UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA INDUSTRIALE

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA DELLA SICUREZZA CIVILE ED INDUSTRIALE

Tesi di Laurea Magistrale in Ingegneria della Sicurezza Civile ed Industriale

ANALISI DEL RISCHIO E SICUREZZA INFORMATICA DELLE MACCHINE: IL CASO STUDIO DI UNA LINEA PRODUTTIVA IN AMBITO MANIFATTURIERO

Relatore: Ing. Lorenzo Baraldo

Laureanda: LISA TESCHIONI

ANNO ACCADEMICO 2022-2023

Riassunto

La tesi è nata con l'obbiettivo di effettuare la valutazione dei rischi di una linea produttiva manifatturiera, costituita da un trasloelevatore e diverse macchine periferiche, nell'ipotesi in cui un cyber attacco comportasse un blocco in uno stato non previsto, riavvio inatteso o funzionamento imprevisto delle macchine costituenti la linea.

La valutazione dei rischi, al solo fine di salvaguardare la sicurezza delle persone, è stata eseguita seguendo il processo fornito dallo standard IEC 62443-3-2, il quale evidenzia due tipologie di analisi: una prima analisi del rischio eseguita sugli asset industriali al fine di identificare quali di questi comportino conseguenze critiche per le persone e quindi, necessitano di un approfondimento attraverso una seconda analisi, l'analisi del rischio di dettaglio. Quest'ultima analisi prevede un'indagine delle vulnerabilità del sistema e del livello di sicurezza attualmente presente.

In questo modo è stato possibile individuare i punti e le modalità di intervento per la mitigazione del rischio, ovvero una lista di contromisure da applicare affinché sia ridotta la probabilità che un attacco informatico abbia successo. Questo ha permesso la riduzione del livello di rischio ad un livello tollerabile dall'organizzazione.

Indice

Introduzione

L'industria 4.0 anche nota come quarta rivoluzione industriale, è resa possibile dalla nascita e dall'adozione di nuove tecnologie edge all'avanguardia che confondono il confine tra l'*Information Technology* (IT) e l'*Operational Technology* (OT), per portare la trasformazione digitale nei reparti di produzione.

Fino a qualche anno fa l'*Information Technology* (IT) e l'*Operational Technology* (OT) erano mondi completamente separati con obbiettivi molto diversi: la missione principale dell'OT era (ed è) la continuità operativa delle macchine e degli impianti, mentre il focus principale dell'IT è sempre stato orientato all'efficienza e alla sicurezza della rete informatica aziendale.

Il vantaggio principale dell'integrazione di sistemi IT e OT è il miglioramento dei processi, ma inevitabilmente porta con sé nuove minacce e nuovi rischi. Se una volta un attacco informatico poteva colpire esclusivamente i sistemi informatici ora è raggiungibile anche la macchina.

A dimostrazione dell'attualità del problema di cyber attacchi è possibile fare riferimento al Rapporto Clusit 2023, ovvero un rapporto redatto da parte dell'Associazione Italiana per la sicurezza informatica, il quale evidenzia come in Italia i cyber attacchi siano in aumento:

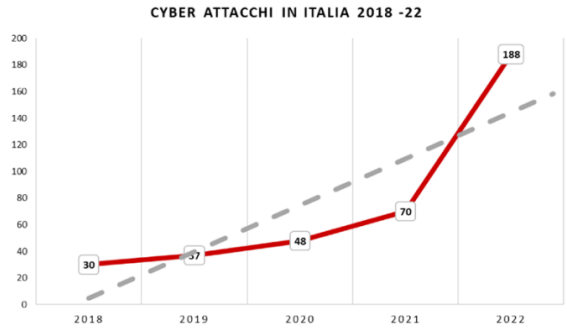


Figura 1: *Andamento dei cyber attacchi in Italia dal 2018 al 2022, rif. Rapporto Clusit 2023*

Esaminando poi i settori attaccati è presente sul podio il settore governativo seguito a brevissima distanza dal comparto manifatturiero.

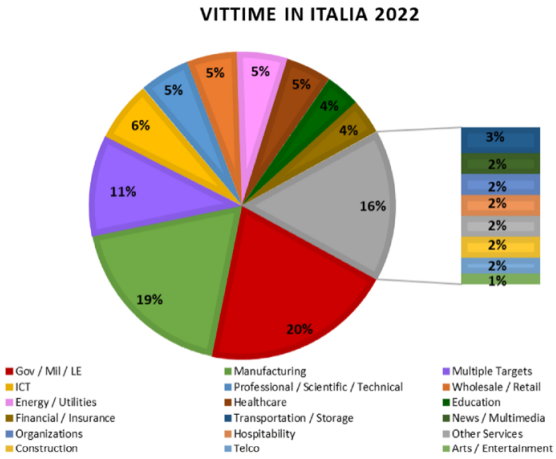


Figura 2: *Percentuale delle vittime di cyber attacchi in Italia nel 2022*
Rif. Rapporto Clusit 2023

Di conseguenza il rischio è presente ed attuale.

Andando poi ad analizzare il panorama normativo ci si trova di fronte al nuovo Regolamento (UE) 2023/1230, il quale stabilisce i requisiti di sicurezza e di tutela della salute per la progettazione e la costruzione di macchine, prodotti correlati e quasi macchine al fine di consentire la loro messa a disposizione sul mercato o la loro messa in servizio.

Tale regolamento ha subito un'evoluzione rispetto alla precedente Direttiva 2006/42/CE, portandosi al passo delle tecnologie attualmente presenti nelle industrie, una modifica sostanziale si ha con l'aggiunta nell' Allegato III del punto 1.1.9 "Protezione dall'alterazione", ove si cita:

"...I componenti hardware che trasmettono segnali o dati, importanti per il collegamento o l'accesso a software che sono fondamentali affinché la macchina o il prodotto correlato rispettino i pertinenti requisiti essenziali di sicurezza e di tutela della salute, devono essere progettati in modo tale da essere adeguatamente protetti da un'alterazione accidentale o intenzionale..."

"...Software e dati critici per il rispetto da parte della macchina o del prodotto correlato dei pertinenti requisiti essenziali di sicurezza e di tutela della devono essere individuati come tali e devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale..."

Evidenziando la necessità di una protezione di componenti software e hardware a cui la macchina è collegata.

Sulla base di queste considerazioni nasce questa tesi, con l'obbiettivo di effettuare su una specifica linea produttiva manifatturiera la valutazione dei rischi di un cyber attacco. Dove i possibili danni derivanti possono essere di diverso genere: di tipo immateriale, andando a ledere la privacy ed il patrimonio intellettuale dell'azienda, di tipo materiale date dal fermo produttivo e dal conseguente tempo e denaro necessario alla ripresa della produzione, danni nei confronti dell'ambiente, ma soprattutto vi può essere danno per le persone ed è su quest'ultimo punto che sarà focalizzata la tesi.

Il primo passo per affrontare il problema è la presa di coscienza di un possibile attacco cyber.

Successivamente risulta efficace contro qualunque attacco cyber l'analisi dell'infrastruttura di automazione e la definizione di quali conseguenze comporterebbe un attacco verso ciascuna macchina, zona produttiva o stabilimento.

Questo tipo di analisi aiuta le aziende a comprendere quale sia l'estensione realistica del problema e a dare una priorità alle modifiche dell'infrastruttura, in base alla gravità delle conseguenze che ci si possono aspettare.

Solo partendo dall'analisi dell'effettivo rischio informatico è possibile procedere ad investigare nel dettaglio quali specifiche contromisure adottare in maniera puntuale o diffusa, con un adeguato compromesso tra costi e benefici.

A questo punto entra in gioco la Cyber Security, ovvero l'insieme dei mezzi volti alla protezione dei sistemi informatici, costituita da elementi tecnici, organizzativi, giuridici e umani; tutti elementi utili per valutare, implementare e mantenere nel tempo la protezione dei sistemi e l'integrità dei dati condivisi. La Cyber Security è soprattutto un processo iterativo, che necessita di essere monitorato ed assestato costantemente attraverso azioni di mantenimento**.** Solo così il flusso di dati condivisibili verso l'esterno sarà al sicuro dalle minacce informatiche, evitando così conseguenze disastrose per le aziende

Il riferimento da adottare è lo standard internazionale IEC 62443**:** l'unica vera difesa orientata al mondo dell'automazione di fabbrica che oggi può essere messa in atto per la security dei dispositivi industriali.

La tesi sarà costituita da quattro capitoli, nel primo capitolo verrà presentato lo standard IEC 62443 e il Regolamento (UE) 2023/1230 che andrà a sostituire la Direttiva 2006/42/CE, nel

secondo e terzo capitolo sarà presentata la valutazione dei rischi, una prima analisi che ha lo scopo di individuare dove si ha un maggiore danno per le persone ed una seconda analisi più dettagliata che mira ad individuare le vulnerabilità degli asset informatici e le possibili contromisure da porre in atto. Si termina con un ultimo capitolo conclusivo.

Capitolo 1

Il Regolamento (UE) 2023/1230 e lo standard IEC 62443

In questo capitolo verrà presentata la normativa europea di settore e lo standard IEC 62443 utilizzato come riferimento per la stesura e la produzione della tesi.

1.1 Regolamento (UE) 2023/1230

Il Regolamento (UE) 2023/1230 stabilisce i requisiti di sicurezza e di tutela della salute per la progettazione e la costruzione di macchine, prodotti correlati e quasi macchine al fine di consentire la loro messa a disposizione sul mercato o la loro messa in servizio.

Il 29 giugno 2023 è stato ufficialmente pubblicato nella gazzetta ufficiale dell'Unione Europea il testo del nuovo Regolamento (UE) 2023/1230 che andrà a sostituire la Direttiva 2006/42/CE.

A seguito della rettifica pubblicata il 4 luglio 2023, il nuovo regolamento macchine verrà applicato a partire dal 20 gennaio 2027**,** ovvero 42 mesi dopo la data di entrata in vigore, e in pari data verrà abrogata l'attuale Direttiva 2006/42/CE.

Il Regolamento si pone l'obiettivo di rispondere all'avanzamento tecnologico con una serie di nuovi presidi che investiranno ampie aree settoriali.

La scelta di adottare un regolamento anziché una direttiva consentirà un'attuazione più uniforme, riducendo i ritardi nel recepimento e le differenze di interpretazione tra gli stati membri.

Le norme del regolamento si applicano a: macchine, quasi-macchine, attrezzature intercambiabili, componenti di sicurezza (compresi software), accessori per il sollevamento, catene, funi, imbragature e dispositivi di trasmissione meccanica rimovibili.

Le principali novità del nuovo regolamento:

1. Modifiche sostanziali alle macchine: il nuovo regolamento si applica anche a prodotti che hanno subito "modifiche sostanziali" tali da influenzarne la conformità ai requisiti di sicurezza.

Nello specifico si applica su modifiche:

- effettuate con mezzi fisici o digitali dopo che il prodotto è stato immesso sul mercato o messo in servizio
- che non sono previste o pianificate dal fabbricante
- che influenzano la sicurezza creando un nuovo pericolo o aumentando un rischio esistente in modo da richiedere l'adozione di: ripari o dispositivi di protezione aggiuntivi, il cui controllo modifica il sistema di comando legato alla sicurezza esistente, o misure di protezione aggiuntive per garantire la stabilità o la resistenza meccanica

In caso di modifiche di questo tipo, il soggetto che le apporta deve osservare e soddisfare tutti gli obblighi previsti dal regolamento per i fabbricanti. Deve quindi analizzare i rischi della macchina, durante l'intero ciclo di vita, considerando aggiornamenti e sviluppi futuri.

2. Il nuovo regolamento introduce la figura dell'importatore e del distributore.
L'importatore è il soggetto che immette sul mercato dell'Unione europea un prodotto proveniente da un paese terzo. Tale soggetto è responsabile della conformità del prodotto e ne risponde in prima persona, inoltre deve assicurarsi che il fabbricante abbia portato a termine le appropriate procedure per la valutazione della conformità del prodotto e deve indicare sul prodotto il proprio nome, indirizzo postale ed indirizzo di posta elettronica.
Il distributore è un soggetto, diverso da fabbricante ed importatore, che mette a disposizione sul mercato un prodotto. Tale soggetto verifica che il prodotto sia correttamente identificato e accompagnato dalla documentazione necessaria e nella dovuta diligenza nel trasporto in modo da non compromettere la conformità ai requisiti di sicurezza.
3. Nel campo di applicazione del nuovo regolamento macchine rientrano i "componenti di sicurezza" che andranno marchiati CE. Tra questi componenti rientreranno anche i componenti digitali, compresi i software. Di conseguenza il software che svolge funzioni di sicurezza immesso sul mercato separatamente dovrà essere marcato CE ed essere accompagnato da una dichiarazione di conformità UE e da istruzioni per l'uso.

4. La documentazione potrà essere fornita in formato digitale, ad esempio rendendola disponibile su un sito internet.
Per quanto concerne la lingua delle informazioni e della documentazione (istruzioni per l'uso, dichiarazione di conformità UE, etc..) essa dovrà essere facilmente comprensibile agli utilizzatori e alle autorità di sorveglianza sul mercato e verrà definita da ogni stato membro.
5. Il nuovo regolamento macchine si applica ai sistemi che utilizzano tecnologie di intelligenza artificiale per gli aspetti che riguardano le possibili influenze sulla sicurezza delle macchine.

In particolare, la valutazione dei rischi dovrà tenere conto dell'evoluzione del comportamento delle macchine progettate per funzionare con diversi livelli di autonomia.

Anche la fase di apprendimento deve essere considerata, limitando il comportamento della macchina, mediante adeguati circuiti di sicurezza, in modo da non oltrepassare i limiti considerati nella valutazione dei rischi.

Infine, anche nei requisiti essenziali di sicurezza e di tutela della salute applicabili alle macchine mobili sono state inserite parti specifiche per le macchine mobili autonome, ovvero senza guidatore; questi prodotti (chiamati AGV) sono sempre più diffusi e stanno soppiantando la movimentazione manuale di oggetti nei più disparati settori, dalle linee produttive, ai magazzini, agli ospedali.

6. La sicurezza informatica è un aspetto che non può più essere trascurato per le macchine poiché oggigiorno la maggioranza delle macchine sono connesse alla rete e possono essere oggetto di attacchi informatici.
Per questo motivo il nuovo regolamento macchine chiede che i circuiti di comando che svolgono funzioni di sicurezza siano progettati in modo da evitare che attacchi malevoli possano causare comportamenti pericolosi delle macchine.

È stato inoltre introdotto un nuovo requisito essenziale di sicurezza e di tutela della salute esplicitamente dedicato alla protezione dei sistemi informatici contro la corruzione.

Nella valutazione dei rischi e nell'individuazione di dispositivi di protezione specifici bisogna considerare la coesistenza di uomo e macchina in uno stesso spazio come avviene nelle applicazioni con robot collaborativi (o cobot). Il requisito essenziale di sicurezza e di tutela

della salute relativo ai rischi dovuti agli elementi mobili è stato quindi modificato per tenere conto delle nuove soluzioni da adottare per garantire la sicurezza delle persone in applicazioni collaborative, tenendo in considerazione anche gli aspetti di stress psicologico che queste situazioni lavorative possono arrecare.

7. La dichiarazione CE di conformità viene sostituita nel nuovo regolamento macchine da una dichiarazione di conformità UE, in linea con il nuovo quadro legislativo.
Quando ad un prodotto si applicano più atti dell'Unione europea deve essere redatta un'unica dichiarazione di conformità UE che li racchiude tutti.
8. L'allegato IV della Direttiva 2006/42/CE, contenente l'elenco dei prodotti ad alto rischio, è diventato l'allegato I del regolamento, i prodotti compresi in questo allegato sono rimasti invariati e sono stati aggiunti i componenti di sicurezza con comportamento auto-evolutivo e le macchine che incorporano sistemi con comportamento auto-evolutivo.
Per sei categorie di prodotto non è prevista la possibilità per il fabbricante di applicare la procedura di valutazione della conformità con controllo interno sulla fabbricazione e quindi, per questi prodotti, sarà sempre necessario l'intervento di un organismo notificato:

- Componenti di sicurezza con comportamento auto-evolutivo
- Macchine che incorporano sistemi con comportamento auto-evolutivo

Inoltre per sei categorie di prodotto non è prevista la possibilità per il fabbricante di applicare la procedura di valutazione della conformità con controllo interno sulla fabbricazione e quindi è stato reso obbligatori ai fini della marcatura CE l'intervento di un organismo notificato per:

- Dispositivi amovibili di trasmissione meccanica
- Ripari per i dispositivi amovibili di trasmissione meccanica
- Ponti elevatori per veicoli
- Apparecchi portatili a carica esplosiva per il fissaggio o altre macchine ad impatto
- Componenti di sicurezza con comportamento totalmente o parzialmente auto-evolutivo mediante approcci di apprendimento automatico che garantiscono funzioni di sicurezza
- Macchine che incorporano sistemi con comportamento totalmente o parzialmente auto-evolutivo che utilizzano approcci di apprendimento automatico che garantiscono

funzioni di sicurezza e che non sono stati immessi sul mercato in modo indipendente, rispetto solamente a questi sistemi.

1.2 La normativa IEC 62443

La serie di standard IEC 62443, definisce le line guida per incrementare la sicurezza digitale degli Industrial Automation and Control Systems (IACS). Questi standard si applicano agli utilizzatori finali (es. proprietari della rete), system integrators, operatori di security e costruttori di sistemi di controllo.

Tutti gli standard IEC 62443 sono organizzati su quattro livelli:

- Prima categoria: include informazioni e concetti generali, modelli e la terminologia. Sono descritti anche i parametri di sicurezza digitali e il ciclo di vita della sicurezza digitale per IACS.
- Seconda categoria: destinata ai gestori della rete.
- Terza categoria: descrive il modello di sviluppo di sistemi attraverso l'integrazione di componenti.
- Quarta categoria: descrive i requisiti dei prodotti che implementano tecniche di protezione da attacchi cyber.

Parti generali:

- IEC/TS 62443-1-1 definisce la terminologia, i concetti e i modelli per la sicurezza dei sistemi di automazione e controllo industriale (IACS), utilizzati in tutta la serie. In particolare, sono definiti sette requisiti fondamentali (FR): Controllo dell'identificazione e dell'autenticazione (FR1), Controllo dell'uso (FR2), Integrità del sistema (FR3), Riservatezza dei dati (FR4), Flusso di dati ristretto (FR5), Risposta tempestiva agli eventi (FR). FR6) e Disponibilità delle risorse (FR7).
- IEC/TS 62443-1-2 include la definizione di termini e acronimi utilizzati negli standard IEC 62443.

Parti relative a policy e procedure:

- La norma IEC 62443-2-1 specifica i requisiti del programma di sicurezza del proprietario delle risorse per un sistema di automazione e controllo industriale (IACS)

e fornisce indicazioni su come sviluppare ed evolvere il programma di sicurezza. Gli elementi di un programma di sicurezza IACS descritti in questo standard definiscono le capacità di sicurezza richieste che si applicano al funzionamento sicuro di un IACS e sono per lo più relative a politiche, procedure, pratiche e personale

- La norma IEC/IS 62443-2-2 Ed.2 specifica un quadro e una metodologia per la valutazione della protezione di un SIGC basata sulla nozione di livello di sicurezza (tecnica) e sulla maturità dei processi connessi. Il concetto di livello di protezione è una valutazione di sicurezza della combinazione di misure tecniche e organizzative e definisce un indicatore della completezza del programma di sicurezza
- IEC/TR 62443-2-3 definisce la gestione delle patch nell'ambiente IACS. In particolare, fornisce un formato definito per lo scambio di informazioni sulle patch di sicurezza dai proprietari degli asset ai fornitori dei prodotti e una definizione di alcune delle attività associate allo sviluppo delle informazioni sulle patch da parte dei fornitori dei prodotti e all'implementazione delle patch da parte dei proprietari degli asset. Il formato e le attività di scambio sono definiti per l'uso nelle patch relative alla sicurezza; tuttavia potrebbe anche essere applicabile a patch o aggiornamenti non correlati alla sicurezza
- IEC 62443-2-4 specifica i requisiti per le capacità di sicurezza per i fornitori di servizi IACS che possono offrire al proprietario dell'asset durante le attività di integrazione e manutenzione di una soluzione di automazione. Alcune di queste funzionalità fanno riferimento a misure di sicurezza definite in IEC 62443-3-3 che il provider di servizi deve garantire siano supportate nella soluzione di automazione

Parti relative al sistema:

- IEC/TR 62443-3-1 fornisce una valutazione attuale di vari strumenti di sicurezza informatica, contromisure di mitigazione e tecnologie che possono essere efficacemente applicate ai moderni sistemi IACS elettronici che regolano e monitorano numerosi settori e infrastrutture critiche. Descrive diverse categorie di tecnologie di sicurezza informatica incentrate sui sistemi di controllo, i tipi di prodotti disponibili in tali categorie, i pro e i contro dell'utilizzo di tali prodotti negli ambienti IACS automatizzati, in relazione alle minacce previste e alle vulnerabilità informatiche note e, cosa più importante, le raccomandazioni preliminari e le linee guida per l'utilizzo di questi prodotti tecnologici di sicurezza informatica e/o contromisure

- La norma IEC 62443-3-2 stabilisce i requisiti per la valutazione del rischio al fine di suddividere un IACS (come sistema in esame) in zone e condotti. Una zona è un raggruppamento di risorse basato sul rischio, mentre le comunicazioni tra le zone avvengono attraverso i cosiddetti "condotti". Questo documento stabilisce inoltre i requisiti per valutazioni dettagliate del rischio di ciascuna zona e condotto e per l'assegnazione del livello di sicurezza obbiettivo (SL-T).
- La norma IEC 62443-3-3 fornisce requisiti tecnici dettagliati del sistema di controllo (SR) associati ai sette requisiti fondamentali (FR), inclusa la definizione dei requisiti per i livelli di sicurezza della capacità del sistema di controllo. Questi requisiti sono destinati ad essere utilizzati, insieme alle zone e ai condotti definiti per il sistema in esame, per la definizione delle capacità di sicurezza appropriate a livello del sistema di controllo.

Parti relative ai componenti:

- La norma IEC 62443-4-1 specifica i requisiti di processo per lo sviluppo sicuro di prodotti utilizzati nell'automazione industriale e nei sistemi di controllo. Definisce un ciclo di vita di sviluppo sicuro allo scopo di sviluppare e mantenere prodotti sicuri
- La norma IEC 62443-4-2 specifica i requisiti tecnici di sicurezza informatica per i componenti, come dispositivi integrati, componenti di rete, componenti host e applicazioni software. I requisiti derivano dai requisiti a livello di sistema definiti nella norma IEC 62443-3-3

In particolare per la redazione della tesi si è fatto riferimento alla:

- IEC 62443-3-2
- IEC/TS 62443-1-1
- IEC/TS 62443-3-3

1.2.1 IEC 62443-1-1

La normativa IEC/TS 62443-1-1 specifica i concetti di zone di sicurezza, condotti e livelli di sicurezza, elementi chiave per affrontare la valutazione del rischio.

IEC/TS 62443-1-1, 5.9 *Security zone:* per grandi/complessi sistemi non è necessario applicare lo stesso livello di sicurezza a tutti i componenti, le differenze possono essere affrontate utilizzando il concetto di *"security zone*", ovvero un raggruppamento di asset logici o fisici che condividono requisiti di sicurezza. È possibile avere sottozone all'interno delle zone offrendo una sicurezza a più livelli, in profondità.

Una zona di sicurezza ha un confine delimitato da ciò che è incluso e ciò che non è incluso.

Il concetto di zona implica anche la necessità di accedere alle risorse, questo definisce comunicazioni e accessi necessari per permettere ad informazioni e persone di muoversi tra le zone di sicurezza.

Le zone possono essere identificate in senso fisico, raggruppando le risorse in base all'ubicazione fisica, o in senso logico (virtuale), raggruppando asset basate su funzionalità o altre caratteristiche.

Come determinare le zone?

- Valutare la comunicazione tra zone: l'accesso per collegare una zona con le risorse al di fuori di essa può avere diverse forme, ad esempio: movimentazione fisica di beni e persone e/o comunicazione elettronica, l'accesso remoto è una tipologia di comunicazione tra le risorse all'interno della zona ed all'esterno.
- Valutare gli accessi fisici: zone di sicurezza fisiche sono previste per delimitare un'area ove i sistemi all'interno richiedono lo stesso livello di fiducia da parte di operatori, sviluppatori e manutentori. Questo non preclude la possibilità di avere una zona con livello di sicurezza fisica superiore all'interno (sottozona) o una zona di accesso alle comunicazioni di livello

superiore all'interno di una zona di sicurezza fisica inferiore. Tutti i dispositivi all'interno del confine dovrebbero essere protetti per soddisfare la stessa politica di sicurezza. I meccanismi di protezione possono variare a seconda dell'asset protetto.

Esempio di sicurezza fisica: l'accesso ad un impianto di produzione è permesso alle persone autorizzate da un agente autorizzato (guardia o ID), l'accesso alle persone non autorizzate è impedito dallo stesso agente e da recinzioni.

IEC/TS 62443-1-1, 5.10 Condotti*:* il canale di comunicazione attraverso cui le zone si parlano è definito "condotto".

Il condotto è un tipo particolare di zona di sicurezza il quale può collegare entità all'interno di una zona o possono connettersi diverse zone. Come per le "zone di sicurezza" può essere dato da costrutti fisici e logici.

Condotti che non attraversano la zona sono generalmente attendibili, altrimenti necessitano di utilizzare un processo end-to-end sicuro. Condotti non attendibili sono quelli che non hanno lo stesso livello di sicurezza dell'endpoint della "zona di sicurezza".

Esempio: Se la WAN è costruita utilizzando comunicazioni affittate o private, allora potrebbe essere considerato un canale fidato. Se utilizza sia reti pubbliche che private, potrebbe essere classificato come non attendibile

IEC/TS 62443-1-1, 5.11 *Security Level:* possono essere definite tre tipologie di livelli di sicurezza *(security level):*

- SL-T: è il livello "Target", ovvero il livello desiderato di sicurezza per un certo prodotto, calcolato durante la fase di *Risk Assessment*.
  Determina l'efficacia richiesta dalle contromisure, dai dispositivi, dai sistemi che devono essere messi in atto per evitare che la sicurezza della zona e/o condotto sia compromessa.
  Esempi contromisure:
  - tecniche: firewall, antivirus…
  - fisiche: porte, lucchetti …
  - amministrative: policy, procedure…

- SL-A: è il livello “Achieved”, ovvero il livello effettivo raggiunto da un certo prodotto. Dopo un opportuno Assessment sul prodotto, questo valore SL-A dovrà essere confrontato con il valore SL-T;
- SL-C:è il livello “Capability”, ovvero quello fornito dal prodotto una volta configurato. Questi livelli indicano che un particolare componente o sistema è in grado di soddisfare gli SL target in modo nativo senza ulteriori contromisure compensative quando correttamente configurato e integrato.

1.2.2 IEC/TS 62443-3-3

Nella IEC/TS 62443-3-3 è specificata la definizione e la classificazione dei livelli di sicurezza, il Security Level è definito come il “Livello di confidenza del grado di vulnerabilità dello IACS da attacchi pericolosi.”

È possibile raggiungere cinque Security Level:

- Security Level 0 (SL0): nessuna protezione richiesta.
- Security Level 1 (SL1): protezione contro la violazione occasionale o casuale.
- Security Level 2 (SL2): protezione contro la violazione intenzionale con mezzi scarsi, con risorse scarse, competenze generiche del sistema e motivazione scarsa.
- Security Level 3 (SL3): Protezione contro la violazione intenzionale con mezzi sofisticati, con risorse moderate, competenze specifiche del sistema e motivazione moderata.
- Security Level 4 (SL4): Protezione contro la violazione intenzionale con mezzi sofisticati con risorse ingenti, competenze specifiche del sistema e forte motivazione.

Per comprendere la classificazione dei livelli di sicurezza, sono stati identificati diversi requisiti di base per la sicurezza dell'automazione industriale.

Questi sono i seguenti requisiti:

1) Controllo dell'accesso (AC): controllare l'accesso a dispositivi selezionati, informazioni o entrambi per proteggere da operazioni non autorizzate del dispositivo o dall'uso di informazioni.

2) Controllo dell'uso (UC): controllare l'uso di dispositivi selezionati, informazioni o entrambi per proteggere da operazioni non autorizzate del dispositivo o dall'uso di informazioni.

3) Integrità dei dati (DI): garantire l'integrità dei dati su canali di comunicazione selezionati per proteggerli da modifiche non autorizzate.

4) Riservatezza dei dati (DC): garantire la riservatezza dei dati sui canali di comunicazione selezionati per proteggerli dalle intercettazioni.

5) Limitare il flusso di dati (RDF): limitare il flusso di dati sui canali di comunicazione per proteggere dalla pubblicazione di informazioni a fonti non autorizzate.

6) Risposta tempestiva all'evento (TRE): rispondere alle violazioni della sicurezza notificando l'autorità competente, riportando le necessarie prove forensi della violazione e intraprendendo automaticamente azioni correttive tempestive in situazioni *mission-critical* o *safety-critical*.

7) Disponibilità delle risorse (RA): garantire la disponibilità di tutte le risorse di rete per la protezione dagli attacchi *denial of service*.

Lo standard contiene poi le tabelle di mappatura tra requisiti e Security Levels Capability (SL-C).

1.2.3 IEC 62443-3-2

Lo scopo della norma IEC 62443-3-2 è la definizione di un insieme di misure che guidano l'organizzazione attraverso il processo di valutazione del rischio di un particolare IACS (sistema di controllo di automazione industriale), di identificazione e di applicazione delle contromisure di sicurezza per ridurre il rischio ad un livello tollerabile.

La procedura è schematizzata nell'immagine seguente:

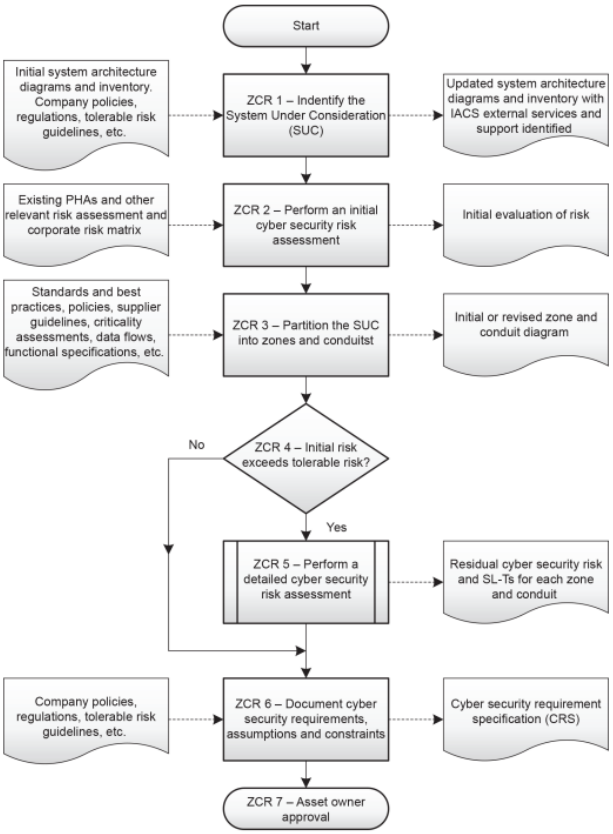


***Figura 2.1.1**: Schema della procedura per eseguire l'analisi del rischio*

Nel dettaglio:

ZRC 1: identificazione del sistema in esame *(system under consideration)*, del perimetro e dei punti di accesso

ZRC 2: valutazione iniziale del rischio. Lo scopo è valutare il peggior scenario di rischio che il SUC *(system under consideration)* presenta in caso di compromissione.

Valutando l'impatto su salute, sicurezza, ambiente, danni economici… La valutazione spesso è eseguita utilizzando una matrice di rischio.

ZRC 3: suddivisione del SUC in zone e condotti.

ZRC 4: il rischio determinato deve essere comparato con il livello di rischio tollerabile dall'organizzazione per valutare se è necessario eseguire una valutazione dettagliata del rischio

ZRC 5: valutazione dettagliata del rischio, la quale deve essere eseguita per ogni zona e condotto o per un insieme di zone e condotti

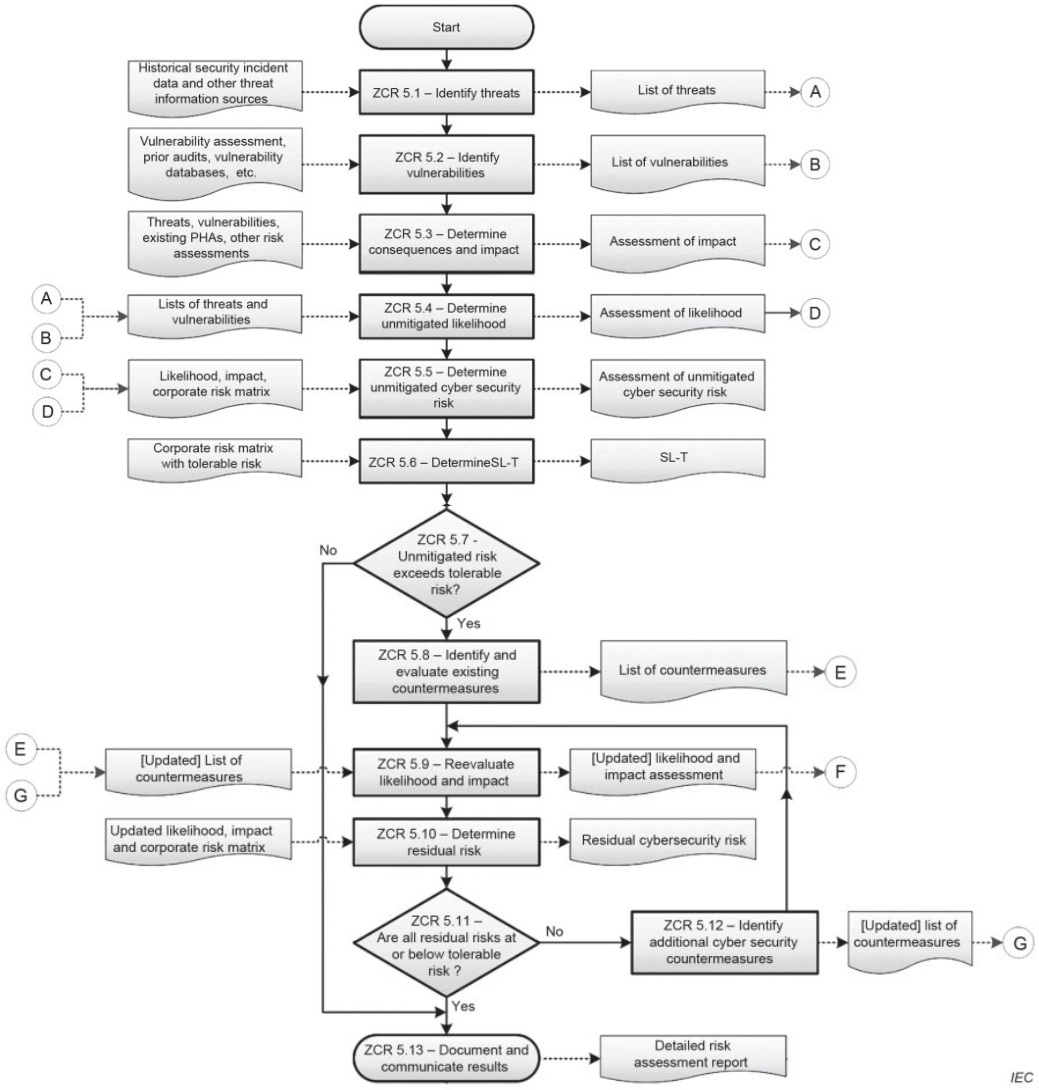


***Figura 2.1.2**: Schema della procedura per eseguire l'analisi del rischio di dettaglio*

La valutazione dettagliata del rischio, a differenza della valutazione iniziale, prevede diversi passaggi:

ZRC 5.1: identificazione delle minacce, per questa fase può essere utile preparare un documento completo delle minacce (esempio: un dipendente non malintenzionato accede fisicamente alla zona e collega una chiavetta USB in un pc).

ZRC 5.2: identificazione delle vulnerabilità, in questo caso è necessario individuare le vulnerabilità associate alle risorse.

ZRC 5.3: determinazione conseguenze e impatti, viene valutato ogni scenario di minaccia per individuare le conseguenze possibili.

ZRC 5.4: determinazione della probabilità, ovvero si valuta la probabilità che la minaccia si realizzi, avendo come input le minacce e le vulnerabilità.

ZRC 5.5: determinazione del rischio residuo di cyber sicurezza

ZRC 5.6: determinazione del livello di sicurezza desiderato

ZRC 5.7: paragono il rischio residuo con il rischio tollerabile.

Ovvero, posso comparare il livello di sicurezza raggiunto *"SL-A"* con il livello di sicurezza tollerabile, corrispondente al livello di sicurezza desiderato *"SL-T":*

- Se SL-A $\geq$ SL-T, è possibile documentare i risultati
- Se SL-A $\leq$ SL-T, è necessario identificare e valutare delle contromisure

ZRC 6: documentazione dei requisiti.

ZRC 7: approvazione proprietario dell'asset

Capitolo 2

Valutazione iniziale del rischio

Nel presente capitolo si applicherà la procedura per la valutazione iniziale del rischio specificata nello standard IEC 62443-3-2 ad un caso studio: centro di lavorazione della lamiera.

2.1 Descrizione del sistema

La descrizione del sistema prevede una descrizione dell'ambiente operativo logico e fisico.

Per quanto concerne l'ambiente fisico, l'azienda è costituita da diversi stabili, per accedere è previsto un controllo degli accessi tramite pass ed addetto alla security. In uno di questi stabili si ha il centro di lavorazione della lamiera, il quale è costituito, in parte, da un magazzino automatico in semplice profondità con nr. 1 trasloelevatore equipaggiato con forcole telescopiche adatte al prelievo e deposito delle unità di carico all'interno dello scaffale.

Il trasloelevatore è una macchina associata ad un sistema automatico complesso con cui costituisce globalmente un magazzino automatizzato.

Le dimensioni di massima del magazzino sono:

- altezza circa 6,6 m;
- lunghezza circa 77 m;
- larghezza circa 6 m.

Il sistema di handling periferico al magazzino automatico è costituito da:

- nr. 1 navetta ingresso lamiere da lavorare NAV 10
- nr. 1 navetta ingresso uscite semilavorati NAV 20
- nr. 1 navetta ingresso uscite semilavorati NAV 30

Le macchine di lavorazione lamiera periferiche (centri di lavorazione) al magazzino automatico e con le quali il trasloelevatore si interfaccia sono:

- nr. 1 catenaria doppio livello interfaccia laser INT 119A1
- nr. 1 navetta interfaccia laser INT 113A1
- nr. 1 navetta interfaccia pannellatrice INT 31B1
- nr. 1 torre interfaccia punzonatrice INT 100B1
- nr. 1 torre interfaccia robot piegatura INT 100C1
- nr. 1 navetta interfaccia punzonatrice INT PSR
- nr. 1 torre interfaccia punzonatrice INT FLD
- nr. 1 navetta interfaccia cella piegatrice automatica NAV 40

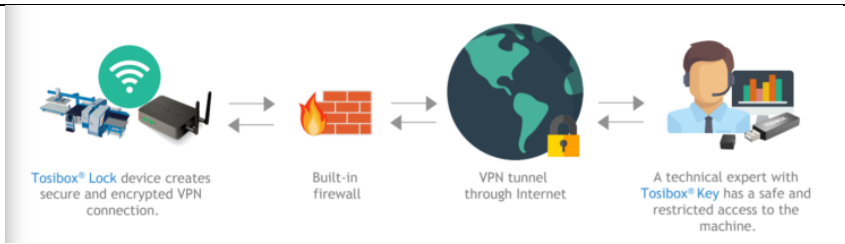
È possibile considerare in totale un n° 8 di macchine, compreso il trasloelevatore, tutte all'interno di protezioni perimetrali.

Di seguito verrà brevemente descritto l'ambiente logico ed il funzionamento di ciascuna macchina.

MACCHINA 1	MAGAZZINO LAMIERA AUTOMATICO - *INTEGRATORE*
Funzionamento macchina	Magazzino per lo stoccaggio di materia prima e semilavorati. È presente n° 1 transloelevatore che preleva la materia prima richiesta dalla macchina operatrice, la deposita sulla baia della macchina operatrice, poi riprende il semilavorato e lo deposita in magazzino in attesa della lavorazione successiva. Il trasloelevatore è una macchina con movimento orizzontale di traslazione e verticale di sollevamento. Tutta la materia prima e semilavorati sono presi dal magazzino lamiera.
Pc – sistema operativo	▪ 1 terminale Citrix ▪ Sistema operativo window 7 (no antivirus)

Interconnessione con altre macchine	Interconnessa con altre macchine per la richiesta di materia prima o semilavorato
Condivisione dati	SERVER integratore scambia informazioni con le 5 reti ▪ LAN aziendale ▪ LAN fornitore 1 ▪ LAN integratore ▪ LAN fornitore 2 ▪ LAN magazzino Lo scambio delle informazioni tra le macchine e il server centrale avviene tramite scambio di file su cartelle condivise o webservice.
ACCESSO 1: Operatore da postazione	**Come:** è sufficiente accendere il pc per accedere al pc virtuale ed al sistema gestionale. All'accensione non sono richieste né credenziali né password, l'utente risulta già loggato.
ACCESSO 2: Fornitore da remoto	**Come:** è possibile accedere attraverso la rete dell'integratore ed effettuare operazioni di avvio/arresto. Sono necessari utente e psw ditta INTEGRATORE, senza nessuna richiesta da parte dell'azienda.
ACCESSO 3: Operatore da remoto	È possibile accedere e visualizzare esclusivamente il gestionale **(**non è possibile avviare o arrestare la macchina)

MACCHINA 2	PUNZONATRICE - *FORNITORE 2*
Funzionamento macchina	Punzonatrice automatica: preleva la materia prima al magazzino, la punzona e ritorna in magazzino prodotti semilavorati pronti alla piegatura
Pc – sistema operativo	▪ PC bordo macchina + macchina virtuale ▪ Sistema operativo window 7 (no antivirus) ▪ Pc a bordo macchina che comanda la macchina, collegato solo alla LAN FORNITORE 2, dall'azienda può solo ricevere e si può collegare ▪ La macchina virtuale ha una doppia scheda di rete, una sulla rete aziendale ed una sulla rete del "fornitore 2"
Interconnessione con altre macchine	Connessa alla **MACCHINA 1** per scambio materia prima e semilavorati
Condivisione dati	Il pc operatore con il software proprietario del Fornitore2 a bordo scambiano dati tramite webservice con il server applicativo dell'integratore. Il pc a bordo macchina ed il pc virtuale si scambiano informazioni condividendo una cartella "fornitore 2" condivisa su entrambi i pc.
ACCESSO 1: Operatore da postazione	**Come:** Accensione del pc a bordo macchina Sono richiesti utente e psw
ACCESSO 2: Fornitori da remoto	**Come:** ▪ Opzione A: tramite sistema Tosibox

	 ▪ Opzione B: tramite team viewer installato sulla macchina L'accesso avviene in autonomia inserendo Username e Password (non è necessaria un'autorizzazione)
ACCESSO 3 Operatore da ufficio:	**Come:** Tramite VNC (installato nel pc dell'operatore) posso accedere al virtuale poiché ha una scheda di rete nella rete aziendale ed una in fornitore 2, successivamente dal pc virtuale apro poi il VNC che va alla macchina.

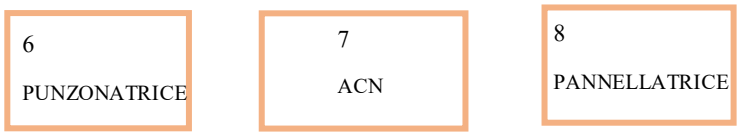
MACCHINA 3	TAGLIO LASER - *FORNITORE 1*
Funzionamento macchina	Laser automatico che richiede la materia prima al magazzino, la taglia e ritorna in magazzino prodotti semilavorati pronti alla piegatura o deposita prodotti finiti su bancali pronti per utilizzo in linea di montaggio.
Pc – sistema operativo	▪ PC a bordo macchina con doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina ed una seconda scheda collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. ▪ Terminale Citrix con cui è possibile visualizzare la schermata del magazzino con doppia scheda di rete, una in rete aziendale ed una in fornitore 1

	▪ Sistema operativo window 7 (no antivirus)
Interconnessione con altre macchine	Connessa alla **MACCHINA 1** per scambio materia prima e semilavorati
Condivisione dati	Su cartella condivisa su rete FORNITORE 1 Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.
ACCESSO 1: Operatore da postazione	**Come:** Accensione del pc a bordo macchina Sono richiesti utente e psw
ACCESSO 2: Fornitore da remoto	**Come:** Tramite teamviewer con licenza del fornitore con una password cablata, accedo al pc a bordo macchina. Non c'è un controllo diretto dell'accesso del fornitore.
ACCESSO 3: Operatore da remoto	**Come:** Pc in rete aziendale e VNC con psw del VNC della macchina

MACCHINA 4	Cella di piegatura - *FORNITORE 3*
Funzionamento macchina	Cella formata da due robot automatici ed una piegatrice: preleva materiale semilavorato dal magazzino o dalla linea di taglio (punzonatrice + pannellatrice) lo piega e ritorna i prodotti piegati finiti su bancali pronti per l'utilizzo in linea di montaggio.
Pc – sistema operativo	▪ Pc window 7 embedded a bordo macchina (presenza sistema antivirus poichè si trova sulla rete AZIENDALE) ▪ La postazione operatore utilizza un pc Windows 7 con doppia scheda di rete una in lan privata isolata e la seconda in rete aziendale ▪ Macchina virtuale
Interconnessione con altre macchine	Connessa alla **MACCHINA 1** per scambio materia prima e semilavorati
Condivisione dati	Cartelle condivise con i dati della macchina tra il pc a bordo macchina e pc che si trovano sulla stessa rete
ACCESSO 1: Operatore da postazione	**Come:** Avviando il pc con credenziali e password si è amministratore della macchina
ACCESSO 2: Fornitori	**Come:** Utilizzano un servizio di teleassistenza (Secomea) che tramite VPN e UltraVNC si collega. L'operatore dal pc a bordo macchina autorizza l'accesso, per la sola visualizzazione oppure per l'accesso ai comandi.
ACCESSO 3 Operatore da remoto	NON POSSIBILE

MACCHINA 5	CELLA DI PIEGATURA – ROBOT FORMER AUTOMATICO -*FORNITORE 1*
Funzionamento macchina	Cella formata da un robot automatico ed una piegatrice: preleva materiale semilavorato dal magazzino o dalla linea di taglio (punzonatrice + pannellatrice), lo piega e ritorna prodotti piegati finiti su bancali pronti per utilizzo in linea di montaggio.
Pc – sistema operativo	▪ PC a bordo macchina con doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina ed una seconda scheda collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. ▪ Terminale Citrix con cui è possibile visualizzare la schermata del magazzino con doppia scheda di rete, una in rete aziendale ed una in fornitore 1 ▪ Sistema operativo window 7 (no antivirus)
Interconnessione con altre macchine	Connessa alla **MACCHINA 1** per scambio materia prima e semilavorati
Condivisione dati	Su cartella condivisa su rete FORNITORE 1 Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.
ACCESSO 1: Operatore da postazione	**Come:** Accensione del pc a bordo macchina Sono richiesti utente e psw

ACCESSO 2: Fornitore da remoto	**Come:** Tramite teamviewer con licenza del fornitore con una password cablata, accedo al pc a bordo macchina. Non c'è un controllo diretto dell'accesso del fornitore.
ACCESSO 3: Operatore da remoto	**Come:** Pc in rete aziendale e VNC con psw del VNC della macchina

MACCHINA 6	PUNZONATRICE - *FORNITORE 1* 
Funzionamento macchina	Punzonatrice automatica: preleva materia prima dal magazzino, la punzona e ritorna in magazzino i prodotti semilavorati pronti alla piegatura oppure invia il semilavorato alla pannellatrice o alla cella di piegatura.
Pc – sistema operativo	▪ PC a bordo macchina con doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina ed una seconda scheda collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. ▪ Terminale Citrix con cui è possibile visualizzare la schermata del magazzino con doppia scheda di rete, una in rete aziendale ed una in fornitore 1 ▪ Sistema operativo window 7 (no antivirus)

Interconnessione con altre macchine	Connessa a **MACCHINA 1 e MACCHINA 8** per scambio materia prima e semilavorati
Condivisione dati	Su cartella condivisa su rete FORNITORE 1 Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.
ACCESSO 1: Operatore da postazione	**Come:** Accensione del pc a bordo macchina Sono richiesti utente e psw
ACCESSO 2: Fornitore da remoto	**Come:** Tramite teamviewer con licenza del fornitore con una password cablata, accedo al pc a bordo macchina. Non c'è un controllo diretto dell'accesso del fornitore.
ACCESSO 3: Operatore da remoto	**Come:** Pc in rete aziendale e VNC con psw del VNC della macchina

MACCHINA 7	SMD + ACN PER CELLA ROBOFORMER - *FORNITORE 1*
Funzionamento macchina	Questa macchina serve a smistare il semilavorato: ▪ può ritornare al magazzino il semilavorato della punzonatrice ▪ oppure inviarlo alla pannellatrice ▪ oppure inviarlo alla cella di piegatura ▪ oppure prelevare il semilavorato dal magazzino per alimentare la pannellatrice o cella di piegatura
Pc – sistema operativo	▪ PC a bordo macchina con doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina ed una seconda scheda collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. ▪ Terminale Citrix con cui è possibile visualizzare la schermata del magazzino con doppia scheda di rete, una in rete aziendale ed una in fornitore 1 ▪ Sistema operativo window 7 (no antivirus)
Interconnessione con altre macchine	Connessa a **MACCHINA 1, MACCHINA 6 e MACCHINA 8** per scambio materia prima e semilavorati
Condivisione dati	Su cartella condivisa su rete FORNITORE 1 Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.
ACCESSO 1:	**Come:**

Operatore da postazione	Accensione del pc a bordo macchina Sono richiesti utente e psw
ACCESSO 2: Fornitore da remoto	**Come:** Tramite teamviewer con licenza del fornitore con una password cablata, accedo al pc a bordo macchina. Non c'è un controllo diretto dell'accesso del fornitore.
ACCESSO 3: Operatore da remoto	**Come:** Pc in rete aziendale e VNC con psw del VNC della macchina

MACCHINA 8	PANNELLATRICE - *FORNITORE 1*
Funzionamento macchina	Pannellatrice automatica: preleva il semilavorato o dal magazzino o dalla punzonatrice (6), lo piega e lo restituisce pronto per l'utilizzo in linea di montaggio. Alcuni particolari su cui non riesce ad effettuare tutte le pieghe, vengono inviati alla cella di piegatura
Pc – sistema operativo	▪ PC a bordo macchina con doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina ed una seconda scheda collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. ▪ Terminale Citrix con cui è possibile visualizzare la schermata del magazzino con doppia scheda di rete, una in rete aziendale ed una in fornitore 1 ▪ Sistema operativo window 7 (no antivirus)
Interconnessione con altre macchine	

	Connessa a **MACCHINA 1 e MACCHINA 6** per scambio materia prima e semilavorati
Condivisione dati	Su cartella condivisa su rete FORNITORE 1 Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.
ACCESSO 1: Operatore da postazione	**Come:** Accensione del pc a bordo macchina Sono richiesti utente e psw
ACCESSO 2: Fornitore da remoto	**Come:** Tramite teamviewer con licenza del fornitore con una password cablata, accedo al pc a bordo macchina. Non c'è un controllo diretto dell'accesso del fornitore.
ACCESSO 3: Operatore da remoto	**Come:** Pc in rete aziendale e VNC con psw del VNC della macchina

2.2 Analisi iniziale del rischio

All'interno dell'attività di Cyber Security Risk Assessment per i sistemi di controllo industriale, l'analisi iniziale del rischio è la prima fase per determinare le potenziali conseguenze nel caso in cui un impianto (o sistema) risulti compromesso da un attacco informatico. Questa analisi permette di identificare le aree più critiche per un impianto, sulle quali condurre successivamente un'analisi di dettaglio (*Low Level Risk Assessment*), che prende in considerazione le vulnerabilità specifiche dei sistemi oggetto di analisi.

Il rischio è il prodotto di due componenti, la probabilità e la gravità del danno.

$$R = D \times P; \tag{2.2.1}$$

R= rischio

D= Severità del danno

P= probabilità

Per il caso in esame la gravità del danno terrà conto esclusivamente del danno alle persone, tralasciando altri aspetti quali: perdita o impatto finanziario comprese le sanzioni normative, danni all'immagine aziendale, impatto sugli investitori e perdita clienti.

Non perché questi non siano importanti ma in questa fase l'obbiettivo è individuare le risorse informatiche con un rischio *safety* maggiore, in modo tale da concentrare le risorse in tali aree e l'oggetto del lavoro ha come obbiettivo la sicurezza dei lavoratori intesa come:

- Blocco della macchina in uno stato non previsto,
- Funzionamento della macchina in un modo non previsto,
- Riavvio "inatteso" della macchina.

Per l'ultimo punto si è usato in maniera impropria "Riavvio Inatteso" per dare importanza alla situazione di riavvio di una produzione/attività/logistica "bloccata" in un momento non previsto che porta l'organizzazione ad una pressione sulla ripartenza che nella maggior parte dei casi potrebbe portare ad una attenzione alla sicurezza meno marcata.

La probabilità è stata ricavata con una matrice di rischio combinando due fattori:

- P_1: la probabilità che l'attacco informatico abbia successo
- P_2: la probabilità di accadimento dell'infortuni

$$P = P_1 \times P_2 \quad (2.2.2)$$

Per quanto concerne il primo fattore è stata assunta una "probabilità ALTA", ovvero non si sono tenute in considerazione le vulnerabilità e le fonti di minaccia in quanto verranno considerate nella valutazione dettagliata del rischio; è stata valutata la probabilità del secondo fattore, ovvero la probabilità, a seguito dell'attacco informatico, che l'evento incidentale abbia luogo. Non tenere conto di questo elemento significherebbe assumere a priori che l'evento abbia luogo.

La combinazione degli elementi sopra permette di individuare la probabilità da combinare con l'entità del danno.

L'analisi iniziale del rischio, nel rispetto della norma IEC 62443-3-2 deve essere effettuata su ogni SUC (*system under consideration*), nel caso in esame e tenendo a mente l'obbiettivo della tesi, il SUC su cui eseguire l'analisi del rischio è costituito da gruppi di macchine, in funzione del fornitore, in quanto condividono le modalità di connessione alla rete, quindi colpendo l'asset informatico di "fornitore x" è possibile arrivare alle macchine relative a "fornitore x".

Nello specifico la linea di lavorazione della lamiera è costituita da:

- Integratore: macchina 1
- Fornitore 1: macchina 3 – macchina 5 – macchina 6 – macchina 7 – macchina 8
- Fornitore 2: macchina 2
- Fornitore 3: macchina 4

Per ogni macchina è stata effettuata una valutazione del rischio, ma per il "fornitore 1" sarà necessario tenere conto delle diverse macchine.

Di seguito le tabelle impiegate per effettuare la valutazione del rischio:

Danno	Conseguenze
1-TRASCURABILE	Infortunio lieve con effetti immediatamente reversibili
2-BASSO	Infortunio lieve *qualche giorno* **<** ***t*** **<** *una settimana*
3-MEDIO	Infortunio o incidente medio-grave con lesioni temporaneamente permanenti *una settimana* < ***t*** < *2/3 mesi*
4-ALTO	Infortunio o incidente grave che porta a lesioni permanenti con effetti irreversibili ***t*** **>** *3 mesi*
5-ESTREMO	Incidente gravissimo che porta a disabilità grave o morte

Tabella 2.2.1*: valori assegnati al danno e le possibili conseguenze associate*
t: *tempo di guarigione*

P_1 e P_2	
1 -TRASCURABILE	La probabilità di accadimento dell'attacco informatico o dell'evento è prossima allo zero
2- BASSA	La probabilità di accadimento dell'attacco informatico o dell'evento è ridotta
3- MEDIA	La probabilità di accadimento dell'attacco informatico o dell'evento è buona
4-ALTA	La probabilità di accadimento dell'attacco informatico o dell'evento è quasi certa

Tabella 2.2.2*: valori assegnati a* P_1 *e* P_2

Valore	Probabilità
$12 \leq R < 16$	ALTA
$6 \leq R < 12$	MEDIA
$3 \leq R < 6$	BASSA
$1 \leq R < 3$	TRASCURABILE

***Tabella 2.2.3**: suddivisione dei livelli di probabilità*

Valore	Rischio
$16 < R$	ESTREMO
$10 \leq R \leq 16$	ALTO
$5 \leq R < 10$	MEDIO
$1 < R < 5$	BASSO
$R=1$	TRASCURABILE

***Tabella 2.2.4**: suddivisione dei livelli di rischio*

P_2: probabilità di accadimento dell'infortunio				
4-Alta				16-Alta
3-Media				12- Alta
2-Bassa				8- Media
1-Trascurabile				4- Bassa
	1-Trascurabile	2-Bassa	3-Media	4-Alta

P_1: probabilità successo attacco informatico

***Tabella 2.2.5**: Matrice delle probabilità per la valutazione iniziale del rischio*

Danno				
5- Estremo	5 - Medio	10 - Alto	15 – Alto	20 - Estremo
4-Alto	4 - Basso	8 - Medio	12 - Alto	16 – Alto
3- Medio	3 - Basso	6 - Medio	9 - Medio	12 - Alto
2-Basso	2- Basso	4 - Basso	6 - Medio	8 - Medio
1-Trascurabile	1 -Trascurabile	2- Basso	3 - Basso	4 - Basso
	1-Trascurabile	2-Bassa	3-Media	4-Alta

Probabilità

***Tabella 2.2.6**: Matrice del rischio*

Vi sono due aspetti riguardo la costruzione della tabella utilizzata per la valutazione del rischio da illustrare:

- nella prima colonna si ha la conseguenza (blocco in uno stato non previsto, funzionamento in uno stato non previsto e riavvio inatteso), per la macchina dovuta all'attacco informatico;
- nella seconda colonna si trova la "situazione di pericolo nel tempo: immediato o successivo", questo poiché si è voluto analizzare il rischio in entrambe le fasi: durante l'attacco informatico ed a seguito di quest'ultimo,

LEGENDA	
A	ALTA
M	MEDIA
B	BASSA
T	TRASCURABILE

La “MACCHINA 1” è un magazzino automatico costituito da un trasloelevatore interconnesso con le altre macchine per scambio di materia prima e prodotto semilavorato.

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- Le machine richiedono alla “MACCHINA 1” un quantitativo di prodotto semilavorato o di materia prima ed è possibile programmare tali carichi con anticipo.
- Se il trasloelevatore dovesse bloccarsi le altre macchine hanno la possibilità di proseguire con la produzione fino ad esaurimento pezzi sul bancale, tali pezzi sono movimentabili anche manualmente.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell’eseguire le “attività pericolose” si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell’eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine.	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o ripresa della produzione	Presenza di un operatore nell'area di movimento della macchina	2. Urto con la testa con scaffalatura o traslo	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Rischio inciampo dovuto alle rotaie di traslazione	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			4.Contatto con superfici ad alte temperature delle trasmissioni e delle resistenze frenanti	Ustioni localizzate	**A**	**M**	**A**	**BASSO**	MEDIO
		Sosta sotto il carrello di sollevamento	5.Rischio urto o schiacciamento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO

		Lavoro in quota per attività di manutenzione	6.Caduta dall'alto	Infortuni gravi e disabilitanti o morte	**A**	**M**	**A**	**ESTREMO**	ESTREMO
		Movimentazione manuale dei carichi caduti ingombranti e/o pesanti	7.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			8.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
			9.Caduta/ scivolamento del lavoratore	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno, ma si può generare una situazione pericolosa data da: Errore nel deposito del carico nella baia delle altre macchine operatrici Rilascio del carico in un punto diverso da quello previsto e pericoloso Prelievo maggiore di materia prima o semilavorato di quello previsto ***Implicando la necessità di un intervento, previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	10. Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o ripresa della produzione	Presenza di un operatore nell'area di movimento della macchina	11. Urto con la testa con scaffalatura o traslo	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO

			12.Rischio inciampo dovuto alle rotaie di traslazione	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			13.Contatto con superfici ad alte temperature delle trasmissioni e delle resistenze frenanti	Ustioni localizzate	**A**	**M**	**A**	**BASSO**	MEDIO
		Sosta sotto il carrello di sollevamento	14.Rischio urto o schiacciamento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
		Lavoro in quota per attività di manutenzione	15.Caduta dall'alto	Infortuni gravi e disabilitanti o morte	**A**	**M**	**A**	**ESTREMO**	ESTREMO
		Movimentazione manuale dei carichi caduti ingombranti e/o pesanti	16.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			17.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
			18.Caduta/ scivolamento del lavoratore	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale	Presenza dell'operatore nell'area di movimento della macchina	19. Urto con il materiale trasportato	Lesioni fisiche	**A**	**B**	**M**	**MEDIO**	MEDIO
			20. Caduta di materiale dall'alto	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO

			21. Rischio d'investimento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
	In assenza di operatore all'interno considerando che "macchina 1" è connessa alle altre macchine per lo scambio di materia prima e semilavorato, un riavvio **non previsto** può comportare un mancato/errato coordinamento tra le diverse macchine ***Implicando la necessità di un intervento per movimentare eventuali carichi sulle altre macchine*** ***Previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	22.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Movimentazione manuale dei carichi caduti ingombranti e/o pesanti	23.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			24.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
			25.Caduta/ scivolamento del lavoratore	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO

La “MACCHINA 2”, è una punzonatrice che preleva materia prima dal magazzino, la punzona e ritorna in magazzino prodotti semilavorati pronti alla piegatura.

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell’eseguire le “attività pericolose” si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell’eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di controllo o movimentazione del materiale	2. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			4.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	5.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO

	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Movimentazione del materiale o cambio punzone	6. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			7.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			8.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione della macchina	9. Urto con la macchina in movimento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
			10. Taglio o abrasione con il punzone	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO
		Movimentazione o controllo della materia prima	11. Taglio o urto con il materiale in movimento	Lesioni fisiche di taglio/abrasione	**A**	**B**	**M**	**BASSO**	MEDIO
	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	12.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Rimozione del materiale o cambio punzone	13. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO

			14.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			15.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

La "MACCHINA 3", è un taglio laser di classe 1 che preleva la materia prima dal magazzino, la taglia e ritorna in magazzino prodotti semilavorati pronti alla piegatura o deposita prodotti finiti su bancali pronti per utilizzo in linea di montaggio

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all'interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l'operatore, quando entra all'interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l'avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all'interno del perimetro accidentalmente, per comodità sarà definito "operatore intrappolato", e valutato quindi il riavvio inatteso in tale situazione.
- L'operazione di taglio laser avviene all'interno di un cabinet in modo tale che nessuna radiazione sia accessibile durante l'uso.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l'operatore a svolgere attività di manutenzione/controllo.
- Nell'assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell'infortunio.

Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.

- Nell'eseguire le "attività pericolose" si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell'eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di manutenzione o movimentazione del materiale	2. Contatto con parti ad elevata temperatura	Ustioni localizzate	**A**	**M**	**A**	**BASSO**	MEDIO
			3. Inalazione polveri e/o fumi	Danno lieve	**A**	**B**	**M**	**BASSO**	MEDIO
			4.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			5.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica ed essendo completamente chiusa in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	6.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di manutenzione, di allineamento del fascio o movimentazione del materiale	7. Contatto con parti ad elevata temperatura	Ustioni localizzate	**A**	**M**	**A**	**BASSO**	MEDIO
			8. Inalazione polveri e/o fumi	Danno lieve	**A**	**B**	**M**	**BASSO**	MEDIO
			9.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			10.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
			11. Rischio elettrico dovuto alle alte tensioni con cui opera il laser	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
			12. Rischio tossicologico dovuto dalla distruzione termica della lente	Intossicazione	**A**	**T**	**B**	**MEDIO**	MEDIO

			13. Rischio criogenico dovuto ai liquidi criogenici impiegati	Ustioni localizzate	**A**	**T**	**B**	**BASSO**	BASSO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Movimentazione o controllo del materiale	14. Urto con il materiale movimentato	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO
			15. Urto con la macchina in movimento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	16.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di manutenzione ed intervento	17. Contatto con parti ad elevata temperatura	Ustioni localizzate	**A**	**M**	**A**	**BASSO**	MEDIO
			18. Inalazione polveri e/o fumi	Danno lieve	**A**	**B**	**M**	**BASSO**	MEDIO
			19. Rischio elettrico dovuto alle alte tensioni con cui opera il laser	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO

			20. Rischio tossicologico dovuto dalla distruzione termica della lente	Intossicazione	**A**	**T**	**B**	**MEDIO**	MEDIO
			21. Rischio criogenico dovuto ai liquidi criogenici impiegati	Ustioni localizzate	**A**	**T**	**B**	**BASSO**	BASSO
			22.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			23.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

La “MACCHINA 4” è costituita da una cella formata da due robot automatici ed una pressa piegatrice: preleva materiale semilavorato dal magazzino o dalla linea di taglio (punzonatrice + pannellatrice) lo piega e ritorna i prodotti piegati finiti su bancali pronti per l’utilizzo in linea di montaggio.

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- L’area di lavoro dei robot presenta tre postazioni di scarico materiale, le quali sono raggiungibili dall’operatore previo abbassamento della protezione metallica e conseguente limitazione dell’area di lavoro dei robot.
- È possibile impiegare le presse piegatrici manuali nel caso in cui non sia possibile impiegare “macchina 4”.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio.

Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.

- Nell'eseguire le "attività pericolose" si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell'eseguire tali operazioni

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	2.Urto con il materiale sostenuto dai robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			4.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO

		Rimozione del materiale sostenuto dal robot	5.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			6.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			7.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica ed essendo completamente chiusa in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	8.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di intervento	9.Urto con il materiale sostenuto dai robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			10.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**A**	**MEDIO**	MEDIO
			11.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO

			12.Inciampo e conseguente caduta del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO
		Rimozione del materiale sostenuto dal robot	13.Caduta di materiale dall'alto	Schiacciamento/ urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			14.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			15.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione robot	16.Urto con il braccio del robot in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			17.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			18.Urto con il materiale trasportato in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			19. Proiezione di pezzi dovuto ad un possibile scontro tra i due robot	Lesioni fisiche	**A**	**T**	**B**	**BASSO**	BASSO

			20. Rischio investimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
		Manutenzione pressa piegatrice	21.Urto con il braccio del robot in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			22.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			23.Urto con il materiale trasportato in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			24. Discesa punzone	Schiacciamento dita	**A**	**B**	**M**	**ALTO**	ALTO
	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	25.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di intervento	26.Urto con il materiale sostenuto dai robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			27.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO

			28.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO
			29.Inciampo e conseguente caduta del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO
		Rimozione del materiale sostenuto dal robot	30.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			31.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			32.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

La “MACCHINA 5” è costituita da una cella formata da un robot automatico ed una piegatrice: preleva materiale semilavorato dal magazzino o dalla linea di taglio (punzonatrice + pannellatrice), lo piega e ritorna prodotti piegati finiti su bancali pronti per utilizzo in linea di montaggio

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- L’area di lavoro dei robot presenta tre postazioni di scarico materiale, le quali sono raggiungibili dall’operatore previo abbassamento della protezione metallica e conseguente limitazione dell’area di lavoro dei robot.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell’eseguire le “attività pericolose” si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell’eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	2.Urto con il materiale sostenuto dai robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			4.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO
		Rimozione del materiale sostenuto dal robot	5.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			6.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO

			7.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica ed essendo completamente chiusa in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	8.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di intervento	9.Urto con il materiale sostenuto dal robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			10.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			11.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO
			12.Inciampo e conseguente caduta del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO

		Rimozione del materiale sostenuto dal robot	13.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			14.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			15.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione robot	16.Urto con il braccio del robot in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			17.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			18.Urto con il materiale trasportato in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			19. Rischio investimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
		Manutenzione pressa piegatrice	20.Urto con il braccio del robot in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			21.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO

			22.Urto con il materiale trasportato in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
			23.Discesa del punzone	Schiacciamento dita	**A**	**B**	M	**ALTO**	ALTO
	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	24.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di intervento	25.Urto con il materiale trasportato dai robot	Lesioni fisiche	**A**	**M**	**A**	**BASSO**	MEDIO
			26.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			27.Movimento del braccio del robot dovuto ad un possibile rilascio dei freni	Lesioni fisiche	**A**	**T**	**B**	**MEDIO**	MEDIO
			28.Inciampo e conseguente caduta del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO

		Rimozione del materiale sostenuto dal robot	29.Caduta di materiale dall'alto	Schiacciamento/urto di parti del corpo	**A**	**B**	**M**	**MEDIO**	MEDIO
			30.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			31.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

La “MACCHINA 6”, è una punzonatrice automatica: preleva materia prima dal magazzino, la punzona e ritorna in magazzino i prodotti semilavorati pronti alla piegatura oppure invia il semilavorato alla pannellatrice o alla cella di piegatura.

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell’eseguire le “attività pericolose” si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell’eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	**Immediato:** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di controllo o movimentazione del materiale	2. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**M**	**A**	**BASSO**	MEDIO
			4.Caduta del carico	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	**Immediato:** La macchina dotata di protezione perimetrale automatica in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore **previo ARRESTO della macchina stessa**	Coordinare e gestire la produzione delle macchine connesse	5.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO

	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Movimentazione del materiale o cambio punzone	6. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			7.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**M**	**A**	**BASSO**	MEDIO
			8.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Riavvio inatteso	**Immediato:** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione della macchina	9. Urto con la macchina in movimento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
			10. Taglio o abrasione con il punzone	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO
		Movimentazione o controllo della materia prima	11. Taglio o urto con il materiale in movimento	Lesioni fisiche di taglio/abrasione	**A**	**B**	**M**	**BASSO**	MEDIO
	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore **previo ARRESTO della macchina stessa**	Coordinare e gestire la produzione delle macchine connesse	12.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Rimozione del materiale o cambio punzone	13. Taglio con il punzone o con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO

			14.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**M**	**A**	**BASSO**	MEDIO
			15.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

La “MACCHINA 7”, è una macchina utilizzata per smistare il semilavorato:

- può ritornare al magazzino il semilavorato della punzonatrice
- oppure inviarlo alla pannellatrice
- oppure inviarlo alla cella di piegatura
- oppure prelevare il semilavorato dal magazzino per alimentare la pannellatrice o cella di piegatura

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.

- Nell'assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell'infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell'eseguire le "attività pericolose" si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell'eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di controllo o movimentazione del materiale	2. Taglio con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			4.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO

Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	5.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di controllo o movimentazione del materiale	6. Taglio con il materiale	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			7.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			8.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
			9.Caduta/ scivolamento del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione del robot	10.Urto con il materiale trasportato in movimento	Lesioni fisiche gravi	**A**	**B**	**M**	**ALTO**	ALTO
		Movimentazione o controllo della materia prima	11. Taglio o urto con il materiale in movimento	Lesioni fisiche di taglio/abrasione	**A**	**B**	M	**BASSO**	MEDIO

	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	12.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Presenza di un operatore nell'area dovuto alla necessità di intervento	13.Inciampo e conseguente caduta del lavoratore	Lesioni fisiche	**A**	**B**	**M**	**BASSO**	MEDIO

La “MACCHINA 8”, è una pannellatrice automatica: preleva il semilavorato o dal magazzino o dalla punzonatrice (6), lo piega e lo restituisce pronto per l'utilizzo in linea di montaggio. Alcuni particolari su cui non riesce ad effettuare tutte le pieghe, vengono inviati alla cella di piegatura

La valutazione del rischio è stata effettuata secondo alcune premesse/ipotesi:

- La macchina è dotata di protezione perimetrale, se un operatore fosse all’interno del perimetro la recinzione risulterebbe aperta e questo comporterebbe il NON avvio della macchina. Inoltre l’operatore, quando entra all’interno delle protezioni perimetrali, è obbligato a portare con sé una chiave che impedisce l’avvio della macchina. Nonostante questo è stata considerata la possibilità che un operatore dimentichi la chiave e rimanga chiuso all’interno del perimetro accidentalmente, per comodità sarà definito “operatore intrappolato”, e valutato quindi il riavvio inatteso in tale situazione.
- In caso di blocco, riavvio inatteso e funzionamento anomalo nei primi istanti non si conosce la CAUSA, in tal caso derivante da attacco informatico, di conseguenza in primo luogo si può pensare ad un guasto della macchina portando l’operatore a svolgere attività di manutenzione/controllo.
- Nell’assegnare il livello di rischio (estremo, alto, medio, basso, trascurabile) non si è tenuto conto della presenza di eventuali misure di prevenzione e protezione. Questo poiché tali misure possono ridurre il danno ma anche la probabilità di accadimento dell’infortunio. Ma lo scopo principale della tesi è lavorare su delle contromisure per la riduzione della probabilità che un attacco informatico abbia successo.
- Nell’eseguire le “attività pericolose” si è tenuto conto della situazione di stress e conseguente disattenzione a cui potrebbero essere sottoposti gli operatori nell’eseguire tali operazioni.

Conseguenza attacco informatico	Situazione di Pericolo nel tempo: • Immediato all'attacco informatico • Successivo all'attacco informatico	Attività pericolosa	Rischio	Conseguenze	Probabilità			Danno	R
					P_1	P_2	P		
Blocco in uno stato non previsto	***Immediato:*** La macchina in caso di "blocco" non provoca pericolo per le persone. Ma si ha un blocco della produzione a causa dell'interconnessione tra le diverse macchine	Coordinare e gestire la produzione delle macchine connesse	1.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Attività di controllo o rimozione del materiale	2. Taglio con il pezzo	Lesione molto lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			3.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			4.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
Funzionamento in uno stato non previsto	***Immediato:*** La macchina dotata di protezione perimetrale automatica in caso di "funzionamento anomalo" non provoca pericolo per le persone, in quanto non presenti all'interno. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	5.Situazione di stress psicologico	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO

	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Rimozione del materiale	6. Taglio con il pezzo	Lesione lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			7.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			8.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
		Cambio lame della pannellatrice	9. Taglio con le lame	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO
Riavvio inatteso	***Immediato:*** Presenza di un operatore intrappolato, a causa di una chiusura accidentale della protezione perimetrale mentre svolgeva attività di manutenzione	Manutenzione o pulizia della macchina	10. Taglio con le lame	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO
			11.Urto con la macchina in movimento	Infortunio grave	**A**	**B**	**M**	**ALTO**	ALTO
		Movimentazione o controllo della materia prima o semilavorato	12. Taglio o urto con il materiale in movimento	Lesioni fisiche di taglio/abrasione	**A**	**B**	**M**	**BASSO**	MEDIO

	In assenza di operatore all'interno in caso di "riavvio inatteso" non si ha pericolo per le persone. Il rischio è il danneggiamento della macchina e questo implica l'intervento dell'operatore ***previo ARRESTO della macchina stessa***	Coordinare e gestire la produzione delle macchine connesse	13.Situazione di stress	Stress	**A**	**A**	**A**	**TRASCURABILE**	BASSO
	Successivo: presenza di un operatore nell'area dovuto alla necessità di manutenzione e/o intervento	Rimozione del materiale	14. Taglio con il pezzo	Lesione molto lieve	**A**	**M**	**A**	**BASSO**	MEDIO
			15.Sforzo fisico eccessivo	Sovraccarico della colonna vertebrale	**A**	**A**	**A**	**BASSO**	MEDIO
			16.Caduta del pezzo	Lesioni fisiche di taglio/abrasione	**A**	**M**	**A**	**BASSO**	MEDIO
		Cambio lame della pannellatrice	17. Taglio con le lame	Lesione lieve	**A**	**B**	**M**	**BASSO**	MEDIO

2.3 Suddivisione del SUC in zone e condotti

Dopo aver eseguito la valutazione iniziale del rischio per ogni SUC (*system under consideration*) in esame, è necessario andare a suddividere quest'ultimo in zone e condotti. Le zone sono raggruppamenti logici di componenti hardware o software che condividono tra loro lo stesso livello di sicurezza. Queste zone sono collegate tra loro attraverso condotti, ovvero canali di comunicazione che dovrebbero prevedere meccanismi di sicurezza aggiuntivi.

Come specificato dalla IEC/TS 62443-1-1 per grandi/complessi sistemi non è necessario applicare lo stesso livello di sicurezza a tutti i componenti, le differenze possono essere affrontate utilizzando il concetto di "security zone". È possibile avere sottozone all'interno delle zone offrendo una sicurezza a più livelli.

Una zona di sicurezza ha un confine delimitato da ciò che è incluso e ciò che non è incluso.

Il concetto di zona implica anche la necessità di accedere alle risorse, questo definisce le comunicazioni e gli accessi necessari per permettere ad informazioni e persone di muoversi tra le zone di sicurezza.

Le zone possono essere identificate in senso fisico, ovvero raggruppando le risorse in base all'ubicazione fisica, o in senso logico (virtuale), ovvero raggruppando asset basate su funzionalità o altre caratteristiche.

Per determinare le zone è necessario:

- Valutare la comunicazione tra zone: l'accesso per collegare una zona con le risorse al di fuori di essa può avere diverse forme (ad esempio movimentazione fisica di beni e persone e/o comunicazione elettronica), l'accesso remoto è una tipologia di comunicazione tra le risorse all'interno della zona ed all'esterno.

- Valutare gli accessi fisici: zone di sicurezza fisiche sono previste per delimitare un'area ove i sistemi all'interno richiedono lo stesso livello di fiducia da parte di operatori, sviluppatori e manutentori. Questo non preclude la possibilità di avere una zona con un

livello di sicurezza fisica superiore all'interno (sottozona) o una zona di accesso alle comunicazioni di livello superiore all'interno di una zona di sicurezza fisica inferiore. Tutti i dispositivi all'interno del confine dovrebbero essere protetti per soddisfare la stessa politica di sicurezza. I meccanismi di protezione possono variare a seconda dell'asset protetto. Un esempio di sicurezza fisica è quando l'accesso ad un impianto di produzione è permesso alle persone autorizzate da un agente (guardia o ID), l'accesso alle persone non autorizzate è impedito dallo stesso agente e da recinzioni.

La stessa norma sopra si individua il concetto di "condotto", ovvero il canale di comunicazione attraverso cui le zone si parlano.

Il condotto è un tipo particolare di zona di sicurezza il quale può collegare entità all'interno di una zona o possono connettersi diverse zone. Come per le "zone di sicurezza" può essere dato da costrutti fisici e logici.

Condotti che non attraversano la zona sono generalmente attendibili, altrimenti necessitano di utilizzare un processo end-to-end sicuro. Condotti non attendibili sono quelli che non hanno lo stesso livello di sicurezza dell'endpoint della "zona di sicurezza".

Ad esempio: se la WAN è costruita utilizzando comunicazioni affittate o private, allora potrebbe essere considerato un canale fidato, nel caso in cui utilizzi sia reti pubbliche che private, potrebbe essere classificato come non attendibile

Sulla base di queste specifiche e con la conoscenza dell'infrastruttura di rete è possibile andare a suddividere il sistema in zone e condotti.

Il sistema in considerazione (*System under consideration)* è, come specificato nei paragrafi precedenti, costituito da gruppi di macchine, in funzione del fornitore, in quanto condividono le modalità di connessione alla rete. Di conseguenza per ogni fornitore, il quale possiede le sue connessioni e tipologie di accessi remoti, verrà effettuata la suddivisione in zone e condotti.

Considerando che vi sono dei punti di accesso comuni ai diversi fornitori, questi potranno condividere zone e condotti.

Di seguito la rappresentazione grafica dell'infrastruttura di rete:

Figura 2.3.1:*Infrastruttura di rete*

2.3.1 Integratore

La parte centrale è composta da un magazzino automatico della materia prima e semilavorati con un traslo centrale per il prelievo e il deposito del materiale su entrambi i lati, il sistema è pilotato da plc collegati tramite switch ad una lan privata isolata, la lan arriva ad uno switch aziendale dove viene convogliata tramite una vlan, Denominata VLan1 isolata verso gli host vmware su cui è ospitato un server virtuale su cui è installata la logica di gestione WMS, i relativi db di gestione e i db con i dati di transito tra ERP Principale e le postazioni operatore dell'impianto, denominato Server integratore. L'implementazione della logica è eseguita dall'integratore dell'Impianto. Il software sviluppato dall'integratore gestisce il magazzino e mostra lo stato dell'impianto. Gestisce anche gli ordini di lavorazione delle singole macchine, fornendo il materiale e le informazioni per la produzione. Lo scambio delle informazioni tra le macchine e il server centrale avviene tramite scambio di file su cartelle condivise o webservice, a seconda del fornitore della macchina.

Nel dettaglio è possibile accedere al magazzino partendo da:

- "server integratore", attraverso una VLAN1, si arriva ad uno switch lan aziendale, e tramite una LAN privata integratore, è possibile arrivare ai due PLC.
- Tramite firewall e VPN, come sopra, attraverso una VLAN 1, si arriva ad uno switch lan aziendale, e tramite una LAN privata integratore, è possibile arrivare ai due PLC.

Per accedere all'applicazione del magazzino integratore dal terminale Citrix viene utilizzato thin client, in quanto il terminale Citrix si trova sulla rete aziendale e tramite quest'ultima connessa al Server integratore è possibile la comunicazione con il magazzino.

INTERFACCIA WMS SYSTEM INTEGRATOR (W-Log) E PLC MAGAZZINO CLL:

L'interfaccia tra WMS e PLC che governa la movimentazione dei vassoi avviene via TCP grazie a delle funzioni proprietarie direttamente dal database del WMS. Il PLC del magazzino è sempre a gestione del system integrator. Il PLC del magazzino si trova direttamente sotto la rete cliente con una classe IP dedicata.

INTERFACCIA WMS SYSTEM INTEGRATOR (W-Log) ED ERP CLIENTE:

L'interfaccia tra WMS e l'ERP del cliente avviene sia via Database Link che tramite scambio file su una cartella condivisa. Tutta l'architettura di rete è stata sviluppata dal cliente.

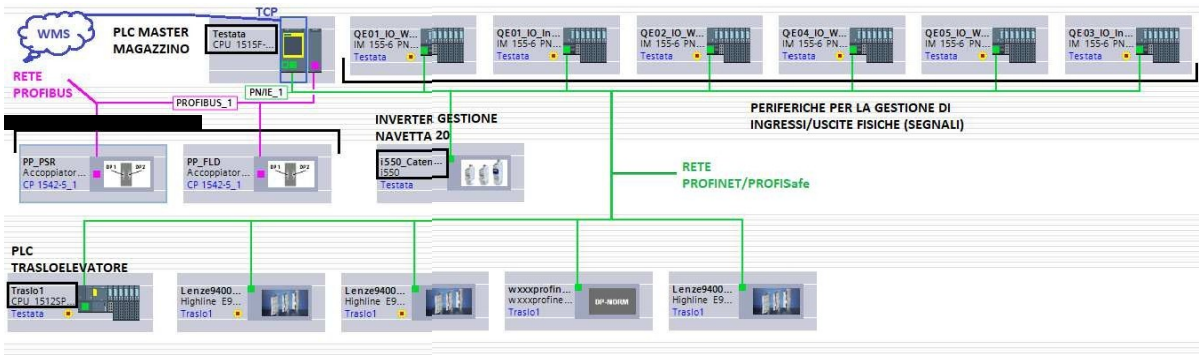


Figura 2.3.1.1: *Interfaccia WMS system integrator (W-Log) ed ERP cliente*

INTERFACCIA WMS SYSTEM INTEGRATOR (W-Log) – MACCHINA FORNITORE 2:

Per quanto riguarda lo scambio dati di più alto livello (richieste cambio vassoi, gestione giacenza, ecc…) questo avviene grazie ad un servizio del WMS (Java) su Server del system integrator dedicato che si collega via TCP al Software proprietario del costruttore "2" installato sulla macchina. Per la parte di basso livello (gestione della movimentazione fisica) lo scambio avviene tra PLC Magazzino e controllore della macchina di taglio via PROFIBUS tramite accoppiatore di rete per separare la rete PROFIBUS magazzino dalla rete PROFIBUS macchina.

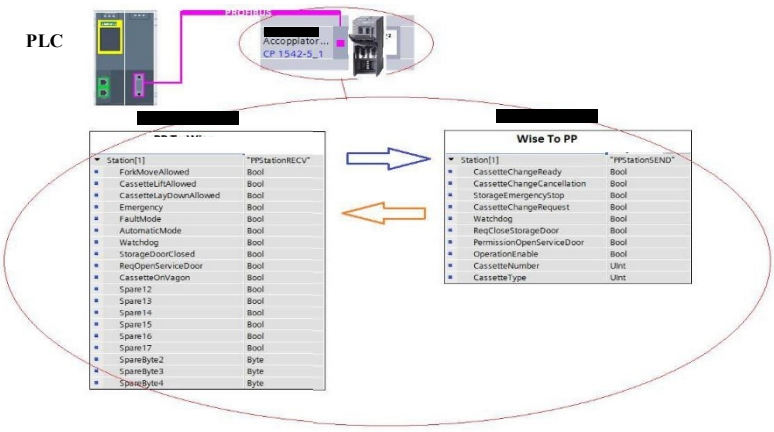


Figura 2.3.1.2: *Interfaccia WMS system integrator (W-Log) – Macchina fornitore 2*

INTERFACCIA WMS SYSTEM INTEGRATOR (W-Log) – MACCHINE FORNITORE 1:

Per quanto riguarda lo scambio dati di più alto livello (richieste cambio vassoi, gestione giacenza, ecc…) questo avviene tramite scambio file di testo su cartella condivisa tra WMS e la singola macchina. La cartella condivisa sitrova sul PC di gestione della singola macchina.

Per la parte di basso livello (gestione della movimentazione fisica) lo scambio avviene tra PLC Magazzino econtrollore della macchina di taglio via segnali digitali. Nessun tipo di BUS.

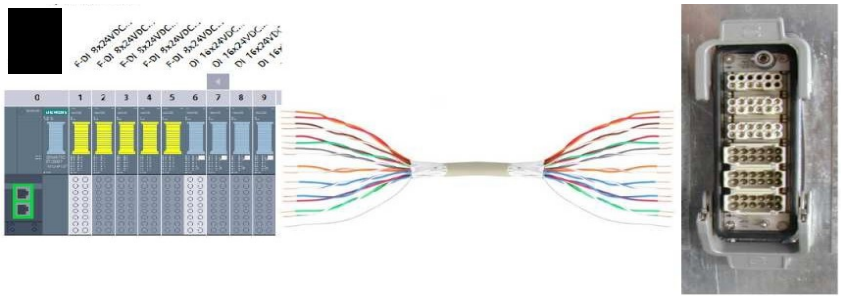


Figura 2.3.1.3: *Interfaccia WMS system integrator (W-Log) – Macchina fornitore 1*

INTERFACCIA WMS SYSTEM INTEGRATOR (W-Log) – MACCHINE FORNITORE 3:

Per quanto riguarda lo scambio dati di più alto livello (richieste cambio vassoi, gestione giacenza, ecc…) questoavviene grazie ad un servizio del WMS (Java) su Server del system integrator dedicato che si collega via TCP al Software proprietario del costruttore "3" installato sulla macchina.

Per la parte di basso livello (gestione della movimentazione fisica) lo scambio avviene tra PLC Magazzino econtrollore della macchina di taglio via segnali digitali. Nessun tipo di BUS.

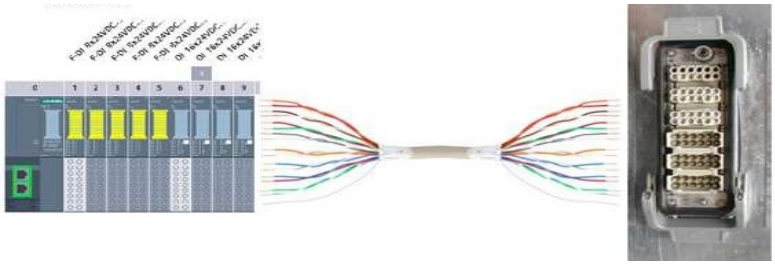


Figura 2.2.3.4: *Interfaccia WMS system integrator (W-Log) – Macchina fornitore 3*

Zona 1	Server integratore
Condotto 1.1	VLAN 1 – Switch
Condotto 2	Firewall e VPN
Condotto 3.2	LAN privata integratore
Zona 2	Terminale Citrix
Condotto 3.1	Lan aziendale
Condotto 4	Thin client
Zona 3	Applicazione magazzino integratore
Zona 4	PLC
Condotto 5	Profibus
Condotto 6	TCP

Tabella 2.2.3.1*: Suddivisione zone e condotti integratore*

2.3.2 Fornitore 1

Il fornitore 1 fornisce varie macchine operatrici che eseguono automaticamente alcune fasi della lavorazione, fasi che possono essere singole o concatenate con l'alimentazione del materiale direttamente dal magazzino centrale o da altra macchina operatrice della sezione.

Il controllo della macchina avviene da una postazione operatore su cui si trova un pc con una doppia interfaccia lan, una in una rete privata isolata a cui solo collegati i vari componenti della macchina. La seconda scheda è collegata ad una seconda rete di interconnessione di tutte le macchine del fornitore 1. La rete viene convogliata tramite una vlan denominata Vlan2 tramite gli switch aziendali e arriva su una lan dedicata del server virtuale di gestione Server1.

Lo scambio di dati tra Server1 e macchine operatrici avviene tramite scambio di file scritti e letti su una cartella condivisa sul Server1.

Il software sui pc si occupa solo della gestione delle varie operazioni sulla base dei dati letti.

Per la visualizzazione dello stato generale e dello scambio di informazioni tra Server1 e macchine su alcune postazioni di lavoro è affiancata una seconda postazione "standard" in rete aziendale da cui si accede al software di gestione dell'integratore e agli altri software gestionali aziendali.

Tutte le postazioni del fornitore 1, hanno accesso ad Internet tramite un firewall a cui arriva la Vlan2.

L'assistenza viene fatta tramite software Teamviewer con licenza del fornitore, installato su tutte i pc a bordo macchina, con una password cablata. Non c'è un controllo diretto dell'accesso del fornitore.

Alcuni pc aziendali su cui è installato il software di preparazione dei programmi di produzione delle macchine operatrici, hanno una doppia scheda di rete con una scheda in Vlan2, per l'accesso diretto ai pc a bordo macchina. Sui pc a bordo macchina è anche installato un VNC server per il controllo remoto da altri pc interni alla rete.

È presente un pc a bordo macchina di “fornitore 1” collegato alla macchina ed un terminale Citrix con cui è possibile visualizzare la schermata del magazzino, poiché tale monitor è, a differenza del primo, sulla rete aziendale.

Nel dettaglio è possibile accedere partendo da:

- “server integratore”, attraverso una VLAN2, si arriva ad uno switch lan aziendale, e tramite una LAN fornitore 1, è possibile arrivare al pc a bordo macchina.

Tramite firewall e VPN attraverso una VLAN 2, si arriva ad uno switch lan aziendale, e tramite una LAN fornitore 1, è possibile arrivare al pc a bordo macchina, questo per avere uno scambio di dati con il server del fornitore 1.

Dalla Lan aziendale è possibile visualizzare il gestionale ERP.

Le macchine gestite dal “fornitore 1” sono connesse e possono comunicare tra loro.

Dal pc a bordo macchina è possibile connettersi direttamente ai PLC.

Zona 1	Server integratore
Condotto 1.2	VLAN 2 - Switch
Condotto 2	Firewall e VPN
Condotto 3.2	Lan fornitore 1
Zona 2	Terminale Citrix
Condotto 3.1	Lan aziendale
Condotto 4	Lan privata isolata "macchina x”
Zona 3	Pc a bordo macchina
Zona 4	PLC
Condotto 5	Teamviewer
Condotto 6	VNC

Tabella 2.3.2.1*: Suddivisione zone e condotti fornitore 1*

2.3.3 Fornitore 2

Fornisce una macchina operatrice alimentata automaticamente dal magazzino automatico.

Il controllo della macchina avviene da due postazioni operatore collegate in lan privata isolata che transita sugli switch aziendali in Vlan3, per arrivare a due VM entrambe con doppia scheda di rete una in Vlan3 e l'altra in lan aziendale, una vm è un client con a bordo il software di gestione dell'integratore e agli altri software gestionali aziendali, a questa vm si collega in RDP l'operatore da una delle due postazioni dotata di doppio monitor. La seconda VM contiene un software del Fornitore2 che raccoglie le statistiche di produzione della macchina.

Alla rete privata è collegato un router VPN utilizzato dal fornitore per l'accesso alla rete interna della macchina, l'interfaccia wan del router è collegata ad una VLAN Fornitori che tramite un firewall aziendale permette l'accesso a internet.

Il pc operatore con il software proprietario del Fornitore2 a bordo scambiano dati tramite webservice con il server applicativo dell'integratore, che ha una scheda lan nella Vlan3.

Nel dettaglio è possibile accedere partendo da:

- "server integratore", attraverso una VLAN3, si arriva ad uno switch lan aziendale, e tramite una LAN fornitore 2, è possibile arrivare al pc a bordo macchina.
- Firewall e VPN, attraverso una VLAN 5, si arriva ad uno switch lan aziendale, e tramite un router VPN e firewall fornitore 2 (tosibox), è possibile arrivare al pc a bordo macchina

I fornitori da remoto possono accedere utilizzando Teamviewer.

È presente un pc a bordo macchina che comunica attraverso un pc virtuale con la rete aziendale, poiché tale pc virtuale ha una rete su fornitore 2 e su rete aziendale.

Il Pc virtuale ha una cartella condivisa che viene vista dal pc a bordo macchina.

È possibile tramite VNC (installato nel pc dell'operatore) accedere al virtuale poiché ha una scheda di rete nella rete aziendale ed una in fornitore 2, successivamente dal pc virtuale apro poi il VNC che va alla macchina.

Dal pc a bordo macchina è possibile connettersi direttamente ai PLC.

Zona 1	Server integratore
Condotto 1.3	VLAN 3 - Switch
Condotto 1.4	VLAN 5
Condotto 2	Firewall e VPN fornitore 2
Condotto 3.3	Lan fornitore 2 – privata ed isolata
Zona 2	Terminale Citrix
Condotto 3.1	Lan aziendale
Condotto 4	Router VPN fornitore 2
Zona 3	Pc a bordo macchina
Zona 4	PLC
Condotto 5	Teamviewer
Condotto 6	Tosibox
Condotto 7	VNC

Tabella 2.3.3.1*: Suddivisione zone e condotti fornitore 2*

2.3.4 Fornitore 3

Il Fornitore3 fornisce una macchina operatrice alimentata automaticamente con dei semi lavorati provenienti dal magazzino automatico.

La postazione operatore utilizza un pc Windows 7 con doppia scheda di rete una in lan privata isolata e la seconda in rete aziendale, comunica con il server applicativo dell'integratore in lan aziendale tramite WEBService, su questo pc è installato l'EDR aziendale, per il gestionale si collega in RDP sun una VM client con a bordo il software di gestione dell'integratore e agli altri software gestionali aziendali.

È presente un pc a bordo macchina ed una macchina virtuale. Il pc a bordo macchina può essere chiamato dal pc virtuale solo se sono "rispettate" alcune condizioni:

- Credenziali e tramite VNC con stessa rete
- Credenziali e firewall che permette di accedere ad un'altra rete (di solito non previsto)
- Credenziali con RDP (desktop da remoto)

Ovvero se rispettate tali condizioni è possibile accedere al pc virtuale e conseguentemente collegarsi al pc a bordo machina.

È possibile accedere partendo da:

"server integratore", attraverso una VLAN4, si arriva ad uno switch lan aziendale, e tramite una LAN fornitore 3 o attraverso LAN aziendale, è possibile arrivare al pc a bordo macchina. Utilizzano un servizio di teleassistenza (Secomea) che tramite VPN e UltraVNC si collega.

L'operatore dal pc a bordo macchina autorizza l'accesso, per la sola visualizzazione oppure per l'accesso ai comandi.

Dal pc a bordo macchina è possibile connettersi direttamente ai PLC.

Zona 1	Server integratore
Condotto 1.3	VLAN 4 - Switch
Condotto 3.4	Lan fornitore 3 – privata ed isolata
Zona 2	Terminale Citrix
Condotto 3.1	Lan aziendale
Zona 3	Pc a bordo macchina
Condotto 4	Secomea
Condotto 5	PLC

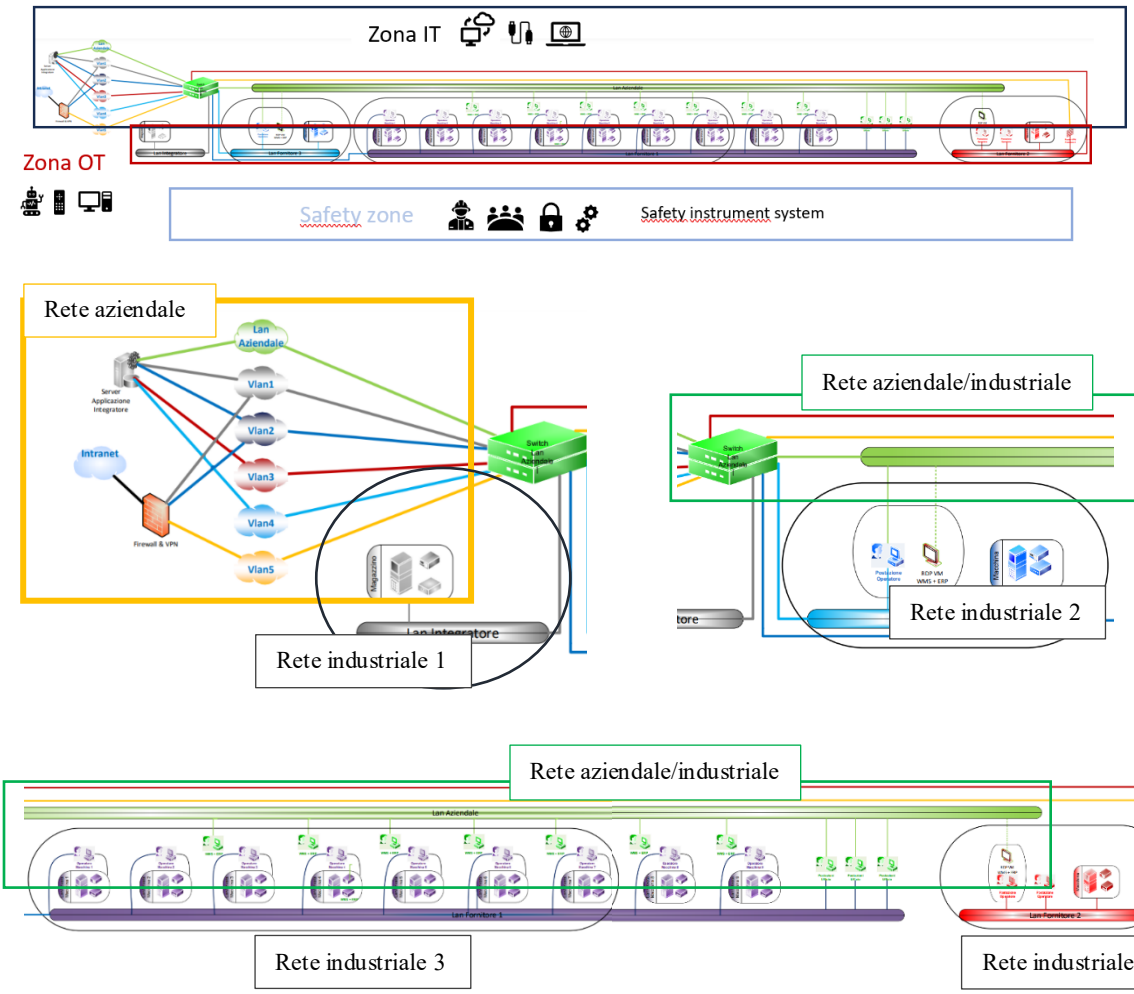
Tabella 2.3.4.1*: Suddivisione zone e condotti fornitore 3*

2.3.5 Suddivisione finale

Dopo aver suddiviso in maniera specifica e dettagliata ogni sistema in esame, risulta necessario per una maggiore comprensione e con il fine di seguire una corretta analisi suddividere il sistema in raggruppamenti di zone e condotti.

In generale è possibile affermare che sono presenti tre zone principali:

- la zona IT comprendente la rete aziendale (web server, file server…) e la rete aziendale/industriale (RDP, WMS + ERP…)
- la zona OT comprendente le reti industriali (PLC, interfaccia uomo-macchina…)
- la zona relativa ai sistemi di sicurezza (allarmi, fotocellule…) separata e non raggiungibile.



2.4 Comparazione tra rischio determinato e rischio tollerato

La presente fase permette di individuare quali sono le risorse informatiche su cui effettuare la valutazione dettagliata del rischio, ovvero quelle risorse per cui il rischio non è tollerabile dall'organizzazione.

Il primo passo è la definizione del livello di rischio tollerato dall'organizzazione e successivamente la comparazione tra rischio determinato e rischio tollerato.

Sulla base dei possibili impatti che possono generarsi a seguito di un attacco informatico, si considera per i sistemi in esame una soglia di accettazione del rischio medio < 10.

Risulta evidente che per ogni sistema in esame sarà necessario approfondire la valutazione del rischio, in quanto, ogni macchina presenta almeno un livello di rischio "ALTO",

In questo modo sarà possibile valutare l'effettiva probabilità di riuscita di un attacco informatico (ALTA, MEDIA, BASSA, TRASCURABILE) ed eventualmente predisporre le adeguate contromisure per poterla ridurre e conseguentemente ridurre il livello di rischio ad un livello accettabile, ovvero < 10.

Capitolo 3

La valutazione dettagliata del rischio

Nel presente capitolo verrà presentata la valutazione dettagliata del rischio effettuata per i sistemi in esame, sarà identificata l'effettiva probabilità di successo di un attacco informatico e saranno predisposte adeguate contromisure.

3.1 Introduzione alla valutazione dettagliata del rischio

La valutazione dettagliata dei rischi è la seconda analisi dei rischi eseguita per la cyber-sicurezza. Il suo scopo è quello di ottenere una comprensione definitiva dell'attuale livello di rischio all'interno di una struttura considerando i potenziali vettori di minaccia e le contromisure esistenti / pianificate, garantire che i criteri di rischio aziendali siano soddisfatti e fornire requisiti di sicurezza informatica.

Il punto di partenza per la valutazione dettagliata del rischio è l'output della valutazione iniziale dei rischi, in questo modo è possibile stabilire quali siano gli asset informatici che necessitano di un ulteriore approfondimento.

In questa fase è necessaria l'analisi delle vulnerabilità, dove viene valutata la rete esistente, i dispositivi connessi, le configurazioni, le versioni del software e altri fattori per identificare quali vulnerabilità sono attualmente presenti all'interno di una struttura e potrebbero essere prese di mira dagli aggressori. Ciò fornisce un input importante per la valutazione dettagliata dei rischi quando si considerano i punti di ingresso nel sistema e si valuta la probabilità di un attacco riuscito e la facilità con cui un utente malintenzionato può spostarsi tra i dispositivi nella rete di controllo.

Un'altra analisi fondamentale è la documentazione dei potenziali vettori di minaccia che permetterebbero agli aggressori l'ingresso nel sistema, ma considerando che potrebbe essere fornito un elenco di centinaia di vettori di minaccia da esaminare ed identificare questo metodo

non risulta efficace. Può essere utile esaminare categorie gestibili di minacce. Questi due fattori permettono di identificare la probabilità che un attacco informatico abbia luogo.

In seguito con la probabilità ottenuta ed il rischio determinato con la precedente analisi iniziale del rischio è possibile determinare se il rischio residuo è maggiore del rischio tollerabile dall'organizzazione ed in tal caso porre adeguate misure di prevenzione e protezione.

Danno					
	5- Estremo	5 - Medio	10 - Alto	15 – Alto	20 - Estremo
	4-Alto	4 - Basso	8 - Medio	12 - Alto	16 – Alto
	3- Medio	3 - Basso	6 - Medio	9 - Medio	12 - Alto
	2-Basso	2- Basso	4 - Basso	6 - Medio	8 - Medio
	1-Trascurabile	1 -Trascurabile	2- Basso	3 - Basso	4 - Basso
		1-Trascurabile	2-Bassa	3-Media	4-Alta
		Probabilità			

Tabella 3.1.1: *Matrice del rischio*

P_2: probabilità di accadimento dell'infortunio				
4-Alta	4-Bassa	8-Media	12-Alta	16-Alta
3-Media	3-Bassa	6-Media	9-Media	12- Alta
2-Bassa	2-Trascurabile	4-Bassa	6-Media	8- Media
1-Trascurabile	1-Trascurabile	2-Trascurabile	3-Bassa	4- Bassa
	1-Trascurabile	2-Bassa	3-Media	4-Alta
	P_1: probabilità successo attacco informatico			

Tabella 3.1.2: *Matrice delle probabilità per la valutazione dettagliata del rischio*

3.2 Analisi delle minacce

Le minacce informatiche**,** perpetuate tramite attacco informatico, sono definite dal *National Initiative For Cybersecurity Careers And Studies (*NICCS) come il tentativo di ottenere un accesso non autorizzato a servizi, risorse o informazioni di sistema altrui.

Consiste nell'atto intenzionale di tentare d'eludere uno o più servizi di sicurezza o i controlli di un sistema informatico per alterare la riservatezza**,** l'integrità e la disponibilità dei dati**.**

Detto in modo semplice, la minaccia informatica è l'azione che sfrutta una vulnerabilità per arrecare un danno al sistema informatico dell'azienda**.**

Nel caso in esame, poiché è stato valutato l'impatto sulle persone in caso di blocco in uno stato imprevisto, funzionamento in uno stato imprevisto e riavvio inatteso, la minaccia deve dar luogo ad una delle situazioni citate.

Dunque per valutare le minacce informatiche si è presa come riferimento la relazione sul panorama delle minacce nel 2022 elaborato dall'Agenzia dell'Unione europea per la sicurezza informatica (ENISA), dove sono state identificate le otto principali tipologie di minaccia:

1. **Ransomware: gli hacker prendono il controllo dei dati di qualcuno e richiedono un riscatto per ripristinare l'accesso**
   Si tratta di una particolare tipologia di malware, dal funzionamento semplice ma dalle conseguenze molto gravi. Una volta installato, il *ransomware* blocca completamente il sistema operativo dell'utente, mostrando una schermata in cui viene richiesto il pagamento di un "riscatto" (*ransom*).
2. **Malware: software che danneggia un sistema**
   Il malware include virus, worm, cavalli di Troia e spyware.
   Con malware si indica un programma che viene installato su un computer, generalmente all'insaputa dell'utente, con l'obiettivo di renderlo vulnerabile ad altri attacchi.
   L'aumento del malware è anche attribuito al *crypto-jacking* (l'uso segreto del computer di una vittima per creare criptovaluta illegalmente) e al malware *Internet-of-Things* (malware mirato a dispositivi connessi a Internet come router o videocamere).

3. **Minacce di ingegneria sociale: sfruttare l'errore umano per ottenere l'accesso a informazioni o servizi**

   Indurre le vittime ad aprire documenti, file o e-mail dannosi, visitare siti Web e concedere così l'accesso non autorizzato a sistemi o servizi. L'attacco più comune di questo tipo è il *phishing* (tramite posta elettronica); o *smishing* (tramite messaggi di testo). Quasi il 60% delle violazioni in Europa, Medio Oriente e Africa include una componente di ingegneria sociale, secondo una ricerca citata da Enisa.

   Le principali organizzazioni impersonate dai *phisher* provenivano dai settori finanziario e tecnologico.

4. **Minacce ai dati: prendere di mira le fonti di dati per ottenere accesso e divulgazione non autorizzati**

   Le minacce ai dati possono essere principalmente classificate come violazioni dei dati (attacchi intenzionali da parte di un criminale informatico) e fughe di dati (rilasci non intenzionali di dati). Il denaro rimane la motivazione più comune di tali attacchi. Solo nel 10% dei casi il movente è lo spionaggio.

5. **Minacce alla disponibilità - negazione di servizio: attacchi che impediscono agli utenti di accedere a dati o servizi**

   Queste sono alcune delle minacce più critiche per i sistemi IT. Aumentano in portata e complessità. Una forma comune di attacco consiste nel sovraccaricare l'infrastruttura di rete e rendere non disponibile un sistema. Gli attacchi sotto forma di minacce alla disponibilità colpiscono sempre più spesso le reti mobili e i dispositivi connessi.

6. **Minacce alla disponibilità - Minacce Internet: minacce alla disponibilità di Internet**

   Questi includono l'acquisizione fisica e la distruzione dell'infrastruttura Internet, nonché la censura attiva di notizie o siti Web di social media.

7. **Disinformazione/disinformazione - diffusione di informazioni fuorvianti**

   Il crescente utilizzo delle piattaforme dei social media e dei media online ha portato a un aumento delle campagne che diffondono disinformazione (informazioni volutamente falsificate) e disinformazione (condivisione di dati errati). L'obiettivo è quello di provocare paura e incertezza.

   La tecnologia *Deepfake,* tramite i "bot", consente di generare audio, video o immagini falsi che sono quasi indistinguibili da quelli reali.

8. **Attacchi alla catena di approvvigionamento: prendono di mira la relazione tra organizzazioni e fornitori**
   Questa è una combinazione di due attacchi: al fornitore e al cliente. Le organizzazioni stanno diventando più vulnerabili a tali attacchi, a causa di sistemi sempre più complessi e di una moltitudine di fornitori, che sono più difficili da controllare.

Tra queste principali tipologie di minaccia gli attacchi *ransomware*, *malware* e le minacce di ingegneria sociale (*phishing o smishing*) sono quelle maggiormente impiegate nel settore manifatturiero ed inerenti allo studio, in quanto, indipendentemente dal loro scopo principale, hanno la possibilità di generare le situazioni precedentemente menzionate.

Al fine di identificare, e ridurre, la probabilità che un attacco informatico abbia successo, tali minacce andranno confrontate con le vulnerabilità presenti.

3.3 Analisi delle vulnerabilità

Una vulnerabilità informatica può essere definita come un componente (esplicita o implicita) di un sistema informatico, in cui le misure di sicurezza sono assenti, ridotte o compromesse. Questo rappresenta un punto debole del sistema e lo espone ad una minaccia informatica. Ovvero consente a un eventuale aggressore, di comprometterne il livello di sicurezza dell'intero sistema. Tali vulnerabilità possono essere anche relative all'ambiente fisico e legate alle risorse umane.

È importante sottolineare la presenza di problemi di asset management, in quanto il perimetro e le risorse sono parzialmente conosciute, comportando difficoltà nella gestione del perimetro e delle risorse e conseguentemente a controllarne il rischio.

Per quanto concerne la valutazione delle vulnerabilità questa è stata effettuata con il supporto del cyber-security manager, in quanto responsabile e conoscitore degli aspetti relativi alla sicurezza di rete ed aziendale.

Un utile strumento per l'individuazione di alcune vulnerabilità è stato l'allegato B della norma IEC 62443-3-3, il quale contiene delle tabelle di mappatura tra requisiti e SL-C, in questo caso utilizzato per ricavare SL-A.

1. Controllo dell'identificazione e dell'autenticazione						
	SL 1	**SL 2**	**SL 3**	**SL 4**	Presente	**SL-A**
1. Identificazione ed autenticazione utente umano	X	X	X	X	SI	**SL 3**
-Identificazione univoca dell'utente		X	X	X	SI	
-Autenticazione multi fattore per reti non attendibili			X	X	SI	
-Autenticazione multi fattore per tutte le reti				X	NO	
2. Identificazione ed autenticazione processo software e dispositivo		X	X	X	SI	**SL 3**
-Identificazione univoca dell'utente			X	X	SI	
3. Gestione account	X	X	X	X	SI	**SL 3**
-Gestione unificata account			X	X	SI	
4. Gestione identificatori	X	X	X	X	NO	**SL 0**
5. Gestione dell'autenticazione	X	X	X	X	NO	**SL 0**
-sicurezza hardware per le credenziali d' identità del processo software			X	X	NO	

6. Gestione accessi wireless	X	X	X	X	NO	**SL 0**
-Identificazione univoca dell'utente		X	X	X	NO	
7. robustezza dell'autenticazione basata su password	X	X	X	X	SI	**SL 1**
-generazione di password e limitazione della durata per gli utenti umani			X	X	NO	
-limitazione durata della password per tutti gli utenti (utenti umani e utenti di servizio)				X	NO	
8. certificati di infrastruttura a chiave pubblica PKI		X	X	X	NO	**SL 0**
9. robustezza dell'autenticazione a chiave pubblica		X	X	X	NO	**SL 0**
-Sicurezza hardware per l'autenticazione a chiave pubblica			X	X	NO	
10. Feedback dell'autenticatore	X	X	X	X	SI	**SL 1**
11. Tentativi di accesso falliti	X	X	X	X	NO	**SL 0**
12. Notifica di utilizzo del sistema	X	X	X	X	SI	**SL 1**
13. Accesso tramite rete non attendibile	X	X	X	X	SI	**SL 1**
-Approvazione esplicita richiesta di accesso		X	X	X	NO	
2. Verifica dell'utilizzo						
14. Rinforzo dell'autorizzazione (previlegio minimo → strettamente necessario. La granularità dell'accesso non è possibile perché non ho il controllo delle singole funzioni)	X	X	X	X	NO	**SL 0**
-Rinforzo dell'autorizzazione per tutti gli utenti		X	X	X	NO	
-Mappatura dei permessi al ruolo		X	X	X	NO	
- supervisore override			X	X	NO	
-Doppia approvazione				X	NO	
15. Verifica dell'utilizzo wireless	X	X	X	X	NO	**SL 0**
-Identificazione e report dispositivi wireless non autorizzati			X	X	NO	
16. Verifica dell'utilizzo di dispositivi mobili e portatili	X	X	X	X	NO	**SL 0**
-Rinforzo dello stato di sicurezza per dispositivi mobili e portatili			X	X	NO	
17. codice mobile	X	X	X	X	NO	**SL 0**
-Controllo dell'integrità del codice mobile			X	X	NO	
18. Blocco della sessione	X	X	X	X	NO	**SL 0**
19. Cessazione sessione remota			X	X	NO	**SL 0**
20. Controllo sessione corrente	X	X	X	X	NO	**SL 0**
21. Registrazione audit		X	X	X	SI	**SL 2**

-Gestione centrale audit, percorso di controllo a livello di sistema			X	X	SI	
22. capacità di archiviazione audit	X	X	X	X	SI	**SL 3**
-Avvisa quando gli audit registrati raggiungono la soglia della capacità di archiviazione			X	X	SI	
23. Risposta agli errori di elaborazione dell'audit	X	X	X	X	NO	**SL 0**
24. timestamps		X	X	X	SI	**SL 4**
-sincronizzazione dell'ora interna			X	X	SI	
-protezione dell'integrità della sorgente dell'ora				X	SI	
25. non ripudio			X	X	NO	**SL 0**
-non ripudio per tutti gli utenti				X	NO	
3. Integrità del sistema						
26. Integrità della comunicazione	X	X	X	X	NO	**SL 0**
-Protezione crittografica dell'integrità			X	X	NO	
27. Protezione da codice dannoso	X	X	X	X	SI	**SL 3**
-Protezione da codice dannoso sul punto di ingresso ed uscita		X	X	X	SI	
-Gestione centrale e segnalazione per protezione da codice dannoso			X	X	SI	
28. Verifica funzionalità di sicurezza	X	X	X	X	SI	**SL 4**
-Meccanismo automatico per la verifica delle funzionalità di sicurezza			X	X	SI	
-Verifica funzionalità di sicurezza durante le normali operazioni				X	SI	
29. Integrità del software e delle informazioni		X	X	X	NO	**SL 0**
-Notifiche automatiche riguardo la violazione dell'integrità			X	X	NO	
30. Convalida dell'input	X	X	X	X	SI	**SL 1**
31. Uscita determinata	X	X	X	X	NO	**SL 0**
32. Gestione dell'errore		X	X	X	SI	**SL 2**
33. Integrità della sessione		X	X	X	SI	**SL 3**
-Invalidazione dell'ID della sessione dopo che la sessione è terminata			X	X	SI	
-Generazione di un ID sessione unico			X	X	NO	
-Casualità dell'ID sessione				X	NO	
34. Protezione delle informazioni di audit		X	X	X	SI	**SL 4**
-Registrazione degli audit su supporti scrivibili una volta				X	SI	
4. Riservatezza dei dati						
35. Riservatezza delle informazioni	X	X	X	X	NO	**SL 0**
-Protezione della riservatezza a riposo o in transito tramite una rete non attendibile		X	X	X	NO	
-Protezione della riservatezza tra i confini della zona				X	NO	

36. Permanenza delle informazioni		X	X	X	NO	**SL 0**
-Epurazione della risorsa di memoria condivisa			X	X	NO	
37. Uso della crittografia	X	X	X	X	Non è richiesto perché rete interna	---
5. Flusso di dati limitato						
38. Segmentazione della rete	X	X	X	X	SI	**SL 1**
-Segmentazione fisica della rete		X	X	X	NO	
-Indipendenza dai sistemi di rete non controllati			X	X	NO	
-Isolamento logico e fisico delle reti critiche				X	NO	
39. Protezione del confine di zona	X	X	X	X	SI	**SL 2**
-Negazione per impostazione predefinita, consenti per eccezione		X	X	X	SI	
-Modalità *"island"*			X	X	NO	
-*Fail closed* In caso di errore, il sistema viene terminato e non è possibile interagire ulteriormente con esso finché la condizione di failure non è stata identificata e risolta.			X	X	NO	
40. Restrizione della comunicazione generica da persona a persona	X	X	X	X	SI	**SL 1**
-Proibire tutte le comunicazioni generiche da persona a persona			X	X	NO	
41. Parzionamento delle applicazioni	X	X	X	X	NO	**SL 0**
6. Risposta tempestiva all'evento						
42. Accessibilità al registro di controllo	X	X	X	X	SI	**SL 1**
-Accesso programmato al registro di controllo			X	X	NO	
43. Monitoraggio continuo		X	X	X	SI	**SL 2**
7. Disponibilità delle risorse						
44. Negazione della protezione del servizio	X	X	X	X	NO	**SL 0**
-Gestire i carichi di comunicazione		X	X	X	NO	
-Limitare gli effetti ad altri sistemi o reti			X	X	NO	
45. Gestione delle risorse	X	X	X	X	NO	**SL 0**
46. Backup del sistema di controllo	X	X	X	X	SI	**SL 3**
-Verifica del backup		X	X	X	SI	
-Automazione del backup			X	X	SI	
47. Recupero e ricostituzione sistemi di controllo	X	X	X	X	SI	**SL 1**
48. Alimentazione di emergenza	X	X	X	X	SI	**SL 1**

49. Impostazioni di configurazione della rete e di sicurezza	X	X	X	X	NO	**SL 0**
-Segnalazione leggibile della macchina delle impostazioni di sicurezza correnti			X	X	NO	
50. Funzionalità minima	X	X	X	X	NO	**SL 0**
51. Inventario dei componenti dei sistemi di controllo		X	X	X	NO	**SL 0**

Tabella 3.3.1*: Tabella di mappatura tra requisiti e SL-C*

Ad integrazione della precedente tabella si hanno i seguenti punti da tenere in considerazione:

1. L'accesso fisico all'azienda ed al sistema in esame è parzialmente controllato. Nello specifico è possibile accedere all'interno dell'azienda e dei diversi stabili informando l'agente di sicurezza di un incontro programmato con un responsabile all'interno dell'azienda, il quale riceverà una mail di notifica senza possibilità di approvazione, offrendo un accesso fisico non autorizzato ai sistemi e alle infrastrutture.
2. L'accesso remoto non è controllato e/o autorizzato, precisamente:
   - gli operatori dell'integratore possono accedere senza necessità di richiesta da parte dell'azienda, con la possibilità di effettuare azioni di avvio ed arresto della "Macchina 1" (se la macchina è in condizioni di sicurezza)
   - per quanto concerne gli operatori relativi agli altri fornitori non si ha la certezza che l'operatore sia effettivamente un fornitore previsto per effettuare la necessaria manutenzione o meno
3. I pc ospitano il sistema operativo window 7, senza protezione antivirus, un sistema operativo obsoleto e conseguentemente esposto a maggiori rischi, questo poiché le reti operative che prima erano isolate vengono connesse alle reti IT per aumentare l'efficienza, ma questo espone ai rischi quei protocolli proprietari che non sono sicuri e apparecchiature OT vecchie di decenni, che spesso non hanno le patch aggiornate.
4. I pc ove è installata l'applicazione team viewer permettono l'accesso ad internet all'operatore (o chiunque ne faccia uso), con il rischio di infettare il sistema, volontariamente o non volontariamente

5. Il fattore umano, in quanto, un'adeguata formazione ha la possibilità di impedire la riuscita di un attacco informatico

È doveroso precisare che il metodo successivamente esposto è un metodo semplificato, poiché una valutazione precisa e dettagliata richiederebbe competenze e conoscenze di cyber-sicurezza molto elevate.

A questo punto poter valutare la probabilità è stata predisposta una tabella contente i cinque punti appena esposti ed una parte dei punti presenti nella §Tabella 3.3.1 (non tutti in quanto alcuni di essi non risultano utili/sfruttabili per un eventuale attacco informatico e di conseguenza non sono stati considerati).

Poiché alle diverse vulnerabilità può corrispondere un diverso livello di protezione si è deciso di assegnare un valore in base al SL, quando presente, altrimenti si assegna a priori il valore pari ad 1, nel dettaglio:

- SL-0: 1
- SL-1: 0,75
- SL-2: 0.5
- SL-3: 0,25
- SL-4: 0

Vulnerabilità considerate			
	Valore minimo	SL-A	**Valore**
1. Identificazione ed autenticazione utente umano	**0**	SL 3	**0,25**
2. Identificazione ed autenticazione processo software e dispositivo	**0,25**	SL 3	**0,25**
3. Gestione account	**0,25**	SL 3	**0,25**
4. Gestione identificatori	**0,75**	SL 0	**1**
5. Gestione dell'autenticazione	**0,25**	SL 0	**1**
6. Gestione accessi wireless	**0,5**	SL 0	**1**
7. robustezza dell'autenticazione basata su password	**0**	SL 1	**0,75**
8. certificati di infrastruttura a chiave pubblica PKI	**0,5**	SL 0	**1**
9. robustezza dell'autenticazione a chiave pubblica	**0,25**	SL 0	**1**
10. Feedback dell'autenticatore	**0,75**	SL 1	**0,75**

11. Tentativi di accesso falliti	**0,75**	SL 0	**1**
12. Notifica di utilizzo del sistema	**0,75**	SL 1	**0,75**
13. Accesso tramite rete non attendibile	**0,5**	SL 1	**0,75**
14. Rinforzo dell'autorizzazione (previlegio minimo)	**0**	SL 0	**1**
15. Verifica dell'utilizzo wireless	**0,25**	SL 0	**1**
16. Verifica dell'utilizzo di dispositivi mobili e portatili	**0,25**	SL 0	**1**
17. codice mobile	**0,25**	SL 0	**1**
18. Blocco della sessione	**0,75**	SL 0	**1**
19. Cessazione sessione remota	**0,25**	SL 0	**1**
20. Controllo sessione corrente	**0,75**	SL 0	**1**
21. Registrazione audit	**0,25**	SL 2	**0,5**
22. capacità di archiviazione audit	**0,25**	SL 3	**0,25**
23. Risposta agli errori di elaborazione dell'audit	**0,75**	SL 0	**1**
24. timestamps	**0**	SL 4	**0**
25. non ripudio	**0**	SL 0	**1**
26. Integrità della comunicazione	**0,25**	SL 0	**1**
27. Protezione da codice dannoso	**0,25**	SL 3	**0,25**
28. Verifica funzionalità di sicurezza	**0**	SL 4	**0**
29. Integrità del software e delle informazioni	**0,25**	SL 0	**1**
30. Convalida dell'input	**0,75**	SL 1	**0,75**
31. Gestione dell'errore	**0,5**	SL 2	**0,5**
32. Integrità della sessione	**0**	SL 3	**0,25**
33. Protezione delle informazioni di audit	**0**	SL 4	**0**
34. Riservatezza delle informazioni	**0**	SL 0	**1**
35. Permanenza delle informazioni	**0,5**	SL 0	**1**
36. Segmentazione della rete	**0**	SL 1	**0,75**
37. Protezione del confine di zona	**0,25**	SL 2	**0,5**
38. Restrizione della comunicazione generica da persona a persona	**0,25**	SL 1	**0,75**
39. Parzionamento delle applicazioni	**0,75**	SL 0	**1**
40. Assenza protezione antivirus	**0**		**1**
41. Parziale controllo dell'accesso fisico	**0**		**1**
42. Accesso ad internet	**0**		**1**
43. Mancanza di controllo accesso remoto da parte dei fornitori	**0**		**1**
44. Fattore umano	**0**		**1**
TOTALE	**13/44**		**33,25/44**

***Tabella 3.3.2**: Tabella contenete le vulnerabilità considerate*

VALORE	P_1
$34 < P \leq 44$	ALTA
$24< P \leq 34$	**MEDIA**
$13< P \leq 24$	BASSA
$P = 13$	TRASCURABILE

Tabella 3.3.3*: suddivisione dei livelli di probabilità P_1*

La suddivisione dei valori è tale poiché non è sempre possibile raggiungere il SL-4 (comportando un valore pari a 0), di conseguenza è stato calcolato il valore minimo, ovvero quel valore che si otterrebbe se il sistema raggiungesse il massimo SL possibile per ogni punto. Tale valore minimo è stato corrisposto ad una probabilità trascurabile, in quanto non sarebbe oggettivamente possibile ridurlo ulteriormente. Questo valore minimo è stato successivamente sottratto al valore massimo ottenibile (44) ed il risultato suddiviso al fine di individuare i range di valori per le diverse probabilità.

Ne consegue che è possibile ritenere la probabilità di riuscita di un attacco informatico MEDIA, rendendo comunque necessario l'incremento di specifiche misure di prevenzione e protezione.

3.4 Identificazione e valutazione di contromisure

Al fine di ridurre la probabilità che un attacco informatico abbia successo e conseguentemente ridurre il rischio per la sicurezza delle persone è necessario individuare ed attuare appropriate contromisure.

La *"defense in depth"*, ovvero la difesa in profondità, è un approccio alla sicurezza informatica in cui vengono stratificati una serie di meccanismi difensivi per proteggere dati e informazioni preziose. Se un meccanismo dovesse fallire, ci si troverebbe di fronte ad un altro meccanismo che interverrebbe immediatamente per contrastare l'attacco. Questo approccio a più livelli con ridondanze intenzionali aumenta la sicurezza di un sistema nel suo complesso e affronta molti vettori di attacco diversi.

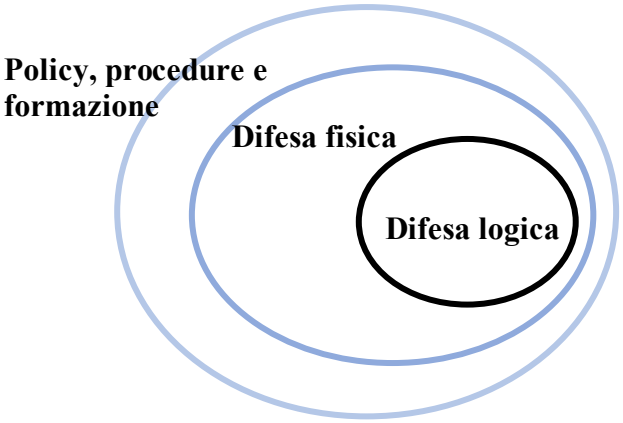


***Figura 3.4.1**:difesa in profondità*

Di seguito verranno elencati i primi punti di miglioramento da porre in atto:

a) La consapevolezza è uno strumento essenziale e si pone come prima linea di difesa per ridurre i rischi di cyber sicurezza, poiché personale vigile, informato e con un'adeguata formazione tecnica associata alle minacce e vulnerabilità di hardware, software e ingegneria sociale è fondamentale per il mantenimento in sicurezza del sistema.
   È necessario prevedere una formazione periodica al fine di illustrare i rischi e le principali minacce presenti, ad esempio dovute ad e-mail di *phishing*, chiavette infette, rischi relativi all'accesso ad internet (vietandone l'uso improprio), etc… e le azioni da porre in atto in caso di situazione sospetta. Poiché questo aspetto è di estrema importanza sarebbe opportuno verificare l'effettiva efficacia della formazione tramite appositi test.

b) In secondo luogo, il miglioramento della modalità di accesso fisico all'area aziendale può fare in modo che gli accessi non autorizzati siano irrealizzabili. Ad esempio, in assenza di pass e nominativo in lista, il visitatore potrà informare la guardia di sicurezza di un incontro previsto con un tecnico o superiore aziendale, il quale riceverà una e-mail (come già previsto) e a cui dovrà dare conferma (attualmente non previsto) oppure una telefonata.
c) Un altro fattore su cui è possibile lavorare è l'incremento di un controllo sugli accessi remoti dei fornitori, cercando di risolvere due problemi:
    - Per quanto riguarda gli operatori dell'integratore i quali possono accedere senza necessità di richiesta da parte dell'azienda, considerando che la ditta dell'integratore gestisce il server, fermo restando che la gestione del personale (ed eventuali intrusi) è a carico della ditta dell'integratore, da parte dell'azienda deve essere previsto un limite di azione, negando quindi la possibilità di avviare o fermare la macchina;
    - per quanto concerne gli operatori relativi agli altri fornitori, per i quali attualmente non si ha la possibilità di verifica dell'identità, può essere prevista una lista di nominativi degli operatori ed un controllo multi fattore per verificarne l'identità.

Per quanto concerne gli aspetti tecnici di software, programmi e dispositivi, questi verranno elencati di seguito:

1. Utilizzo di un NAC: *Network Access Control.*

   Il NAC è un sistema di sicurezza nato per il controllo degli accessi a una rete locale. Con il passare degli anni, però, si è evoluto sino a diventare una soluzione molto più versatile, utilizzabile anche per segmentare la rete o per automatizzare il riconoscimento e il tracciamento dei dispositivi che vogliono connettersi a una LAN.
   Grazie alla gestione delle policy, ad esempio, è **possibile bloccare l'accesso alla rete di dispositivi non sicuri**. I NAC di ultima generazione, infatti, permettono il controllo dello stato di sicurezza degli endpoint, che consente di scoprire quali sono i dispositivi infetti o non sicuri. L'integrazione con altri strumenti di sicurezza – come antivirus e antimalware – consente ai NAC di offrire livelli di sicurezza ancora più elevati.

Una soluzione di *Network Access Control*, dunque, si compone di applicativi, servizi e policy che consentono ai responsabili IT o agli addetti alla sicurezza informatica aziendali di proteggere nel miglior modo possibile il perimetro informatico.
In particolare, i sistemi NAC garantiscono questi risultati grazie a un processo composto da tre diversi passaggi:

- autenticazione del dispositivo che vuole connettersi al network;
- verifica della conformità alle policy di sicurezza;
- monitoraggio del comportamento dell'endpoint ed eventuale applicazione di misure di sicurezza.

Non solo, un sistema di controllo degli accessi alla rete è in grado anche di scoprire e monitorare tutti gli endpoint connessi alla LAN aziendale, categorizzarli per tipologia (computer o smartphone e sistema operativo utilizzato) e "reagire" ai loro comportamenti in base a norme e policy configurate centralmente dal team IT o di sicurezza informatica aziendale.
Grazie alle policy, in particolare, sarà possibile determinare in maniera granulare quali dispositivi possono accedere automaticamente al network e quali, invece, verranno messi "in attesa" di un controllo manuale da parte di un responsabile. Ad esempio, sarà possibile stabilire che tutti gli smartphone non aggiornati ad Android 8 o superiore non possano accedere; oppure che i computer Windows siano automaticamente esclusi dall'accesso alla rete.
Le policy, inoltre, possono essere utilizzate per impedire l'accesso alle risorse di rete a dispositivi sprovvisti di antivirus o altre soluzioni di sicurezza informatica che esporrebbero l'intero network a pericoli inutili. A seconda della configurazione scelta, poi, i NAC possono "suggerire" ai dispositivi non conformi quale aggiornamento o applicativo installare, così da rispettare i "requisiti minimi" imposti e consentire loro di accedere alla rete.

2. Prevedere il termine della sessione remota automaticamente dopo un periodo di inattività configurabile o manualmente da parte dell'operatore che ha avviato la sessione. Questo permetterebbe di evitare operazioni non legittime da parte di operatori non autorizzati, ad esempio a seguito dell'allontanamento dalla postazione dell'operatore che stava lavorando tramite la sessione remota.

Il termine della sessione manuale presenta come vantaggio il controllo da parte dell'operatore, ma al tempo stesso ne prende gli svantaggi quali ad esempio una possibile dimenticanza.

D'altro canto un'interruzione automatica della sessione, se con una tempistica accuratamente stabilita, evita la possibilità di azioni illegittime.

3. Installazione di un sistema antivirus studiato affinché sia implementabile sui pc bordo macchina con le dovute restrizioni e policy in modo che non impatti sulla produzione.
4. Per la macchina relativa al fornitore 2 è possibile utilizzare per l'assistenza remota il sistema Tosibox, andando a disattivare l'opzione impostando nelle opzioni di Teamviewer di accettare in ingresso solamente connessioni LAN, in questo modo sarà possibile effettuare l'accesso solo ed esclusivamente via Tosibox.

   Ove questo non sia possibile sarà necessario impedire l'accesso a qualsiasi sito web diverso da quello necessario (Teamviewer).
5. Attraverso una configurazione del sistema di controllo, questo avrà la capacità di impedire ulteriori accessi avviando il blocco della sessione dopo un periodo di tempo configurabile di inattività o tramite avvio manuale. Il blocco della sessione rimarrà in vigore fino a quando l'utente umano proprietario della sessione o un altro utente umano autorizzato ristabilisce l'accesso utilizzando appropriate procedure per l'identificazione e l'autenticazione.
6. Attraverso l'aggiornamento della release il sistema di controllo avrà la capacità di limitare il numero di sessioni simultanee per interfaccia per un dato utente (umano, processo software o dispositivo) ad un numero configurabile di sessioni.
7. Applicazione del principio di previlegio minimo con modifiche alle impostazioni del NAC e del firewall, tale principio prevede di assegnare agli utenti solo i privilegi necessari per svolgere le loro attività. Ciò significa che gli amministratori dovrebbero possedere solo i privilegi necessari per svolgere il proprio lavoro e non dovrebbero avere accesso indiscriminato a tutte le risorse aziendali. In questo modo anche se un utente malintenzionato riuscisse ad ottenere un accesso, le azioni effettuabili sarebbero limitate alla tipologia di account (e previlegio) senza la possibilità di raggiungere qualsiasi zona.
8. I sistemi ed apparecchi critici, ovvero che necessitano di un'elevata protezione (le macchine utensili) possono essere isolati in un segmento di rete dedicato, in un'isola sicura, con l'aiuto di piccoli firewall come Microwall. I necessari collegamenti tra i sistemi sull'isola e la rete circostante vengono registrati prima e descritti attraverso

una lista positiva di regole. Solo i pacchetti di dati espressamente ammessi vengono inoltrati, tutti gli altri vengono rifiutati e, all'occorrenza, protocollati. I sistemi isolati vengono così protetti efficacemente da attacchi di hacker o malware e da errori umani poiché viene impedito lo spostamento laterale. Pertanto, in caso di violazione del perimetro della rete, i segmenti di rete impediscono agli hacker di spostarsi lateralmente all'interno della rete.

Inoltre, la segmentazione fornisce un modo logico per isolare un attacco attivo prima che si diffonda nella rete.

La valutazione della vulnerabilità ha permesso la definizione di un SL-T (livello di sicurezza target) il quale è stato raggiunto tramite l'individuazione (ed applicazione) di possibili contromisure.

Si è così ottenuto un "valore corretto" che verrà impiegato per identificare il livello di probabilità raggiunto.

La tabella di seguito identifica il valore ottenuto per ogni vulnerabilità e la contromisura associata (identificata con il numero o lettera all'interno della parentesi) che ha permesso la riduzione del valore. Nonostante non sia segnato in ogni riga la formazione degli operatori è la base su cui costruire un'adeguata protezione verso gli attacchi hacker (e non solo), senza la quale, si potrebbe dire, nessuna misura fisica o logica ha efficacia.

Vulnerabilità considerate		**Applicazione contromisure**		
	Valore	**Contromisura**	SL-A=**SL-T**	**Valore corretto**
1. Identificazione ed autenticazione utente umano	**0,25**	-	SL 3	**0,25**
2. Identificazione ed autenticazione processo software e dispositivo	**0,25**	-	SL 3	**0,25**
3. Gestione account	**0,25**	-	SL 3	**0,25**
4. Gestione identificatori	**1**	-	SL 0	**1**
5. Gestione dell'autenticazione	**1**	-	SL 0	**1**
6. Gestione accessi wireless	**1**	✓ (1)	SL 2	**0,5**
7. robustezza dell'autenticazione basata su password	**0,75**	-	SL 1	**0,75**
8. certificati di infrastruttura a chiave pubblica PKI	**1**	-	SL 0	**1**
9. robustezza dell'autenticazione a chiave pubblica	**1**	-	SL 0	**1**
10. Feedback dell'autenticatore	**0,75**	-	SL 1	**0,75**
11. Tentativi di accesso falliti	**1**	-	SL 0	**1**

12. Notifica di utilizzo del sistema	**0,75**	-	SL 1	**0,75**
13. Accesso tramite rete non attendibile	**0,75**	-	SL 1	**0,75**
14. Rinforzo dell'autorizzazione (previlegio minimo)	**1**	✓ (1,7)	SL 2	**0,5**
15. Verifica dell'utilizzo wireless	**1**	✓ (1)	SL 3	**0,25**
16. Verifica dell'utilizzo di dispositivi mobili e portatili	**1**	✓ (1)	SL 3	**0,25**
17. codice mobile	**1**	-	SL 0	**1**
18. Blocco della sessione	**1**	✓ (5)	SL 1	**0,75**
19. Cessazione sessione remota	**1**	✓ (2)	SL 2	**0,5**
20. Controllo sessione corrente	**1**	✓ (6)	SL 3	**0,25**
21. Registrazione audit	**0,5**	-	SL 2	**0,5**
22. capacità di archiviazione audit	**0,25**	-	SL 3	**0,25**
23. Risposta agli errori di elaborazione dell'audit	**1**	-	SL 0	**1**
24. timestamps	**0**	-	SL 4	**0**
25. non ripudio	**1**	-	SL 0	**1**
26. Integrità della comunicazione	**1**	-	SL 0	**1**
27. Protezione da codice dannoso	**0,25**	-	SL 3	**0,25**
28. Verifica funzionalità di sicurezza	**0**	-	SL 4	**0**
29. Integrità del software e delle informazioni	**1**	-	SL 0	**1**
30. Convalida dell'input	**0,75**	-	SL 1	**0,75**
31. Gestione dell'errore	**0,5**	-	SL 2	**0,5**
32. Integrità della sessione	**0,25**	-	SL 3	**0,25**
33. Protezione delle informazioni di audit	**0**	-	SL 4	**0**
34. Riservatezza delle informazioni	**1**	-	SL 0	**1**
35. Permanenza delle informazioni	**1**	-	SL 0	**1**
36. Segmentazione della rete	**0,75**	-	SL 2	**0,5**
37. Protezione del confine di zona	**0,5**	-	SL 2	**0,5**
38. Restrizione della comunicazione generica da persona a persona	**0,75**	-	SL 1	**0,75**
39. Parzionamento delle applicazioni	**1**	-	SL 0	**1**
40. Assenza protezione antivirus	**1**	✓ (3)		**0**
41. Parziale controllo dell'accesso fisico	**1**	✓ (b)		**0**
42. Accesso ad internet	**1**	✓ (4)		**0**
43. Mancanza di controllo dell'accesso remoto da parte dei fornitori	**1**	✓ (c)		**0**
44. Fattore umano	**1**	✓ (a)		**0**
TOTALE	**33,25/44**			**24/44**

***Tabella 3.4.1**: vulnerabilità e contromisure associate*

A questo punto, ne consegue che è possibile ritenere la probabilità di riuscita di un attacco informatico BASSA.

Effettuando una rivalutazione del rischio e mantenendo costanti gli altri valori, quali il danno e la probabilità di accadimento dell'infortunio, permane un solo rischio residuo ALTO

Nonostante il rischio permanga ALTO è necessario ricordare che la tesi si è svolta con l'obbiettivo di individuare contromisure atte a prevenire ed evitare un possibile attacco informatico con conseguenze safety, senza quindi lavorare su eventuali misure di protezione e prevenzione da applicare a tali rischi.

In questo caso l'utilizzo di adeguati dispositivi di protezione individuali: elmetto, scarpe antinfortunistiche ed in particolare un adeguato dispositivo anticaduta, ovvero l'imbragatura di sicurezza con prolunga, la quale dovrà essere ancorata ai punti di aggancio della piattaforma a cestello e/o del ponteggio, permette la riduzione di un possibile DANNO alla persona; inoltre un'adeguata formazione ed un adeguato addestramento degli operatori addetti alla manutenzione permette di ridurre la probabilità che tale caduta avvenga, in quanto consapevoli del rischio e delle modalità di svolgimento in sicurezza del lavoro.

Macchina 1: Magazzino automatico Lavoro in quota per attività di manutenzione a seguito di un attacco informatico												
Rischio	Conseguenze	Probabilità			Danno	R	Misure di prevenzione e protezione	Probabilità			Danno	R
		P1	P2	P				P1	P2	P		
Caduta dall'alto	Infortuni gravi e disabilitanti o morte	B	M	M	ESTREMO	ALTO	Utilizzo DPI Formazione ed addestramento operatori	B	**B**	B	**BASSO**	**BASSO**

		
EN 361	**EN 345**	**EN 397**

Un maggiore livello di sicurezza può essere raggiunto impostando un'uscita predeterminata, ovvero il raggiungimento da parte del trasloelevatore di una "posizione di sicurezza" come ultimo comando in caso di arresto, qualunque sia la posizione in cui si trovi in quel momento.

Quindi idealmente si avrà un abbassamento del traslo fino ad una altezza rispetto al piano di calpestio < 2m ed un successivo movimento laterale per portarlo in una posizione prestabilita.

Tale movimentazione può essere effettata manualmente tramite pulsantiera palmare dal personale autorizzato il quale è stato formato ed informato sull'utilizzo e che adotti le misure previste per la sicurezza.

In questa circostanza il rischio di caduta dall'alto non sussisterebbe poiché la definizione di lavoro in quota, ricavabile dal D. Lgs. 81/2008, noto anche come Testo Unico Sicurezza sul Lavoro (TUSL) definisce i lavori in quota come un'attività lavorativa che espone il lavoratore al rischio di caduta dall'alto da una quota posta ad un'altezza superiore a 2 m rispetto ad un piano stabile. È giusto sottolineare che questo non significa che una caduta da un'altezza di 1,90m (o inferiore) non possa essere pericolosa, ma si può ritenere minore il danno conseguente rispetto ad altezze più elevate.

Inoltre questa misura di prevenzione non provocherebbe l'introduzione di nuovi rischi ancora non valutati, in quanto è già stata presa in considerazione la possibilità (seppur bassa) che un operatore rimanga intrappolato durante un riavvio improvviso della macchina.

Capitolo 4

Conclusioni

4.1 Conclusioni

La tesi si è svolta con l'obbiettivo di condurre per una linea manifatturiera l'analisi dei rischi derivanti da un attacco di cybersicurezza, tenendo in considerazione le sole conseguenze *safety*, l'esclusività di questo aspetto ha rivolto il lavoro verso la protezione delle persone.

Lo standard IEC 62443-3-2, impiegato per la produzione della tesi, dichiara che non esiste una ricetta semplice per la protezione di un sistema di automazione e controllo industriale (IACS) e c'è una buona ragione per questo. Questo perché la sicurezza è una questione di gestione del rischio. Ogni IACS presenta un rischio diverso per l'organizzazione a seconda delle minacce a cui è esposta, la probabilità che si verifichino tali minacce, le vulnerabilità intrinseche del sistema e le conseguenze se il sistema dovesse essere compromesso.

Detto ciò questo standard si propone di guidare l'organizzazione attraverso il processo di valutazione del rischio, di identificazione e applicazione di contromisure di sicurezza. Ma affinché il processo di valutazione possa essere efficacemente applicato, richiede, da parte dell'organizzazione, un chiaro ed esaustivo inventario dei propri sistemi di automazione e controllo industriale. Inoltre, è necessario che l'organizzazione sia conscia della consapevolezza e del livello di formazione del proprio personale in merito al rischio di cyber-sicurezza.

La tesi ha portando all'individuazione di contromisure utili a ridurre la probabilità di un possibile attacco informatico ed il lavoro ha permesso l'identificazione di alcuni punti chiave da considerare nel caso in cui venga introdotta (o sostituita) un'ulteriore macchina all'interno della linea. Risulta utile domandarsi: quale sistema operativo ospita il pc? Come è possibile accedere da remoto e quale range di azione è possibile (sola visualizzazione o movimentazione

della macchina)? Per questa ragione vengono fornite all'azienda le tabelle impiegate, al fine di verificare o adeguare la macchina introdotta al livello di sicurezza obbiettivo.

È bene ricordare che una corretta gestione del rischio prevede l'implementazione di un sistema per la gestione del rischio. Non è sufficiente analizzare, valutare e predisporre delle contromisure, in quanto, come l'organizzazione è in continua evoluzione lo sono anche le vulnerabilità IT e le possibili minacce, le quali richiedono un'attenzione costante durante tutto il ciclo di vita del macchinario.

A tal proposito lo standard IEC 62443-2-1 delinea i requisiti e le definizioni per il sistema di gestione della sicurezza della rete IACS, comprese le responsabilità degli utenti e dei proprietari dei dispositivi. Responsabilità che non sono in capo ad un solo utente, ma ogni attore all'interno dell'azienda ha il compito di collaborare per una maggiore sicurezza aziendale.

Bibliografia e sitografia

- Rapporto Clusit sulla sicurezza informatica 2023
- https://h-on.it/it/cyber-security-industria-4-0/
- https://www.europarl.europa.eu/news/it/headlines/society/20220120STO21428/cibersicurezza-le-minacce-principali-e-quelle-emergenti
- https://blog.osservatori.net/it_it/sicurezza-informatica-gestione-cyber-security-azienda
- https://www.canalesicurezza.it/network-access-control-come-funziona-quanto-conta-in-azienda/

Normativa consultata

- IEC 62443-3-2
- IEC/TS 62443-1-1
- IEC/TS 62443-3-3
- Direttiva 2006/42/CE
- Regolamento (UE) 2023/1230