UNIVERSITÁ POLITECNICA DELLE MARCHE

FACOLTÁ DI INGEGNERIA

Corso di laurea triennale in Ingegneria Gestionale

ASPETTI ORGANIZZATIVI DELLA SICUREZZA AZIENDALE IN AMBIENTE INDUSTRY 4.0

ORGANIZATIONAL ASPECTS OF COMPANY SAFETY IN INDUSTRY 4.0 ENVIRONMENT

Relatore:

Maurizio Bevilacqua

Tesi di laurea di:

Lucrezia Ventura

Anno accademico 2020/2021

INDICE

INTRODUZIONE

Negli ultimi dieci anni abbiamo assistito, e stiamo tutt'ora continuando a farlo, ad una vera e propria rivoluzione riguardante il modo di interagire con il mondo esterno. Rivoluzione che non si limita alle azioni quotidiane ma che ha coinvolto anche il modo di operare all'interno delle aziende. Sono nate nuove tecnologie, con la conseguente introduzione di nuovi macchinari, robot e dispositivi a supporto degli operatori, i quali hanno visto modificate anche i loro compiti.

Le nuove interazioni tra uomo e macchina e l'uso di robot sempre più autonomi, che per piccole anomalie potrebbero modificare improvvisamente il loro modo di operare, hanno portato anche a rivedere il ruolo della sicurezza all'interno dell'azienda smart. Inoltre, non basta più considerare solo la salute dell'operatore, ma bisogna pensare anche alla cyber security per la tutela della grande quantità di dati che vengono scambiati in rete.

Le tecnologie introdotte, se da una parte hanno portato a nuovi aspetti da considerare nella sicurezza, dall'altro sono fondamentali a sostegno della stessa, permettendo la riduzione di rischi e un maggiore controllo dello stato di salute dei lavoratori.

La tesi ha lo scopo di studiare i nuovi e diversi aspetti della sicurezza in aziende smart, esaminando i nuovi rischi a cui si può andare incontro, ma analizzando anche in quale modo le nuove tecnologie introdotte possono essere da supporto agli operatori e ai responsabili della sicurezza per la salvaguardia loro e dell'attività aziendale.

Nel CAPITOLO 1 viene fatta un'analisi preliminare di cosa si intende per Industria 4.0, dai primi passi verso la quarta rivoluzione industriale fino alla nuova legislazione introdotta nel nostro Paese. Vengono inoltre spiegate le tecnologie abilitanti del nuovo paradigma 4.0.

Nel CAPITOLO 2 si tratta la sicurezza nell'azienda in generale, partendo dall'analisi del rischio e andando poi nel particolare della *Safety 4.0* (a tutela del

lavoratore) e la *Cyber Security* (a tutela dei dati che corrono in rete); viene inoltre introdotto il concetto di *Safety Intelligence*. Infine, sono stati analizzati i nuovi possibili rischi a cui si può andare incontro, sia dal punto di vista fisico che psicologico, e le azioni preventive a sostegno della sicurezza: formazione del personale e manutenzione.

Nel CAPITOLO 3 viene illustrato come le nuove tecnologie di Industria 4.0 possono avere un ruolo fondamentale a sostegno della sicurezza, facendo un focus su due grandi pilastri abilitanti: *l'Internet of Things* fondamentale per la connessione in rete dei dispositivi e il *Digital Twin* che permette di ricreare un modello digitale partendo da uno reale.

INDUSTRIA 4.0

1. Industria 4.0 e la quarta rivoluzione industriale

Il termine "Industria 4.0" nasce con l'avvento della quarta rivoluzione industriale, con la quale, attraverso l'uso di tecnologie innovative, si vuole arrivare a elevati livelli di automazione e interconnessione dei processi produttivi.
Questo termine raggruppa le aziende organizzate con sistemi automatizzati che lavorano in maniera autonoma e a stretto contatto con gli operatori e l'ambiente circostante; sfruttano inoltre delle tecnologie che permettono di connettere tali sistemi tra loro all'interno dell'azienda e con l'esterno.

Le precedenti rivoluzioni sono state innescate dalle richieste del mercato o dalle tecnologie a disposizione per soddisfarle. La prima e la seconda hanno permesso di facilitare il lavoro nelle fabbriche e aumentarne la produttività attraverso l'introduzione di macchine meccaniche, nella prima rivoluzione, e del nastro trasportatore nella seconda; la terza rivoluzione ha portato all'automazione di passaggi ricorrenti nel processo produttivo. Ad oggi però, le esigenze dei clienti sono in continua evoluzione, per cui i mercati richiedono elevata flessibilità così da adattare le merci prodotte in modo rapido ed efficiente, e la quarta rivoluzione si pone l'obiettivo di soddisfare queste necessità attraverso l'interconnessione tra tutte le risorse e l'automazione dei processi.

Non è stato definito un anno di nascita esatto per questo fenomeno, a differenza delle precedenti rivoluzioni, ma le basi per la sua implementazione sono state poste nel 2013 quando alla Fiera di Hannover fu diffuso il report del progetto di un gruppo di lavoro dedicato all'Industria 4.0.

In Europa il primo Paese ad approcciarsi a questo processo di innovazione è stato la Germania e, successivamente, altri Paesi adottarono delle politiche con lo scopo di favorire le imprese ad adeguarsi alla quarta rivoluzione industriale.

In particolare, l'Italia aderì nel 2016 e negli ultimi anni la transizione da Industria tradizionale a Industria 4.0 è stata al centro dello sviluppo economico. Guardando all'ultimo periodo durante questa emergenza sanitaria, le tecnologie caratterizzanti l'Industria 4.0 hanno permesso di garantire il funzionamento di buona parte delle attività anche durante la pandemia. Infatti, degli studi hanno riscontrato che "le imprese che stavano ancora implementando tali soluzioni hanno avuto modo di metterle alla prova nella realtà; mentre per quelle che non avevano iniziato ad adottare le tecnologie per l'Industry 4.0, la crisi è stata un campanello d'allarme".[1]

Il modello tedesco si basa sul concetto di *Cyber Physical System* (CPS), cioè un sistema capace di interagire in tempo reale con la realtà in cui si trova ad operare; in questo modo, mondo fisico e mondo virtuale sono continuamente connessi.

I pilastri fondamentali su cui questa si basa sono quattro:

- Interoperabilità, consiste nella capacità di un sistema di interagire e funzionare insieme ad altri. Una tecnologia sfruttata per questo scopo è l'*Internet of Things* (IoT) che permette di collegare tra di loro le macchine utilizzate in azienda, con lo scopo di arrivare a una totale automazione.
- Trasparenza delle informazioni, tramite il concetto di *digital twin* il quale permette di rappresentare la realtà tramite modelli virtuali, e di sfruttarli per effettuare simulazioni e analisi di potenziali situazioni reali.
- Assistenza tecnica, dal momento che le tecnologie utilizzate, come gli apparecchi per la realtà aumentata, offrono la possibilità di individuare e risolvere problemi con maggiore facilità e in minor tempo.
- Decentramento delle decisioni, incorporando capacità decisionali automatiche direttamente sulle macchine. In questo modo non è

[1] Maci L., (2021) *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare*

richiesto l'intervento diretto dell'operatore che quindi ricopre solo un ruolo di supervisore.[2]

Come appena evidenziato, l'industria 4.0 non ha introdotto solo nuove tecnologie, ma anche nuovi compiti per gli operatori, i così detti "Operatori 4.0" che assumono un ruolo diverso all'interno del processo produttivo, ma non per questo meno importante. Essi devono essere in grado di interagire con robot e con le tecnologie introdotte nella *smart factory*, devono saper adattare le proprie capacità alle continue innovazioni e devono saper identificare, elaborare e utilizzare grandi quantità di dati e informazioni da grandi data base.

A cambiare sono anche gli spazi di lavoro, grazie alla possibilità di poter svolgere alcune professioni anche da remoto, e la nozione di salute del lavoratore, non più solo intesa come salute fisica ma anche psicologica.

[2] Muhammad Atif Javed, Faiz Ul Muram, Hans Hansson, Sasikumar Punnekkat, Henrik Thane, (2021), *Towards dynamic safety assurance for Industry 4.0*

2. *Le tecnologie abilitanti di Industria 4.0*

Quando si pensa alla quarta rivoluzione industriale non bisogna pensare a una singola innovazione ma a un insieme di tecnologie legate dal filo conduttore di Internet, queste sono:

1) Internet delle cose industriale, cioè l'IoT applicato ai macchinari utilizzati all'interno dell'azienda, che quindi hanno la capacità di essere collegati tramite Internet e di conseguenza di scambiare grandi quantità di dati senza l'intervento umano. I sistemi connessi in rete sono detti *Cyber Physical Systems*.
2) Big Data, rappresentano un insieme di dati trasmessi o ricevuti talmente vasto da rendere necessaria la definizione di nuove tecnologie e metodologie per estrapolare, gestire e processare informazioni entro un tempo ragionevole. Le fonti di questi dati possono essere varie e permettono di classificarli in *human generated*, *machine generated* e *business generated*. L'aspetto innovativo dei big data è la vasta quantità di attività che si possono svolgere con questa enorme quantità di informazioni che contengono; inoltre, se fino a poco tempo fa sarebbero serviti computer molto costosi per elaborare grandi porzioni di dati, ora per accedere a una piattaforma di analisi è sufficiente un semplice laptop.
3) Integrazione verticale e orizzontale dei sistemi, resa possibile attraverso una connessione totale dei soggetti.

   L'integrazione verticale permette la connessione tra diversi livelli della filiera, quindi ad esempio, con fornitori e clienti; in questo modo l'azienda può contare su un forte vantaggio competitivo, perché riesce a rispondere con maggiore facilità ai cambiamenti della domanda di mercato.

   Quella orizzontale, invece, connette l'azienda con altre appartenenti allo stesso livello, introducendo nuovi livelli di informazione, flessibilità ed efficienza operativa.

4) Simulazioni, fondamentali per il sostegno ad attività di programmazione e progettazione della produzione.
5) Cloud, è una tecnologia che permette sia la memorizzazione dei dati che l'elaborazione degli stessi, in questo modo il processo diventa molto più immediato da gestire e di conseguenza si ha una riduzione dei costi.
6) Realtà aumentata, attraverso appositi dispositivi come tablet, visori e smart glasses permette di sovrapporre elementi digitali a immagini reali semplicemente inquadrando l'oggetto.
7) Robot autonomi, sono capaci di supportare gli operatori interagendo con loro o tra di loro grazie all'IoT e ai Big Data. Molte aziende affidano ai robot compiti anche complessi, in modo da eliminare dal processo operazioni pericolose, pesanti o anche solo noiose e ripetitive. L'uso di questi dispositivi permette di aumentare l'efficienza e la sicurezza degli operatori e diminuire errori, costi e tempi di produzione.
8) Stampa 3D è la tecnologia utilizzata per la produzione additiva di oggetti fisici partendo da un disegno digitale in 3D realizzato con software CAD. Il principale vantaggio derivante dall'uso di questa tecnologia è la possibilità di realizzare, attraverso un singolo processo, prodotti che ne richiederebbero molti di più.
9) Cyber security, comprende l'insieme dei mezzi e delle tecnologie necessari a proteggere i dati condivisi in rete da possibili attacchi e a garantirne la veridicità.

   Industria 4.0 infatti richiede un'apertura verso il mondo per permettere ai sistemi di collegarsi tra loro, ma allo stesso tempo è necessario effettuare controlli sulle porte di comunicazione dei vari sistemi da e verso l'esterno per evitare possibili attacchi o violazione di privacy.[3]

[3] Forcina A., Falcone D., (2021), *The role of Industry 4.0 enabling technologies for safety management: A systematic literature review*

Ognuna delle tecnologie sopra citate ha impatto nell'ambito di quattro aree di sviluppo:

- Big Data, Internet of Things e Cloud Computing riguardano l'utilizzo dei dati e la loro conservazione.
- La seconda area è quella degli *analytics*. I robot automatizzati, infatti, attraverso la tecnologia *"machine learning"* possono perfezionare la loro resa imparando dai dati memorizzati ed elaborati in passato. In questo modo le aziende possono trarre numerosi vantaggi, visto che nell'azienda tradizionale solo l'1% dei dati raccolti vengono effettivamente utilizzati.
- La realtà aumentata e le interfacce touch influenzano l'interazione tra uomo e macchina
- L'ultima area riguarda il passaggio dal digitale al reale come la manifattura additiva attraverso la stampa 3D e le interazioni machine-to-machine.[4]

[4] Maci L., *op. cit.*

SICUREZZA AZIENDALE

1. Sicurezza aziendale: cosa si intende

Quando si parla di sicurezza aziendale ci si riferisce a tutti gli obblighi a carico del datore di lavoro e alle procedure da mettere in atto al fine di tutelare gli operatori e di mantenere un ambiente di lavoro sano.

Infatti, i principali obiettivi del SGSL (Sistema di Gestione della Salute e della Sicurezza sul Lavoro) sono l'identificazione, la prevenzione, l'attuazione delle misure necessarie e la documentazione di possibili rischi a cui si può andare incontro nel corso dell'attività aziendale.

Il SGSL in particolare si propone di:

- Ridurre i costi di salute e sicurezza sul lavoro, in particolare quelli derivanti da incidenti, infortuni e malattie professionali minimizzando i rischi a cui possono essere esposti lavoratori e soggetti esterni
- Aumentare l'efficienza e le prestazioni dell'azienda
- Migliorare i livelli di salute e sicurezza sul lavoro
- Migliorare l'immagine dell'impresa

Solitamente, soprattutto nelle grandi aziende, le responsabilità vengono divise tra i vari soggetti che si occupano dell'organizzazione della prevenzione e della protezione sul lavoro. Le responsabilità operative appartengono al datore di lavoro, al dirigente (colui che organizza il lavoro di altre persone sotto di lui), al preposto (colui che vigila e sorveglia la corretta esecuzione dei lavori in sicurezza da parte dei lavoratori) e al lavoratore. Questi devono poi interfacciarsi con soggetti con responsabilità consultive: il RSPP (Responsabile del Servizio di Prevenzione e Protezione) il medico competente o il RLS (Rappresentante dei Lavoratori per la Sicurezza).[5]

La gestione della sicurezza aziendale si è evoluta nel tempo con il succedersi delle varie rivoluzioni industriali: si è partiti da un modello di gestione molto semplice basato solo sull'esperienza dell'imprenditore durante la prima rivoluzione industriale, che è stato poi integrato dall'uso di tecnologie

[5] Zaritto A., (2015), *La gestione della sicurezza in azienda*

innovative e dall'analisi dei rischi, fino ad arrivare al modello attuale adottato nell'industria 4.0.

L'evoluzione tecnologica dell'ambiente di lavoro, infatti, comporta inevitabilmente che anche l'argomento della salute e della sicurezza affronti sostanziali cambiamenti. L'approccio non può più essere, quindi, un approccio di tipo reattivo, basato su vecchie logiche *command-and-control*, ma un approccio sistemico: ormai si deve parlare di *Total Safety Management*.

Questo nuovo modello è guidato da una *intelligence*, temine che sta a indicare "la raccolta, l'analisi, l'interpretazione e la comunicazione di dati e informazioni usati per i processi di decision making"[6]. Questo termine può essere applicato a diversi contesti, ma nel caso in esame si parla di *safety intelligence,* per cui i dati, dopo esser stati raccolti ed elaborati, serviranno per la stesura di piani volti a garantire la sicurezza sul luogo di lavoro.

[6] Bing Wang, (2020) *Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework*

Safety intelligence

La *safety intelligence*, come già specificato, indica l'insieme delle attività di raccolta e analisi di dati e informazioni al fine di sviluppare piani e prendere decisioni riguardo qualsiasi aspetto organizzativo; nel nostro caso particolare possiamo applicarla alla sicurezza dell'azienda.

Una delle funzioni chiave della *safety intelligence*, applicata a questo campo, è quella di integrare dati e informazioni dall'interno e dall'esterno e trasformarli in informazioni utili alla gestione della sicurezza. In questo modo i dati non necessari vengono eliminati, portando a una velocizzazione e semplificazione del processo decisionale; questo è un aspetto davvero rilevante, soprattutto perché ci troviamo nell'era dei Big Data in cui dati e informazioni abbondano.

A tal proposito, è importante sottolineare la differenza tra *safety data* e *safety information*; i primi vengono raccolti ma solo quelli davvero utili al processo decisionale verranno presi in considerazione e, una volta elaborati, diventano *safety information*.

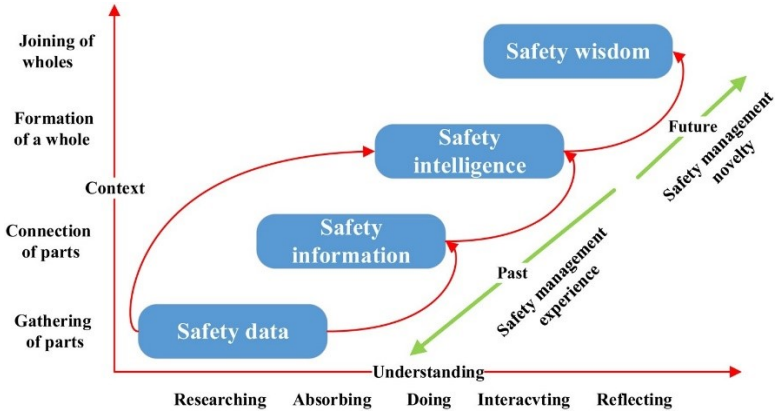

Figura 1: processo di gestione dei *safety data* e valore che questi assumono nel tempo.
Fonte: Bing Wang , op. cit

La figura 1 illustra il processo che da una prima fase di raccolta di *safety data* (*gathering of parts*), passa a una seconda fase in cui i dati vengono elaborati e trasformati in informazioni (*connection of parts*). Successivamente, mettendo insieme le informazioni a disposizione, si crea un piano. Fino a questa fase le azioni compiute riguardavano tutte il passato, per quanto riguarda i dati raccolti, e il presente, per i piani da mettere in atto. Nell'ultima fase, invece, sulla base dei

piani sviluppati si creano delle "conoscenze" da mettere in atto nei periodi futuri (*Safety wisdom*[7]).

Esistono tre tipologie di *safety intelligence*, basate sull'intervallo temporale che le decisioni ricoprono e, di conseguenza, sul loro impatto sulla gestione aziendale. La necessità di creare tre diversi livelli di safety intelligence nasce dal fatto che i safety managers elaborano strategie e pianificano investimenti con lo scopo di raggiungere, nel lungo periodo, gli obiettivi di sicurezza prefissati; ma questi, in ogni modo, per essere messi in atto, devono essere trasformati in decisioni a livello esecutivo. Infatti, nel processo decisionale, i piani sviluppati vengono continuamente aggiornati per ricreare con maggiore fedeltà la realtà.

Si considerano quindi tre livelli di *safety intelligence* ordinati gerarchicamente:

- Livello strategico, basato su decisioni di lungo termine (3-5 anni) che porteranno l'azienda a effettuare o meno investimenti per la sicurezza. Questo tipo di *safety intelligence* è gestita da managers con elevata esperienza che si trovano ai livelli strategici più alti nella gestione della sicurezza. È molto utile per determinare il quadro generale in cui si trova uno specifico fattore di rischio e si basa fortemente su previsioni e su azioni di gestione della sicurezza passate.
- Livello tattico-esecutivo, basato su processi decisionali a medio termine (cioè nell'arco di settimane o mesi) che porteranno all'aggiornamento del sistema di gestione della sicurezza. Lo scopo principale di questa tipologia di *safety intelligence* è di effettuare una identificazione e valutazione dei rischi per permettere ai managers di allocare risorse nella maniera migliore.
- Livello operativo, riguarda decisioni di breve periodo (decisioni giornaliere) basate su informazioni più dettagliate rispetto a quelle dei livelli precedenti. Visto il breve lasso di tempo in cui tali decisioni devono essere prese, i soggetti che si occupano della sicurezza a questo livello hanno bisogno di accedere ai dati in maniera più tempestiva.

[7] conoscenza di sicurezza

Ovviamente, nonostante la suddivisione nei tre livelli, ognuno di essi completa e influenza l'altro: l'intelligence strategica definisce i requisiti per quella tattico-esecutiva, che a sua volta li definisce per quella operativa.

I benefici che la *safety intelligence* apporta alla gestione della sicurezza quindi, sono vari e riguardano l'accelerazione del processo decisionale, il miglioramento dell'accessibilità delle informazioni (eliminando i dati superflui e quindi fornendo solo informazioni utili e attendibili), la gestione e riduzione dei rischi, l'aumento dell'efficienza e dell'efficacia delle operazioni volte alla sicurezza, la promozione della condivisione di informazioni riguardanti la sicurezza e il risparmio in termini di tempi e costi.

La *safety intelligence* è fondamentale nei processi decisionali riguardanti la sicurezza. Molti ricercatori, infatti, partendo dal modello decisionale di Hebert Simon[8], hanno sviluppato un modello decisionale composto da intelligence, progettazione, scelta, implementazione e controllo.
La prima fase di entrambi i modelli è quella della *safety intelligence* appunto, dove il responsabile delle decisioni sulla sicurezza identifica il problema e le sue cause e ne raccoglie dati e informazioni.
Successivamente egli converte i dati raccolti in informazioni utili e attuabili per la risoluzione dei problemi di sicurezza. Da qui poi seguiranno una fase di sviluppo di possibili alternative per la soluzione del problema, la scelta di una delle possibili alternative proposte, l'attuazione e infine le fasi di monitoraggio e revisione della strategia messa in atto. Possiamo quindi affermare che la *safety intelligence* rappresenta la base per il processo decisionale, in particolare in termini di sicurezza.[9]

[8]Herbert Alexander Simon (1916-2001), premio Nobel per l'economia. Ha sviluppato un modello decisionale basato su tre fasi: intelligence, progettazione e scelta.
[9] Bing Wang , op. cit.

Safety 4.0

Con l'evoluzione dei sistemi produttivi e l'introduzione di nuove tecnologie, è necessario rivedere anche gli aspetti organizzativi della sicurezza in azienda. Viene introdotto quindi un sistema di *Safety 4.0* cioè un sistema integrato di gestione dei dati che garantisca la sicurezza e la possibilità di intervenire sul sistema in tempo reale in modo da ridurre i costi dovuti a errori di misurazione, valutare e prevenire i rischi e avviare azioni correttive in maniera tempestiva.

Questo si basa sul concetto di *Total Safety Management* che porta all'integrazione della sicurezza nella strategia aziendale, a una responsabilizzazione dei dipendenti e all'utilizzo di metodi di analisi del rischio più solidi. L'obiettivo della sicurezza, quindi, non è più l'analisi di una singola attività critica, ma lo studio dell'intero processo di lavorazione all'interno del quale bisogna individuare i punti che potrebbero non funzionare e intervenire su di essi. Con l'integrazione della sicurezza nella strategia aziendale, il valore della salute viene visto come uno degli elementi chiave della politica aziendale, e quindi andrà ad influenzare anche l'immagine che l'azienda stessa crea di sé.[10]

Nel contesto di Industria 4.0 la sicurezza non assume più il significato tradizionale di protezione dei lavoratori, sia dal punto di vista fisico che psicologico, ma bisogna considerare anche la presenza di grandi quantità di dati da proteggere.

Infatti, nell'era dei *big data* in cui tutti i sistemi sono collegati in reti interne o esterne all'azienda, oltre all'incolumità degli operatori bisogna gestire anche la protezione dei dati attraverso la così detta *cyber security* (o sicurezza cibernetica). Nasce quindi la necessità di proteggere dati e informazioni che circolano in rete da possibili attacchi hacker.

[10] Kontogiannis T., Leva M. C., Balfe N., (2017) *Total Safety Management: Principles, processes and methods* da Safety Science, Volume 100, Parte B, p. 128-142

2. Analisi del rischio

La gestione del rischio aziendale è fondamentale per identificare, valutare e tenere sotto controllo le possibili minacce gravanti sull'attività aziendale e che potrebbero portare al non raggiungimento degli obiettivi prefissati.

In molti settori questa è un'attività fondamentale e spesso complessa visto l'ingente numero di requisiti a cui bisogna adempire, in particolare in determinati settori. Per permettere alle aziende un'implementazione sistematica, e quindi più semplice, dei piani di gestione del rischio, possono essere seguiti i principi ISO 31000, a prescindere dal settore in cui esse operano. Inoltre, un metodo ormai consolidato che permette alle aziende di determinare i propri punti di forza e debolezza e di conseguenza le modalità di gestione della salute e sicurezza, è il "Framework per la salute e sicurezza sul lavoro" (FSSL), sviluppato da APQI, Confindustria, Inail e Accredia attraverso il comitato tecnico scientifico del Premio Imprese per la Sicurezza nel 2011.[11]

Ovviamente, nessuna azienda è in grado di evitare completamente ogni tipo di rischio (finanziario, operativo, di mercato…), ma una buona gestione è in grado di portare a conseguenze non necessariamente negative. Le quattro fasi della gestione del rischio prevedono:

1) **Identificazione del rischio**

   Vengono identificati i diversi tipo di rischio in cui l'azienda può incorrere, i quali devono essere documentati in appositi registri.

   Per ottenere una completa visione della situazione aziendale è possibile ricorrere al metodo FAAPO (Fattore umano, Attrezzature, Ambiente, Prodotto, Organizzazione) che permette di ispezionare tutti possibili aspetti che possono essere messi a rischio, dal personale agli oggetti.

2) **Analisi del rischio**

   Analizzando i vari fattori si assegna a ogni rischio identificato una certa *probabilità* che questo si verifichi e si documentano le possibili conseguenze.

[11] Benedetti F., Bertorelli G., Bianconi R., Leuzzi F., Tronci M., (2016), *Il framework per la salute e sicurezza sul lavoro: i fattori abilitanti e i risultati, Rivista degli infortuni e delle malattie professionali,* VI serie, anno CIII, n. 3/2016, pp. 627-660.

3) **Valutazione del rischio**

   Si determina la portata del rischio, cioè la *gravità* dell'evento negativo che potrebbe verificarsi. Inoltre, in questa fase viene definito anche qual è il livello di rischio accettabile e si assegna maggiore priorità ai rischi con maggiore probabilità di verificarsi e che porteranno a conseguenze più gravi; questi saranno affrontati con maggiore tempestività.

4) **Mitigazione e successivo monitoraggio del rischio**

   Viene elaborata una strategia di risposta al rischio per controllarlo o minimizzarlo e per assicurarsi che i piani messi in atto funzionino bisogna effettuare un monitoraggio continuo.[12]

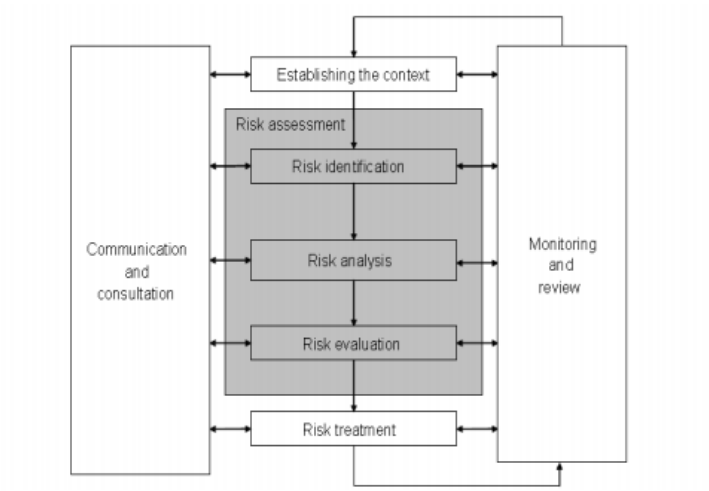

Figura 2: Processo per la gestione del rischio
Fonte: Giovanni Mottana, *Tecniche di valutazione del rischio*

Dalla seconda e terza fase del processo di gestione del rischio, si deduce che esso dipende da due fattori: la *probabilità* che l'evento negativo si verifichi e la *magnitudo* dell'evento stesso, cioè la gravità delle conseguenze che ne derivano. Quando si sviluppano delle strategie di mitigazione e controllo del rischio si può approcciare a tecniche attive o passive; le prime tendono a ridurre la probabilità che l'evento si verifichi, mentre le seconde cercano di ridurre la gravità delle conseguenze una volta che questo si sia verificato.

[12] Mottana G., (2012), *Tecniche di valutazione del rischio*

Nello sviluppo della strategia, per raggiungere il livello di rischio desiderato, bisogna sempre dare priorità alla diminuzione della probabilità del verificarsi dell'evento; considerando però che l'efficienza delle operazioni compiute tende a diminuire. Si arriverà quindi a un punto in cui l'investimento in attività di prevenzione del rischio non porterà a una diminuzione adeguata della probabilità che l'evento negativo si verifichi. A quel punto si punterà sulla mitigazione della gravità delle conseguenze.

Lo sviluppo di strumenti digitali ha permesso di risolvere molte carenze del processo di analisi del rischio tradizionale, come la poca profondità dell'analisi, la possibile perdita di concentrazione del team di valutazione a causa della ripetitività delle azioni e la durata di tutto il processo o un'inadeguata propagazione delle incertezze. Questo ha portato alla nascita di tecniche di identificazione e analisi dei rischi modificate. Le nuove tecniche partono sempre dall'approccio tradizionale dell'analisi ma la maggior parte di queste operano per gestire la complessità di grandi impianti, generando un output che dovrà poi essere riesaminato per identificare i problemi chiave. Per le imprese è fondamentale che in output si abbiano informazioni attendibili in modo da poter ridurre ulteriormente i rischi rispetto al processo tradizionale.

In particolare, i sistemi digitali dinamici di simulazione risultano essere molto utili nel processo di analisi dei rischi in molti casi, ad esempio quando:

- Si conosce bene la situazione che si sta studiando, in modo da interpretare nella maniera corretta gli output ottenuti;
- Nella valutazione è possibile rappresentare e considerare deviazioni e fallimenti delle prestazioni relative alle persone e ai processi produttivi;
- I risultati dell'analisi rimangono accessibili durante tutto il ciclo di vita dell'impianto, in modo da poter effettuare operazioni e cambi di gestione anche durante il suo funzionamento;
- Il mantenimento e la gestione dei cambiamenti al piano attuato nella simulazione non comportano un elevato dispendio di risorse[13]

[13] Lee J., Cameron I., Hassall M., (2019), *Improving process safety: What roles for Digitalization and Industry 4.0*

3. Principali rischi nell'industria 4.0

Sotto alcuni punti di vista, l'industria 4.0, come ogni tipo di industria, potrebbe essere definita "*safety-crictical*" se le innovazioni in termini di automazione e digitalizzazione non vengono adottate con cautela e portano quindi a eventi improvvisi che creano situazioni di pericolo per operatori o per l'attività aziendale in generale. Se infatti, piuttosto che un approccio olistico, prevarrà un approccio incentrato solo sull'economia, il rischio di un impatto negativo sulla salute dei lavoratori è possibile in diversi ambiti: intensificazione del carico di lavoro, aumento dei vincoli organizzativi, sovraccarico informativo, spersonalizzazione con perdita del senso di appartenenza e di attaccamento al lavoro, difficoltà nella separazione tra vita privata e vita professionale.

Oltre a possibili rischi per gli operatori, non è da sottovalutare il pericolo a cui è esposta la grande quantità dati e le informazioni condivise nel sistema. Nonostante i numerosi vantaggi apportati dalla possibilità di connettere in rete i vari sistemi, infatti, questa può portare anche a numerosi rischi. Rischi dovuti alla poca consapevolezza degli imprenditori, sia di piccole che di grandi imprese, che prestano poca attenzione a esaminare la possibilità e l'impatto di eventi sfavorevoli. Altro fattore che porta all'aumento del rischio di furto dei dati è il fatto che i dispositivi connessi, e di conseguenza anche i soggetti, sono in continuo aumento.
Inoltre, la tecnologia può, per quanto possibile, contrastare l'attacco ai dati da soggetti esterni, ma non potrà mai proteggere i dati da chi ha l'autorizzazione ad accederne; questo comporta una selezione molto attenta del personale autorizzato ad avere accesso alle informazioni più sensibili dell'azienda, devono essere quindi persone fidate per l'imprenditore.

Altro tema importante che può essere causa di rischi è *l'obsolescenza*, nel senso che i macchinari utilizzati hanno una vita solitamente più lunga dei sistemi informativi che li regolano, quindi, non è detto che con il passare degli anni i

macchinari resteranno compatibili con i sistemi informatici che invece evolveranno.

Un rischio di particolare importanza che invece riguarda il personale non dal punto di vista strettamente fisico ma più che altro psicologico, è l'*iperconnettività* che coinvolge non solo i sistemi produttivi ma anche gli operatori. Infatti, molti di essi sono dotati di dispositivi come pc, cellulari o tablet da usare appositamente per il lavoro forniti direttamente dall'azienda per cui lavorano. Grazie a questi possono avere continuo accesso alla propria posta elettronica, ad esempio, e possono essere contattati in ogni momento; questa situazione però può portare al *tecnostress*, termine usato per rappresentare il rischio da iperconnessione, che si manifesta se i lavoratori sono, o si sentono obbligati, ad essere disponibili a lavorare in ogni momento della giornata, anche fuori dall'orario di lavoro. Questo problema si è rivelato essere in forte crescita soprattutto nel periodo che stiamo vivendo, visto il continuo aumento di personale che lavora in smart working a causa dell'emergenza pandemica.
Una soluzione per prevenire tale problematica è la creazione delle così dette "pause digitali" che consistono in pause ogni determinati intervalli di tempo per gli operatori che lavorano ai videoterminali o in interruzioni vere e proprie di connessione fuori dall'orario di lavoro.

Un ulteriore rischio a cui si può andare incontro nel processo di trasformazione delle industrie tradizionali in industrie digitali è causato dall'uso di robot, cobot e altre forme di intelligenza artificiale che, se da una parte permettono all'operatore di evitare azioni fisicamente pesanti o ripetitive, dall'altra possono creare una sensazione di *autonomia ridotta* o la paura di *perdere le proprie funzioni* poiché i lavoratori si vedono "sostituiti" dalla macchina.[14]
Altro aspetto da considerare nell'uso di queste tecnologie è la stretta vicinanza che si crea tra uomo e robot, che comporta la necessità di installare opportuni sensori

[14] Tronci M, Mercadante L, Ricciardi P, *Industria 4.0: rischi e opportunità per la tutela e la sicurezza dei lavoratori*

sulle macchine che permettano di individuare l'avvicinarsi dell'operatore e che regolino di conseguenza la velocità dei movimenti o che ne causino l'arresto in sicurezza.
Sia in passato che attualmente, per le macchine per le quali non è prevista l'interazione con l'operatore, vengono usate delle barriere metalliche all'interno delle quali viene confinato il robot in modo da rendere impossibile l'accesso dell'uomo mentre questo è in movimento. Possono essere previsti dei cancelli che permettono all'operatore di avvicinarsi alla macchina quando questa è spenta per effettuare operazioni di manutenzione o di programmazione.
Grazie alla continua evoluzione dei sistemi nei vari reparti dell'azienda, è stata resa possibile l'automazione anche di operazioni di immagazzinamento e trasporto all'interno dell'impianto. Questo comporta una particolare attenzione all'uso delle attrezzature utilizzate a tale scopo, come traslo elevatori o veicoli per il trasporto delle merci a guida automatica; per entrambi vengono definiti dei limiti di velocità, la quale sarà sicuramente inferiore a quella dell'operatore, e spesso vengono previsti dei sensori per il controllo del veicolo che permettono il suo arresto o il rallentamento.

Un altro esempio che potrebbe portare a rischi per la sicurezza all'interno dei reparti è l'uso di carrelli elevatori, i quali possono incorrere in rovesciamenti o ribaltamenti. Per evitare che questi eventi si verifichino si utilizzano, ad esempio, forche a sbalzo che permettono di contrastare il peso dell'unità da trasportare e si definiscono dei limiti massimi di velocità e di sollevamento del carico. Inoltre, gli operatori che ne fanno uso devono essere adeguatamente formati sia riguardo la guida dei veicoli che riguardo la gestione di eventuali situazioni di pericolo che possono verificarsi.

4. Prevenzione del rischio: formazione e manutenzione

Quando si gestisce il rischio in azienda è possibile intervenire su due aspetti: la probabilità che l'evento negativo si verifichi è la pericolosità dell'evento, cioè la sua magnitudo.

Per migliorare entrambi questi aspetti è fondamentale attuare, oltre alle precauzioni necessarie, azioni di formazione, sia del personale che del datore di lavoro e di chi gestisce la sicurezza, e manutenzione degli impianti.

La prima delle attività sopra citate, cioè la formazione del personale, incide sul comportamento del lavoratore rendendolo consapevole dei rischi e capace di evitarli. Vista l'importanza di questo aspetto, la legge italiana ha deciso di emanare una normativa di riferimento aggiornata: il Testo Unico 81 del 2008 e il Decreto legge 106 del 2009, in cui dichiara che ogni datore di lavoro deve garantire questa formazione ai propri collaboratori, che potranno così evitare di danneggiare sé stessi e gli altri.

Per incentivare le aziende sotto questo punto di vista, i Ministeri di Economia e Finanze, Sviluppo economico, Lavoro e Politiche sociali hanno firmato un decreto sul "credito d'imposta formazione 4.0" grazie al quale, dal 22 giugno 2018, le aziende che intendono effettuare corsi di formazione 4.0 possono beneficiare di un bonus. Per averne l'accesso non è necessario aver effettuato investimenti in strumenti di industria 4.0, quindi ne possono beneficiare anche le aziende di produzione di servizi, non solo le aziende manifatturiere. Lo scopo della formazione è di far acquisire ai lavoratori competenze sulle tecnologie 4.0 nell'ambito di informatica, delle tecniche e tecnologie di produzione.[15]

La manutenzione, invece, nello scenario produttivo moderno è una delle questioni più critiche e le aziende stanno provvedendo alla propria trasformazione sia dal punto di vista tecnologico che gestionale.

Nel corso del tempo, infatti, si è passati da una manutenzione volta alla correzione dei guasti a una volta alla loro prevenzione, detta appunto "manutenzione

[15] M. Tronci, L. Mercadante, P. Ricciardi, op. cit.

preventiva". In questa categoria sono incluse sia la manutenzione programmata che quella predittiva.[16] Quest'ultima è nata grazie agli strumenti tecnologici che permettono di apprendere e fornire informazioni elaborando i dati forniti dall'IoT. In questo modo l'azienda può sviluppare dei modelli di comportamento delle macchine che permettono di individuare il periodo di tempo prima che il guasto si verifichi, l'elemento che si romperà e in che modo gestirlo al meglio.

Oltre alla diminuzione dei rischi, un altro vantaggio di questa tipologia di manutenzione è la riduzione dei tempi di manutenzione e fermo macchina, che eviterà così anche il bloccaggio del processo produttivo permettendo all'azienda di essere più efficiente con le scadenze.

Per ottimizzare la gestione delle varie tipologie di manutenzione è necessario far fronte tempestivamente ai guasti, tenere traccia di eventuali riparazioni effettuate e monitorare le scadenze previste in ambito di sicurezza. Per fare questo, un approccio tradizionale basato su documentazione cartacea non è sufficiente poiché richiederebbe tempi troppo lunghi e avrebbe margini di errore troppo alti, per questo servono soluzioni software che permettano di gestire persone e scadenze, di coordinare gli interventi da effettuare e di fornire e memorizzare le informazioni.[17]

Uno strumento fondamentale per tale scopo possono essere i CPS (Cyber Physical Systems), che come spiegato inizialmente sono i sistemi connessi alla rete e che quindi possono comunicare tra loro, attraverso i quali, quindi, è possibile attivare attività di diagnostica a distanza. Permettono inoltre di raccogliere una quantità significativa di dati in tempo reale sullo stato attuale delle macchine, che saranno poi la base per l'analisi dei Big Data.

L'operatore di manutenzione 4.0 quindi, deve essere in grado di gestire e interpretare informazioni analizzando i Big Data, oltre alla capacità di interagire con strumenti digitali e robot adattando continuamente le proprie competenze alle innovazioni. Inoltre, esso può trarre un grande vantaggio dalle tecnologie introdotte dalla quarta rivoluzione industriale, come la realtà aumentata e i Cyber

[16]Silvestri L., Forcina A., Introna V., Santolamazza A., Cesarotti V., (2020), *Maintenance transformation through industry 4.0 technologies A sistematic literature review*

[17] www.futureindustry.it, *Manutenzione predittiva industria 4.0*

Physical Systems che, grazie all'IoT che permette la connessione in rete dei dispositivi, permettono all'operatore di avere dei feedback in tempo reale e una formazione migliore.[18]

[18] Gallo T., Santolamazza A., (2021), *Industry 4.0 and human factor: How is technology changing the role of the maintenance operator?*

5. *Cyber security*

In un'ambiente di industria 4.0, dove un ruolo rilevante è rivestito anche dalle attrezzature elettroniche e dalle informazioni in esse memorizzate, oltre alla *cyber safety*, è importante considerare anche la *cyber security*.

La prima sappiamo che si occupa dell'incolumità delle persone che operano in azienda, mentre la seconda comprende tutte quelle attività atte a salvaguardare gli strumenti elettronici da soggetti esterni.

Nel contesto industriale si parla di *Industrial Cyber Security*, termine con cui si indicano tutti i mezzi dell'automazione di fabbrica che hanno l'obiettivo di rendere immuni da possibili attacchi i sistemi di controllo. Molte delle nuove tecnologie adottate possono portare infatti a scenari di sicurezza non previsti, ad esempio, le telecamere di sicurezza permettono maggior controllo degli ambienti ma allo stesso tempo, se non sono correttamente configurate, possono essere vulnerabili e quindi utilizzabili per effettuare attacchi.

L'industria 4.0 quindi richiede di avere da una parte un'apertura verso il mondo per favorire l'integrazione tra sistemi diversi, ma dall'altra è fondamentale mettere in atto un controllo stretto della comunicazione verso l'esterno per proteggersi da possibili attacchi.[19]

A livello globale le minacce continuano a evolversi e sta aumentando il numero di soggetti esposti a *data breach*[20], più che raddoppiati rispetto al 2018.

La maggior parte delle violazioni riguarda settori che trattano dati medici o finanziari interessanti per i cybercriminali, come quello dei servizi medici, rivenditori ed enti pubblici; questo però non esclude che qualsiasi azienda connessa in rete non possa essere colpita da cyber attacchi per spionaggio aziendale o per attacchi ai dati dei clienti. Tuttavia, la protezione delle tecnologie di Operational Technology è ancora un aspetto sottovalutato dalle aziende e questo porta l'Italia, così come gli altri stati in cui il manufatturiero è una delle principali

[19] Zanetta L., *La trasformazione digitale delle PMI: il Piano Nazionale Impresa 4.0 e gli altri strumenti a supporto dell'innovazione digitale delle imprese*

[20] *Data breach*: violazione di sicurezza che comporta, accidentalmente o in modo illecito, la perdita, la modifica o la divulgazione non autorizzata.

fonti di reddito, ad essere tra i primi Paesi più deboli dal punto di vista della sicurezza.

La fase preliminare nella gestione della sicurezza, sotto questo punto di vista, consiste nell'analisi dell'infrastruttura di automazione e nella definizione del livello di minaccia a cui e sottoposta ciascuna macchina, reparto produttivo o stabilimento, oltre alle possibili conseguenze a cui si può andare incontro. Grazie a questa analisi le aziende possono passare alla definizione di contromisure da adottare avendo anche un giusto compromesso tra costi e benefici.

Quello della *cyber security* è un ambito molto complesso, nel quale un semplice antivirus non è sufficiente, infatti, la misura più efficacie per proteggere i dati è l'applicazione dello standard internazionale ISA 99/IEC 62443 che copre tutte le fasi del ciclo di vita dei sistemi di controllo, partendo dall'analisi inziale delle vulnerabilità fino alle attività volte al mantenimento dei livelli di sicurezza desiderati.

Oltre a questo, l'ISO ha pubblicato nel dicembre 2018 un rapporto tecnico con alcune raccomandazioni che devono seguire i costruttori delle macchine per fare in modo che immettano sul mercato prodotti sicuri anche da eventuali attacchi informatici.[21]

[21] Intervista a Ugo Gecchelin e Stefano ferrari, *Industria 4.0 e i rischi per la sicurezza dei dati. 2^ parte - il quadro normativo*, Marzo 2020

TECNOLOGIE PER LA GESTIONE DELLA SICUREZZA

L'introduzione di nuove tecnologie ha rivoluzionato i processi produttivi e i rapporti tra macchine e risorse umane. Per questo è necessario ripensare a piani da seguire per gestire al meglio la sicurezza, sia riguardante compiti già esistenti che sono stati rivoluzionati, sia compiti nuovi nati con l'avvento della quarta rivoluzione industriale. Basti pensare che in passato l'uomo e la macchina operavano a dovuta distanza, spesso posizionando i macchinari all'interno di gabbie di protezione, mentre ora, in alcuni casi, è possibile la loro cooperazione; ad esempio, nei casi di "*machine learning*" in cui la macchina, in fase di programmazione, è guidata dall'operatore nei movimenti che dovranno essere memorizzati e ripetuti da questa.

L'impatto dell'industria 4.0 sulla sicurezza non è a priori né favorevole né sfavorevole. Come sostiene la pubblicazione Inail "Sfide e cambiamenti per la salute e la sicurezza sul lavoro nell'era digitale" infatti, dipende da come queste tecnologie verranno sfruttate: se ci si concentrerà solo sugli aspetti economici, senza considerare le esigenze di salute e sicurezza dei lavoratori, si rischia di avere un impatto negativo.

Il passaggio a industria 4.0, quindi, è in parte evoluzione e in parte rivoluzione, infatti, l'innovativo sistema di pensiero e la trasformazione digitale attuata hanno rivoluzionato il modo di definire la programmazione in azienda, portando a numerosi benefici non solo economici. Ad esempio, si è arrivati allo sviluppo di software avanzati di progettazione e strumenti di monitoraggio migliori, che hanno portato alla possibilità di ottenere diagnosi in tempo reale e un conseguente aumento della sicurezza.

Tra i principali vantaggi introdotti dall'automazione ci sono, ad esempio, una diminuzione del rischio da lavoro correlato[22] o lo sforzo fisico dell'operatore.

Buona parte degli svantaggi, invece, riguardano da una parte, i nuovi rapporti tra uomo e macchina e nuovi contratti di lavoro - esempi possono essere il

[22] Indica la percezione di squilibrio avvertita dal lavoratore quando le richieste dell'ambiente di lavoro eccedono le capacità individuali.

tecnostress[23] o il rischio che corre l'operatore a contatto con le macchine, soprattutto i robot collaborativi. D'altra parte, possiamo avere il furto di informazioni talvolta importanti per l'azienda, dovuto al fatto che i sistemi sono perennemente interconnessi in rete.

Una delle tecnologie chiave utilizzata per ottenere risultati in industria 4.0 è il concetto di *digital twin,* largamente sfruttato per analizzare in profondità i limiti dei sistemi in modo da indirizzarsi verso scelte migliori. Questa tecnologia può essere applicata a ogni sistema, spesso affiancata all'*Internet of Things*, utile sia per creare il modello digitale che per la comunicazione in tempo reale.

[23] Stress causato dall'uso prolungato o eccessivo di tecnologie e strumenti informatici

1. Miglioramenti nel campo della sicurezza

Come spiegato nel primo capitolo, i pilastri fondamentali su cui ci si basa per la transizione da azienda tradizionale a "*smart"* sono svariati, e molti di essi permettono di apportare miglioramenti alla gestione della sicurezza, soprattutto per quanto riguarda l'identificazione e la prevenzione dei rischi.

Ad esempio, nell'industria dell'edilizia sono stati sviluppati dei dispositivi innovativi di Internet of Things che, una volta indossati, permettono di monitorare il battito cardiaco e altri parametri dell'operatore i quali, se superano un certo valore, inviano a quest'ultimo dei segnali. Dai risultati di uno studio è emerso che grazie a questi dispositivi è aumentata la consapevolezza dei lavoratori sui possibili rischi ed è stato possibile creare ambienti di lavoro più sicuri.

Altri dispositivi fondamentali per la sicurezza sono i sensori. Questi possono essere posizionati ad esempio nel luogo di lavoro e, attraverso la rete creata, permettono di raccogliere e memorizzare dati sulle condizioni dell'ambiente di lavoro.

Un grande contributo apportato dalla digitalizzazione delle operazioni è il fatto che molti compiti, soprattutto quelli ripetitivi o molto pesanti, possono essere affidati alla macchina invece che all'operatore. Spesso questi lavori sono considerati di "bassa qualità" e se venissero affidati a un operatore, questo potrebbe sentirsi come se le proprie competenze non venissero sfruttate a pieno; in questo modo invece egli si sentirà maggiormente motivato a svolgere la propria mansione. Se ne trova larga applicazione, ad esempio, nei grandi magazzini logistici di commercio elettronico.[24]

L'uso di tecnologie per il miglioramento della sicurezza sul posto di lavoro ha avuto un ruolo importante per la nascita di uno studio in seguito a due gravi incidenti mortali avvenuti a Hong Kong. In entrambi i casi i corpi dei lavoratori sono stati trovati a distanza di parecchie ore dal momento dell'incidente; questo perché, quando essi si trovano a lavorare in aree desolate è difficile conoscere il loro stato di salute a distanza e le informazioni per il primo soccorso, che quindi tarda ad arrivare. L'uso del GPS funziona molto bene in situazioni all'aperto ma

[24]Tronci M., Mercadante L., Ricciardi P., *Industria 4.0: Rischi e opportunità per la tutela e la sicurezza dei lavoratori*

ha scarse prestazioni all'interno poiché i segnali hanno una bassa capacità di penetrazione attraverso i muri; entra in gioco quindi, l'Internet of Things che permette la comunicazione anche a maggiori distanze e in spazi chiusi.[25]

Un ulteriore importante contributo alla sicurezza è la dotazione di dispositivi di protezione individuale *smart* che sfruttano l'intelligenza artificiale per rilevare dati in maniera intelligente. Un esempio possono essere i dispositivi per la rilevazione della temperatura corporea fondamentale per il contenimento dei contagi da Covid-19. Altre tecnologie, dette di *DPI Detenction,* permettono il controllo degli accessi e la rilevazione di dispositivi di sicurezza dei lavoratori in tempo reale garantendone la sicurezza.

[25] Zhiheng Zhao, Leidi Shen, Chen Yang, Wei Wu, Mengdi Zhang, George Q. Huang, (2020), *IoT and digital twin enabled smart tracking for safety management*

1. Internet of Things

L'*Internet of Things* ha permesso il passaggio da una rete di computer a una rete di svariati oggetti connessi tra loro detti *Smart Objects* (oggetti intelligenti). Grazie a questa tecnologia, infatti, oggetti di uso quotidiano o industriale vengono dotati di una identità digitale e comunicano dati e informazioni agli utenti con i quali interagiscono attraverso una piattaforma digitale; questo può essere un valore aggiunto per il supporto alla gestione e al controllo della sicurezza sul posto di lavoro.

Vista la crescente applicazione di questa tecnologia, dovuta a prestazioni sempre migliori e prezzi di acquisto decrescenti, negli ultimi anni sono state sviluppate diverse soluzioni adatte al campo della sicurezza per gestire situazioni in modo dinamico come dei rilevatori di frequenza (*Radio Frequency Identification*, RFID), dispositivi indossabili, reti di sensori ecc.

RFID permettono il tracciamento di oggetti e persone in azienda non più attraverso i tradizionali barcode ma attraverso lettori di codici che sfruttano le onde radio, quindi senza contatto a distanza più o meno ampie. L'elemento che permette il funzionamento di questa tecnologia è il tag, composto da un'antenna e un chip, che viene posto sull'oggetto a identificare e da un lettore che comunica con il tag. Un'evoluzione più recente di questa tecnologia è il BLE che si basa sulla stessa struttura del RFID ma i tag permettono una lettura da distanze maggiori e i lettori possono essere semplici dispositivi a disposizione dell'operatore come tablet o cellulari.

Per evitare incidenti e infortuni sul lavoro vengono usate tecnologie di Internet of Things che permettono di monitorare la posizione dell'operatore durante lo svolgimento delle proprie mansioni o in situazioni di emergenza. Alcuni studi hanno analizzato degli esempi di applicazione, uno di questi consiste nel dotare l'operatore di un braccialetto RFID che rilevi la sua posizione e ogni volta che egli si avvicina alla zona definita pericolosa, manda un segnale di stop alle

apparecchiature. Un altro esempio è quello presentato da Kim & Kim[26] riguardante l'industria siderurgica e consiste nel posizionare i tags all'interno degli elmetti di protezione dei lavoratori e i lettori sul macchinario pericoloso, ad esempio una gru da carico, e questi, grazie agli infrarossi, permettono di indicare la distanza tra operatore e macchina che verrà poi comunicata ad un server centrale di raccolta di questi dati.

Sono stati inoltre introdotti dei dispositivi di Internet of Things indossabili per tenere sotto controllo lo stato di salute degli operatori durante le ore di lavoro. Questi vanno ad integrare i sistemi ALI (*Active Leading Indicators*) per identificare e prevenire situazioni pericolose e per misurare la fatica umana in determinate circostanze lavorative. Gli ALI infatti, servono per monitorare la frequenza cardiaca e la temperatura degli operatori e, grazie all'IoT, quando questi raggiungono una soglia critica, inviano loro un segnale. Un esempio di applicazione è per i lavoratori dell'industria mineraria che devono compiere azioni spesso faticose.

Tra i dispositivi di Iot più diffusi troviamo i sensori. In uno studio sono stati introdotti, ad esempio, dei sistemi con sensori che permettono la misurazione dei livelli di anidride carbonica negli ambienti chiusi e, confrontando le prestazioni di questi con quelle di sistemi con sensori tradizionali, è emerso che questi inviavano il segnale di allerta da 3 a 7 volte più rapidamente rispetti ai tradizionali. Altri studi, invece, ne hanno proposto l'implementazione all'interno dei magazzini; un esempio possono essere i sensori utilizzati per lo spostamento, all'interno dell'impianto, di carrelli trasportatori di tipo AGV (*Automated Guided Vehicle*) senza conducente i quali, attraverso appunto dei sensori sono in grado di rilevare eventuali ostacoli nelle vicinanze e di conseguenza di regolare la loro velocità di viaggio. Un altro esempio anche se non strettamente legato alla sicurezza per questo tipo di trasportatori, sono dei sensori che sfruttano un laser per poter individuare la posizione esatta del carrello all'interno dell'edificio; è il caso in cui il percorso che questi devono compiere viene programmato

[26] Kim K., & Kim M. (2012). *RFID-based location-sensing system for safety management. Personal and Ubiquitous Computing*, 16(3), 235-243.

autonomamente dal veicolo che, in base alla posizione in cui si trova e a quella che deve raggiungere, è in grado di definire la traiettoria da seguire.

Altri studi hanno illustrato l'uso dell'IoT per valutare possibili rischi legati alla salute degli operatori che lavorano nella catena del freddo, ossia quella che si occupa di prodotti surgelati. Dai risultati dello studio è emerso che, oltre al controllo della qualità dei prodotti, l'Iot è fondamentale, attraverso una logica Fuzzy, per il mantenimento delle condizioni di salute degli operatori. Infatti, la frequenza dei rischi legati ai lavoratori è stata ridotta ed è aumentato il livello di soddisfazione ed efficienza degli stessi.[27]

Altri studi hanno dimostrato come l'Iot sia strettamente legato ai sistemi BMI (*Building Information Modeling*) poiché permette, oltre alla funzione di costruzione e monitoraggio, anche la possibilità di gestire la sicurezza degli operatori.[28]

Altre volte è possibile considerare anche una combinazione di varie soluzioni. Un esempio è stato discusso durante la Conferenza Internazionale dell'Industria 4.0 e dello Smart Manufactoring del 2019 e consiste in una integrazione verticale di tre diverse funzioni:

1) Identificare in modo univoco tutte le attrezzature all'interno del reparto attraverso *smart labels* (spiegare in una nota cosa sono) e in questo modo monitorare la loro manutenzione in tempo reale
2) Prevedere in maniera affidabile l'obsolescenza delle attrezzature attraverso *sensori virtuali*
3) Gestire segnali di allerta in caso di condizioni pericolose per i lavoratori attraverso dei dispositivi indossabili e altri sensori ambientali

In questo modo il sistema può interagire con gli utenti sia in modo tradizionale, attraverso cabine di controllo da remoto, che in tempo reale direttamente nell'area di lavoro. È un prototipo di sistema studiato appositamente per vari tipi di utenti,

[27] Tsang YP, Choy KL, Wu C-H, et al (2018) *An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks*
[28] Forcina A., Falcone D., (2021), *The role of Industry 4.0 enabling technologies for safety management: A systematic literature review*

che vanno dai lavoratori che accedono all'area considerata pericolosa per eventuali manutenzioni, ad esempio, ai *HSE managers*[29] che supervisionano la sicurezza degli operatori durante le operazioni nelle aree pericolose, fino agli *auditors*, che devono visitare periodicamente l'impianto per verificare che le misure di prevenzione vengano adottate nella maniera corretta.[30]

Altri alleati dell'Inernet of Things sono il *machine learning* e il *deep learning* che permettono di fornire all'azienda un'analisi avanzata dei dati e di poter effettuare previsioni anche in ambiti in cui questo risulta molto difficile. L'obiettivo di entrambe queste tecnologie è di fornire al computer la capacità tipicamente umana di imparare seguendo esempi e attraverso l'esperienza. Il deep learning è utilizzato nell'automazione industriale per rilevare la presenza di persone e oggetti quando questi sono troppo vicini alle macchine.

[29] Health, Safety & Environment managers

[30] Gnoni M. G., Bragatto P. A., Milazzo M. F., Setola R., *Integrating IoT technologies for an "intelligent" safety management in the process industry,* 2019

1. Digital twin

Il digital twin consiste nella creazione di un modello digitale che ricalchi fedelmente l'ambiente reale in modo da poter effettuare analisi e simulazioni utili in seguito per prendere decisioni. Un ulteriore contributo fornito da questa tecnologia è la possibilità di far comunicare tra loro modelli fisici e digitali, condividendo dati e informazioni solitamente in modo bidirezionale.
La possibilità di avere flussi bidirezionali permette di supportare lo sviluppo di strumenti di *early warning* in modo da poter realizzare sistemi proattivi di sicurezza in ambienti di lavoro complessi. Per *early warning* si intende un sistema che permetta di individuare eventi o segnali che possano costituire un rischio o una minaccia per il lavoratore o, se utilizzati in rete, per i dati. In questo modo l'azienda può prevenire eventuali eventi negativi agendo prima che questi si verifichino.
Le aree principali in cui ci si serve del supporto del digital twin sono tre: il monitoraggio in tempo reale dello stato del sistema, l'analisi e previsione di guasti e la manutenzione.

I pilastri principali per l'utilizzo del digital twin sono dal lato digitale, strumenti di simulazione ad alta affidabilità, mentre dal lato reale, sensori e tecnologie di misurazione collegati tramite dispositivi di Industrial Internet of Things. Oltre a questi, per creare il digital twin di un modello fisico sono necessarie tecnologie come *Cloud Systems* e *Big Data Analytics* per la conservazione e l'elaborazione di dati e informazioni scambiati tra i due modelli.

Essendo una tecnologia abbastanza complessa, i primi passi sono stati mossi negli anni '70 nel settore aerospaziale e dell'aviazione, mentre ha iniziato a comparire in letteratura e ricerca negli anni 2000. Infatti, la crescente diffusione del paradigma 4.0 ha portato all'applicazione di questo nuovo strumento ad altri settori, in particolare in quello industriale; ora è largamente diffuso nel settore manufatturiero. Nonostante questo, le applicazioni degli strumenti di Digital Twin nel contesto della sicurezza sono ancora poche, ma rappresentano comunque un importante ramo nella ricerca ingegneristica.

In letteratura sono presenti dei framework utili a chi si occupa della realizzazione di modelli di Digital Twin nel campo della sicurezza che permettono di valutarne le capacità complessive basandosi su tre criteri principali: l'acquisizione dei dati, la loro elaborazione e criteri di sicurezza.
Il primo si riferisce al modo in cui i dati vengono acquisiti dal mondo fisico in base agli strumenti e alle tecnologie adottate; possiamo avere dati casuali, storici e dati in tempo reale da sensori fisici. Gli ultimi sono quelli maggiormente raccolti e rappresentano il metodo più utile per supportare il servizio Digital Twin.
Il criterio del trattamento dei dati invece, permette di definire tre diversi metodi per l'elaborazione dei dati raccolti: tecniche statistiche, metodi di simulazione e tecniche di apprendimento. Le prime di basano sull'uso di semplici modelli analitici, mentre le tecniche di apprendimento automatico consentono un'elaborazione più complessa. Possiamo quindi definire queste tecniche secondo una scala gerarchica incrementale in base alla complessità delle prestazioni: la tecnica statistica tradizionale potrebbe fornire un aiuto più limitato, mentre con i modelli di simulazione si avrà un livello leggermente superiore vista la possibilità di poter ricreare possibili scenari ottenendo così risultati più affidabili, infine, con le tecniche di apprendimento si avranno le massime prestazioni da parte dei modelli vista la loro capacità di riprodurre la conoscenza e la capacità di ragionamento umana.
L'ultimo criterio, quello della sicurezza, dipende strettamente dalla fonte di rischio che genera il problema di cui si occupa l'applicazione di digital twin che si va ad analizzare. Permette di determinare tre categorie divise secondi rischi basati sulla macchina, sull'uomo o sulle interazioni uomo-macchina. Quest'ultima categoria è la più importante poiché permette una collaborazione uomo-macchina più efficiente e sicura.[31]

Un esempio di applicazione del digital twin è quello proposto in [32] per il controllo della sicurezza sul posto di lavoro per operatori di grandi magazzini

[31] Agnusdei G. P., Elia V., Gnoni M. G., (2021), *A classification proposal of digital twin applications in the safety domain.*
[32] Zhiheng Zhao, Leidi Shen, Chen Yang, Wei Wu, Mengdi Zhang, George Q. Huang, (2020), *IoT and digital twin enabled smart tracking for safety management*

composti da celle di refrigerazione, che quindi sono tenuti a lavorare in condizioni poco "piacevoli" per il corpo umano. È stato creato quindi un framework chiamato *iSafeTrack,* con lo scopo di collegare gli attributi del mondo cibernetico utilizzando dispositivi e tecnologie Iot per diversi stakeholders, che possono essere operatori, supervisori o figure manageriali superiori. Ognuna di queste tre categorie sarà coinvolta in maniera diversa per l'accesso ai dati e alle funzioni: gli operatori sono i soggetti tracciati quindi forniscono esclusivamente informazioni, i supervisori possono monitorare i vari spostamenti e lo stato di salute dal modello digitale e, in caso di emergenza, fanno partire segnalazioni di assistenza, mentre il safety manager è l'unico ad avere l'autorizzazione a definire i parametri ed è il responsabile dell'efficienza del sistema di sicurezza.
Le risorse fisiche sono rappresentate dall'uomo, macchinari e materiali e, tramite i dati raccolti in tempo reale dai dispositivi Iot, ne vengono creati i corrispettivi digitali. A questo punto ogni spostamento o cambiamento che avverrà nel mondo reale verrà aggiornato anche nel suo modello digitale; ad esempio, in cambiamento dello stato di salute dell'operatore può essere rappresentato con un cambio di colore nel modello cyber.

CONCLUSIONI

Sulla base dell'analisi dei documenti scelti, si può concludere che la gestione della sicurezza all'interno delle aziende sta subendo cambiamenti significativi. In particolare, è bene evidenziare che la transizione 4.0, in questo campo, sta avendo sicuramente sia i suoi effetti positivi che negativi. Infatti, da una parte le tecnologie abilitanti dell'Industria 4.0 sono da supporto al safety manager nel controllo e nella gestione della salute dei lavoratori; d'altra parte, le nuove interazioni che si creano tra uomo e macchina, la connessione dei dispositivi nella rete e la grande quantità di dati che circolano al suo interno creano nuovi fattori di rischio da tenere sotto controllo. Inoltre, nella gestione della sicurezza cambia anche il ruolo dei lavoratori, i quali, in molti casi, diventano parte attiva nella salvaguardia della loro salute.

Dunque, se prevarrà un approccio olistico, che quindi andrà a considerare la totalità degli aspetti collegati alla nuova organizzazione di Industria 4.0, si potranno avere grandi effetti positivi sulla sicurezza e di conseguenza anche sull'attività aziendale in generale, se invece, in caso contrario, si seguirà un approccio puramente economico, si incontreranno molte conseguenze negative sulla sicurezza dei lavoratori.

Emerge inoltre, che l'utilizzo delle nuove tecnologie per la gestione della sicurezza rappresenta ancora la base di numerosi studi in ingegneria, ma solo alcuni di questi vengono poi effettivamente attuati all'interno delle aziende.

BIBLIOGRAFIA

Agnusdei G. P., Elia V., Gnoni M. G., (2021*), A classification proposal of digital twin applications in the safety domain*

Bing Wang, (2020) *Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework*.

Benedetti F., Bertorelli G., Bianconi R., Leuzzi F., Tronci M., (2016), *Il framework per la salute e sicurezza sul lavoro: i fattori abilitanti e i risultati, Rivista degli infortuni e delle malattie professionali*, VI serie, anno CIII, n. 3/2016, pp. 627-660.

Forcina A., Falcone D., (2021) *The role of Industry 4.0 enabling technologies for safety management: A systematic literature review*.

Kim K., & Kim M., (2012). *RFID-based location-sensing system for safety management. Personal and Ubiquitous Computing*, 16(3), 235-243.

Gallo T., Santolamazza A., (2021), *Industry 4.0 and human factor: How is technology changing the role of the maintenance operator?*

Gnoni M. G., Bragatto P. A., Milazzo M. F., Setola R., (2019) *Integrating IoT technologies for an "intelligent" safety management in the process industry.*

Kontogiannis T., Leva M. C., Balfe N., (2017) *Total Safety Management: Principles, processes and methods da Safety Science*, Volume 100, Parte B, p. 128-142

Lee J., Cameron I., Hassall M., (2019) *Improving process safety: What roles for Digitalization and Industry 4.0.*

Maci L., (2021) *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare*.

Mottana G., (2012) *Tecniche di valutazione del rischio*.

Muhammad Atif Javed, Faiz Ul Muram, Hans Hansson, Sasikumar Punnekkat, Henrik Thane, (2021), *Towards dynamic safety assurance for Industry 4.0.*

Silvestri L., Forcina, A., Introna, V., Santolamazza, A., Cesarotti, V., (2020) *Maintenance transformation through industry 4.0 technologies A sistematic literature review.*

Tronci M., Mercadante L., Ricciardi P., *Industria 4.0: rischi e opportunità per la tutela e la sicurezza dei lavoratori*

Tsang YP, Choy KL, Wu C-H, et al (2018) *An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks*

Zanetta L., *La trasformazione digitale delle PMI: il Piano Nazionale Impresa 4.0 e gli altri strumenti a supporto dell'innovazione digitale delle imprese.*

Zaritto A., (2015) *La gestione della sicurezza in azienda*.

Zhiheng Zhao, Leidi Shen, Chen Yang, Wei Wu, Mengdi Zhang, George Q. Huang, (2020), *IoT and digital twin enabled smart tracking for safety management*

Intervista a Ugo Gecchelin e Stefano Ferrari, (2020) *Industria 4.0 e i rischi per la sicurezza dei dati. 2^ parte - il quadro normativo*.

www.futureindustry.it, *Manutenzione predittiva industria 4.0*