di corrente o blackout (es. tramite UPS, gruppi elettrogeni, etc.)?	SR 7.5	30

Physical Access security

I sistemi SCADA sono sistemi “fisici” e, di conseguenza, soggetti a possibili attacchi di *tampering* e manomissione. Tutti gli asset sui quali è distribuito il sistema SCADA devono essere protetti da accessi non autorizzati attraverso una corretta protezione e gestione degli accesi ai locali in cui sono conservati gli asset, oltre che attraverso l’implementazione di misure di *hardening* fisico dei dispositivi.

SCADA Asset Protection

Tale Sotto-Dominio prevede i seguenti requisiti:

ID Domanda	Tematica	Domanda/e	Rif. ISA 62443	Peso (%)
7.1.1	Meccanismi di accesso fisico ai locali	Come avviene l'accesso fisico ai locali (es. sala server o sala di controllo)? Ci sono meccanismi per registrare gli accessi (es. tramite badge o registro cartaceo)?	-	40
7.1.2	Sistemi di protezione fisica	Sono presenti sistemi di protezione come videosorveglianza o allarme (es. sensori di movimento e anti-intrusione)?	-	30
7.1.3	Protezione delle interfacce di Debug	Vengono utilizzate interfacce per finalità di Debug o testing (es. JTAG debugging)? Se si, sono state adottate contromisure per prevenire utilizzi non autorizzati di tali interfacce?	HDR 14.3	10
7.1.4	Meccanismi di rilevamento dell’accesso alle interfacce di Debug	L'accesso ad interfacce di Debug o JTAG viene registrato all'interno dei log?	HDR 14.3 RE 1	5
7.1.5	Hardening fisico dei sistemi	Sono state adottate contromisure per prevenire l'accesso fisico alle macchine e relative interfacce fisiche (es. porte USB) alle persone non autorizzate?	HDR 14.6	10
7.1.6	Meccanismi di allarme per accessi fisici non autorizzati	Sono presenti meccanismi di allarme per allertare in caso di accessi fisici non autorizzati?	HDR 14.6 RE 1	5

7. APPLICAZIONE DEI FRAMEWORK A DUE REALTA' INDUSTRIALI ED ILLUSTRAZIONE DEI PRINCIPALI RISULTATI

Successivamente alla definizione dei OT Security Framework e SCADA Security Framework descritti nei procedenti capitoli, è stato possibile applicare operativamente tali Framework nel contesto di due progettualità eseguite presso realtà industriali rilevanti. In particolare, l'OT Security Framework è stato applicato ad uno stabilimento produttivo di una importante azienda multinazionale operante nel settore Food & Beverage. Lo SCADA Security Framework è stato invece applicato al sistema SCADA centrale di una azienda italiana operante nel settore Utilities (distribuzione dell'acqua pubblica). Tali progettualità hanno quindi permesso di validare l'effettiva funzionalità dei Framework definiti, oltre che delineare parzialmente lo stato dell'arte in cui si ritrova il panorama industriale relativamente all'OT Security.

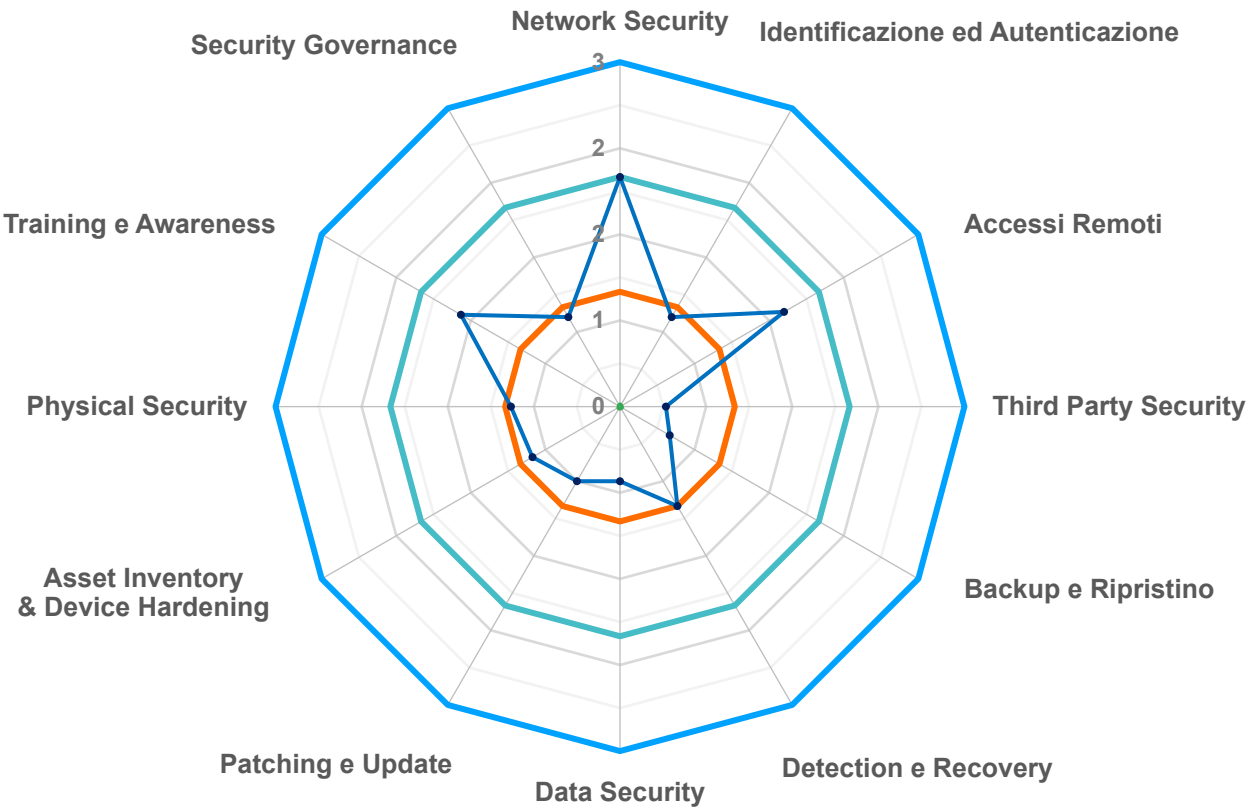
Di seguito, saranno illustrati i principali risultati emersi dell'applicazione dei due Framework definiti.

Applicazione dell'OT Security Framework ad una realtà industriale nel settore Food & Beverage

L'attività progettuale svolta presso l'azienda in analisi ha previsto l'esecuzione di un OT Security Audit presso lo stabilimento produttivo aziendale più all'avanguardia in termini di Cyber Security, al fine di valutare lo stato complessivo delle misure di OT Security messe in atto ed identificare eventuali aree di miglioramento. Tale attività ha richiesto sia l'esecuzione di interviste da remoto con le figure chiave del Plant (Plant Director, Technical Area Manager, Automation manager), sia lo svolgimento di una visita ispettiva presso lo stabilimento per valutare l'effettiva implementazione delle misure di sicurezza individuate.

Overview dei risultati

Le attività svolte hanno messo in luce un'interesse ed una attenzione generale relativamente alle tematiche di OT Security. L'azienda presenta una funzione interna dedicata alla gestione della OT Cyber Security e sono attivamente eseguite attività di Assessment, accompagnate dalla definizione ed implementazione delle relative attività di rimedio identificate. Essendo però tale piano di OT Security iniziato solo negli ultimi anni, molte aree dell'OT Security Framework risultano ancora parzialmente scoperte e con evidenti lacune. Dal grafico a Radar di seguito illustrato che illustra il livello di copertura dei Domini del Framework è infatti possibile notare la presenza di alcune "punte di diamante" (Network Security, Accessi Remoti, Training & Awareness), coincidenti proprio con le aree a cui è stata data maggior attenzione alle tematiche di OT Security, accompagnate però da una scarsa implementazione di misure di sicurezza relative ai restanti Domini.



0 : Non Implementato | 1 : Implementato Ad-Hoc | 2 : Implementato | 3 : Ottimizzato

Di seguito, vengono descritti con un maggiore dettaglio i risultati emersi relativamente ad ogni Dominio dell'OT Security Framework.

Network Security

La rete OT è segregata e segmentata secondo un Blueprint di rete aziendale e le comunicazioni vengono filtrate attraverso diversi livelli di Firewall che prevedono un Firewall IT, un Firewall OT ed una serie di Firewall di cella. Su tali Firewall non risultano essere presenti misure di protezione da attacchi DoS/DDoS.

Nel Plant risultano essere presenti due reti Wi-Fi, una per la manutenzione ed una utilizzata per i lettori di codici a barre di magazzino. Entrambe tali reti sono configurate secondo lo Standard WPA2 con chiave pre-condivisa (WPA2-PSK) che risulta essere insicuro e obsoleto, in quanto potrebbe essere soggetto ad attacchi che catturino l'handshake fra i dispositivi.

Identificazione ed Autenticazione

E' stata rilevata l'assenza di un sistema di gestione delle utenze centralizzato (es. Active Directory) dedicato all'ambiente OT. Infatti, attualmente l'accesso ai sistemi OT avviene localmente e l'attuale modello di autenticazione prevede l'utilizzo di utenze generiche di tre tipologie: operatore, manutentore e admin. Non è stato rilevato l'utilizzo di account nominali con privilegi definiti in linea

con le mansioni svolte. Inoltre, è stata rilevata la presenza di un file Excel ove sono ubicate le credenziali per accedere ad alcuni sistemi OT.

Accessi Remoti

La procedura per gli accessi remoti prevede l'utilizzo di un virtualizzatore di tipo 2 contenente diverse macchine virtuali dedicate ai vari fornitori. La configurazione di rete prevede la terminazione della connessione VPN nella stessa VLAN delle VM, il fornitore accede quindi alla rete di Plant tramite la VM dedicata. Per accedere alla VPN è previsto un meccanismo di Multi-Factor Authentication (MFA), ma non è necessaria un'approvazione interna per le sessioni remote e non è previsto un periodo di time-out di sessione per le macchine virtuali.

Third Party Security

Pur non essendo presente una lista puntuale dei fornitori, tutti i fornitori che abitualmente accedono allo stabilimento sono segnalati all’interno di un sistema di sicurezza centralizzato. Inoltre non risultano essere stati associati degli owner a ciascun fornitore.

In ambito ISO 27001, nel momento in cui sono definiti o rinnovati i contratti con i fornitori di beni o servizi IT, vengono utilizzati contratti standard e specifiche checklist per assicurare che le necessarie clausole di sicurezza delle informazioni siano incluse nei contratti con i fornitori (es. ruoli e responsabilità, SLA, modalità di accesso remoto e aggiornamenti dei sistemi, etc.).

Al momento non sono definite simili checklist per la gestione dei contratti con i fornitori di sistemi e servizi in ambito OT.

Backup e ripristino

Attualmente è stato rilevato che le attività di backup vengono effettuate in maniera Ad-Hoc, nel momento in cui è necessario ad esempio cambiare delle configurazioni dei sistemi. In questo caso, la prassi prevede il salvataggio manuale delle informazioni (es. logica PLC, architetture di rete, etc.) su uno spazio SharePoint dedicato. Non risultano quindi essere definite procedure o soluzioni automatizzate per la gestione dei backup.

Detection & Recovery

Il traffico di rete OT viene analizzato da una soluzione dedicata (Nozomi) e gli Alert generati vengono monitorati tramite il SIEM, gestito da un team SOC con capacità OT.

Attualmente, le log sources relative ai sistemi OT risultano essere quelle di Nozomi e del Firewall di supervisione. I log degli altri dispositivi OT (es. Firewall OT, PLC, HMI, Scada, etc.) non sono al momento raccolti.

Non si ha evidenza che l'organizzazione abbia predisposto un piano di Disaster Recovery e relativo processo di "lesson learned" a seguito di un "outage". Inoltre, non si ha evidenza che

all'interno del perimetro del Plant vi siano meccanismi per rispondere ad eventuali blackout prolungato dell'energia elettrica.

Data Security

Fatto salvo avere evidenza di un meccanismo di protezione (Microsoft Information Protection) del dato per quanto concerne informazioni sensibili presenti all'interno del Plant (es. ricette, parametri di produzione, etc.), non si rilevano ulteriori meccanismi di protezione.

Più in generale, viene utilizzato utilizza Microsoft Information Protection come soluzione di Data Loss Prevention, con il relativo sistema di tagging e classificazione dei documenti.

Patching & Update

Non risulta essere presente un piano di Patch Management strutturato. Gli aggiornamenti vengono eseguiti in modalità Ad-Hoc e solo quando strettamente necessario per motivi di operatività.

Asset Inventory & Device Hardening

Risulta essere presente un sistema di OT Asset Inventory sviluppato internamente. Tale Asset Inventory viene aggiornato manualmente dalle funzioni TAM & Automation per tutte le nuove linee e sono in corso le attività di tracciamento dei sistemi esistenti. In particolare vengono inserite informazioni quali ad esempio: stabilimento, modello del dispositivo, vendor e ownership del dispositivo.

Sui sistemi OT non risulta essere stata implementata una soluzione di Antivirus/EDR.

Gli apparati di rete (es. Firewall OT) risultano essere configurati in linea con Standard e Best Practice, mentre al momento non risultano essere applicate particolari misure di hardening sui dispositivi OT.

In particolare, non sono state definite le seguenti misure:

- Numero massimo di tentativi di login
- Rilevazione automatizzata di modifiche non autorizzate
- Dismissione sicura dei sistemi
- Verifica dell'Integrità dei componenti
- Input Validation
- Banner di utilizzo
- Principio di Least Functionality
- Hardening fisico dei dispositivi

Physical Security

Sono state rilevate le seguenti misure di Physical Security:

- Sistema di videosorveglianza con copertura parziale del Plant (aree ingresso e carico/scarico).
- Single-entry-point che garantisce il passaggio di tutto il personale, interno ed esterno, da un singolo punto di passaggio.
- Presenza di una Policy che governa gli accessi di personale interno ed esterno al Plant.
- Aree sensibili (es. Sala Server IT/OT) protette da serrature, la cui chiave è custodita in reception.

Tuttavia è emerso che è possibile uscire dai tornelli senza registrare l'uscita e rientrate successivamente. Inoltre, i badge assegnati possono essere potenzialmente copiati ed utilizzati da personale estraneo per accedere la Plant.

Training e awareness

Risulta essere presente un programma di training generico in ambito Cyber Security erogato annualmente a tutto il personale del Plant, per il quale saranno integrate anche tematiche di OT Cyber Security. Il Plant è stato il primo fra tutti i Plant aziendali ad effettuare il pilota del programma di Training dedicato all’ambito di OT Cyber Security. Non sono tuttavia previsti esami dedicati al termine di entrambi i programmi di formazione.

Security Governance

Al momento, non risulta essere presente un Framework documentale dedicato alla gestione delle tematiche di OT Security. Tuttavia sono in corso di definizione alcune procedure specifiche da applicare in casi particolari (es. procedura di accesso remoto).

Le Job Description del Technical Area manager, del responsabile di Automazione e del Plant Director non definiscono chiaramente le loro responsabilità in termini di sicurezza informatica dei sistemi dei plant (es. gestione utenze, backup, hardening and patching, gestione e segnalazioni incidenti, rapporti con le terze parti, gestione accessi remoti, etc.)

Non risultano essere eseguiti Risk Assesment periodici, ma vengono prese in considerazione le criticità emerse dai Security Assesment eseguiti precedentemente da Terze Parti.

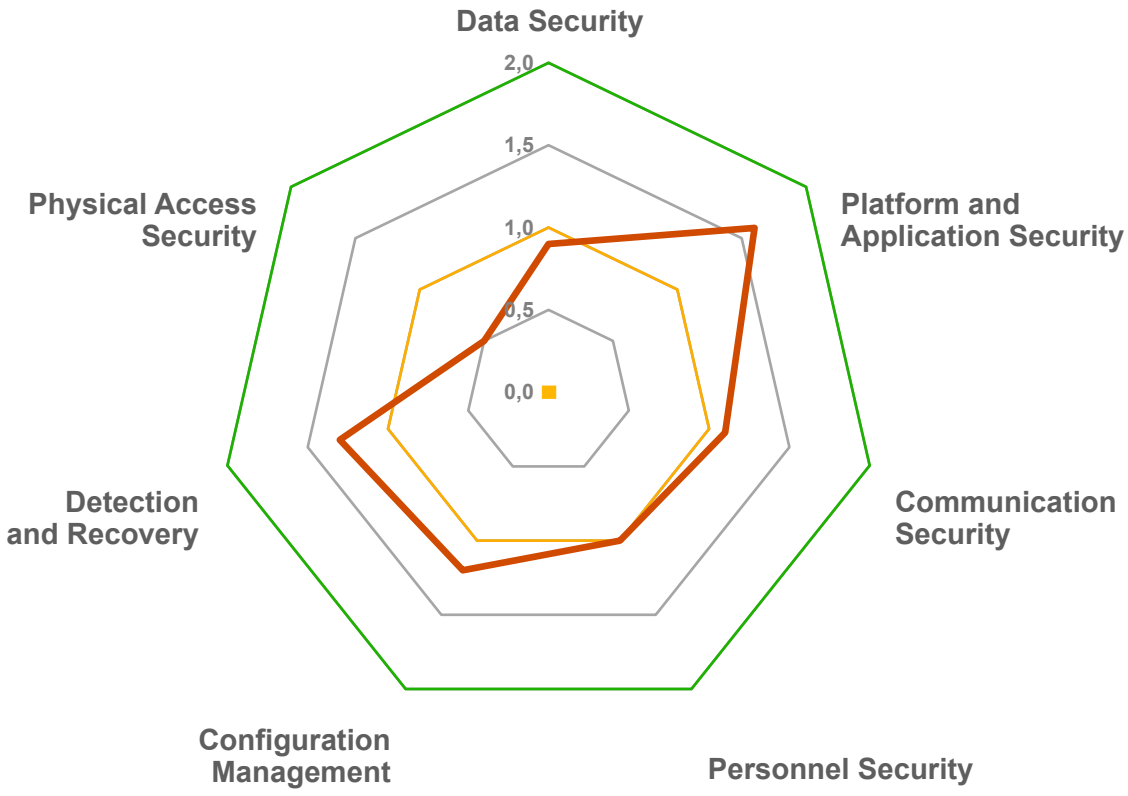
Applicazione dello SCADA Security Framework ad una realtà industriale nel settore Utilities

L'attività progettuale svolta presso l'azienda in analisi ha previsto l'esecuzione di un OT Security Assessment al fine di valutare lo stato complessivo delle misure di OT Security messe in atto per proteggere il sistema SCADA centrale dell'azienda, responsabile del trattamento dell'acqua, ed identificare eventuali aree di miglioramento. Tale attività ha richiesto l'esecuzione di interviste da remoto con le figure chiave mi ambito OT, responsabili della gestione del sistema SCADA.

Overview dei risultati

Dalle attività svolte è emersa la presenza di alcune misure di sicurezza applicate al sistema SCADA centrale, dimostrando una certa attenzione relativamente alle tematiche di OT Security. Ciò nonostante, come osservabile nel grafico di seguito illustrato, le misure implementate non sono sufficienti per garantire un buon livello di Security e, nel caso dei Domini Data Security e Physical Access Security, sono presenti grave lacune di sicurezza.

Rispetto all'analisi svolta relativamente all'altra progettualità, la situazione generale presenta un livello di Cyber Security non brillante, ma abbastanza stabile e con meno "dislivelli" rispetto al precedente caso.



0 : Non Implementato | 1 : Parzialmente Implementato | 2 : Implementato

Di seguito, vengono descritti con un maggiore dettaglio i risultati emersi relativamente ad ogni Dominio dello SCADA Security Framework.

Data Security

È stato rilevato che, nonostante esista una soluzione di backup, essa non comprende tutte le componenti del sistema SCADA centrale (ma solo alcuni server). Inoltre, è stato evidenziato come il backup di alcune informazioni essenziali venga effettuato localmente e in maniera manuale. Non si ha evidenza infine di attività di verifica dell'integrità dei backup e di attività di test di restore.

Non sono state rilevate misure di protezione dei dati in quanto non vi è una Policy che governi la classificazione e trattamento dei dati confidenziali.

Durante la fase di decomissioning dei dispositivi, il processo prevede l'eliminazione in maniera sicura dei dati contenuti in essi e la distruzione dei supporti su cui sono salvati.

Infine è stato rilevato che, nonostante venga utilizzata una soluzione di Antivirus, essa non sia abilitata sulle componenti del sistema SCADA centrale in quanto risulta entrare in conflitto con alcuni processi della piattaforma.

Platform and Application Security

È emersa la presenza di un inventario (asset inventory) delle diverse componenti del sistema SCADA centrale.

Non vengono effettuati controlli in merito all'integrità delle componenti prima dell'avvio delle macchine (verifica dell'integrità del BIOS/UEFI).

Risultano essere utilizzati dei Tablet al fine di permettere agli operatori in campo di collegarsi remotamente al sistema SCADA centrale. Tale procedura avviene tramite VPN che permette al Tablet di raggiungere alcuni client predisposti agli accessi remoti. Tali tablet vengono gestiti centralmente tramite una soluzione di MDM (Mobile Device Management).

Non si ha evidenza dell'utilizzo di meccanismi che permettano di distribuire il traffico di rete in maniera equa sulle risorse disponibili per evitare la degradazione delle prestazioni del sistema SCADA centrale.

Communication Security

La rete del sistema SCADA centrale risulta essere segregata dal resto dell'infrastruttura di rete. È stata riscontrata la presenza di più Firewall dedicati alla protezione della rete SCADA centrale, di stabilimento e dei diversi Plant. Non è stata rilevata però un'attività di revisione periodica delle regole di tali Firewall.

Non risultano essere presenti contromisure specifiche per prevenire attacchi di tipo DoS (Denial of Service) o DDoS (Distributed DoS), che mirano a rendere indisponibile l'infrastruttura di rete.

Gli accesi remoti ai sistemi OT avvengono tramite tecnologia VPN. Per raggiungere remotamente il sistema SCADA centrale sono stati previsti dei *client ad-hoc* per svolgere questa mansione. Non sono utilizzate soluzioni dedicate per la gestione sicura degli accessi remoti.

Sono presenti reti wireless tramite le quali è possibile raggiungere i sistemi dello SCADA centrale. Tali reti non risultano essere sufficientemente protette (uso di WPA2 con password condivisa).

Personnel Security

È stato rilevato un piano di Training & Awareness relativo ai principali temi di Cyber Security. Tale programma prevede, oltre alle attività di formazione, anche l'esecuzione di più campagne di Phishing.

Nonostante in questo programma siano coinvolti anche i dipendenti OT, non sono state rilevate sessioni Ad-Hoc per sensibilizzare in merito alle tematiche di OT Cyber Security (es. sessioni di OT Incident Simulation o esercizi Table Top).

Configuration Management

Per autenticarsi sul sistema SCADA centrale, gli operatori accedono prima sui Client attraverso le loro credenziali di dominio personali. Ogni profilo del sistema SCADA ha un set di permessi diversi da quelli dell'utenza di dominio.

Relativamente gli accessi remoti, l'autenticazione si basa sulle credenziali di dominio e non è prevista l'autenticazione multifattoriale.

Il sistema è stato sviluppato e configurato internamente, seguendo le direttive e guideline del Vendor e seguendo i principi di di "Least Functionality" e "Segregation of Duties".

Gli aggiornamenti di sistema vengono effettuati solo a fronte di vulnerabilità significative o al presentarsi di importanti problematiche. È stata rilevata in uso una versione della System Platform non più supportata dal Vendor (versione in uso: 2017; ultima release: 2023).

Detection and Recovery

Il traffico di rete OT risulta essere monitorato tramite soluzioni specializzate nell'analisi del traffico industriale (Nozomi). Tuttavia, non è stata rilevata una raccolta dei log strutturata. I log generati dal sistema SCADA centrale vengono analizzati sporadicamente e soltanto per fini diagnostici, e non di sicurezza. In merito ai log del sistema operativo, essi vengono raccolti localmente con le modalità, tempistiche e configurazioni di default. Entrambe le tipologie di log raccolti non sono protetti da eliminazione o manomissione e risultano accessibili a chiunque abbia le credenziali per accedere alla macchina.

Nonostante sia stata rilevata la presenza di un SIEM (IBM QRadar), tale soluzione raccoglie e analizza solamente i log relativi ai server. Risultano scoperti i Client e i log applicativi generati dal sistema SCADA centrale.

Infine, non è stata rilevato un piano di Disaster Recovery che permetta di riprendere l’operatività anche in caso di perdita della sala di telecontrollo o del sistema SCADA centrale.

Physical Access Security

L'accesso alla sala server è adeguatamente protetto da accessi non autorizzati (es. doppia porta, etc.), ma non è stata ricevuta alcuna evidenza della presenza di meccanismi per limitare e registrare gli accessi alla sala telecontrollo.

Non sono state rilevate misure di sicurezza fisiche come la videosorveglianza e sistemi di allarme anti-intrusione dedicate alla protezione della sala di telecontrollo.

Non sono state rilevate misure per proteggere i client presenti in sala di telecontrollo da accessi fisici non autorizzati e manomissioni (misure di anti-tampering).

8. CONCLUSIONI

In questa tesi sono stati definiti due Framework di sicurezza da applicare ai sistemi industriali. Per fare ciò, è stato prima necessario introdurre le principali tematiche relative alla sicurezza dei sistemi industriali, ovvero:

- Una panoramica sul contesto industriale odierno (Capitolo 2).
- Una descrizione dell'ecosistema industriale in tutte le sue componenti, con un riferimento al modello architetturale definito dal *Purdue Model* (Capitolo 3).
- Un'illustrazione dei principali vettori di attacco ai quali può essere soggetto un sistema industriale, ed il loro relativo collocamento all'interno dell'architettura del *Purdue Model* (Capitolo 3).
- Una panoramica sull'attuale Standard di riferimento per l'OT Security, ovvero l'IEC/ISA 62443, con relativo focus sulla sezione 3-3 e sul concetto di *Functional Requirement* e *System Requirement* (Capitolo 4).

Una volta illustrati i concetti essenziali al fine della definizione dei Framework di sicurezza, è stato quindi possibile dettagliare il processo di definizione e la struttura dell'OT Security Framework (Capitolo 5) e dello SCADA Framework (Capitolo 6). Il primo Framework vuole offrire una check-list completa che permetta di valutare l'OT *Security Posture overall* di uno stabilimento industriale, valutando l'implementazione di controlli di sicurezza relativi a tutte le tematiche (Domini) di OT Security. Attraverso lo SCADA Security Framework, è invece possibile valutare lo stato di sicurezza dei sistemi SCADA, con controlli e Domini specifici per tali tipologie di sistemi.

Dopo aver approfonditamente dettagliato i Framework di sicurezza definiti, è stata mostrata una loro effettiva applicazione durante le attività di Audit e Assessment presso due importanti realtà industriali operanti nel settore Food & Beverage e Utilities (Capitolo 7). Sono stati quindi illustrati i principali risultati emersi dall'applicazione di tali Framework, permettendo di delineare un'approssimativa sagoma dell'attuale livello di sicurezza all'interno degli stabilimenti industriali.

9. BIBLIOGRAFIA E SITOGRAFIA

- Framework for SCADA Security Policy, Dominique Kilman and Jason Stamp, 2005
- IEC 62443 3-3, IEC, 2013
- IEC 62443 4-2, IEC, 2019
- Using ISA/IEC 62443 Standards to Improve Control System Security, Tofino Security, 2014
- Industrial Cybersecurity (Prima edizione), Pascal Ackerman, 2017
- Industrial Cybersecurity (Seconda edizione), Pascal Ackerman, 2021

- “Industry 1.0 To 4.0 – Brief History Of The Industrial Revolution”, https://sustainability-success.com/industry-1-0-to-4-0-2-3-revolution/
- “Difference between OT and IT networks" https://www.geeksforgeeks.org/difference-between-ot-and-it-networks/
- “What Is the Purdue Model for ICS Security?" https://www.zscaler.it/resources/security-terms-glossary/what-is-purdue-model-ics-security
- “Structuring the ISA/IEC 62443 Standards" https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards
- “The Ultimate Guide to Protecting OT Systems with IEC 62443” https://verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/

Dedico un ringraziamento finale al mio collega Andrea, che mi ha introdotto al magnifico mondo dell'OT Security e mi ha supportato durante la definizione dei Framework, e ad Alessandro, il mio Manager, che mi ha aiutato ad introdurmi nel mondo del lavoro.

Infine, un ringraziamento a tutto il team Cyber di Bologna, che mi ha permesso di passare un bellissimo anno lavorativo.