UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea triennale in INGEGNERIA GESTIONALE

ASPETTI DI GESTIONE DELLA SICUREZZA DI IMPIANTI IN OTTICA INDUSTRIA 4.0

ASPECTS OF PLANT SAFETY MANAGEMENT FROM AN INDUSTRY 4.0 PERSPECTIVE

Relatore: Chiar.mo/a

Prof. Maurizio Bevilacqua

Tesi di Laurea di:

Vittorio Adamo

A.A. 2020 / 2021

Indice

Introduzione

Il presente lavoro ha lo scopo di presentare alcuni aspetti che la sicurezza assume in ottica dell'industria 4.0. Lo scopo è quello di sensibilizzare l'ipotetico datore di lavoro, che legge la suddetta tesi, sul tema della sicurezza e dei cambiamenti che sono avvenuti con l'avvento della quarta rivoluzione industriale.

Il primo capitolo è una semplice introduzione con definizioni dei concetti di Impianto Industriale, Sicurezza, Pericolo, Industria 4.0 e Cyber-Sicurezza. Successivamente nel secondo capitolo si analizza la gestione e l'analisi dei rischi; una buona attività di gestione del rischio consente infatti all'azienda di usufruire di grandi vantaggi in termini sia economici che di produttività, in quanto si hanno meno riduzioni di personale a causa di infortuni e più armonia aziendale oltre a grandi risparmi sui costi assicurativi.
Nel terzo capitolo vengono esposti quali sono stati i miglioramenti che la sicurezza ha avuto nel corso degli ultimi decenni, illustrati attraverso la definizione di tre fasi.
Nel quarto capitolo si propone un nuovo paradigma di sicurezza da seguire per l'industria, soprattutto manifatturiera in ambito dell'Industria 4.0. Il nuovo paradigma si concentra su cinque settori e può essere rappresentato dall'acronimo CHESS.
Il quinto capitolo guiderà alla stesura vera e propria del documento, in quanto vengono illustrati i vari aspetti che la Sicurezza può assumere come Sicurezza sul Lavoro, Sicurezza dei Processi e infine Sicurezza Informatica, di quest'ultima si troverà un approfondimento sulla Tecnologia Blockchain.

In fine nel sesto capitolo vengono esposte le misure di sicurezza da applicare in azienda per fronteggiare la pandemia di Covid-19 a cui poi seguono le conclusioni del rapporto di tesi.

1. Definizioni

1.1 Definizione di Impianto Industriale

Per Impianto Industriale si intende un complesso di capitali, macchine, mezzi e addetti atti a sfruttare le risorse materiali ed energetiche per trasformarli in prodotti finiti a maggior valore aggiunto attraverso trasformazioni chimico fisiche o processi di fabbricazione e/o montaggio. Ogni impianto industriale si suddivide in Impianti Tecnologici o di Servizio.

1.1.1 Gli Impianti Tecnologici

Sono costituiti dalle macchine che trasformano il materiale da lavorare; al fine di rendere efficiente l'impianto è necessario prestare attenzione alla scelta del sistema di produzione adatto durante la fase di progettazione dell'impianto stesso.

1.1.2 Gli Impianti di Servizio

Invece comprendono da tutte quelle strutture che pur non producendo direttamente valore aggiunto al prodotto, tuttavia, creano una condizione necessaria per garantire un corretto funzionamento degli impianti tecnologici.

1.2 Definizioni di Sicurezza, Pericolo e Rischio riferiti agli Impianti

1.2.1 Sicurezza

La parola *Sicurezza* deriva dal latino "sine cura": senza preoccupazione" e può essere definita come l'essere consapevoli che una certa azione non provocherà dei danni futuri. La sicurezza è un concetto relativo che deve essere compreso in presenza di qualche pericolo o rischio. Il concetto di rischio è legato sia ai pericoli creati dall'uomo che a quelli creati dalla natura; di conseguenza. La sicurezza costituisce una capacità di ridurre o eliminare la probabilità che si verifichino eventi pericolosi. Il numero di compiti relativi alla sicurezza in qualsiasi organizzazione è enorme, così come le responsabilità che accompagnano le decisioni e le scelte che devono essere fatte. Gli aspetti noti (tecnici) della sicurezza nelle aziende, vale a dire: l'identificazione dei rischi e l'analisi dei rischi, la valutazione dei rischi, sono solo una parte del dominio più ampio della gestione dei rischi, da parte dei responsabili della sicurezza aziendale. Altri elementi sono, ad esempio, la

formazione e l'educazione alla sicurezza, la formazione sul posto di lavoro, la risposta e la pianificazione delle emergenze, la pianificazione della continuità aziendale, gli aspetti etici della sicurezza, l'ingegneria dell'affidabilità, l'apprendimento dagli incidenti, la comunicazione dei rischi, la percezione del rischio, gli aspetti psico-sociali del rischio, gli aspetti economici della sicurezza, la governance dei rischi e molti altri.

In fine, negli Impianti Tecnologici, se consideriamo una popolazione di *N* elementi identici funzionanti in condizioni prestabilite per un tempo *t* quali apparecchi, utensili, impianti, si definisce la *Sicurezza S(t)*, di uno qualunque degli elementi, riferiti al tempo *t*, nei confronti di un evento sfavorevole (incidente) prodotto da un guasto come il rapporto:

$$S(t) = n(t) / N$$

Con *n(t)* numeri di elementi non affetti da guasto dopo un guasto di funzionamento. Quindi la Sicurezza assume un valore tra 0 e 1.

1.2.2 Pericolo

La parola Pericolo (deriva dal latino "periculum": esperimento, rischio), e può essere definita come la potenzialità di una determinata entità di causare danni. Per entità si intende, invece, una macchina, un impianto, una sostanza, ecc...

La quantità "**1- S(t)**" viene denominata come *Pericolo* o *Insicurezza* ed assume un valore tra 0 e 1

1.2.3 Fattore di rischio

Da non confondere con il pericolo è il Fattore di Rischio che, invece, è legato alla presenza simultanea di una fonte di pericolo con persone. Esso viene misurato come entità di rischio (o *Indice di Rischio R*) ed è legato alla probabilità o alla frequenza *Pr* del verificarsi di un evento dannoso, alla severità (o magnitudo *M*) delle sue conseguenze, alla sicurezza di come è realizzato l'impianto, l'attrezzo o la macchina e al tempo *t* di funzionamento.

In definitiva: **R(t) = [1 – S(t)] x Pr x M**

Al verificarsi di un evento sfavorevole non necessariamente segue un danno; *Pr* rappresenta la probabilità che il danno si verifichi in presenza di un guasto. È utile sottolineare come a parità di sicurezza, il rischio può assumere diversi valori poiché dipende da *Pr* e *M* inoltre tra questi due parametri esiste una relazione di proporzionalità inversa. Per esempio, eventi ad alta magnitudo sono quelli che tendono a presentarsi meno frequentemente. Se si vuole ridurre l'indice di rischio **R**, a parità di sicurezza, si può agire su due elementi:

- Riducendo la frequenza o probabilità dell'evento dannoso, in questo caso si parla di interventi di prevenzione;
- Riducendo la severità o magnitudo dell'evento dannoso, in questo caso si parla di intervento di protezione.

Per ridurre il rischio **R** si possono prevedere interventi di prevenzione e protezione insieme. Un aspetto molto importante nel processo di valutazione del rischio è la scelta del livello di accettabilità dell'entità del rischio.

1.3 Definizione Industria 4.0

Il termine "Industria 4.0" si riferisce alla quarta rivoluzione industriale ed è stato introdotto per la prima volta alla Fiera delle Tecnologie Industriali di Hannover, nel 2011 da un consorzio di aziende tedesche, con l'intenzione dichiarata di migliorare l'efficacia dell'industria manifatturiera tedesca.

L'industria 4.0 è il successore di tre rivoluzioni industriali:

- La prima rivoluzione fu innescata dalla generazione di vapore ed energia idroelettrica; le macchine sono state sviluppate per la produzione di prodotti.
- La seconda rivoluzione fu guidata dall'elettrificazione, che aprì la strada verso le linee di produzione e assemblaggio di massa.
- La terza rivoluzione si concentrò sull'elettronica e sulle tecnologie dell'informazione; le macchine programmate come robot e veicoli a guida automatica (AGV) hanno migliorato l'automazione.

La quarta rivoluzione industriale, invece, a differenza delle altre rivoluzioni non riguarda una singola invenzione rivoluzionaria, ma comprende diversi "ingredienti

tecnologici" che si stanno ancora evolvendo in nuove tecnologie abilitanti attraverso la convergenza e la combinazione reciproca. Si possono considerare almeno 13 sottocategorie di tecnologie chiave dell'industria 4.0 che sono caratterizzate da due tendenze comuni: "l'integrazione tra il mondo fisico e quello digitale" e "la connettività sia a livello locale che con rete diretta universale".

Queste nuove tecnologie possono essere suddivise in quattro gruppi:

1.3.1 Le Tecnologie di Interfaccia Fisico-Digitale

Esse presentano un'alta quota di componenti hardware e una connettività di rete estesa, che collegano il cyber-spazio con la realtà di macchine, prodotti e persone al lavoro. Il gruppo comprende i ***Sistemi Cyber-Fisici***, il concetto di ***Internet of Things*** e le ***Tecnologie di Visualizzazione*** come la Realtà Aumentata, Virtuale e Mista.

1.3.2 Le Tecnologie di Rete

Esse presentano una elevata quota di componenti software e una connettività di rete estesa che forniscono funzionalità online, come il ***Cloud Computing*** o le ***Soluzioni di Interoperabilità*** **e** ***Sicurezza Informatica*** oppure della ***Tecnologia Blockchain***.

1.3.3 Le Tecnologie di Elaborazione dei Dati

Esse presentano un'elevata quota di componenti software ma un basso livello di connettività che supportano l'analisi dei dati e forniscono input basati sulle informazioni per il controllo e il processo decisionale. Queste tecnologie si riferiscono alla simulazione e alla modellazione, tra cui il ***Digital Twin***, il ***Machine Learning e l'Intelligenza Artificiale*** e ***L'analisi dei Big Data.*** Sebbene le tecnologie di elaborazione dei dati possano essere gestite localmente, esse vengono sempre più fornite attraverso piattaforme di Cloud Computing.

1.3.4 Le Tecnologie di Processo Fisico-Digitale

Esse presentano un'elevata quota di componenti hardware ma un basso livello di connettività e comprendono apparecchiature utilizzate nella produzione come la ***Stampa 3D*** e la robotica avanzata come i ***Cobot***. Altre tecnologie menzionate meno frequentemente sono fisiche, come i **Nuovi Materiali** o le soluzioni di ***Gestione***

***dell'Energia**,* ma negli ultimi anni sono diventate sempre più intrecciate con le tecnologie digitali.

Oggigiorno, tutte queste tecnologie, che caratterizzano l'Industria 4.0, sono solitamente riportate separatamente, tuttavia sono profondamente interdipendenti nella loro applicazione. Molte delle capacità analitiche implicite nei sistemi *Cyber-Fisici* e nell'*Internet of Things* sono fornite dalle tecnologie di elaborazione dei dati, spesso offerte come applicazioni di servizio fornite tramite il *Cloud Computing*. Le *Soluzioni di Interoperabilità e Sicurezza Informatica* garantiscono l'opportunità di estendere la loro applicazione all'interno dell'azienda e con partner commerciali. I *Nuovi Materiali* e i *progetti* stampabili *in 3D* sono sviluppati con *soluzioni* avanzate *di Simulazione e Modellazione*. La *Robotica* avanzata sfrutta l'apprendimento automatico e *l'Intelligenza Artificiale*.

Nel complesso, *l'Internet of Things* e il *Cloud Computing* sono le tecnologie più spesso menzionate e caratterizzano il fenomeno della Quarta Rivoluzione Industriale insieme al gruppo delle *Tecnologie Informatiche*. La definizione di "Industria 4.0" si riferisce ampiamente ai *sistemi Cyber-Fisici* e alle *Soluzioni di Interoperabilità e Sicurezza Informatica,* che emergono ripetutamente anche in connessione con *Smart Manufacturing* e *Cloud Manufacturing.* La *Stampa 3D* e la *Robotica Avanzata*, anche se rilevanti, appaiono in misura minore; la *Tecnologia Blockchain* è stata inclusa dopo il 2017. Infine, i *Nuovi Materiali* e le *Soluzioni di Stoccaggio dell'Energia* sono poco menzionati.

1.4 Definizione di Cyber-Sicurezza

Il termine cyber-sicurezza presenta diverse definizioni:

- "La capacità di proteggere o difendere l'uso del cyberspazio dagli attacchi informatici"
- "La conservazione della riservatezza, dell'integrità e della disponibilità di informazioni nel ciberspazio"
- "Tutte le attività necessarie per proteggere il cyberspazio, i suoi utenti e le persone interessate dalle minacce informatiche"

- "La prevenzione dei danni, la protezione e ripristino dei sistemi informatici di comunicazione elettronica, i servizi di comunicazione elettronica, le comunicazioni via cavo e comunicazione elettronica, comprese le informazioni ivi contenute, per garantirne la disponibilità, l'integrità, l'autenticazione, la riservatezza.

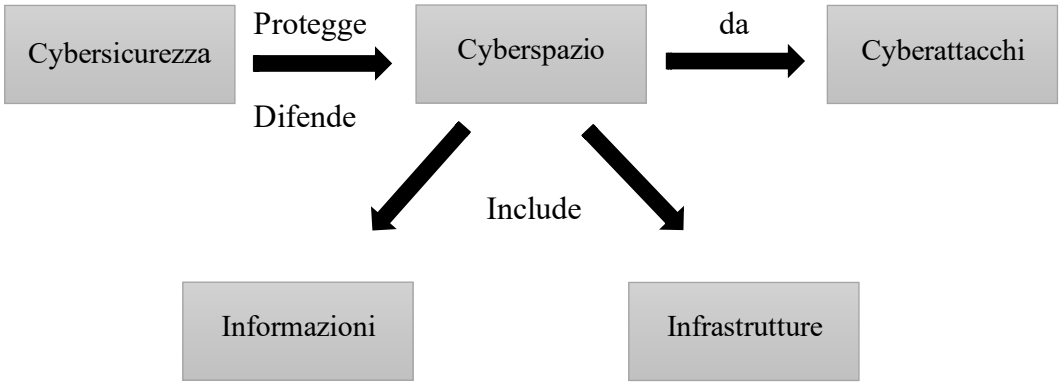


Fig. 1. Visione schematica del concetto di Cyber-Sicurezza

Nella figura vi è una visione schematica del concetto di cibersicurezza che fonde le informazioni delle definizioni appena menzionate. Si può dunque affermare che la sicurezza informatica mira a proteggere il cyberspazio (che include sia informazioni che infrastrutture) da qualsiasi minaccia informatica o attacco informatico.

2. La Gestione e l'analisi del Rischio

L'obiettivo principale dell'analisi dei rischi è sostenere il processo decisionale valutando e quantificando i rischi associati al funzionamento e alla progettazione di un sistema tecnico. La valutazione del rischio e la gestione del rischio forniscono importanti contributi a sostegno del processo decisionale.

Meyer e Reniers definiscono la gestione del rischio operativo come "*l'applicazione sistematica di politiche, procedure e pratiche gestionali ai compiti di identificazione, analisi, valutazione, trattamento e monitoraggio dei rischi*".

Inoltre, la formazione scientifica e le discipline che affrontano i diversi settori e voci del set di gestione del rischio sono sempre più diversificati. La gestione della sicurezza e del rischio non è più terreno esclusivo di ingegneri, medici e scienziati della sicurezza; infatti, scienze come psicologia, sociologia, matematica pura, chimica e fisica, filosofia, economia, comunicazione, business e management, criminologia e diritto sono coinvolte nel miglioramento della sicurezza in questi giorni.

2.1 Progettazione del quadro di gestione del rischio

Al giorno d'oggi, l'implementazione di una corretta gestione del rischio o di un sistema di sicurezza all'interno delle organizzazioni è diventata un requisito legale oltre che morale. La gestione del rischio è una delle nove aree di conoscenza propagate dal Project Management Institute (PMI).

Esso è un processo sistematico che aiuta le organizzazioni a capire qual è il rischio, chi è a rischio, quali sono i controlli attuali per tali rischi e i giudizi che devono essere fatti sull'adeguatezza o meno di tali controlli. Se non sono adeguati, è necessaria un'azione per gestire il livello di rischio fino a un livello accettabile e ragionevole. Pertanto, la valutazione e la gestione dei rischi sono un insieme di principi e metodi sviluppati per concettualizzare, valutare e gestire i rischi e le minacce riconosciute (chiamate anche pericoli).

Negli ultimi anni si è assistito all'emergere dell'Enterprise Risk Management (ERM), spesso indicato come una nuova tendenza aziendale che si basa sui principi

della gestione tradizionale del rischio. Si tratta di un approccio più strutturato e disciplinato che allinea strategia, processi, persone, tecnologia e conoscenza, allo scopo di valutare e gestire le incertezze che l'impresa deve affrontare quando crea valore.

2.2 Gestione dei rischi e prestazioni

Un principio fondamentale della gestione è la misurazione delle prestazioni. Essa molto importante perché identifica il divario di prestazioni esistenti tra le prestazioni attuali e quelle desiderate ma soprattutto fornisce un'indicazione dei progressi verso la riduzione delle lacune. Gli indicatori di prestazione chiave (KPI), accuratamente selezionati, identificano con precisione dove agire per migliorare le prestazioni.

Un successivo indicatore molto importante è l'indicatore di rischio chiave (KRI). Molti ricercatori si sono occupati dei KRI e dei modi in cui possono contribuire a rilevare e ridurre il rischio a livello di impresa. Con questi indicatori è possibile monitorare un rischio specifico, fornire una direzione in avanti e informazioni sul rischio che può esistere o meno, non solo un sistema di allarme per le azioni future.

C'è una lacuna sulla questione del collegamento di KRI e KPI in tutti i campi di ricerca. Non esiste un quadro sistematico per collegare efficacemente questi due indicatori e utilizzarli nella cooperazione. L'idea è che in cooperazione dovrebbero essere in grado di fornire dati utili per migliorare le prestazioni di un'azienda (sulla base di metodologie utilizzate nei problemi di prestazione) e la gestione del rischio in generale.

2.3 Identificazione dei rischi

L'obiettivo dell'identificazione del rischio è generare un elenco completo dei rischi in base agli eventi che potrebbero creare, migliorare, prevenire, degradare, accelerare o ritardare il raggiungimento degli obiettivi. Un'identificazione completa è fondamentale perché un rischio che non è identificato in questa fase non sarà incluso in ulteriori analisi dei rischi. Nell'area di produzione è possibile identificare il rischio operativo associato a:

- Gestione dei Processi di Produzione,
- Manutenzione
- I metodi operativi e gli strumenti utilizzati,
- Materiale
- Fonti Umane,
- Macchine e Tecnologie di produzione,
- Ambienti Macchina.

Il concetto di Industria 4.0 genera nuove categorie di rischi in questo settore a causa dell'aumento della vulnerabilità e delle minacce. La connessione del cyber-spazio, la produzione sofisticata di tecnologie ed elementi e l'utilizzo dell'outsourcing dei servizi è il fattore principale che aumenta la vulnerabilità. L'identificazione di nuovi tipi di rischi è presentata nella tabella 1. Tale identificazione ha suggerito un quadro per l'attuazione della gestione dei rischi.

Categorie di rischio operativo	***Rischio***
Gestione dei processi di produzione	Rischio di informazioni associato a perdite di dati, perdita di integrità e informazioni disponibili.
Manutenzione	Problema di disponibilità e integrità dei dati per la manutenzione.
Metodi e strumenti operativi utilizzati	Errori nell'elaborazione dei dati.
Macchine e tecnologie di produzione	Sensibilità e vulnerabilità dei dati: problema relativo agli attacchi informatici.
Fonti umane	Basso numero di lavoratori qualificati
Ambienti macchina	Attacchi dalla rete Internet, problemi legati alla compatibilità elettromagnetica e alle emissioni elettromagnetiche che colpiscono le macchine di produzione.

La tabella 1. Identificazione di nuovi rischi

I risultati mostrano che la maggior parte dei fattori di rischio comuni nell'area di produzione sono correlati alla sicurezza delle informazioni. Le tecnologie di fabbricazione utilizzate - macchine, robot, ecc. - fanno attualmente parte delle tecnologie dell'informazione e della comunicazione (TIC).

2.4 Progettazione del quadro

La progettazione di un framework adatto è stato il passo successivo. L'idea di questo progetto era di combinare e attuare i requisiti chiave per ERM e ISMS. Questa idea

porta all'implementazione sicura del concetto di Industria 4.0 nelle aziende manifatturiere. Le soluzioni proposte aiutano a ridurre al minimo i rischi aziendali legati alla strategia aziendale e all'implementazione del sistema di sicurezza delle informazioni certificato.

Il framework per l'implementazione integrata è descritto in base al ciclo PDCA Deming (Plan-Do-Check-Act). Questo quadro consente di soddisfare i requisiti per l'ISMS e un sistema di gestione della qualità. La tabella 2 presenta le attività per l'attuazione di un sistema di gestione integrato per ogni fase del PDCA.

Plan	*Visione organizzativa e obiettivi*	Stabilire politiche (compresa la politica ISMS), obiettivi, processi e procedure pertinenti alla gestione dei rischi e al miglioramento della sicurezza delle informazioni per fornire risultati in conformità con le politiche e gli obiettivi generali dell'organizzazione.
Do	*Processi*	Implementare e gestire i criteri, i controlli, i processi e le procedure
Check	*Prestazione*	Valutare e, se del caso, misurare le prestazioni del processo rispetto alla politica ISMS, agli obiettivi e all'esperienza pratica e riferire i risultati alla direzione per la revisione.
Act	*Miglioramento*	Intraprendere azioni correttive e preventive, sulla base dei risultati dell'audit interno e della revisione della gestione o di altre informazioni pertinenti, per ottenere un miglioramento continuo del sistema.

La tabella 2. Attività di attuazione di un sistema di gestione integrato

Il sistema integrato dovrebbe essere sistematicamente documentato, comunicato, attuato e continuamente migliorato. I principi e i processi di base sono presentati nella figura 2. Il documento sottolinea il fatto che la politica di sicurezza dovrebbe essere estesa dagli aspetti di gestione del rischio a una politica aziendale integrata. In tal modo vengono presi in considerazione i requisiti di tutte le parti interessate, nonché i requisiti legali e normativi, e vengono stabiliti obiettivi e strategie di rischio aziendale appropriati.

Il nucleo di un sistema di gestione integrato implementato deve basarsi sull'applicazione funzionale ed efficace della gestione dei processi aziendali. Ciò significa che l'analisi, la descrizione e l'ottimizzazione sono chiavi per il supporto e la gestione dei processi. L'analisi dei rischi è il passo più importante per l'attuazione del quadro proposto.

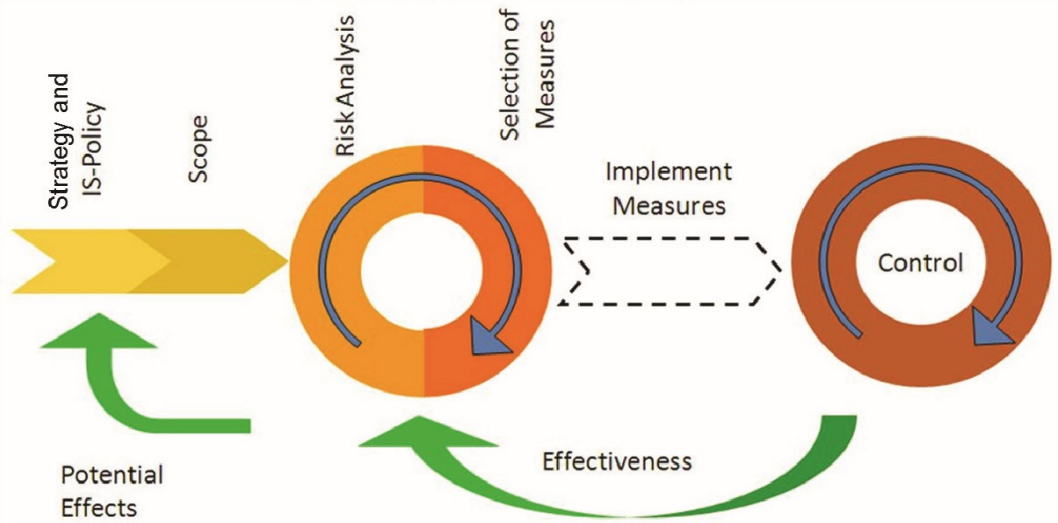


Fig. 2. Principi e processi di attuazione del quadro progettato

2.5 Integrazione della gestione delle prestazioni e dei rischi

L'istituzione della gestione dei processi aziendali può aiutare a identificare i rischi e adottare misure dal piano di trattamento del rischio e continuità aziendale. Pertanto, i trattamenti di rischio identificati e i piani di continuità aziendale sono adeguatamente integrati nei processi di produzione. Le misure sono implementate, mantenute, testate e regolarmente aggiornate per supportare l'efficacia delle prestazioni aziendali. Il framework sviluppato adotta principi dai campi di BPM (Business Process Management) e PPM (Process Performance Management) e li combina con elementi dalla gestione del rischio a un nuovo concetto. La gestione del rischio negli ambienti di produzione intelligenti si basa sull'incorporare concetti sia da BPM che da PPM e procede sulle seguenti ipotesi:

- La governance dei processi aziendali e l'esame dei rischi di processo sono essenziali per la gestione del rischio sulla base di dati operativi in tempo reale nell'Industria 4.0
- Per indagare le prestazioni, il rischio e il raggiungimento degli obiettivi dei processi, gli approcci di BPM, PPM e RM devono essere integrati e combinati.
- I rischi devono essere valutati mediante strutture di dati e indicatori chiaramente definiti in uno schema di calcolo designato che si basa su tali strutture.

A causa dell'elevato volume di dati che deriva dai processi, i potenziali tipi di danno e la loro probabilità di occorrenza possono essere previsti in modo più preciso. Tuttavia, potrebbero essere necessarie nuove procedure di valutazione per gestire la complessità degli scenari. Inoltre, è concepibile un adeguamento dei criteri di valutazione (per la probabilità di occorrenza e danno).

Come accennato, ogni rischio può essere monitorato dai KRI che hanno influenzato i KPI in relazione alle prestazioni aziendali. Questa idea è presentata nella figura 3 che segue. I rischi individuati sono stati registrati in un modello di rischio. Questo modello mostra gli importanti gruppi di rischi identificati e aiuta a classificarli in categorie. I diversi colori utilizzati nella figura 3 (per illustrare meglio il processo) dividono i rischi in: rischi operativi (rossi) e strategici (verdi). Ogni gruppo di rischio può anche avere un colore diverso (cfr. figura 3), ad esempio per categorizzazione, priorità o responsabilità. Come mostrato nella figura 3, ogni gruppo di rischio può essere suddiviso in rischi individuali.

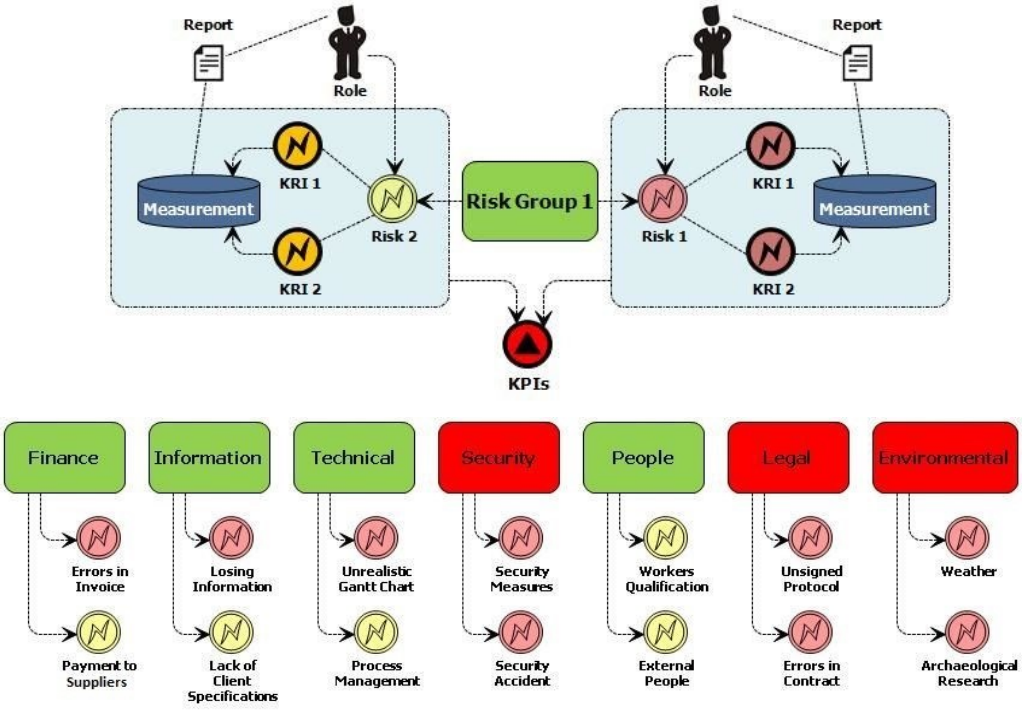


Fig. 3. Modello di gruppi di rischio e relazioni tra rischi - KRI - KPI.

3. I miglioramenti della Sicurezza

Nel corso degli ultimi decenni sono avvenuti dei miglioramenti in ambito della sicurezza, per spiegarli al meglio si possono definire tre fasi:

- La fase Proattiva (pre-incidente)
- La fase di Incidente
- La fase Reattiva (post-incidente)

3.1. La fase Proattiva

Con il termine proattivo si intende nel linguaggio aziendale chi opera con il supporto di metodologie e strumenti utili a percepire anticipatamente i problemi, le tendenze o i cambiamenti futuri, al fine di pianificare le azioni opportune in tempo. Nella fase proattiva, infatti, è possibile osservare due varietà di tendenze.

3.1.1 La prima tendenza

Essa è una cooperazione sempre maggiore tra le imprese, principalmente a livello operativo e soprattutto su questioni reattive come le indagini sugli incidenti e le esercitazioni di evacuazione.

3.1.2 La seconda tendenza

Essa, invece, riguarda la riduzione statica e dinamica delle valutazioni dei rischi:

- Le analisi dinamiche del rischio includono tecniche matematiche avanzate sviluppate nel mondo accademico, tra cui le di catene di Markov. Nella stessa linea di pensiero, i big data e l'Internet of Things hanno sempre più iniziato ad essere incorporati, dove e quando possibile, in tali valutazioni dinamiche dei rischi.

  Inoltre, l'economia operativa, compresa l'analisi costi-benefici e l'analisi costi-efficacia, viene migliorata e utilizzata con una tendenza crescente. Alcuni argomenti specialistici sono anche esplorati, introdotti e sviluppati nelle aziende, come analisi dei rischi per la sicurezza, scienza della gestione delle prestazioni, modelli mentali e principi morali o etici per il calcolo dei rischi.

- L'attenzione ai rischi sistemici, in base alla quale si guarda analiticamente all'intero sistema in tutte le sue parti, porta all'assunzione di barriere di sicurezza a livello sistemico.

3.2. La fase d'incidente

Nella fase dell'incidente, si possono anche osservare diverse tendenze. I dati in tempo reale e i big data, nonché tutti i progressi nei dispositivi e nelle possibilità di comunicazione hanno portato a valutazioni e decisioni del rischio migliori e più oggettive. Gli esercizi di simulazione su larga scala dei disastri sono resi più reali mentre vengono elaborati "giochi seri" per esercitare decisioni e compiti in fase di incidente.

3.3. La fase reattiva

All'indomani di un incidente, un'importante tendenza al miglioramento riguarda una migliore collaborazione tra soccorritori, vigili del fuoco, operatori industriali, servizi medici, servizi logistici, esperti di comunicazione e accademici. Ma anche l'uso di tecnologie innovative (ad esempio droni), e strutture organizzative per affrontare i problemi in una fase post-incidente (ad esempio aspetti trauma-psicologici), sono miglioramenti che non possono essere ignorati.

4. Un nuovo paradigma di sicurezza

La sezione precedente ha fornito le tendenze evolutive della sicurezza che si possono individuare nell'attuale ricerca accademica e nella pratica industriale. Tuttavia, queste tendenze rappresentano il pensiero "all'interno della scatola", e di solito sono "più dello stesso concetto / approccio" o, nella migliore delle ipotesi, miglioramenti incrementali e ottimizzazione della tecnologia esistente, pratiche di gestione, accordi organizzativi e fattori umani. Per promuovere veramente la sicurezza all'interno dell'industria, come parte del concetto di industria 4.0, è necessario pensare "fuori dalla scatola" ed è necessaria una vera rivoluzione.

Le rivoluzioni iniziano con idee radicalmente nuove. Queste nuove idee si formano attraverso modelli mentali, la volontà di cambiare le cose e la consapevolezza che cambiare le cose porterà a una situazione migliorata, che nel caso degli impianti di produzione, si tradurrà nella loro redditività e licenza di operare. Questo nuovo paradigma di sicurezza per l'industria manifatturiera dovrebbe consistere in cinque settori di interesse. Il nuovo paradigma di sicurezza può essere rappresentato dall'acronimo CHESS, che riassume cinque settori molto importanti in cui è necessario un progresso rivoluzionario:

- Pensiero a grappolo e collaborazione intensificata
- Elevata trasparenza e controllo efficace;
- Istruzione, formazione e apprendimento;
- Integrazione della sicurezza;
- Innovazione in materia di sicurezza e valutazione dinamica dei rischi.

L'innovazione richiesta può essere esemplificata da una serie di idee concrete, che possono essere realizzate solo se cambia l'attuale mentalità degli operatori, degli accademici e delle autorità.

4.1 Pensiero a grappolo e collaborazione intensificata

Dovrebbero essere ricercate la cooperazione a livello proattivo e strategico, come le strategie congiunte di gestione delle emergenze e strumenti decisionali e la cooperazione reattiva a livello operativo, come le esercitazioni congiunte di evacuazione. Alcuni parchi industriali lavorano già insieme per migliorare

strategicamente la logistica orizzontale, l'uso dell'energia (o dei servizi pubblici in generale), e nelle questioni ambientali (ad esempio i flussi di rifiuti); tuttavia, di solito non riescono a collaborare molto più intensamente per quanto riguarda il miglioramento proattivo e strategico della sicurezza.

Le nuove misure concrete sono, ad esempio, l'istituzione di un consiglio multi-impianto o di un consiglio dei cluster, per stabilire una cooperazione e un miglioramento strategico proattivo istituendo un bilancio per il "finanziamento della sicurezza dei cluster"; utilizzare squadre di "valutazione del rischio di volo" e squadre di "audit interno volante" nei cluster; stabilire una matrice di pianificazione delle emergenze a grappolo; prendere in considerazione varie forme di rischi, quali gli effetti domino (escalation degli incidenti) e gli incidenti nelle valutazioni dei rischi; stabilire un approccio di aggiornamento del sistema di gestione della sicurezza dei cluster e stabilire una cultura della sicurezza dei cluster.

4.2 Alta trasparenza e ispezione efficiente

Il secondo campo rivoluzionario, l'elevata trasparenza e un'ispezione più efficiente, possono trovare utile ispirazione nel settore dell'aviazione. In questo settore, viene elaborato un sistema maturo di procedure e accordi per affrontare la segnalazione di tutti gli incidenti e le mancate cose al fine di imparare il più possibile in un contesto di "cultura giusto".

I seguenti approcci innovativi possono essere introdotti ed elaborati nell'industria manifatturiera: istituire una banca dati nazionale per segnalare tutti i tipi di incidenti e incidenti da parte delle aziende manifatturiere; stabilire una "cultura giusto" negli impianti di produzione e nei parchi industriali contenenti aziende manifatturiere; istituire un sistema di diffusione in cui le imprese e le autorità/squadre di ispezione possano imparare da tutti gli incidenti che si verificano nel settore; stabilire un'intesa tra i membri del Consiglio di sicurezza dei cluster e i servizi di ispezione per rendere le ispezioni molto più efficienti; e di utilizzare droni per raccogliere continuamente dati da tutto il cluster per motivi di sicurezza.

4.3 Istruzione, formazione e apprendimento

Anche il terzo settore rivoluzionario, che si occupa dell'educazione alla sicurezza, dell'apprendimento della sicurezza e della formazione alla sicurezza, merita un'attenzione particolare. Non solo è necessario imparare da tutti i tipi di incidenti, ma anche dai modelli di sicurezza, dalle teorie e dalle conoscenze in generale. Qui c'è anche un compito per la società: dovrebbero esserci corsi su "affrontare il rischio e l'incertezza", o "sicurezza operativa", a partire dall'istruzione primaria. Se le persone hanno familiarità con la sicurezza fin dalla più tenera età, possono imparare molto di più nell'istruzione superiore. Inoltre, ci si può aspettare che le conoscenze molto più approfondite in materia di sicurezza di tutte le persone attraverso un'istruzione regolare, siano utilizzate nella vita e nelle imprese per prendere decisioni migliori e ridurre le perdite, sia a livello di lavoro privato che pubblico.

A questo proposito, si possono suggerire alcune innovazioni interessanti. I sistemi di gestione della conoscenza della sicurezza d'impianti dovrebbero, ad esempio, essere presenti al meglio in ogni stabilimento di produzione; Dovrebbero essere disponibili sessioni di formazione in cui i responsabili della sicurezza degli impianti e i servizi di ispezione della sicurezza siano congiuntamente presenti; L'apprendimento della sicurezza dovrebbe essere supportato da una scienza adeguata/convalidata/scientificamente studiata per la gestione delle prestazioni; un corso come "conoscenze di base sulla valorizzazione e la definizione delle priorità dei problemi di sicurezza" dovrebbe essere insegnato ai bambini delle scuole primarie; La "gestione del rischio e il processo decisionale basato sul rischio" dovrebbero essere insegnati nelle scuole superiori e nelle università, sia come corso separato, sia nell'ambito dei corsi esistenti; La "sicurezza dei processi" (e la sicurezza intrinseca) dovrebbe essere insegnata a tutti i gli ingegneri chimici e industriali ed essere considerata essenziale nel programma educativo.

4.4 Integrazione della sicurezza

Il quarto settore rivoluzionario riguarda principalmente le pratiche di sicurezza antiterrorismo più efficaci nell'industria manifatturiera. Attualmente, gli sforzi di sicurezza negli impianti di produzione si basano su rischi di sicurezza ad alta frequenza e a basso impatto, vale a dire contro ladri e sabotaggi o, nella migliore

delle ipotesi, contro eventuali terroristi. Tuttavia, è necessario un adeguato aggiornamento verso misure di sicurezza antiterrorismo. Ma più in generale, la sicurezza dovrebbe essere trattata in modo integrato con la gestione della sicurezza aziendale.

Alcuni modi innovativi per migliorare questo quarto settore sono effettuare valutazioni delle minacce, valutazioni delle vulnerabilità della sicurezza o, in generale, valutazioni sui dei rischi per la sicurezza in tutti gli impianti/cluster di produzione (insieme alle valutazioni dei rischi per la sicurezza e in modo integrato). Si può inoltre utilizzare una "visione a grappolo" per adottare misure antiterrorismo, oltre a una visione dell'impianto. Bisogna dare priorità alla sicurezza del trasporto all'interno di una zona industriale (valutazione dei rischi di trasporto e misure basate su tali valutazioni, corsie sicure, postazioni sicure, ecc.); per istituire gruppi di sicurezza cluster. Si può ulteriormente sviluppare un database degli incidenti di sicurezza, istituire ispezioni di sicurezza per gli impianti di produzione e per i parchi industriali (insieme alle ispezioni di sicurezza) e prendere sul serio le misure antiterrorismo, preferibilmente basate su studi scientifici.

4.5 Innovazioni in materia di sicurezza e valutazioni dinamiche dei rischi

Il quinto campo rivoluzionario, l'innovazione della sicurezza e le valutazioni dinamiche dei rischi, è il campo più evidente su cui lavorare. Questo campo richiede il minimo cambiamento nella mentalità degli operatori, degli accademici e delle autorità. Alcune innovazioni che, se applicate insieme, farebbero delle tendenze evolutive un vero e proprio campo rivoluzionario, sono menzionate di seguito: utilizzare i big data e l'Internet of Things per innovare la conoscenza del rischio e il processo decisionale in materia di sicurezza all'interno degli impianti di produzione e dei parchi industriali; utilizzare tecniche dinamiche di valutazione del rischio (effettuare grandi investimenti nel loro sviluppo e applicazione in loco) per far progredire le conoscenze e il processo decisionale in tempo reale; investire nella ricerca per la scienza della gestione delle prestazioni e gli indicatori di prestazione di sicurezza (dovrebbe essere proattivo principalmente) per vedere quali indicatori funzionano e quali no (ciò richiede studi longitudinali su larga scala); sviluppare modelli per una grande varietà di scenari di incidenti gravi di sicurezza e scenari di

attacco terroristico e impiegarli per l'apprendimento e l'esercizio fisico; sviluppare la scienza rispetto alla leadership e ai modelli mentali richiesti dai dipendenti e l'impatto sulla sicurezza; sviluppare tecniche alternative di valutazione del rischio in base alle quali vengono presi in considerazione sia i principi etici/morali che le informazioni economiche.

5. I Diversi tipi di Sicurezza

Dopo l'analisi sulla gestione dei rischi e la proposta di un nuovo paradigma di sicurezza che dovrebbe essere attuato, è giusto soffermarsi sui vari aspetti che la sicurezza assume all'interno degli impianti e delle aziende stesse, essi si possono suddividere in:

- La sicurezza sul Lavoro
- La sicurezza dei Processi
- La sicurezza Informatica

5.1 La Sicurezza sul Lavoro

Con il termine Sicurezza sul Lavoro si intende la condizione di far svolgere a tutti coloro che lavorano la propria attività lavorativa in sicurezza, senza esporli a rischio di incidenti o malattie professionali.

Il testo fondamentale che si occupa di regolamentare la sicurezza sul lavoro è il *Testo Unico in materia di salute e sicurezza sul lavoro* (Decreto Legislativo numero 81 del 09/04/2008).

Esso analizza tutti gli aspetti fondamentali riguardo la sicurezza, come i soggetti interessati ed i principali adempimenti da seguire oggetto della disciplina italiana in materia di sicurezza sul lavoro.

5.1.1 Soggetti Interessati

I principali soggetti interessati dalla normativa in materia di sicurezza del lavoro sono ovviamente due:

- Il *datore di lavoro*, definito dal Testo Unico in materia di salute e sicurezza sul lavoro come: il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

Perciò ai fini della sicurezza sul lavoro, il datore di lavoro è chiunque sia al vertice dell'organizzazione del lavoro e dell'attività produttiva, a prescindere da qualsiasi forma di investitura formale.

- Il *lavoratore*: definito come la persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore così definito è equiparato il socio lavoratore di cooperativa o di società, anche di fatto, che presta la sua attività per conto delle società e dell'ente stesso.

Nel concetto di lavoratore rientrano nella più ampia accezione oltre che i normali lavoratori dipendenti, anche gli apprendisti, i tirocinanti e persino i lavoratori autonomi, nello specifico, qualsiasi prestatore di lavoro, a prescindere dalla tipologia di contratto utilizzata, nonché a prescindere dall'effettiva esistenza di un regolare contratto di lavoro.

Il datore di lavoro è ai fini del Testo Unico in materia di salute e sicurezza sul lavoro, il principale soggetto sul quale ricadono obblighi, prescrizioni e anche sanzioni in materia di sicurezza sul lavoro.

Il lavoratore, invece, è il soggetto che deve essere tutelato in applicazione della specifica disciplina, da parte del datore di lavoro, nello svolgimento della sua attività lavorativa. Il lavoratore è comunque tenuto a cooperare con il datore di lavoro ed a rispettare tutte le prescrizioni e tutti gli obblighi in materia di sicurezza imposti dal datore di lavoro.

5.1.2 I Principali Adempimenti definiti dal Testo Unico in materia di salute e sicurezza sul lavoro

I principali adempimenti, definiti dal Testo Unico in materia di salute e sicurezza sul lavoro, ci si devono adeguare tutte le aziende, anche se aventi un solo dipendente, sono:

- *Il Documento Valutazione dei Rischi*: è il documento redatto a conclusione della valutazione dei rischi, deve avere data certa e contenere:
  - Una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
  - L'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati;
  - Il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
  - L'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
  - L'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;
  - L'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento;
  - il contenuto del documento deve anche rispettare altre indicazioni previste dalle specifiche norme sulla valutazione dei rischi specifici (es. rischi da agenti fisici, chimi, biologici, ecc.).

- *Nomina del responsabile della Sicurezza del servizio di prevenzione e protezione dai rischi professionali:* È il responsabile del servizio di prevenzione e protezione dai rischi professionali, che provvede*:*
  - All'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
  - Ad elaborare, per quanto di competenza, le misure preventive e protettive, e i sistemi di controllo di tali misure;

- Ad elaborare le procedure di sicurezza per le varie attività aziendali;
- A proporre i programmi di informazione e formazione dei lavoratori;
- A partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica;
- A fornire ai lavoratori le informazioni sui rischi e sulle misure preventive e protettive

Può essere nominato RSPP: il datore di lavoro, a patto che abbia almeno il diploma di scuola superiore e tre anni di esperienza continuativa nel proprio settore lavorativo a seguito di un corso di 16 ore e relativa attestazione o un dipendente a seguito di un corso di circa 68 ore (dipende dalla tipologia di attività), oppure un soggetto esterno che possiede i titoli adeguati. L'attestato ha durata quinquennale e sono previsti aggiornamenti periodici.

- *Designazione e formazione del Rappresentante dei lavoratori per la sicurezza*: Il Rappresentante dei lavoratori per la sicurezza è la persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro.
  L'elezione o la designazione del Rappresentante dei lavoratori deve essere oggetto di comunicazione all'INAIL. È obbligatorio un corso di formazione della durata di 32 ore.

- *Designazione e formazione squadra antincendio:* Si tratta di un gruppo di lavoratori incaricati di attuare le misure di prevenzione nonché di adottare i provvedimenti che si rendano necessari in situazioni di emergenza, quali:
  - incendio;
  - evacuazione dei lavoratori in caso di pericolo grave e immediato.

Nelle aziende fino a cinque lavoratori, il datore di lavoro può assumere direttamente tale incarico dopo specifico corso di formazione. La durata del corso di formazione è in funzione del rischio di incendio della sede dell'attività (basso-medio-alto).

- *Designazione e formazione addetti squadra primo soccorso*: Ai sensi del testo unico il datore di lavoro, oltre a designare e formare gli addetti al Primo

soccorso, predispone un protocollo/piano per la gestione delle emergenze sanitarie, per poter attuare concretamente tutte le misure necessarie all'organizzazione del servizio. Nelle aziende fino a cinque lavoratori, il datore di lavoro può assumere direttamente tale incarico dopo specifico corso di formazione. La durata del corso dipende dalla classificazione dell'azienda. (gruppo A=16 ore, gruppo B e C =12 ore). È previsto aggiornamento triennale.

- *Nomina del medico competente:* La nomina del medico competente è obbligatoria nei casi in cui è obbligatoria la sorveglianza sanitaria. Se l'azienda è sottoposta all'obbligo di sorveglianza sanitaria i lavoratori devono effettuare visita medica preventiva.
- *Formazione obbligatoria dei lavoratori:* La formazione in materia di sicurezza sul lavoro, deve essere effettuata contestualmente all'assunzione, soltanto se non è possibile, deve essere completata entro 60 giorni. Nella formazione obbligatoria (generale e specifica) dei lavoratori il modulo generale, uguale per tutte le attività, è di sei ore. La formazione specifica varia a seconda del settore di attività.

5.2 La Sicurezza dei Processi

Nel campo della Sicurezza dei processi c'è un crescente interesse verso il concetto di cultura della sicurezza. La ricerca esistente sul campo presuppone un nesso tra cultura della safety e security. La concettualizzazione della cultura della sicurezza non è affatto conclusiva. In linea con questa visione, la cultura organizzativa può contribuire a creare sicurezza, essendo un mezzo per diffondere conoscenze critiche per la sicurezza. Pertanto, il concetto di sicurezza intrinseco potrebbe essere ottenuto in un processo o nella progettazione del prodotto che eviti i pericoli invece di controllarli. Questa fase si raggiungerebbe attraverso quattro metodi principali:

- Ridurre al minimo (ridurre la quantità di materiale pericoloso),
- Sostituire (sostituire un materiale con un altro meno pericoloso),
- Moderare (utilizzando condizioni di processo meno pericolose)
- Semplificare (il processo di progettazione è meno complicato e quindi meno soggetto a guasti).

La sicurezza del processo è identificata come parte integrante dello sviluppo e della produzione del processo piuttosto che come un "componente aggiuntivo" del processo. La sicurezza dei processi differisce dalla sicurezza sul lavoro in quanto si concentra esclusivamente sulla prevenzione e la mitigazione di incidenti di processo gravi come incendi, esplosioni ed emissioni tossiche. La valutazione/gestione della sicurezza dei processi include diversi passaggi essenziali. Sebbene ogni fase sia altrettanto importante:

- L'identificazione del rischio
- La valutazione del rischio
- La gestione dei rischi

possono essere considerate le fasi chiave della gestione della sicurezza dei processi. L'obiettivo primario della sicurezza dei processi è quello di prevenire il rilascio indesiderato di sostanze chimiche/agenti biologici altamente pericolosi in luoghi, che potrebbero esporre l'uomo a gravi pericoli. La gestione della sicurezza dei processi è un approccio per valutare i processi che hanno il potenziale di causare incidenti catastrofici come incendi, esplosioni o rilasci tossici.

5.3 La Sicurezza Informatica

All'interno dei contesti dell'Industria 4.0, la sicurezza informatica svolge un ruolo di primo piano nella prevenzione della perdita di competitività delle aziende. In effetti, le apparecchiature industriali critiche sono oggi vulnerabili a una serie di attacchi informatici, che sono in grado di influenzare l'intero modello di business. Secondo i rapporti annuali sulla sicurezza informatica di Cisco 2018, il 31% delle organizzazioni ha subito attacchi informatici alla tecnologia operativa (OT); mentre, il 38% si aspetta che gli attacchi si estendano dalla tecnologia dell'informazione alla tecnologia operativa. Sebbene la sicurezza informatica sia percepita come una priorità dal 75% degli esperti, solo il 16% afferma che la propria azienda è ben preparata ad affrontare le sfide della sicurezza informatica. Ciò è dovuto principalmente alla mancanza di standard accurati a cui le aziende possono fare riferimento, nonché alla mancanza di competenze manageriali e tecniche necessarie per attuarle.

Le organizzazioni europee e internazionali si stanno muovendo in questa direzione. Ad esempio, nel 2017, l'Organizzazione europea per la cyber-sicurezza (ESCO) ha raccolto in un documento tutte le norme e le specifiche esistenti relative alla cyber-sicurezza in riferimento al mercato unico digitale europeo. Questo documento aiuta a capire quali schemi (se esistenti) possono essere utilizzati dalle aziende per affrontare le sfide della sicurezza informatica. Inoltre, la Commissione elettrotecnica internazionale (IEC) ha pubblicato una guida sulla sicurezza delle informazioni e sulla privacy dei dati, che fornisce linee guida da coprire nelle pubblicazioni IEC e spiega come attuarle. Le pubblicazioni dell'IEC sono raccomandazioni (accettate dai comitati nazionali dell'IEC) per uso internazionale.

Nell'attuale scenario in rapida crescita, si prevede che la sicurezza informatica diventerà parte integrante della strategia, del design e delle operazioni delle aziende che abbracciano il paradigma dell'Industria 4.0.

5.3.1 Sfide correlate alla sicurezza informatica (ESCO)

L'analisi delle sfide operative, dal punto di vista della sicurezza informatica, porta alla seguente serie di sfide che devono essere affrontate per garantire un ragionevole livello di sicurezza per l'Industria 4.0:

- Convergenza tra safety e security
- Sicurezza informatica dell'IoT industriale,
- Rilevamento intrusioni/anomalie su ICS,
- Gestire le minacce fisiche informatiche,
- Gestire i cambiamenti comportamentali e organizzativi,
- Garantire la sicurezza lungo tutta la catena del valore.

5.3.2 Convergenza tra Safety e Security:

Affinché vi sia convergenza tra Safety e Security si inizia con la valutazione dei rischi e l'analisi delle minacce da parte di professionisti congiunti della safety (con il termine safety si indica la protezione da rischi e incidenti fortuiti che possono pregiudicare l'incolumità o la salute). e della security (con il termine security si indica la protezione da minacce e attacchi deliberati a cose o persone), consentendo di qualificare e quantificare le minacce informatiche e il

loro potenziale impatto sui processi industriali. Un focus speciale deve essere impostato per risolvere i requisiti contraddittori tra safety e security nella progettazione del sistema per evitare situazioni "fail open".

La progettazione di funzioni fail-safe e fail-secure e lo sviluppo di meccanismi di autoguarigione sono necessari per garantire la safety e security attraverso la progettazione di una nuova automazione industriale. Infine, i gruppi congiunti di risposta alla sicurezza sono tenuti a gestire in modo efficiente gli incidenti informatici che interessano ICS critici.

5.3.3 Sicurezza informatica dell'IoT industriale:

Qualsiasi implementazione dell'IIoT deve fornire sicurezza end-to-end dall'edge fino al cloud. Questa progettazione per la protezione deve includere la protezione avanzata dei dispositivi endpoint, la fornitura di identità univoche a ogni endpoint, la protezione delle comunicazioni, la gestione e il controllo di criteri e aggiornamenti e l'utilizzo dell'analisi e dell'accesso remoto per gestire e monitorare l'intero processo di sicurezza. La trasmissione di dati sensibili è limitata a dispositivi edge e cloud autentici e le tecniche di anonimizzazione vengono applicate prima che grandi quantità di dati siano analizzate da parti esterne.

5.3.4 Rilevamento delle intrusioni sui sistemi di controllo industriale:

è necessario un mix di approcci basati sul protocollo e sul comportamento per rilevare efficacemente gli attacchi informatici a ICS. Con l'ICS emergente dell'Industria 4.0 in ambienti meno prevedibili in cui non tutte le azioni autorizzate possono essere predefinite, l'efficienza degli approcci basati su regole e politiche degli esperti può diminuire. Le tecniche di rilevamento che coinvolgono l'apprendimento automatico possono migliorare i tassi di rilevamento e consentire il rilevamento di 0 giorni. L'IoT industriale deve essere considerato sia come potenziale obiettivo che come vettore di minaccia, in particolare in scenari che coinvolgono botnets di dispositivi IoT. Pertanto, il rilevamento deve essere applicato non solo a livello di rete, ma il più possibile sull'endpoint. Ciò richiede di affrontare una serie di vincoli ambientali e di potere.

5.3.5 Gestire le minacce cyber-fisiche:

Affrontare la sicurezza delle risorse industriali richiede un approccio integrato ai rischi fisici e informatici. È probabile che avversari qualificati sfruttino i punti più deboli della catena di sicurezza lungo tutti gli strati fisici e informatici. Da questo punto di vista hanno un vantaggio rispetto ai difensori, che tradizionalmente sono segmentati in diverse unità organizzative con competenze e strumenti diversi. La politica dei fornitori dei produttori di automazione stabilisce una forte limitazione alla correlazione degli eventi fisici e di sicurezza informatica che interessano gli ambienti di produzione. Gli attori dominanti applicano politiche proprietarie nel tentativo di costringere i clienti ad acquisire l'intera gamma di prodotti dal loro marchio, limitando l'interoperabilità, l'esportazione dei dati e la supervisione da parte di prodotti terzi. Ciò impedisce alle industrie di acquisire consapevolezza selezionale in tempo reale su eventi fisici e informatici. Per superare questa limitazione è necessaria una buona collaborazione tra i fornitori di automazione e IT. È richiesta la geolocalizzazione interna ed esterna di personale, utensili, parti e materiali di consumo. La comprensione dei comportamenti normali e anomali, sia in officina che sulla rete industriale, richiede complesse tecniche di elaborazione e correlazione degli eventi. Questi possono essere basati su regole umane (basate su criteri) o su approcci basati sull'apprendimento automatico. Una limitazione agli approcci basati sulle regole umane richiede competenze significative e possono essere indovinati da avversari. Una limitazione agli approcci basati sull'apprendimento automatico è che devono essere addestrati su set di dati di grandi dimensioni e possono essere sovvertiti da tecniche di machine learning contraddittorie.

La gestione delle minacce richiede di valutare gli scenari di attacco considerando gli attacchi all'hardware, alla rete e anche a livello umano durante l'intero ciclo di vita del sistema durante la fase di progettazione di un sistema e anche in seguito durante il funzionamento. Ciò richiede la formazione di team di risposta interdisciplinari in grado di reagire in caso di minaccia.

5.3.6 Cambiamenti organizzativi e comportamentali:

Una strategia olistica di sicurezza informatica richiede consapevolezza e competenze a tutti i livelli, dai decisori strategici fino al personale in attività. Ciò richiede una formazione durante l'istruzione, ma anche soprattutto una formazione sul posto di lavoro, adattata alla situazione e alle esigenze specifiche di un'organizzazione. Questo processo è completato da una sicurezza incentrata sull'uomo che impedisce agli utenti di prendere decisioni sbagliate attraverso HMI ben progettato.

5.3.7 Sicurezza lungo tutta la catena del valore:

Una valutazione della sicurezza richiede la modellazione delle dipendenze informatiche lungo l'intera catena del valore. Mentre la logistica collaborativa basata su eventi e in tempo reale consente di reagire rapidamente a qualsiasi cambiamento nella catena del valore, possono altresì verificarsi situazioni uniche che richiedono politiche uniche. Ciò richiede esperti qualificati e un buon software di gestione. Nella fase successiva, la manutenzione predittiva consente di ridurre i ritardi e le interruzioni e quindi aumentare l'efficienza.

5.4 Panorama delle minacce

L'ENISA presenta un'analisi delle minacce alla sicurezza informatica nel campo dell'ICS e dello SCADA Esse sono classificate nella seguente tabella per probabilità (bassa, media, alta) e impatto (medio alto, alto, alto- critico, critico):

Minacce	***Probabilità***	***Impatto***
Minacce persistenti avanzate (APTs)	Bassa	Alto
Malware (Virus, Troian):	Alta	Alto
Exploit kits and rootkits:	Media	Alto
Minaccia interna	Bassa	Critico
Interruzione del sistema di comunicazione:	Bassa	Alto-critico
Intercettazioni:	Bassa	Alto-critico
Negazione del servizio:	Bassa	Medio-alto
fuga di dati \ informazioni sensibili:	Bassa	Medio-alto

La tabella 3. Classificazione minacce per probabilità e impatto

5.5 La Tecnologia Blockchain

L'Industry 4.0 ha introdotto l'industria manifatturiera a nuove tecnologie come i cyber-fisici, Internet of Things (IoT), analisi dei big data. Si prevede che queste tecnologie porteranno con sé molti vantaggi e potenziali opportunità, come l'autoconsapevolezza, l'auto-previsione, l'auto-confronto, l'auto-riconfigurazione e l'auto-manutenzione. Tuttavia, questi paradigmi utilizzano ancora una rete industriale centralizzata. Di conseguenza, l'attuale produzione soffre di problemi legati a flessibilità, sicurezza, privacy, trasparenza, efficienza, integrità dei dati, resilienza, affidabilità dei dati, ecc.

Recentemente, la tecnologia blockchain ha ricevuto un'attenzione significativa nella tecnologia finanziaria. Tuttavia, essa possiede la capacità e il potenziale significativo per sostenere in modo sostenibile l'iniziativa Industria 4.0 ed eliminare i problemi ad essa correlati.

Blockchain è un libro mastro distribuito che viene simulato e condiviso tra i membri di una rete peer to peer (P2P). Recentemente, il concetto di blockchain ha attirato molta attenzione nelle tecnologie con natura distribuita come l'IoT perché migliora la sicurezza e la privacy, aumenta la tolleranza di errore del sistema, fornisce un regolamento e una riconciliazione più rapida, crea una rete scalabile e aiuta a risparmiare costi e tempo rimuovendo gli intermediari.

La tecnologia blockchain è decollata in diversi settori, come la comunicazione macchina-macchina nel sistema di rete elettrica, il sistema di tracciabilità della catena di approvvigionamento alimentare, il funzionamento logistico decentralizzato, la condivisione decentralizzata dei dati tra le applicazioni sanitarie e i servizi finanziari per il settore bancario. Tuttavia, non esiste uno studio sistematico sull'incorporazione della tecnologia blockchain nei sistemi di produzione.

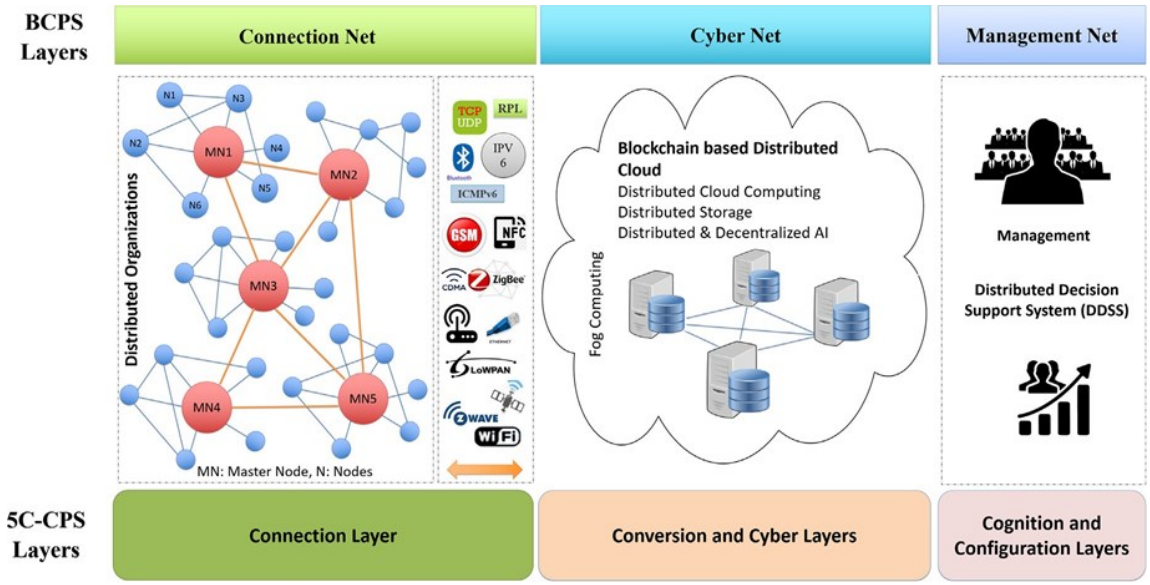
L'architettura strutturale della tecnologia blockchain può intrinsecamente creare diverse caratteristiche chiave come descritto di seguito:

A. Immutabile: impossibile modificare la crittografia avanzata (funzioni hash).

B. Trasparente: ogni computer della rete dispone di una copia del libro mastro.
C. Autentico: tutte le parti nella transazione hanno dati accurati, tempestivi, coerenti e completi.
D. Decentralizzato: non esiste una singola entità di controllo.
E. Distribuito: distribuito su una posizione e/o organizzazione diverse location.
F. Nessun intermediario- algoritmi auto-eseguibili, ad esempio Smart Contract.
G. Anonimo: le chiavi pubbliche e private possono essere utilizzate per l'interazione senza bisogno di informazioni private

5.5.1 Una struttura CPS (BCPS) abilitata per blockchain

BCPS (Fig. 4) mira a risolvere le sfide associate all'attuazione nel mondo reale della struttura 5C-CPS affrontando (a) interoperabilità, b) integrità dei dati, c) sicurezza e privacy e (d) resilienza.



La Fig.4. Struttura BCPS

La tabella 4 riassume i requisiti chiave per ogni layer di 5C-CPS e i potenziali impatti della tecnologia blockchain.

5C-CPS Architecture	Characteristics	Requirements	Blockchain Impact						
			A	B	C	D	E	F	G
Configuration	• Intelligent Decision Making • Supervisory Control (ERP, MES, SCM CMM, and PLM) • Intelligent Business structure	Self-Configure, Self-Adjust, Self-Optimize Sustainable Business Plans		✓	✓	✓	✓	✓	
Cognition	• Decision Support Systems • Integrated simulation and Synthesis	Real-Time Data Access Trustworthy of Data Source Availability of Structured Data [27]	✓	✓	✓		✓	✓	
Cyber	• Big Data • Digital Twins • Cloud Computing • Similarity Modeling • Data Warehousing (DW) • Cyber-Cyber Interactions	Redundancy in storage, bandwidth, and computation [28] Efficient Connectivity: Bandwidth, Latency, availability, robustness Cross-Domain Integration and Interoperability [29] Handling Design complexity [30] Security and Privacy	✓	✓	✓	✓	✓	✓	✓
Conversion	• AI Analytic Tools • AI/Machine Learning Models/PHM Tools • Distributed and decentralized Intelligence • Fog/Edge Computing • Deep Learning	Resilience Adaptive, Reliable and Robust Fast Computation	✓	✓	✓	✓	✓		
Connection	Networking: Physical-Physical Interactions, Physical-Human Interactions Smart Nodes (Sensors, Actuators, Process, Machine, etc.)	Efficient Connectivity: Bandwidth, Latency, availability, robustness Security and Privacy Interoperability	✓	✓	✓	✓	✓	✓	✓

La tabella 4. Requisiti chiave per ogni layer di 5C-CPS

L'architettura dettagliata di BCPS è descritta come segue:

- *Rete di Connessione*

  Connettività avanzata, gestione dei dati, integrità e sicurezza sono le caratteristiche principali di questo livello. Il fattore più importante per questa connettività e integrazione globale è "Interoperabilità". Vi sono otto aspetti per stabilire una "interoperabilità tecnica" di successo: sicurezza, privacy, accessibilità, multilinguismo, sussidiarietà, soluzioni multilaterali, uso di norme aperte e software open source. Blockchain aiuta ad affrontare la sicurezza e la privacy utilizzando degli algoritmi crittografici avanzati e un meccanismo di consenso globale. La sussidiarietà migliora attraverso un quadro decentralizzato presentato dalla blockchain. Il multilinguismo e le soluzioni multilaterali possono essere integrati attraverso una migliore interconnettività tra i nodi (computer, sensori, attuatori, ecc.). In genere, i nodi con maggiore capacità (nodi master) potrebbero essere utilizzati come server locale (Micro-Cloud) per i nodi con restrizioni di risorse per archiviare i propri dati, eseguire attività computazionali e interagire con altri nodi. Una chiave pubblica può essere assegnata a ciascun nodo master per la comunicazione diretta con altri nodi. Pertanto, tutti i nodi sarebbero in grado di interagire tra loro, condividere dati e persino condividere le loro

capacità computazionali e di rete tra loro. Si prevede che l'integrazione dello storage distribuito e della rete condivisa aumenterebbe la ridondanza e migliorerebbe la resilienza della rete.

- *Rete Informatica*

  Questo livello è responsabile della conversione dei dati in informazioni significative e della gestione delle interazioni cyber-fisiche e cyber-informatiche al fine di raggiungere l'integrità, la tolleranza ai guasti e la resilienza. La sicurezza informatica, i big data, il cloud computing, la connettività di rete, la privacy e la trasparenza sono le principali caratteristiche da considerare in questo livello. Diverse tecniche come la griglia e il cloud computing vengono in genere utilizzate per aumentare la velocità di calcolo, la resilienza del sistema, la scalabilità della rete e fare un uso efficiente delle risorse. Il ruolo di queste tecniche è quello di distribuire il carico di calcolo e archiviazione tra diversi computer all'interno della rete. Una struttura blockchain potrebbe essere essenziale per questo sviluppo verso il calcolo distribuito fornendo sicurezza dei dati, archiviazione distribuita dei dati e facilitando l'accesso ai dati attraverso una rete P2P.

  In questo livello, l'integrazione degli strumenti di intelligenza artificiale è essenziale per la conversione di dati grezzi in informazioni significative, estendendo l'intelligenza ai singoli nodi. Una rete abilitata con l'intelligenza artificiale è necessaria per i sistemi di produzione odierni e, cosa più importante, l'intelligenza artificiale distribuita e decentralizzata (DDAI) supererà le piattaforme intelligenti centralizzate. Con l'aiuto della blockchain, gli strumenti di intelligenza artificiale possono eseguire e coordinare le loro conoscenze in modo distribuito. Man mano che i moduli DDAI vengono formati con dati più affidabili e globali, la loro robustezza e affidabilità aumentano, l'affidabilità migliora ricevendo un feedback diretto dalle operazioni e i costi di implementazione si riducono in modo significativo a causa dell'adattamento della condivisione delle risorse P2P e dell'apprendimento automatico (AutoMl).

- *Rete di Gestione*

A questo livello, informazioni complete a livello cibernetico vengono utilizzate in un sistema di supporto alle decisioni basato sui dati al fine di ottenere un processo decisionale informato e rapido, produttività, resilienza e infine sostenibilità della produzione. Negli attuali sistemi di produzione, i componenti DSS e/o i suoi utenti sono dispersi geograficamente e richiedono una piattaforma affidabile e distribuita per l'integrità delle informazioni aziendali con l'obiettivo di ottenere competenza, efficienza e competitività. Un DSS basato sulla blockchain sarebbe decentralizzato e distribuito, il che significa che le decisioni vengono prese raggiungendo un accordo globale e considerando tutte le restrizioni all'interno di una rete decentralizzata. Pertanto, tutti i nodi possono partecipare al processo decisionale. A causa dei principali vantaggi della tecnologia blockchain, un tale design sarebbe indipendente dalla posizione, tollerante ai guasti, sicuro, autonomo ed estensibile.

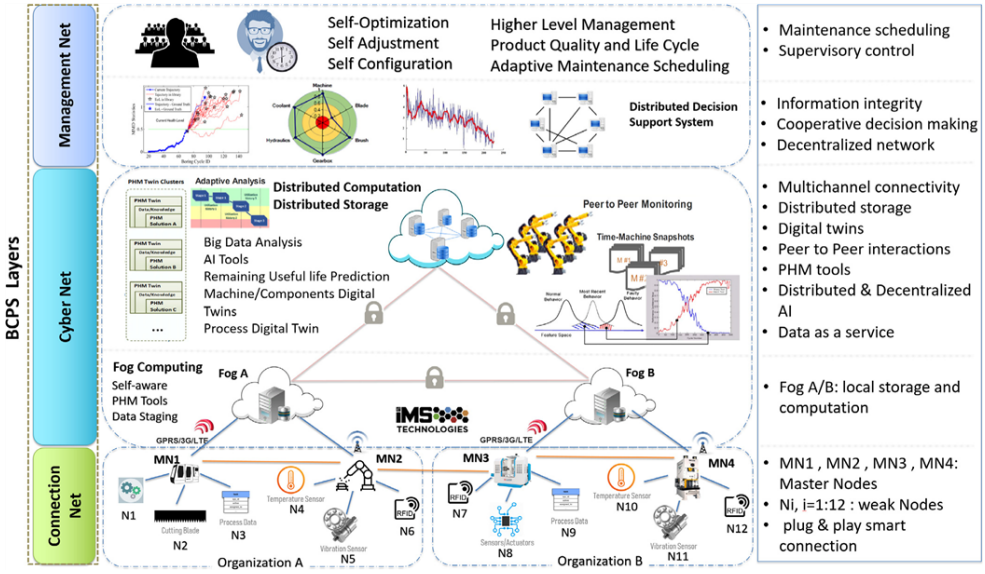
La tabella 5 riassume le esigenze e le esigenze delle parti interessate e il potenziale contributo dell'architettura BCPS proposta per affrontarle.

BCPS Layers	Stakeholder Needs and Requirements	Blockchain Contribution
Management Net	Trustworthiness, resilience, security, and efficiency of decision support systems	Advanced cryptography, Distributed, Decentralized
	Overhead cost reduction	Smart contract, P2P interactions
	Bureaucracy reduction	Smart contract, P2P interactions
	Data security and Privacy	Advanced cryptography
	Supervisory control, resource management	P2P interactions- transparency
	Ownership as a Service (OaaS)	Assets tokenization [51,52], smart contract
Cyber Net	Conversion of data to meaningful information	Training AI models on more data available through shared datasets, Distributed & Decentralized AI
	Elimination of single point of failures	Load and resource (computation, storage, networking) distribution among Nodes
	Data security and Privacy	Advanced cryptography
	Efficient Data storage	Micro clouds, data storage in each Node
	Data as a Service (DaaS)	Smart contract, P2P interactions
Connection Net	Transparency in the supply chain	Tracking components from their origin step by step – Transparency
	Interconnectivity between devices	P2P interactions, Master Nodes
	Automation	Smart contract, P2P interactions
	Efficient connectivity (Bandwidth, Latency, robustness, etc.)	Shared resources, Master Nodes, P2P interactions
	Data security and Privacy	Advanced cryptography

La tabella 5. La blockchain impatta sulle esigenze e sui requisiti degli stakeholder

5.5.2 Struttura BCPS basata su PHM

La fig. 5 presenta un caso di studio PHM che illustra come ogni funzione di BCPS viene implementata nel monitoraggio sanitario delle macchine di produzione. Di conseguenza, quattro macchine diverse sono state configurate in due diverse posizioni geografiche; 'Posizione A' e 'Posizione B'. I Dati raccolti da entrambe le macchine vengono spinti a dispositivi di calcolo “della nebbia”. Le informazioni significative estratte nel livello nebbia vengono spinte in una rete cloud distribuita per l'analisi PH



La Fig. 5. Un caso di studio sulla struttura BCPS basata su PHM.M avanzata

Blockchain può risolvere in modo significativo i problemi con l'attuale PHM in tutti i livelli della struttura 5C-CPS affrontando

- Disponibilità dei dati,
- PHM intelligente,
- Sistema di supporto alla manutenzione predittiva (PMSS).

- *Disponibilità dei dati*

  Nell'architettura 5C-CPS; sicurezza, privacy e capacità sono le principali preoccupazioni nel trasferimento dei dati dal livello di connessione al livello di

conversione e oltre al livello informatico. Per affrontare questa lacuna, l'incorporazione di "Nodi Master" è stata proposta nel primo livello di BCPS come intermediario in modo tale che le loro capacità possano essere condivise con altri nodi nella stessa rete locale. Gli attacchi informatici a sensori e attuatori, reti di comunicazione e interfacce fisiche sono i principali problemi di sicurezza nelle interazioni fisico Cyber, che potenzialmente possono essere affrontati con la struttura BCPS proposta.

- *PHM intelligente*

  Gli strumenti di intelligenza artificiale basati su PHM devono imparare e adattarsi all'ambiente di produzione che cambia dinamicamente. Tuttavia, alcuni dei dati richiesti sono limitati all'accesso pubblico a causa della privacy e della sicurezza. Per le applicazioni PHM, una piattaforma DDAI abilitata per blockchain potrebbe fornire maggiori dati di formazione per gli agenti di apprendimento in modo sicuro e privato e aumentare l'affidabilità e le prestazioni dei sistemi. Ad esempio, le macchine CNC in diverse fabbriche possono scattare un'istantanea dei loro dati, analizzarli con un agente di intelligenza artificiale locale incorporato e infine crittografare e condividere i dati con le entità interessate (addetti alla manutenzione e i produttori di CNC o strumenti) attraverso l'interconnettività raggiunta a livello di "Cyber Net".

- *Sistema di supporto alla manutenzione predittiva (PMSS)*

  Informazioni supplementari quali il costo delle apparecchiature di fabbricazione, il ciclo di vita, i tempi di inattività degli ordini, i tempi di inattività di sostituzione, la distribuzione del carico di lavoro, ecc. raccolti dai livelli "Rete di connessione" e "Rete informatica", potrebbero costituire un sistema di supporto integrato per condurre un'intenzione predittiva intelligente. L'integrazione di queste informazioni in un DSS operante a livello di "Rete di gestione" si tradurrebbe in un sistema decisionale intelligente per le applicazioni PHM.

5.5.3 Sfide Blockchain

Vale la pena considerare che la blockchain è nella fase iniziale di sviluppo e potrebbero esserci alcune sfide per la sua implementazione nei sistemi di produzione che richiedono più ricerca e sviluppo.

Esse sono:

- La mancanza di conoscenza e infrastruttura:

  A livello aziendale purtroppo vi sono pochi sviluppatori di software di talento, inoltre essi soffrono di una mancanza di strumenti adeguati da usare per lo sviluppo di un solido ecosistema blockchain. Infine, l'attuale applicazione IoT fa uso di protocolli di sicurezza che richiedono una gestione centralizzata che può creare complessità per l'implementazione di Blockchain
- L'Implementazione in tempo reale che comprende:
  - La verifica di latenza in alcune tecnologie contabili distribuite
  - Natura ad alta intensità energetica della tecnologia
  - Potenziali minacce alla sicurezza come il mining egoistico e il 51% di attacchi
- I Meccanismi di consenso specifici:

  Il PoW sta promuovendo inaspettatamente la centralizzazione, però non esiste un meccanismo di consenso avanzato e affidabile
- I Problemi legali e di conformità

  Vi sono incertezze su normative, standard e accordi e inoltre la condivisione dei dati di produzione può essere un argomento delicato per molti produttori

- La capacità di memoria

  Il volume dei dati di produzione è enorme. Il design attuale della blockchain non può memorizzare grandi quantità di dati e soprattutto i protocolli blockchain sottostanti creano un traffico overhead significativo
- I costi di implementazione che si suddividono in
  - Costo per implementare e distribuire
  - Costo per sostituire l'infrastruttura esistente
  - Risorse necessarie per mantenerlo attivo e funzionante

6. La Sicurezza al tempo del COVID-19

Una polmonite di causa sconosciuta è stata rilevata nella città di Wuhan, in Cina, il 31 dicembre 2019, essa è stata chiamata COVID-19. Dall'11 febbraio al 14 aprile, il numero di casi di infezione da COVID-19 nel mondo è aumentato da 45,134 a 2,004,383 in 210 paesi. Per questo motivo è stata dichiarata dall'OMS la pandemia globale. In attesa del rilascio del vaccino, sono state diffuse delle regole di sicurezza da seguire all'interno degli Impianti Industriali.

6.1 Trasmissione Virus

Il SARS.Cov2-19 è un virus che si ritiene sia trasmissibile da persona a persona con tre modalità:

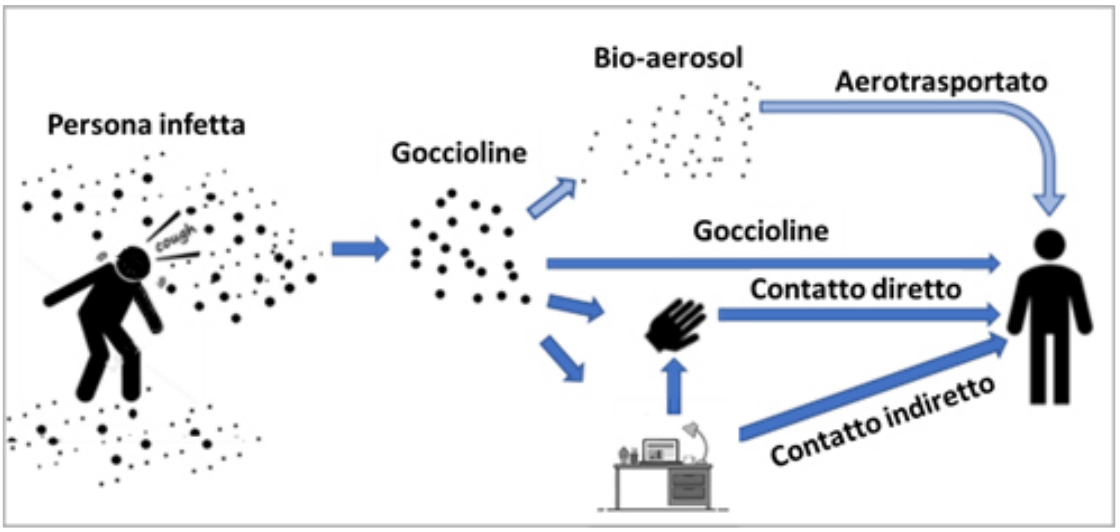
- per contatto ravvicinato e diretto con una persona infetta;
- per inalazione di goccioline liquide prodotte dalla persona infetta;
- tramite contatto con superfici contaminate dal virus.

Ai fini delle modalità di trasmissione è determinante il fatto che le persone infette tossendo, starnutendo, parlando e respirando emettono goccioline di liquido infettate con il virus, che possono:

depositarsi sulle superfici vicino alla persona infetta e quindi essere poi riprese da chi tocca tali superfici (contatto indiretto);

- essere inalate da chi si trova vicino alla persona infetta o in un ambiente contaminato.

Il contatto diretto con le secrezioni respiratorie sembra essere, in queste situazioni, la principale via di trasmissione; a oggi le fonti ufficiali non riportano alcuna evidenza della possibile trasmissione per via aerea (bio-aerosol).



La Fig. 6. Rappresentazione trasmissione Covid-19

L'OMS ha segnalato quale principale meccanismo di esposizione al virus quello del contatto diretto o indiretto con le secrezioni respiratorie (goccioline) di una persona infetta (colore blu scuro); in blu chiaro è indicato il meccanismo dell'aerotrasporto di goccioline contaminate che non è ad oggi evidenziato dalle fonti ufficiali. (vedi figura 6)

6.2 Modi per prevenire la diffusione del COVID-19 sul posto di lavoro

Le misure a basso costo riportate di seguito aiuteranno a prevenire la diffusione di infezioni sul tuo posto di lavoro, come raffreddori, influenza, e proteggeranno i clienti, appaltatori e dipendenti.

I datori di lavoro devono:

- Assicurati che i tuoi luoghi di lavoro siano puliti e igienici.
  Le superfici (ad esempio scrivanie e tavoli) e gli oggetti (ad esempio telefoni, tastiere) devono essere puliti regolarmente con disinfettante poiché la contaminazione sulle superfici toccate da dipendenti e clienti è uno dei principali modi in cui il COVID-19 si diffonde
- Promuovere un lavaggio regolare e accurato delle mani da parte di dipendenti, appaltatori e clienti.
  Mettere dispenser di strofinamento delle mani igienizzante in luoghi importanti intorno al posto di lavoro. Assicurarsi che questi distributori

siano regolarmente ricaricati. Mostrare manifesti che promuovono il lavaggio delle mani. Assicurati che il personale, gli appaltatori e i clienti abbiano accesso a luoghi in cui possono lavarsi le mani con acqua e sapone.

- Promuovere una buona igiene respiratoria sul posto di lavoro
  Esporre manifesti che promuovono l'igiene respiratoria e combinarlo con altre misure di comunicazione. Assicurarsi che le maschere facciali e / o i tessuti di carta siano disponibili sul posto di lavoro, per coloro che sviluppano un naso che cola o tosse sul lavoro, insieme a bidoni chiusi per smaltirli igienicamente.
- Consigliare a dipendenti e appaltatori di consultare i consigli di viaggio nazionali prima di fare viaggi di lavoro.

Inoltre, per prevenire l'infezione da Covid-19, oltre a seguire correttamente tutte le procedure di distanziamento e sicurezza, è fortemente consigliata la vaccinazione attraverso i vaccino approvati dall'agenzia italiana del farmaco.

Conclusioni

Il mondo della Sicurezza si muove inesorabilmente verso un cambiamento guidato dal continuo e progressivo svilupparsi ed affermarsi delle nuove tecnologie. La presente tesi si è presa il compito di fornire al lettore una panoramica sugli aspetti di gestione della sicurezza da attuare nella Industry 4.0.
Il termine Industry 4.0 racchiude in sé tutte le nuove tecnologie come l'Iot, i Big Data che ovviamente comportano una nuova serie di misure di sicurezza da attuare oltre a quelle già presenti negli Impianti Industriali.
Opporsi caparbiamente ai necessari cambiamenti nella maniera di attuare e negli strumenti da utilizzare imposti dalla quarta rivoluzione industriale è insensato e controproducente.

Questo cambiamento è, purtroppo, mal visto da alcuni, che interpretano i nuovi strumenti tecnologici come minacce alla necessità dell'uomo come operaio. Questa è un'idea probabilmente sbagliata, in quanto l'adozione di tali strumenti porterà ad un miglioramento delle condizioni di lavoro delle persone.

In quest'ottica è interessante notare come grandi passi avanti a livello di innovazione siano stati fatti proprio nella riprogettazione dei Dispositivi di Sicurezza, che garantiscono un livello sempre maggiore di protezione e di informazione riguardo all'ambiente di lavoro.

A seguito di queste nuove attrezzature di sicurezza, si ridisegna sia il concetto di Impianto, ma soprattutto il ruolo dell'operaio che, dotato di strumenti tecnologici all'avanguardia, diventa "ibrido", in grado cioè di interagire in modo funzionale con i macchinari e con l'ambiente in cui opera.

Bibliografia e altre fonti

- Mark P. Taylora, Peter Boxallb, John J.J. Chena, Xun Xuc, Angela Liewd, Adebayo Adenijib (), "*Operator 4.0 or Maker 1.0? Exploring the implications of Industrie 4.0 for innovation, safety and quality of work in small economies and enterprises"*,

- Thomas Burns*, Dr John Cosgrove, Frank Doyle (), *"A Review of Interoperability Standards for Industry 4.0"*,

- Giovanna Culot, Guido Nassimbeni, Guido Orzes, Marco Sartor (), *"Behind the definition of Industry 4.0: Analysis and open questions"*,

- Muhammad Atif Javed, Faiz Ul Muram, Hans Hansson, Sasikumar Punnekkat, Henrik Thane (), *"Design and Towards dynamic safety assurance for Industry 4.0"*,

-Jiri Tupa, Jan Simota, Frantisek Steiner (),*" Aspects of risk management implementation for Industry 4.0"*,

-Jose Alcides Gobbo Junior∗, Christianne M. Busso, Simone Cristina O. Gobbo, Henrique Carreão (), *"Making the links among environmental protection, process safety, and industry 4.0"*,

-G. Reniersa (), *"On the future of Safety in the manufacturing industry"*,

-Miklos Kiss, Gabor Breda, Lajos Muha (), *"Information security aspects of Industry 4.0"*,

-T. Pereira, L. Barreto, A. Amaral (), *"Network and information security challenges within Industry 4.0 paradigm"*,

- Marianna Lezzi, Mariangela Lazoi, Angelo Corallo (), *"Cybersecurity for Industry 4.0 in the current literature: A reference framework"*,

-Jay Lee, Moslem Azamfar, Jaskaran Singh (), *"A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems"*

-Mr Shashank Kumar, Dr Rakesh D. Raut, Dr Vaibhav S. Narwane, Dr Balkrishna E. Narkhede (), *"Applications of industry 4.0 to overcome the COVID-19 operational challenges"*,

-Vincenzo Nastasi (2012), *"La Sicurezza negli Impianti"*,

-World Health Organization (2020), *"Getting your workplace ready for COVID-19",*

-AICARR (2020), *"Gli impianti e la diffusione del Covid-19 nei luoghi di lavoro",*

-https://www.informazionefiscale.it/Sicurezza-sul-lavoro-testo-unico-legge-81-2008,

Ringraziamenti

Ringrazio il Prof. Maurizio Bevilacqua, per avermi guidato e supportato nella fase più importante del mio percorso accademico.

Ai miei genitori, che sono il mio punto di riferimento e che mi hanno sostenuto sia economicamente che emotivamente e che mi hanno permesso di percorrere e concludere questo cammino. Grazie "alla mia mamma" e a tutti gli sforzi fatti che hanno contribuito al raggiungimento di questo traguardo, è la mia più fidata consigliera e il mio punto di riferimento. Mi ha sempre sostenuto nell'affrontare ogni difficoltà, mi ha consigliato nelle scelte più difficili. Grazie "al mio babbo" che mi ha sempre spronato a dare il massimo. Grazie "alla mia sorellina" che mi ha sempre tirato su di morale con il suo sorriso.

Al mio *"Gruppo d'idioti"*, Alberto, Giorgio, Giuseppe, Leonardo, Davide, Jacopo, Simone, Francisco, Alice, Corinne, Daniela, Elisa, Ivana, Ilaria, Greta, senza i quali il mio percorso universitario non sarebbe stato lo stesso, che hanno reso divertente ogni tempo passato insieme.

Ai miei coinquilini di "Casella", Daniele, Alessandro, Andrea, Alessio, Marco, compagni di serate indimenticabili, di chiacchierate interminabili, di risate e momenti unici, senza di loro non sarei mai arrivato a questo traguardo.

Alle mie amiche di università, Chiara, Sara, Matu, Viviana, Sara, Maria Stella, Fabiola che mi sono state sempre a fianco, mi hanno supportato e sopportato in questi anni e soprattutto mi hanno aiutato nei momenti più difficili.

In ultimo, ma non per importanza, un sentito ringraziamento al Dott. Pietro Coletta, alla stoma terapista Concettina e a tutti i medici ed infermieri e addetti ai lavori dei reparti di Chirurgia, Cardiologia, Gastroenterologia, Rianimazione dell'Ospedale Torrette di Ancona il vostro aiuto è stato letteralmente fondamentale per la mia vita.