UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea triennale in ingegneria gestionale

ANALISI DEGLI STRUMENTI PER LA GESTIONE DELLA SICUREZZA IN AMBIENTE INDUSTRY 4.0

ANALYSIS OF SAFETY MANAGEMENT INSTRUMENTS IN INDUSTRY 4.0 ENVIRONMENT

Relatore: Chiar.mo/a

Prof. **Maurizio Bevilacqua**

Tesi di Laurea di:

Andrea Salvatori

Anno Accademico **2019** / **2020**

a Martina

Indice

Introduzione 4

1. Dalla prima rivoluzione industriale all'industry 4.0 5

1.1 Industrializzazione ed evoluzione del ruolo della sicurezza 5

1.2 Il paradigma Industry 4.0 e le tecnologie fondamentali 7

1.2.1 Internet of things (Iot) 9

1.2.2 Cyber-security 9

1.2.3 Big data and Analytics 10

1.2.4 Simulazione e Realtà aumentata 12

1.2.5 Cloud computing 14

1.2.6 Manifattura additiva 15

1.2.7 Integrazione verticale ed orizzontale 17

1.2.8 Robot autonomi 18

2. Impatto di "Industry 4.0" sulla gestione delle risorse e lo stato dell'arte della standardizzazione 20

2.1 Implicazioni di "Industry 4.0" per l'innovazione, la sicurezza e la qualità del lavoro nelle piccole economie e imprese 20

2.1.1 Le risorse che condizionano la sicurezza e le interazioni interne ed esterne al "sistema P3" 22

2.1.2 I risvolti economici pre-industry 4.0 e la necessità di cambiamento 23

2.2 Analisi dei requisiti degli standard per garantire "Safety & Security" aziendale. 26

2.2.1 Monitoraggio della conformità agli standard di sicurezza 35

2.2.2 Determinazione di un pacchetto di MIPs in uno scenario applicativo relativo ad una comunicazione end-to-end sicura in CPPS 41

3. Analisi del rischio e implementazione di sistemi di gestione della sicurezza per applicazioni "Industry 4.0" 45

3.1 Safety intelligence come modello di gestione dei dati e delle informazioni sulla sicurezza 45

3.2 Aspetti introduttivi dell'analisi del rischio 49
3.2.1 Sviluppo di un framwork di Project Risk Management 51
3.3 Fase operativa del Safety Management System 59
3.3.1 Il software W-ARTEMYS applicato al caso Parmalat e GEA Procomac 65
3.3.2 Il digital twin OTS per la simulazione del sistema di sicurezza 72
Conclusioni 76
Bibliografia 77
Sitografia 79
Ringraziamenti 81

Introduzione

I grandi cambiamenti introdotti dalle nuove esigenze del mercato hanno creato il presupposto per lo sviluppo della cosiddetta quarta rivoluzione industriale, nota anche come Industry 4.0. Questa digitalizzazione dell'intero complesso aziendale ha portato anche ad una maggiore attenzione, da parte dei top management delle imprese, verso la sicurezza che, in questa nuova prospettiva, richiede un'analisi sia dal punto di vista dei pericoli per gli operatori, sia dal punto di vista della sicurezza delle infrastrutture informatiche che assumono un ruolo primario.
Nel capitolo 1 viene introdotta l'evoluzione dei sistemi produttivi fino ad arrivare al nuovo paradigma industry 4.0. Uno degli elementi cruciali di questo progresso è l'evoluzione dell'approccio relativo al concetto di sicurezza che diventa un elemento di successo finanziario per le imprese al pari delle classiche componenti. Successivamente vengono passate in rassegna le nove tecnologie abilitanti, indicandone gli aspetti peculiari e le applicazioni che costituiscono lo stato dell'arte delle imprese digitalizzate.

Il capitolo 2 intende evidenziare le principali criticità nell'adozione di un ambiente industry 4.0 nelle piccole e medie imprese e in particolare come queste intendono affrontare il problema della sicurezza da un punto di vista organizzativo e competitivo, attraverso l'analisi della situazione economico-gestionale pre-industry 4.0. Successivamente viene fornito un quadro delle normative standard in materia di sicurezza secondo il modello RAMI 4.0. e le metodologie che permettono di monitorare la conformità degli standard di sicurezza, che sta a rappresentare un primo tentativo di uniformare quelle attività che vogliono interfacciarsi a questa nuova era dell'industria.

Il terzo capitolo entra nel merito della gestione della sicurezza attraverso una prima implementazione di un modello di gestione dei dati basato su "safety intelligence" e di come queste informazioni sulla sicurezza possono essere utilizzate per effettuare un analisi dei rischi. La fase del ciclo di vita della gestione della sicurezza presenta come ultimo step la messa in opera delle tecniche di gestione della sicurezza, come l'utilizzo di strumenti di realtà aumentata e la verifica ad ampio spettro, attraverso un gemello digitale, che il sistema realizzato sia coerente e funzionale con le effettive problematiche di ciascuna realtà industriale.

1. Dalla prima rivoluzione industriale all'industry 4.0

1.1 Industrializzazione ed evoluzione del ruolo della sicurezza

L'industrializzazione ha subito notevoli trasformazioni sin dai suoi inizi nel XVIII secolo. Il passo successivo all'introduzione di macchinari a vapore, che permise di superare i limiti del lavoro manuale, riguardò l'introduzione dell'elettricità, che avvenne nel XIX secolo, grazie alla quale l'elevata distribuzione di energia erogata da una stazione centrale consentì l'utilizzo di macchinari meno ingombranti e più veloci. Nel XX secolo, l'importanza sempre maggiore del ruolo assunto dall'elettronica e lo sviluppo di linee d'assemblaggio motorizzate hanno consentito una maggiore automatizzazione della produzione con miglioramento delle prestazioni generali("industria 3.0").

Da pochi anni si è iniziato a parlare della cosiddetta quarta rivoluzione industriale nella quale è in atto una rivoluzione globale nella produzione e dove la completa digitalizzazione dell'intera catena del valore la fa da padrona. L'esame di queste trasformazioni permette di evidenziare la coevoluzione della filosofia di produzione e dell'approccio alla salute e sicurezza sul lavoro (SSL). L'industrializzazione ha creato un bisogno urgente e crescente di lavoro e ha portato all'aumento di condizioni di lavoro deplorevoli in cui uomini, donne e bambini hanno rischiato la vita e l'incolumità fisica per guadagnarsi da vivere. L'inesperienza della forza lavoro e l'ignoranza dei datori di lavoro riguardo la SSL hanno portato a pagare un prezzo elevato e, sotto la conseguente pressione pubblica, i legislatori sono stati costretti a intervenire. I sindacati, le leggi sul lavoro, i regolamenti e gli standard sono emersi gradualmente e, sebbene persistano ancora alcune statistiche allarmanti, oggi si può affermare con certezza che le condizioni sul posto di lavoro sono migliorate enormemente. Va sottolineato che l'evoluzione nel campo della salute e sicurezza sul lavoro ha sempre seguito sviluppi rivoluzionari nell'industria e in particolare, le conseguenze delle reazioni al progresso tecnologico e dei cambiamenti nei metodi di lavoro hanno influito fortemente sul tema della SSL fornendo l'impulso per l'implementazione di soluzioni affidabili e sostenibili ai problemi[1].

È possibile dunque vedere com'è cambiato l'approccio al tema della sicurezza in funzione dell'aumento della complessità dei sistemi (figura 1.1):
fino agli anni 60' si parla di Safety-I, dove l'approccio alla sicurezza era orientato alla comprensione delle condizioni negative e sostituirle con delle nuove. L'aumento della complessità dei sistemi ha portato successivamente a valutare gli aspetti positivi e capire come riutilizzarli al fine di migliorare la sicurezza (safety-II). Oggi si prendono in considerazione approcci molto sofisticati che hanno alla base il concetto di "resilience", con il quale si intende la capacità di creare un sistema in grado di estendere i propri confini per trovare la sua adattabilità e robustezza a seguito di una perturbazione. Tale principio si è poi evoluto in "antifragility" tramite cui, si mira al rafforzamento e all'apprendimento durante il processo dello stesso sistema preso in considerazione.[2]

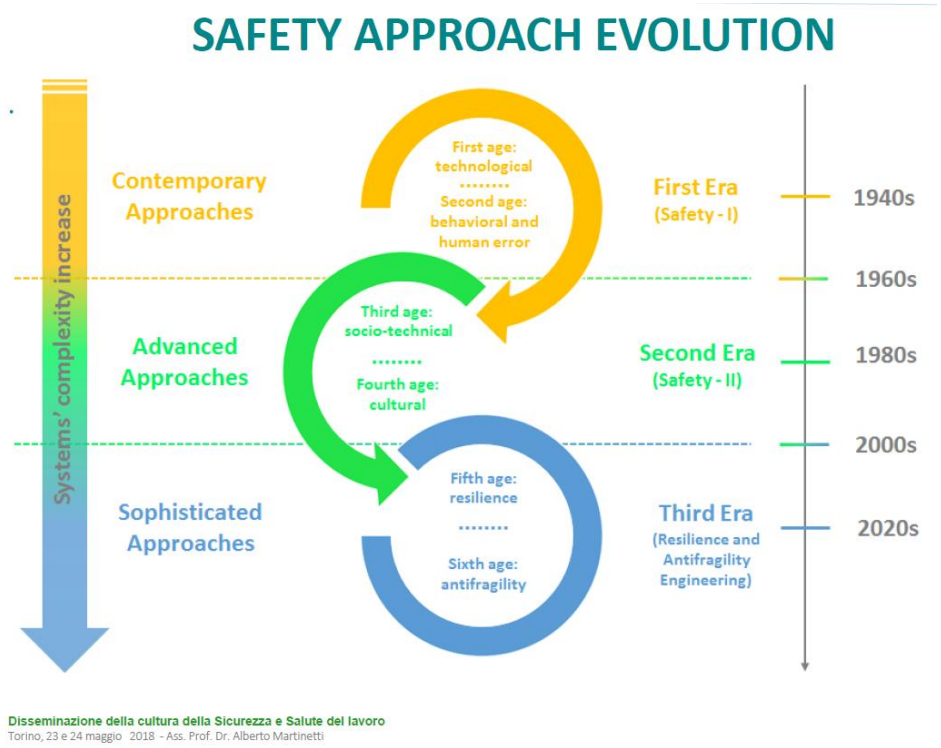

Figura 1.1 *Evoluzione dell'approccio alla sicurezza in funzione dell'incremento della complessità dei sistemi. <https://research.utwente.nl/files/30603033/Martinetti_24052018_rel2.pdf>*

Si può affermare quindi che, nella maggior parte dei paesi industrializzati, la reattività sta cedendo il posto alla proattività, poiché c'è maggiore consapevolezza da parte delle

imprese e in particolare dei decisori che la “salute e sicurezza sul lavoro” sta diventando una componente di successo finanziario tanto quanto lo sono il raggiungimento di standard qualitativi elevati e la riduzione dei costi di esercizio.[1]

1.2 Il paradigma Industry 4.0 e le tecnologie fondamentali

Il concetto di industria 4.0 nasce per la prima volta alla fiera di Hannover nel 2011 in Germania, e da lì ha continuato a diffondersi in altri stati con l’obiettivo di aumentare l’efficienza degli impianti di produzione attraverso la comunicazione “intelligente” tra le macchine, portandole a collaborare per espletare nel miglior modo possibile tutte le operazioni ad esse assegnate[5]; a tal proposito sono state intervistate più di 2000 aziende le quali prevedono di aumentare in maniera dirompente il loro grado complessivo di digitalizzazione.

Si prospetta che al termine di questo processo di trasformazione, che verosimilmente avrà una lunga durata considerato che ad oggi si è ancora in fase di sperimentazione nella stragrande maggioranza dei casi, le aziende industriali di successo diventeranno vere e proprie imprese digitali con i prodotti fisici in posizione centrale nel processo produttivo e “potenziati da interfacce digitali e servizi innovativi basati sui dati permettendo a queste imprese digitali di collaborare con clienti e fornitori in ecosistemi digitali industriali”[6]. Inoltre la caratteristica di questa nuova rivoluzione, ovvero quella di dotare i sistemi di produzione di tecnologie avanzate di acquisizione dati, è fortemente accompagnata dalla necessità di generare valore e innovazione nel campo dei servizi. In quanto pioniera di questa rivoluzione, la Germania “ha sviluppato un piano strategico in quattro fasi per trasformare le industrie dell’era dell’informazione in “industries 4.0”:

1. costruire dapprima una rete CPS(Cyber-Physical Systems) ovvero una rete di sistemi fisici interconnessi;
2. ricercare i concetti di “fabbrica intelligente” e “produzione intelligente”;
3. scendendo più in basso, integrare gli elementi delle catene del valore a livello orizzontale(creare delle catene di informazioni solide tra l’azienda e gli stakeholder come fornitori, dipendenti, distributori e in taluni casi di spicco

anche clienti), a livello verticale (riguarda la comunicazione e condivisione di informazioni, all'interno dell'azienda, ma in maniera trasversale rispetto alla sua struttura gerarchica della stessa) e a livello end to end (massima integrazione di tutti i processi);

4. infine perseguire il raggiungimento di otto obiettivi di pianificazione che includono la standardizzazione, una gestione efficiente, un'infrastruttura industriale affidabile, sicurezza e protezione, organizzazione e progettazione del lavoro, formazione della forza lavoro, creazione di un quadro normativo e miglioramento dell'efficienza delle risorse"[7].

La realizzazione di un sistema basato sul concetto di industria 4.0 può avvenire attraverso l'implementazione e la coesione delle cosiddette nove tecnologie abilitanti nei processi 4.0, minuziosamente definite da uno studio condotto dalla società Boston Consulting e brevemente schematizzate in figura 1.2, le quali hanno sempre trovato poca applicazione a livello pratico ma che, ad oggi e per i prossimi anni, stanno rappresentando una solida base, specialmente per le aziende in grado di effettuare grandi investimenti, per la creazione di nuovi modelli di business. Ad esempio, Google, Amazon e Netflix utilizzano la tecnologia "big data and analytics" per monitorare la scelta del cliente durante il processo decisionale. In particolare, questo strumento aiuta le aziende ad analizzare i dati reali per migliore la produttività e ridurre l'aleatorietà di un processo decisionale, rendendo di conseguenza la catena di fornitura più efficientemente sostenibile, soprattutto per quello che concerne aziende automobilistiche, manifatturiere, farmaceutiche e chimiche.

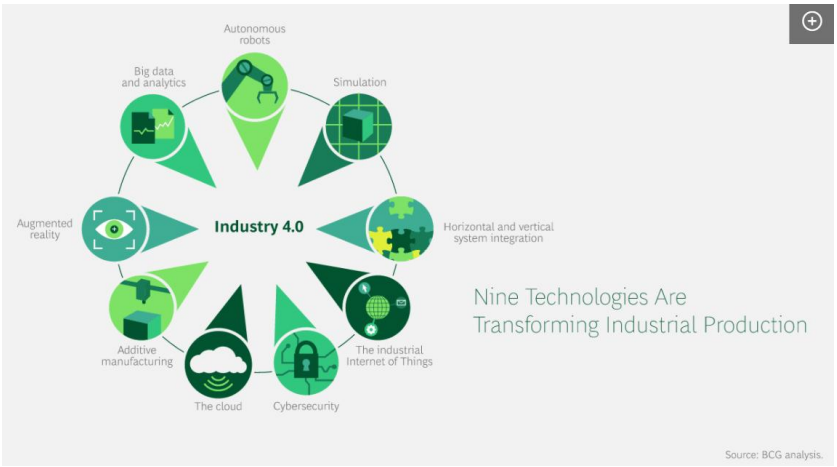

Figura 1.2 *Le 9 tecnologie che stanno trasformando la produzione industriale. <https://www.bcg.com/it-it/capabilities/operations/embracing-industry-4.0-rediscovering-growth>*

1.2.1 Internet of things (Iot)

L'espressione "Internet Of Things" è stata coniata più di 20 anni fa; non a caso le tecnologie IoT sono sempre più numerose ed evolute allo stesso tempo, così come lo sviluppo di nuovi ambiti applicativi. "Si parla di -Internet delle cose- per riferirsi a quel percorso di sviluppo tecnologico in base al quale, attraverso la rete internet, potenzialmente ogni oggetto dell'esperienza quotidiana (non necessariamente computer, tablet, smartphone) acquista una sua identità nel mondo digitale. Come detto, l'IoT, si basa sull'idea di oggetti "intelligenti" e tra loro interconnessi in modo da scambiare le informazioni possedute, raccolte e/o elaborate".[1] Di conseguenza l'IoT dipende da una serie di tecnologie, come ad esempio l'identificazione a radiofrequenza (RFID), le quali garantiscono l'individuazione e l'acquisizione automatica dei dati o altresì sensori di rete wireless per monitorare le condizioni fisiche e ambientali e fornire informazioni sugli oggetti, come la loro posizione e i loro movimenti. È chiaro che, oltre all'utilizzo dovuto alla pianificazione e al controllo intelligente delle macchine, l'IoT sta assumendo una notevole importanza relativamente alla sicurezza intesa sia come sicurezza informatica che come rischio di incidenti sul luogo di lavoro. Rispettivamente quindi, se da un parte diventa fondamentale dotarsi di architetture software adeguate a gestire enormi quantità di dati e fare in modo che questi vengano conservati da agenti negativi esterni o interni, dall'altro lato risulta importante evidentemente considerarequelle "situazioni critiche" del sistema che possono provocare incidenti qualora non sia l'operatore in prima persona a prendere delle decisioni ma sono le reti stesse.

1.2.2 Cyber-security

Si tratta di una delle sfide più importanti per l'implementazione di industry 4.0. La quarta rivoluzione industriale rende necessario l'utilizzo di protocolli di comunicazione standard per la connessione e per assolvere agli scopi operativi[8]. L'attività della "Cyber-security" è quella di proteggere i sistemi informatici e dell'informazione a livello digitale da attacchi interni, e soprattutto esterni. Per poter competere a livello

[1] *<https://blog.osservatori.net/it_it/cos-e-internet-of-things>*

mondiale, le grandi aziende devono necessariamente dotarsi di infrastrutture informatiche che, attraverso l'utilizzo di internet, gli permettano di interfacciarsi con tutti i vari stakeholder. La problematica risiede nel fatto che l'utilizzo di queste infrastrutture riguarda molteplici aspetti aziendali, come la gestione dei flussi logistici, della catena di approvvigionamento, della linea di produzione o della distribuzione ecc. Questo comporta inevitabilmente che la vulnerabilità del sistema informatico possa esporre nel tempo tutto il complesso aziendale a gravi rischi, quali furti o sabotaggi.

1.2.3 Big data and Analytics

Una tra le numerose proposte di caratterizzazione dei Big Data è stata data dal McKinsey Global institute, il quale afferma che "un sistema di Big Data si riferisce a *dataset*[2]*,* la cui taglia/volume è talmente grande che eccede la capacità dei sistemi di database relazionali di catturare, immagazzinare gestire ed analizzare"[3].

La novità non sta tanto nel concetto relativo all'accesso e alla memorizzazione di grandi quantità di informazioni, quanto nell'interpretazione della definizione data dall'analista di mercato Doug Laney, che agli inizi degli anni 2000 ha articolato la definizione di Big Data come "le tre V":

1. Volume: "le organizzazioni raccolgono dati da diverse fonti, tra cui transazioni commerciali, dispositivi intelligenti (IoT), apparecchiature industriali, video, social media e altro ancora. In passato, i costi relativi all'archiviazione sarebbero stati un problema ma oggi sono decisamente più accessibili, grazie a piattaforme come i data Lakes e Hadoop.".
2. Velocità: "con la crescita dell'internet delle cose, i flussi di dati verso le imprese devono essere gestiti in modo tempestivo ed ad una velocità senza precedenti.".

[2] *Un dataset costituisce un insieme di dati strutturati in forma relazionale, cioè corrisponde al contenuto di una singola tabella di base di dati, oppure ad una singola matrice di dati statistici, in cui ogni colonna della tabella rappresenta una particolare variabile, e ogni riga corrisponde ad un determinato membro del dataset in questione. <https://it.wikipedia.org/wiki/Dataset>*

[3] *<https://it.wikipedia.org/wiki/Big_data>*

3. Varietà: “I dati sono disponibili in tutti i tipi di formati, dai dati strutturati e numerici nei database tradizionali, ai documenti di testo non strutturati, e-mail, video, audio, dati di stock e transazioni finanziarie”.

L’aspetto relativo alla sicurezza e ai rischi connessi ai Big Data entra in gioco grazie a SAS (analytics software and solution), che amplia “le tre v” aggiungendo due aspetti: uno relativo alla variabilità dei big data, intesa come la capacità delle aziende di gestire repentini cambiamenti, ad esempio essere in grado di individuare rapidamente cambi di tendenze nel mercato per essere pronti a integrare o aggiornare il proprio portafoglio marchi in corrispondenza delle esigenze di mercato e l’altro relativo alla veridicità, ovvero alla qualità dei dati, i quali provengono da fonti più disparate; questo motivo risulta complesso cercare di collegarli e soprattutto correlarli, rischiando di perderne il controllo. Una volta che si sono poste le basi sugli aspetti prettamente relativi ai “Big Data”, diventa cruciale il modo in cui essi vengono utilizzati e da qui il termine “Analytics”.

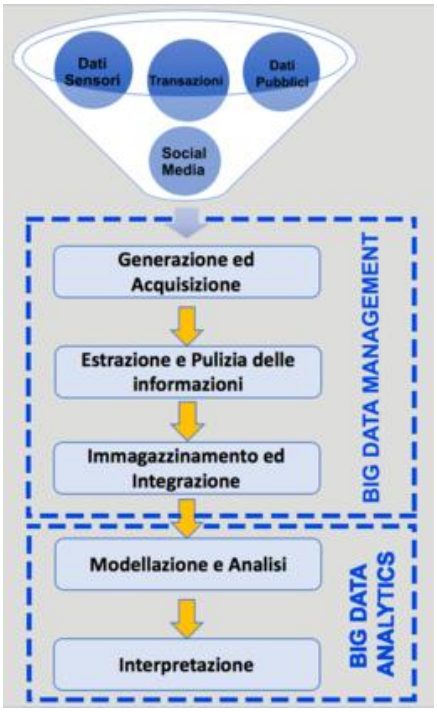

Figura 1.3 *Ciclo di vita dei Big Data.<https://it.wikipedia.org/wiki/Big_data>*

Combinando Big Data e Analytics è possibile ottenere risultati di business quali la determinazione delle cause di guasti in tempo reale che permette all'operatore di agire in maniera proattiva piuttosto che reattiva, una volta che il guasto è avvenuto, o ancora di rilevare un comportamento fraudolento prima che questo impatti negativamente sull'azienda[4]. In generale è possibile riassumere con lo schema in figura 1.3, il ciclo di vita dei Big Data, sottolineando come ogni fase sia fondamentale per ottenerne un utilizzo efficiente.

1.2.4 Simulazione e Realtà aumentata

L'aumento delle conoscenze e delle capacità di calcolo (Cloud e Edge computing) permette agli ingegneri di lavorare con grandi quantitativi di dati nella risoluzione di problemi, la cui complessità sta aumentando negli anni. È lecito quindi aspettarsi che le grandi aziende saranno scoraggiate nell'investire su eventuali esperimenti nei propri stabilimenti, in primis a causa dell'incremento dei costi e dell'incertezza in merito al ritorno economico di un progetto e in secondo luogo a causa dell'impraticabilità stessa dell'esperimento. Per questi motivi, è aumentato l'interesse nei confronti delle simulazioni in ambienti controllati. La simulazione, al giorno d'oggi, richiede l'ausilio di strumenti sempre più evoluti "sia per verificare il comportamento dei singoli dispositivi, sia per analizzare il comportamento dei sistemi nel loro complesso".
Esistono diverse tecnologie di simulazione:

1. DSS (Decision Support System) che consentono di simulare il comportamento di un sistema senza entrare nei dettagli fisici del sistema stesso e quindi utilizzare un approccio a scatola nera (es. Deep Learning).
2. Tecnologie di simulazione a supporto della progettazione e ingegnerizzazione dei prodotti: si tratta di tutti gli strumenti impiegati per predire il comportamento di un prodotto o di una porzione dello stesso.
3. Tecnologie di simulazione a supporto dell'analisi dei processi dell'industria manifatturiera e di processo: in questo caso stiamo parlando di modelli CAM ad esempio, i quali dal disegno arrivano alla produzione attraverso strumenti che impartiscono istruzioni alle macchine o alla loro pianificazione.

[4] *<https://www.sas.com/it_it/insights/big-data/what-is-big-data.html>*

A titolo di esempio si porta l'eccellenza di Dallara, azienda nota per le realizzazione di auto sportive ad alte performance nonché fornitrice ufficiale del telaio per il campionato del mondo di indycar, la quale fonda il suo lavoro su un simulatore di guida sviluppato ad hoc, che prende in esame oltre sessantamila parametri e li elabora in tempo reale, dando ai progettisti informazioni utili per migliorare le performance della vettura.[5]
Grazie ai modelli simulativi implementabili si è in grado, a questo punto, di creare una Realtà Virtuale (VR) che è esattamente una simulazione della vita reale generata dal calcolatore e che permette di sperimentare una versione simulata della realtà.
Molto spesso si tende a confondere le due espressioni "Realtà Virtuale e Realtà Aumentata (AR)" ma la differenza tra loro è notevole: a differenza della realtà virtuale, la quale è "un mondo completamente virtuale, la cui fruizione è strettamente legata all'utilizzo di appositi visori, che "isolano" l'utente dal mondo esterno", la realtà aumentata rappresenta il mondo reale arricchito con oggetti o dettagli virtuali e quindi non utilizza un ambiente totalmente artificiale bensì un ambiente esistente, sovrapponendovi nuove informazioni. Sicuramente una delle applicazioni più importanti che riguarda la realtà aumentata è rappresentata dal mondo industriale. Sotto questo punto di vista, tale strumento gioca un ruolo fondamentale per l'innovazione del settore secondario, contribuendo a migliorare la formazione del personale e a fornire un controllo qualità più efficace oltre che a una migliorata modalità di progettazione, volta maggiormente all'innovazione.

Tra le tecnologie che compongono la realtà aumentata troviamo ad esempio la cosiddetta AR senza indicatore, che consiste nell'utilizzo del GPS, della bussola digitale e dell'accelerometro per fornire dati basati sulla posizione dell'operatore ; è utile inoltre, come si può intuire, in tutte quelle applicazioni incentrate sulla localizzazione in generale. Un'altra tecnologia AR è quella basata sulla proiezione che incide un fascio di luce artificiale su una superficie reale e rileva l'interazione dell'operatore distinguendo tra una proiezione attesa (oppure nota) e la proiezione alterata (causata dall'interazione umana).

[5] *<https://ricomincioda4.fondirigenti.it/le-potenzialita-della-simulazione-avanzata-nellindustria-4-0/>*

Il futuro della realtà aumentata non riguarderà soltanto i processi industriali ma anche le nostre vite, ad esempio per quello che riguarda l'utilizzo degli smartphone, senza avere caratteri invadenti e migliorando l'esperienza dell'utente oltre qualsiasi misura. [6]

1.2.5 Cloud computing

"il cloud computing indica un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione di dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita"[7].

Questa cosiddetta "nuvola informatica" è definita come tale perché le informazioni alle quali si accede si trovano in uno spazio virtuale, detto appunto cloud. Ciò permette di risparmiare notevole spazio sul disco rigido o su un dispositivo di archiviazione locale salvando i dati in un database remoto. Vi è un rilevante risparmio sui costi delle infrastrutture poiché i servizi cloud consentono di pagare solo ciò che viene utilizzato dall'azienda. Non a caso, prima che questa diventasse una tecnologia praticabile, le aziende dovevano acquistare, costruire e mantenere costose infrastrutture per la gestione delle informazioni. Da notare che il cloud computing non è esattamente un semplice accesso ai file su più dispositivi come generalmente siamo abituati a vederlo, bensì si tratta un sistema articolato in 3 tipologie di servizi:

1. Software as a service: comporta la licenza di una applicazione software per i clienti.
2. Infrastructure as a service: prevede un metodo per somministrare tutto, dai sistemi operativi ai server e all'archiviazione, fino alla connettività basata su IP come parte di un servizio su richiesta. Le aziende possono, quindi, evitare di acquistare software o server e procurarsi queste risorse con un servizio in outsourcing su richiesta.

[6] *<https://www.industry4business.it/connected-enterprise/connected-factory/realta-aumentata-che-cose-e-come-funziona/>*
[7] *<https://it.wikipedia.org/wiki/Cloud_computing>*

3. Platform as a service: in questo caso la differenza principale con il software as a service è che invece di fornire software online, è in realtà una piattaforma per la creazione di software che viene consegnato via internet.[8]

1.2.6 Manifattura additiva

Additive manufacturing "è un sistema per generare oggetti tridimensionali basato sulla creazione di un modello trasversale dell'oggetto da costituire, sulla superficie di un medium fluido capace di alterare il suo stato fisico in risposta a stimoli sinergici quali radiazione incidente, bombardamento di particelle o reazioni chimiche, in lamine adiacenti che rappresentano le sezioni trasversali adiacenti successive dell'oggetto che si integrano tra loro, provvedendo ad una progressiva crescita per apposizione dell'oggetto desiderato, per cui un oggetto è creato da una superficie sostanzialmente planare del medium fluido durante il processo di formazione."[9]

La stampa 3D è il principale fattore di stravolgimento dei tradizionali paradigmi produttivi, tanto che si parla di una vera e propria rivoluzione visto che la produzione, che prima avveniva nella maggior parte dei casi per asportazione di materiale dal grezzo di partenza, inizia dalla realizzazione di un modello 3D, attraverso la progettazione CAD, a cui segue un processo semi-automatico, svolto da un software di progettazione, di conversione del file in formato STL (Standard Triangulation Language), che prevede la scomposizione dell'oggetto in vari layer (strati) stampabili dalle stampanti 3D. A valle del processo di stampa, in alcuni casi, è necessaria un'attività post-produzione e finitura, per ottenere le specifiche di finitura superficiale e le proprietà meccaniche richieste dal progettista nel disegno tecnico.

Naturalmente il termine "produzione additiva" fa riferimento sia alla specifica tecnologia di fabbricazione, in questo caso la stampa 3D, sia a tutte le implicazioni aziendali legato a questo tipo di manifattura che ricadono su aspetti economici, finanziari, logistici e strategici. Basti pensare semplicemente ai costi di manodopera

[8] *<https://www.focusindustria40.com/cloud-computing/>*

[9] *<https://it.wikipedia.org/wiki/Produzione_additiva>*

dovuti all'assemblaggio di parti: è evidente che stampare un prodotto "già assemblato" comporta notevoli riduzioni dei suddetti costi. Essendo inoltre la domanda dei clienti molto variabile di giorno in giorno, con questa tecnologia si riesce a cambiare più spesso e più rapidamente il design dei prodotti, riducendo significativamente i costi di trasporto attraverso infrastrutture informatiche con le quali si invia il prodotto al cliente in modalità telematica, il quale procederà alla stampa 3D autonomamente. [10]

Entrando nel dettaglio, la rivista "Internet 4 Things" suggerisce quattro metodi di applicazione della manifattura additiva:

1. Stampa a getto di inchiostro: la tecnica prevede che sul letto della stampante venga posto un getto di resina o di grasso su cui viene gettato inchiostro e legante che solidificando strato per strato realizza il prodotto.
2. Digital light processing (DLT): Questa tecnica prevede l'uso di una vasca di polimeri liquidi che vengono posti all'azione della luce di un proiettore che li indurisce. La piastra esegue quindi un movimento verso il basso con il polimero di nuovo liquido e ripete successivamente la stessa operazione fino a quando non si arriva al prodotto finito.
3. Laminated object manufacturing (LOM): si utilizzano carta, plastica o laminati sotto forma di strati che sono incollati e tagliati, con una lama o con l'ausilio di un laser, fino al raggiungimento della forma desiderata.
4. Electron beam melting (EBM): La fusione del materiale avviene per effetto dell'azione di una fonte di energia ad alta concentrazione rappresentata da elettroni

Lo scenario futuro prevede un ulteriore abbassamento del costo delle stampanti 3D e un conseguente approccio a questa tecnologia da parte di un maggior numero di settori diversi tra loro, come ad esempio il settore medico, nell'ambito della realizzazione di protesi per trattare patologie particolari.

[10] *<https://www.internet4things.it/iot-library/che-cose-il-3d-printing-e-come-si-colloca-nellambito-industry-4-0-e-iot/>*

1.2.7 Integrazione verticale ed orizzontale

L'integrazione verticale ed orizzontale nella fabbrica digitalizzata è conseguenza dell'implementazione delle tecnologie precedentemente illustrate quali l'IoT, il cloud computing e i Big Data, ed è diventata una leva strategica su cui si fonda il concetto di smart factory.[11]

Più nel dettaglio, si parla di integrazione verticale quando la comunicazione e la condivisione delle informazioni avviene all'interno dell'azienda e in maniera trasversale rispetto alla struttura gerarchica della stessa, in modo da coinvolgere un maggior numero di soggetti possibili e di tagliare i cosiddetti "tempi morti" che molto spesso intercorrono tra l'acquisizione dei dati e il momento decisionale. L'integrazione orizzontale attiene ai soggetti esterni dell'azienda, quindi fornitori, distributori e talvolta anche clienti, i quali sono legati da una rete di condivisione delle informazioni che vanno dall'approvvigionamento delle materie prime, all'invio di informazioni attraverso il cloud per gestire al meglio la manutenzione delle macchine (evitando quanto più possibile azioni reattive), fino ad avere, in casi sporadici, informazioni che possono raggiungere il cliente, il quale per personalizzare e ordinare il prodotto, si interfaccia direttamente con le macchine presenti nello stabilimento aziendale.[12] Occorre evidenziare in base a questo secondo punto di vista, l'importanza del software di Product Life Management (PLM), il quale, durante la gestione del ciclo di vita del prodotto, permette di integrare dati, processi, sistemi aziendali, "creando una conoscenza diffusa delle informazioni tecniche del prodotto e garantendo uniformità nei processi di sviluppo del medesimo."[13] Il software integra moduli collaborativi nello sviluppo del prodotto quali CAD/CAM/CAE, che permettono di gestire la documentazione tecnica e di progetto, il tutto in termini di economicità e di "learning", avanzando progressivamente nella direzione di lavoro efficiente. È un sistema integrato con altri applicativi aziendali come ERP, che risulta complementare al PLM, in quanto non risulta focalizzato prevalentemente sul prodotto ma integra tutti i processi di

[11] *<https://www.ip4fvg.it/focus-tecnologie-abilitanti-integrazione-orizzontale-e-verticale/>*

[12] *<https://mynext.it/2018/09/integrazione-verticale-e-orizzontale-dei-sistemi-cosa-significa/>*

[13] *<https://quattropuntozero.confartigianato.it/wp-content/uploads/2017/11/Guida-pratica-Confartigianato-Industria-4.0-versione-estesa-web.pdf>*

business rilevanti di un'azienda e tutte le funzioni aziendali in un unico sistema in grado di supportare il management.

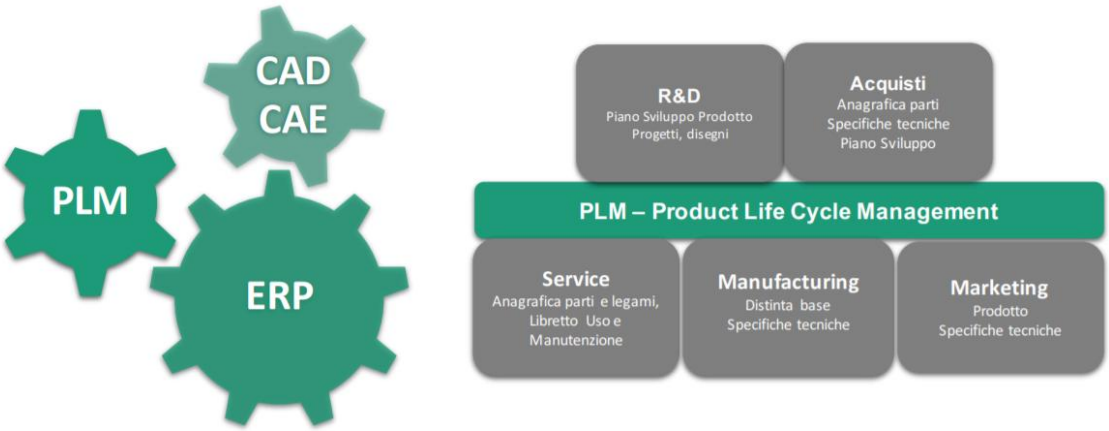

Figura 1.4 *Integrazione orizzontale attraverso il software PLM. <https://quattropuntozero.confartigianato.it/wp-content/uploads/2017/11/Guida-pratica-Confartigianato-Industria-4.0-versione-estesa-web.pdf>*

1.2.8 Robot autonomi

Murphy Robin, nel libro *Introduction to Al robotics,* definisce i robot intelligenti come "creature meccaniche che possono funzionare autonomamente". In particolare, definite creature perché "capaci di attuare il processo di decision making in modo autonomo con percezione, azione e ragionamento" e meccaniche perché sono assemblate dall'uomo. Oggi siamo di fronte a questa enorme trasformazione grazie anche al contributo di sensori sempre più potenti e intelligenti e di software capaci di gestire i movimenti dei robot con elevato coefficiente di sicurezza. Un robot è intelligente "quando ha mobilità, percezione sensoriale, un sistema nervoso centrale digitale, la fornitura di energia e comunicazione tramite voce e gesti". Di recente sono stati sviluppati i *cobot,* ovvero una tipologia di robot collaborativi piccoli e agili, che proprio per queste caratteristiche permettono di aumentare le aree di stoccaggio all'interno dei magazzini, che sono in grado di svolgere compiti pericolosi, noiosi e pesanti senza fatica e con elevatissima accuratezza. L'elemento chiave che differenzia queste tipologie di robot da quelli impiegati nella terza rivoluzione industriale, consiste nella forte collaborazione con l'operatore umano e nella capacità di apprendere i movimenti che deve effettuare da quest'ultimo, permettendo quindi di ridurre costi e interventi di tecnici e programmatori. In particolare, l'interazione uomo-cobot avviene attraverso un monitoraggio in tempo

reale di entrambi attraverso una rete di sensori installati nelle aree di lavoro condiviso o attraverso dispositivi che permettono l'utilizzo della realtà aumentata. Se da un lato è vero che già nel 2025 si prospetta un maggior impiego dei cobot nelle linee produttive grazie al miglioramento dell'intelligenza artificiale e alla possibilità di effettuare operazioni che l'essere umano svolgerebbe impiegando una quantità di tempo molto maggiore, dall'altra lo sviluppo dei cobot procede ancora verso la direzione dell'interazione in quanto allo stato attuale non si è in grado di garantire al 100% che le capacità di interfaccia dei cobot nei confronti dell'ambiente circostante e di osservare e decidere autonomamente, siano equiparabili a quelle dell'essere umano.[14]

Sicuramente "la robotica è lo strumento che offre maggiore tutela alle aziende rendendole più reattive ai mutamenti, a breve e a lungo termine. Un alto livello di resilienza permette di attenuare l'impatto di tutte le problematiche tipiche dei momenti di recessione o emergenza, aiutando a fornire la direzione corretta per potersi adattare in modo fluido e proseguire il proprio cammino con continuità.".[15]

[14] *<https://www.focusindustria40.com/robotica-collaborativa/>*

[15] *<https://www.industriequattropuntozero.it/2020/06/19/i-robot-mobili-autonomi-nellindustria-dei-beni-di-largo-consumo/>*

2. Impatto di “Industry 4.0” sulla gestione delle risorse e lo stato dell’arte della standardizzazione

2.1 Implicazioni di “Industry 4.0” per l’innovazione, la sicurezza e la qualità del lavoro nelle piccole economie e imprese

Nel XX secolo e, in particolar modo nell’era moderna, l’accesso al capitale per le imprese è un fattore rilevante. I piccoli paesi e le aziende manifatturiere spesso hanno dei vincoli sugli investimenti locali ed esteri, e ciò impedisce a molte piccole e medie imprese di replicare all’interno dei propri stabilimenti dei sistemi altamente automatizzati. D’altro canto queste imprese che presentano le difficoltà appena illustrate hanno da sempre cercato di “produrre innovazione” combinando fattori quali la conoscenza ad ampio spettro da parte dei dipendenti delle attività di produzione che implicano intrinsecamente la progettazione, sia a livello di dettaglio che concettuale o il funzionamento delle attrezzature e dei macchinari stessi. Ma nella prospettiva che stiamo trattando diventa sempre maggiore l’importanza, soprattutto per le piccole e medie imprese che competono attraverso l’innovazione, nel valutare “la possibilità per le persone (intese come dipendenti) di utilizzare le proprie capacità ed esplorare il proprio potenziale creativo nell’ambito di industry 4.0”[3].

È noto, come accennato precedentemente, come uno degli elementi fondamentali nella definizione dei principi dell’industria 4.0 debba essere il dipendente: tutti i soggetti direttamente e indirettamente interessati dal processo di trasformazione devono essere adeguatamente coinvolti nei processi decisionali e i rischi percepiti devono essere presi seriamente. Tuttavia, “gli attuali approcci di trasformazione si concentrano principalmente sugli aspetti tecnologici e organizzativi”[4]. Volendo combinare i due aspetti, si prospetta una situazione più complessa da analizzare per le fabbriche digitali e intelligenti in quanto, se da un lato possiamo avere una forza lavoro altamente qualificata il cui potenziale umano può essere utilizzato più pienamente, dall’altro troviamo i lavoratori che “semplicemente badano alle macchine”, percependo bassi salari in quanto non possiedono grandi competenze e godono di scarsa autonomia. Il

rischio quindi, da questo punto di vista è che le abilità di questi operatori nel tempo si "atrofizzino" compromettendo la possibilità di sviluppare il concetto di "fabbrica dell'apprendimento". È evidente anche dai dati mostrati in figura 2.1, che muoversi verso stabilimenti sempre più automatizzati comporta graduali riduzioni degli incidenti sul luogo di lavoro; se però la progettazione dei sistemi di controllo viene effettuata incorporando poco o per nulla l'input dell'operatore come parte integrante del processo, i risultati che si ottengono, comportano miglioramenti modesti rispetto a quello che i decisori si attenderebbero.

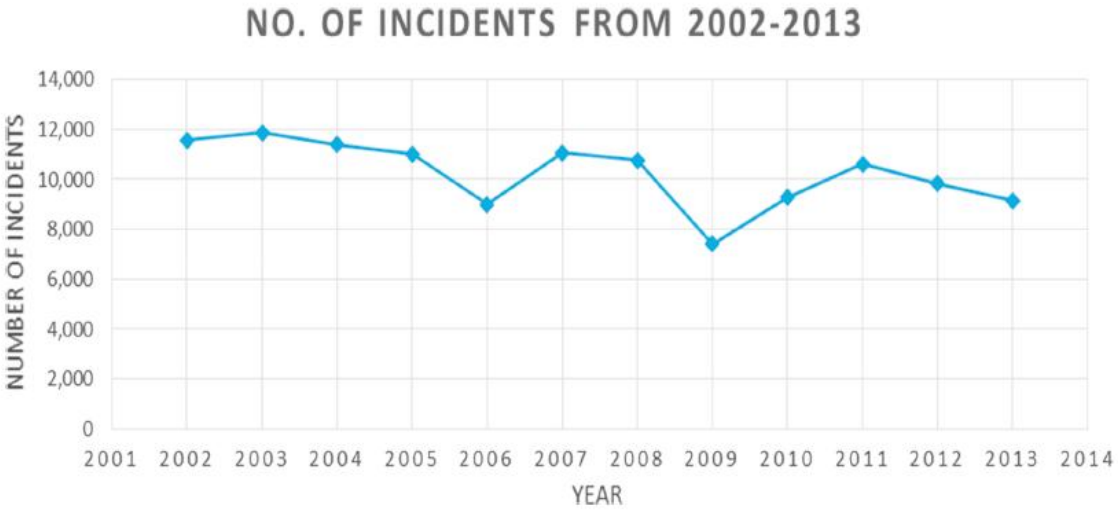

Figura 2.1 *Stima del numero totale di incidenti di rilascio chimico significativo nell'aria, per gli Stati Uniti. <https://www.atsdr.cdc.gov/>*

Si evince quindi che il principale problema nel passaggio da una cosiddetta "industria 3.0" alla industria 4.0, riguarda il trade off tra i cambiamenti tecnologici in atto e le forme di auto-organizzazione responsabile da parte dei dipendenti in ambito professionale, i quali, secondo recenti interviste effettuate in una azienda metalmeccanica che sta attraversando processi di trasformazione digitale, ritengono che in queste mutevoli condizioni, i miglioramenti della sicurezza non dovrebbero essere avviati esclusivamente dalla direzione, bensì sono i dipendenti stessi che devono partecipare attivamente al processo, quasi come "imprenditori" che sviluppano soluzioni per problemi di sicurezza e protezione emergenti, mentre la direzione dovrebbe fungere da promotore e dirigere le iniziative proposte dagli operatori[4].

Il problema è piuttosto impegnativo poiché con l'introduzione di industria 4.0 i contrattempi che possono potenzialmente ledere alla sicurezza di tutti gli attori presenti all'interno degli stabilimenti, stanno interessando un numero maggiore di campi e presentano profili di valutazione sempre più ampi. Si ribadisce quindi che per affrontare il problema, sarà necessario adottare misure per garantire un ruolo più "attivo intellettualmente per gli operatori" che garantisce all'operatore maggiore discrezionalità nelle scelte e supporta una rinnovata attenzione in merito alla sicurezza[3].

2.1.1 Le risorse che condizionano la sicurezza e le interazioni interne ed esterne al "sistema P3"

Un'analisi degli eventi di sicurezza del processo suggerisce che emergono da una combinazione di fattori interconnessi, come evidenziato nell'incidente di Deepwater Horizon (BP., 2010). Pertanto, le considerazioni sulla sicurezza dei processi richiedono collaborazioni interdisciplinari di alta qualità sostenute da una prospettiva di sistema che consideri il ruolo di impianto, persone e procedure con le loro importanti interazioni (Seligmann et al., 2012, 2019). Questa prospettiva attraversa l'intero ciclo di vita del prodotto e del processo e la figura 2.2 mostra questa prospettiva di alto livello e le interazioni tra gli "attori" del sistema e l'ambiente in cui risiede il sistema, vale a dire uno "schema P3"[16]. Questa rappresentazione è un sistema dinamico con molte parti in movimento che si evolve nel tempo come un sistema quadridimensionale. Le dinamiche complesse del sistema derivano da influenze esterne di input e disturbi (1), che a loro volta hanno numerose uscite sull'ambiente in cui si trova (2). Esiste anche una gamma più ampia di guasti interni all'interno dei componenti del sistema P3, che a volte portano ad ulteriori "auto-interazioni" all'interno delle 3 principali categorie di componenti del sistema (3, 6, 11). Ad aggiungere complessità sono le interazioni e le interfacce tra pianta e persone (4, 5), tra persone e procedure (7, 8) così come procedure e impianto (9, 10). Queste considerazioni sono aspetti importanti nella progettazione dell'integrità del sistema e nel mantenimento di tale integrità nel tempo all'interno di un ambiente dinamico. Questo è il cuore della sicurezza dei processi e la natura 4-D del sistema

[16] *Schema P3 è uno schema impianto, procedure e persone*

presenta molte sfide a tutti i soggetti coinvolti. Dietro il pensiero dei sistemi di processo e la prospettiva dei processi integrati ottimali ci sono le varie forme di principi primari e di modellazione empirica basata sui dati. Modellazione estesa dei processi durante il ciclo di vita del prodotto e del processo ha supportato i progressi passati e attuali. I modelli consentono agli utenti di indagare sui comportamenti del sistema e, si spera, di prendere decisioni migliori. La modellazione è ancora più centrale nell'attuale ondata di digitalizzazione e un elemento importante nell'implementazione dell'Industria 4.0. L'utilizzo di modelli "adatti allo scopo" può informare e migliorare le decisioni umane (figura 2.1) . I sistemi di alto livello visualizzano l'acquisizione di attori chiave, capacità di creazione se tali modelli sono correttamente sviluppati, utilizzati e i risultati interpretati correttamente.[9]

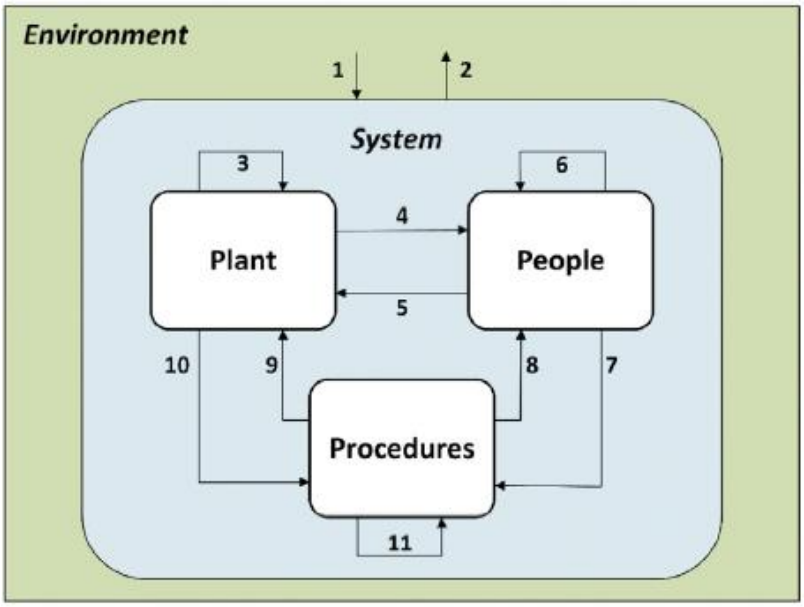

Figura 2.1 *Sistema di alto livello che illustra le relazioni reciproche degli attori chiavi e le relazioni con l'esterno dell'intero sistema. <https://doi.org/10.1016/j.psep.2019.10.021.>*

2.1.2 I risvolti economici pre-industry 4.0 e la necessità di cambiamento

Gli incidenti relativi alla sicurezza dei processi possono comportare più vittime, danni ambientali, perdite economiche e danni all'immagine aziendale. In particolare, sono

state esaminate le principali perdite economiche dovute a problemi di sicurezza e di conseguenti danni alle proprietà con necessità di interruzione momentanea dell'attività di business (in figura 2.2 vengono prese come riferimento industrie petrolifere, del gas e petrolchimiche onshore dal 1996 al 2014), evidenziando come, la precedente rivoluzione industriale (industria 3.0) non abbia contribuito a una particolare attenzione ai problemi di sicurezza, causando l'aumento delle perdite nell'arco di 20 anni.

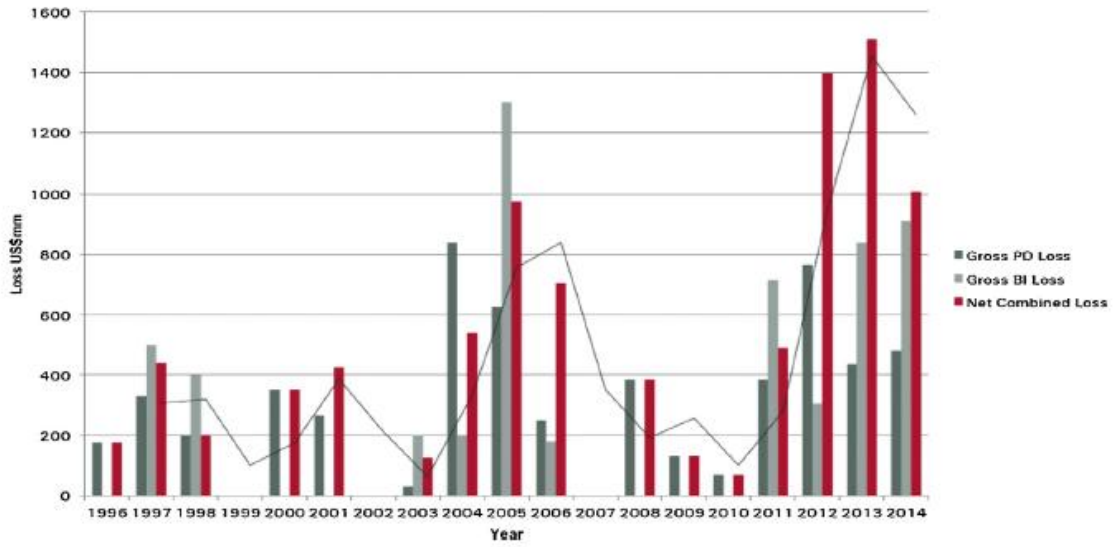

Figura 2.2 *Perdite maggiori nell'industria petrolifera, del gas e petrolchimica onshore dal 1996 al 2014. <https://doi.org/10.1016/j.psep.2019.10.021.>*

La caratteristica d'interesse è la classificazione delle cause che hanno scaturito le suddette perdite economiche:

- Guasti meccanici (40-50%)
- Guasti nelle procedure pratiche e operative (20-30%)
- Controllo inadeguato del processo di lavoro (15%)
- Identificazione dei pericoli inadeguata (10%)

In particolare, un'identificazione inadeguata dei pericoli rappresenta anche un fattore secondario in circa il 40% delle perdite maggiori. Questi quattro scenari comuni a molteplici aziende riguardano aspetti relativi al modello P3 in figura 2.1, e si riferiscono a una serie di fasi del ciclo di vita, dall'idea, alla progettazione sino alle operazioni.

La gestione della sicurezza dei processi è stata una priorità crescente per le industrie di processo, compresi i miglioramenti negli indicatori principali, come l'integrità delle barriere di sicurezza e l'audit dell'efficacia della gestione del rischio. [9]
In particolare si è cercato di rispondere alle criticità attraverso l'utilizzo di tecnologie ampiamente collaudate e l'implementazione di strumenti tipici dell'indutstria 4.0 come mostrato in tabella 2.3:

Criticità	*Soluzioni implementate*
Guasti meccanici	- Sensori di linea di corrosione e spessore delle pareti - Collegamenti a sistemi di ispezione con dati di impianto in tempo reale - Maggiore connettività con sistemi di monitoraggio remoti o localizzati - Apprendimento automatico e analisi predittiva applicati ai dati
Guasti nelle procedure pratiche e operative	- Simulatori di addestramento degli operatori basati su modelli dinamici di impianto di processo(es. Operator Training Simulator) - Visualizzazione digitale e interfacce operatore migliorate
Progettazione e analisi dei rischi	- CAD 3D dell'impianto - Software di analisi dei rischi qualitativi come ExpHAZOP - Modelli dinamici che analizzano come la riduzione dei costi di manutenzione aumentano i rischi

Tabella 2.3 *Alcune soluzioni portate dalle industrie di processo per fronteggiare le criticità più comuni dalle quali derivano i problemi sulla sicurezza.*

2.2 Analisi dei requisiti degli standard per garantire "Safety & Security" aziendale

Quando si parla di sicurezza in un contesto di industria 4.0, si fa riferimento a due concetti distinti: *Safety e Cyber security*. Per "Safety" si intende "la tutela del lavoratore che collabora con macchine interconnesse esponendosi a rischi meccanici, elettrici, radioattivi ecc." mentre la Cyber-security, una delle nove tecnologie abilitanti di questa quarta rivoluzione industriale, cela dietro il proprio significato un'innovazione nel concetto di sicurezza, che non si ferma più soltanto alla cosiddetta "Safety" citata in precedenza, ma deve tenere in considerazione anche le minacce informatiche che possono presentarsi molto frequentemente in corrispondenza di macchine interconnesse tra loro attraverso l'ausilio di reti informatiche interne ed esterne.[17]

Quindi da un lato, prima dell'avvento di industria 4.0, le infrastrutture informatiche permettevano e permettono tuttora di gestire la sicurezza dal punto di vista dei possibili incidenti sul lavoro; in questa nuova ottica, se da una parte garantiscono una forte integrazione verticale e orizzontale permettendo alle imprese di gestire in modo più efficiente i flussi con gli attori esterni ed interni all'impresa, dall'altro bisogna fare interfacciarsi con delle potenziali vulnerabilità e anomalie dei sistemi che si hanno a disposizione.[10]

Essendo industry 4.0, almeno nelle fasi iniziali, un campo molto complesso sotto tutti i punti di vista, si è reso necessario sin da subito creare un modello che promuovesse un'architettura di riferimento, per scomporre le funzioni, i servizi e i processi in componenti più facilmente manipolabili.

Alcuni consorzi d'impresa mondiali hanno elaborato proposte di modelli di riferimento differenti, ciascuna in grado di porre sotto la lente di ingrandimento una diversa prospettiva del contesto. Quelli che attualmente sono emersi riguarda il modello di architettura "industrie 4.0" (RAMI 4.0), elaborate da "Platform industrie 4.0", e l'architettura di riferimento IIRA (per l'"internet industriale" del consorzio "industrial internet"[18].

---

[17] *<http://www.key-4.com/la-sicurezza-nellindustria-4-0/>*

[18] *<https://www.agendadigitale.eu/industry-4-0/industry-4-0-tutti-gli-standard-e-i-modelli-di-riferimento/>*

In particolare il modello RAMI 4.0 è un modello tridimensionale che descrive le aree in cui agisce industry 4.0 (figura 2.5)

- Layers (Strati): Proprietà strutturali di un asset o di un insieme di asset (componenti della fabbrica):
  - Business: descrive gli aspetti commerciali
  - Functional: descrive le funzioni tecniche di un asset in relazione al sistema industry 4.0
  - Information: descrive i dati che sono utilizzati, generati o modificati dalle funzionalità tecniche dell'asset
  - Communication: descrive le modalità di accesso alle informazioni ed alle funzioni di un asset connesso da parte degli altri asset
  - Integration: rappresenta lo strato di interaccia tra il mondo fisico e il mondo delle informazioni
  - Asset: rappresenta gli oggetti reali in termini di ingombri, servizi, schemi di collegamento, archivi ecc.
- Hierarchy levels (Livelli di gerarchia): fa riferimento al modello a piramide dell'automazione industriale, definito dalle norme IEC 62264/61512 al quale sono stati aggiunti alcuni livelli specifici per la fabbrica 4.0 (product, field device, connected world).

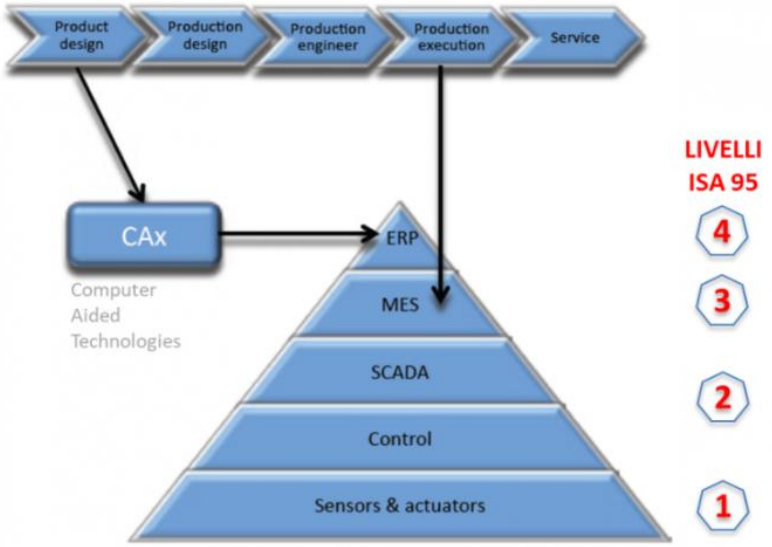

Figura 2.4 *Modello di riferimento ISA 95. <https://ceimagazine.ceinorme.it/ceifocus/il-background-tecnologico-e-normativo-di-industria-4-0/ >*

In figura 2.4 la parte bassa della piramide è il cosiddetto “campo” o “shop-floor”. La comunicazione tra controllo e campo avviene attraverso “fieldbus” specializzati supportati da associazioni di produttori (ad es. Profibus/Profinet, FieldComm Group, Ethercat,…) o da produttori singoli (ad es. DeviceNet, Interbus,…). I più diffusi “fieldbus” sono ormai anche standard pubblici, essendo stati recepiti dalla IEC e raggruppati nella sin troppo vasta famiglia di standard IEC 61158.

Il livello più alto della piramide, sopra lo SCADA, è costituito dal MES (Manifacturing Execution System) che ha lo scopo di gestire e programmare la produzione della fabbrica e dall’ERP (Enterprise Resource Planning) che integra i software gestionali dell’azienda. I livelli 3 e 4 fanno riferimento al modello funzionale basato sul Purdue Reference Model utilizzando il Common Information Model, cioè uno standard aperto che definisce come rappresentare e gestire tutti gli elementi in ambiente di IT aziendale **(3)**. Lo scopo primario della Norma IEC 62264 (ISA 95) è la definizione delle interazioni B2M e M2B (dove B=business e M=manufacturing) per gestire gli scambi dati tra i livelli 3 e 4. Le transazioni avvengono con un meccanismo provider/consumer che scambia file XML con schemi predefiniti (B2M Markup Language).
Ogni programma di gestione dell’azienda (ad es. per la manutenzione o la programmazione della produzione) può interagire con altri programmi scambiandosi file XML standardizzati. Se, ad esempio, la funzione controllo costi vuole acquisire i dati di produzione non farà altro che richiedere alla funzione controllo del processo l’invio del file XML che li contiene, file che sarà scritto con una sintassi standardizzata. E così via per tutte le transazioni inter-aziendali.

- Life Cycle & Value Stream (Ciclo di vita e flusso del valore): viene rappresentato il ciclo di vita della fabbrica, definito in accordo alla norma IEC 62890 “Life cycle management for systems and products used in industrial-process measurement, control and automation). Si tratta di una rappresentazione complessa poiché esistono diversi cicli di vita, come quello relativo ad un

ordine, a quello della supply-chain della fabbrica, a quello di un prodotto e così via, i quali interagiscono tra loro.[19]

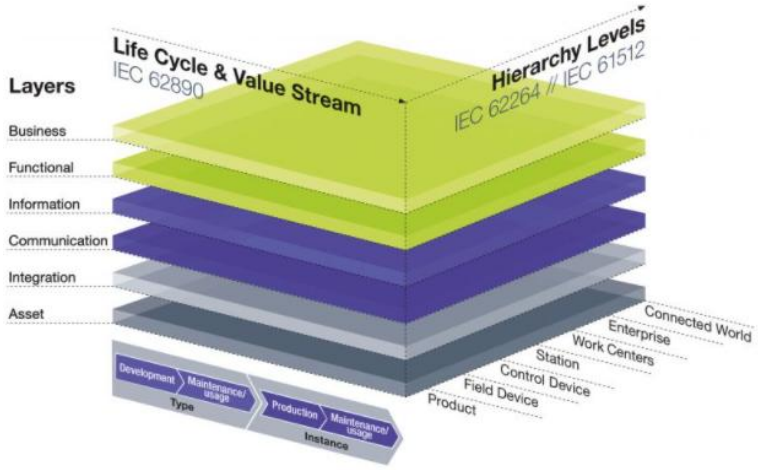

Figura 2.5 *Modello dell'architettura di riferimento industrie 4.0 (RAMI 4.0). <https://doi.org/10.1109/DESSERT.2019.8770010.>*

Per quanto riguarda il quadro normativo correlato all'attività di protezione e sicurezza nell'impresa, il modello RAMI 4.0 ha evidenziato tre classi di normative rispettivamente per la sicurezza informatica (security), per la sicurezza funzionale e per la sicurezza dei macchinari (safety):

- Network and system security IEC 62443: Vengono descritti quattro livelli di sicurezza:
    - Security level 1: protezione contro la violazione occasionale o casuale
    - Security level 2: protezione contro la violazione intenzionale con mezzi e risorse scarse
    - Security level 3: protezione contro la violazione intenzionale con mezzi sofisticati e risorse moderate
    - Security level 4: protezione contro la violazione intenzionale con mezzi sofisticati e risorse ingenti

  I requisiti di sicurezza per ogni installazione variano a seconda della criticità dell'impianto ed adempiono agli eventuali cogenti di legge. Viene espressamente richiesto di proteggere le singole apparecchiature da

[19] *<https://ceimagazine.ceinorme.it/ceifocus/il-background-tecnologico-e-normativo-di-industria-4-0/ >*

manipolazione di terzi malevoli senza compromettere le funzionalità proprie e i devices e degli impianti attraverso una particolare attenzione sul controllo accesi. Infatti la norma sottolinea il principio del "privilegio minimo", secondo cui ogni parte attiva del sistema (anche umana) deve fruire dei privilegi di accesso strettamente necessari all'espletamento delle sole funzioni previste dal proprio ruolo (IEC 62443-4-2).

Un'altra norma della stessa famiglia (IEC 23443-3-3) richiama espressamente la necessità dell'identificazione e dell'autenticazione dell'utente attraverso l'ausilio (oltre che degli strumenti più semplici e conosciuti) di token fisici, certificati crittografici (a chiave simmetrica o a doppia chiave protette a livello hardware), anche in combinazione tra di loro con una durata temporale infinita. Inoltre ogni dispositivo deve essere predisposto per l'integrazione di un sistema di gestione delle identità di stabilimento.

È compito dei produttori predisporre una lista di ruoli con accessi diversificati su cui verranno mappati i singoli utenti in fase di configurazione, siano questi umani, processi software, oppure altre apparecchiature che devono interagire con il componente certificato.[20]

- Information security management system ISO/IEC 27000: comprende gli standard di sicurezza delle informazioni che si supportano reciprocamente e che insieme forniscono un quadro riconosciuto a livello globale delle "best practices" per la gestione della sicurezza delle informazioni.

  Le norme della serie definiscono i requisiti per creare un SGSI (Sistema di gestione per la sicurezza delle informazioni) e per coloro che certificano questi sistemi, forniscono una guida per progettare, attuare, mantenere e migliorare un SGSI, esprimono le linee guida nei vari ambiti di utilizzo di un SGSI e infine valutano la conformità di un SGSI.

  È applicabile a tutte le organizzazioni di qualsiasi tipo e dimensione, le quali sono incoraggiate a valutare i loro rischi informativi ed a trattarli in base alle loro esigenze, utilizzando il manuale e i suggerimenti del caso. Data la natura

[20] *<https://www.cybersecurity360.it/legal/lo-standard-iec-62443-4-2-per-la-cyber-security-industriale-le-linee-guida/>*

dinamica del rischio e della sicurezza delle informazioni, il SGSI incorpora un feedback continuo e attività di miglioramento per rispondere ai cambiamenti delle minacce, delle vulnerabilità o degli impatti degli incidenti.[21]

- Functional Safety IEC 61511: si tratta di uno standard tecnico che definisce le pratiche nell'ingegnerizzazione di sistemi che garantiscono sicurezza in un processo industriale attraverso l'uso di strumentazione. Tali sistemi sono indicati come SIS (Safety Instrumented Systems).

  In particolare la norma "copre i requisiti di progettazione e gestione per i SIS durante l'intero ciclo di vita della sicurezza. Il suo ambito comprende: l'idea iniziale, progettazione, implementazione, funzionamento e manutenzione fino allo smantellamento.

  Lo standard si compone di tre parti:

  - Framework, definizioni, sistemi, requisiti hardware e software
  - Linee guida nell'applicazione di IEC 61511-1
  - Guida per la determinazione dei livelli di integrità della sicurezza richiesti

  ISA 84.01/IEC 61511 richiede un sistema di gestione per SIS identificato. Un SIS è composto da una combinazione separata e indipendente di sensori, risolutori logici, elementi finali e sistemi di supporto progettati e gestiti per raggiungere un livello di integrità della sicurezza (SIL) specificato. Un SIS può implementare una o più funzioni strumentate di sicurezza (SIF), che sono progettate e attivate per affrontare uno specifico pericolo di processo o evento pericoloso. Il sistema di gestione del SIS dovrebbe definire il modo in cui un proprietario / operatore intende valutare, progettare, verificare, installare, mettere in servizio, convalidare, far funzionare, mantenere e migliorare continuamente il proprio SIS. Dovrebbero essere definiti i ruoli essenziali dei vari membri del personale a cui è stata assegnata la responsabilità per il SIS e dovrebbero essere sviluppate procedure, se necessario, per supportare la coerente esecuzione delle loro responsabilità.

[21] *<https://it.wikipedia.org/wiki/ISO/IEC_27000-series>*

ISA 84.01 / IEC 61511 utilizza un ordine di grandezza metrico, il SIL, per stabilire le prestazioni necessarie. Un'analisi dei rischi e dei pericoli viene utilizzata per identificare le funzioni di sicurezza richieste e la riduzione del rischio per eventi pericolosi specificati. Le funzioni di sicurezza assegnate al SIS sono funzioni strumentate di sicurezza; la riduzione del rischio allocata è correlata al SIL. La progettazione e la base operativa sono sviluppate per garantire che il SIS soddisfi il SIL richiesto. I dati sul campo vengono raccolti attraverso le attività del programma di integrità meccanica e operativa per valutare le prestazioni effettive del SIS. Quando le prestazioni richieste non sono soddisfatte, è necessario agire per colmare il divario, garantendo un funzionamento sicuro e affidabile.

La norma IEC 61511 fa riferimento alla norma IEC 61508 (lo standard principale) per molti articoli come i produttori di hardware e strumenti, pertanto la norma IEC 61511 non può essere completamente implementata senza riferimento alla norma IEC 61508. La norma IEC 61511 è l'implementazione dell'industria di processo della norma IEC 61508.”.[22]
Infatti lo standard IEC 61508 è stato sviluppato come uno standard indipendente dal dominio in cui è adottato e quindi adattabile a tutte le tipologie di domini mentre la IEC 61511 è sviluppata principalmente per considerare le peculiarità di un dominio specifico.[11]

- Safety of machinery - I – IEC 62061: “ IEC / EN 62061, "sicurezza del macchinario: sicurezza funzionale dei sistemi di controllo elettrici, elettronici ed elettronici programmabili", è l'implementazione specifica del macchinario della IEC / EN 61508. Fornisce requisiti applicabili alla progettazione a livello di sistema di tutti i tipi di macchinario, sistemi di controllo elettrico legati alla sicurezza e anche per la progettazione di sottosistemi o dispositivi non complessi. La valutazione del rischio si traduce in una strategia di riduzione del rischio che, a sua volta, identifica la necessità di funzioni di controllo legate alla sicurezza. Queste funzioni devono essere documentate e devono includere:

[22] *<https://en.wikipedia.org/wiki/IEC_61511>*

specifica dei requisiti funzionali e specifica dei requisiti di integrità della sicurezza.

I requisiti funzionali includono dettagli come frequenza di funzionamento, tempo di risposta richiesto, modalità operative, cicli di lavoro, ambiente operativo e funzioni di reazione ai guasti. I requisiti di integrità della sicurezza sono espressi in livelli chiamati SIL (Safety Integrity Level). A seconda della complessità del sistema, alcuni o tutti gli elementi nella tabella 14 devono essere considerati per determinare se la progettazione del sistema soddisfa il SIL richiesto.

- Safety of machinery - II – ISO 13849: "è uno standard di sicurezza che si applica a parti dei sistemi di controllo delle macchine assegnate a fornire funzioni di sicurezza (chiamate parti legate alla sicurezza di un sistema di controllo). Viene suddiviso principalmente in due parti:
    - ISO 13849-1, Parte 1: principi generali per la progettazione, fornisce requisiti di sicurezza e guida sui principi di progettazione e integrazione delle parti relative alla sicurezza dei sistemi di controllo (hardware o software).
    - ISO 13849-2, Parte 2: validazione, specifica le procedure da seguire per la validazione mediante analisi o test, le funzioni di sicurezza del sistema, la categoria raggiunta e il livello di prestazioni raggiunto.

Nella Parte 1 si identifica come la progettazione del sistema di sicurezza si basi sulla valutazione dei rischi eseguita dal produttore della macchina. Questa valutazione del rischio evidenzia le funzioni di sicurezza richieste per mitigare il rischio e il livello di prestazioni che queste funzioni devono soddisfare. Il livello di prestazioni di una funzione è determinato dalle caratteristiche architettoniche del controllore (classificato per categorie), dal MTTFd[23] dei componenti e del sistema e dalla copertura diagnostica media implementata nel sistema. Il principio di base consiste nel ritenere che il sistema

[23] *MTTFd: "Tempo medio per un guasto pericoloso. In un sistema di sicurezza MTTFD è la componente delle modalità di guasto che può portare a guasti che possono creare rischi per il personale, l'ambiente o le apparecchiature." < https://en.wikipedia.org/wiki/MTTFd>*

di controllo non solo deve essere in grado di svolgere la funzione di sicurezza a un livello tale da mitigare il rischio identificato, ma lo deve anche fare in presenza di un guasto."[24]

L'introduzione della Norma EN ISO 13849-1 ha comportato la determinazione di nuovi requisiti in merito alle procedure anche per la costruzione delle macchine. Nella pratica, l'azienda PILZ, leader nella fornitura di soluzioni per l'automazione, sostiene che la realizzazione di parti del sistema legate alla sicurezza è un processo che si realizza mediante l'iterazione di sei diverse fasi:

- Fase 1 – definizione dei requisiti delle funzioni di sicurezza: si tratta della fase più importante ove è necessario stabilire le caratteristiche essenziali per le funzioni di sicurezza. Nel caso dell'implementazione di un riparo mobile, ad esempio, è necessario che all'apertura del riparo stesso vengano bloccati istantaneamente tutti i movimenti pericolosi della macchina e in ogni caso un riavvio della stessa a riparo mobile aperto non deve essere possibile
- Fase 2 – determinazione del "Performance Level" richiesto (PL): il grado di pericolosità di ogni situazione va suddiviso in cinque livelli che vengono denominati con delle lettere minuscole che vanno da "a" (Contributo della funzione di controllo alla riduzione del rischio è basso) ad "e" (contributo della funzione di controllo alla riduzione del rischio elevato). Sulla base del grafico del rischio viene determinato il PL richiesto per la funzioni di sicurezza

  Gravità della lesione (S): S1= lesione lieve; S2= lesione grave
  Frequenza e/o durata dell'esposizione al pericolo(F): F1= da raramente a spesso e/o breve durata; F2= da spesso a durata continua e/o prolungata
  Possibilità di evitare il pericolo (P): P1= possibile in determinate condizioni; P2= quasi impossibile

- Fase 3 – Progettazione e realizzazione tecnica delle funzioni di sicurezza; riprendendo l'esempio fatto in fase 2, per il blocco del riparo mobile è necessario utilizzare un finecorsa di sicurezza codificato. In questo modo si è in

[24] *<https://en.wikipedia.org/wiki/ISO_13849>*

grado di comandare più ripari mobili in serie senza che le funzioni di controllo perdano efficacia.

A questo scopo la codifica offre un elevato livello di protezione contro la manipolazione. La relativa verifica di sensori avviene attraverso un sistema di sicurezza multifunzionale.

- Fase 4 – Determinazione del "Performance Level" e valutazione quantitativa: per la determinazione del PL raggiunto, la funzione di sicurezza viene suddivisa in tre parti: sensore, logica e attuatore. Ogni parte di questo sistema apporta un proprio contributo alla funzione di sicurezza. I componenti PILZ dispongono di tutti i valori richiesti ed a questo scopo PILZ mette a disposizione un efficace software di calcolo denominato "PAScal"
- Fase 5 – Verifica: questa fase evidenzia il confronto tra il "Performance Level" necessario e quello raggiunto; in particolare quest'ultimo deve essere superiore a quello necessario, stabilito in fase di valutazione dei rischi. Questa eventualità garantisce il via libera alla costruzione della macchina
- Fase 6 – Validazione: oltre a quanto previsto dai requisiti qualitativi, nella realizzazione dei sistemi di sicurezza è anche importante evitare errori sistematici grazie alla validazione dei risultati ottenuti.[25]

2.2.1 Monitoraggio della conformità agli standard di sicurezza

Le nuove tecnologie e i requisiti dell'industria 4.0 creano una nuova domanda di standardizzazione, che gioca un ruolo chiave nel migliorare la "Safety & Security" nelle diverse realtà.

È chiaro che le variabili in gioco e la maturità ancora scarsa di queste tecnologie fa si che, oltre alle normative implementate dal modello RAMI 4.0, l'aspetto sicurezza, nel senso più ampio del suo termine, sia un campo ancora poco esplorato e di notevole interesse; in particolare l'attenzione è attualmente posta sulla necessità di verificare che il sistema IT utilizzato da ciascuna impresa, sia conforme a tutte le normative di sicurezza applicabili, in modo da rendere più tollerabili eventuali incidenti.

[25] *<https://www.pilz.com/it-IT/support/knowhow/law-standards-norms/functional-safety/en-iso-13849-1>*

Come mostrato in Figura 2.6, è possibile verificare la conformità agli standard di sicurezza attraverso un quadro di monitoraggio che utilizza un sistema (Evidence Gathering Mechanism) per raccogliere delle prove da un numero di componenti del sistema target sulla base di una serie di MIP (Measurable Indicator Points). I MIP, classificati in indicatori di sicurezza informatica misurabili (MSI), indicatori di sicurezza sul lavoro (MSFI), e altri indicatori organizzativi relativi ad aspetti di diritto (MSLI), sono estratti dagli standard e dalle linee guida esistenti per affrontare i requisiti specifici del sistema target (ad esempio sistemi di controllo degli accessi per la linea di produzione dovrebbe essere agli attacchi dei canali laterali). Queste informazioni vengono poi utilizzate per definire se il sistema di destinazione funziona in modo sicuro e conforme agli standard.

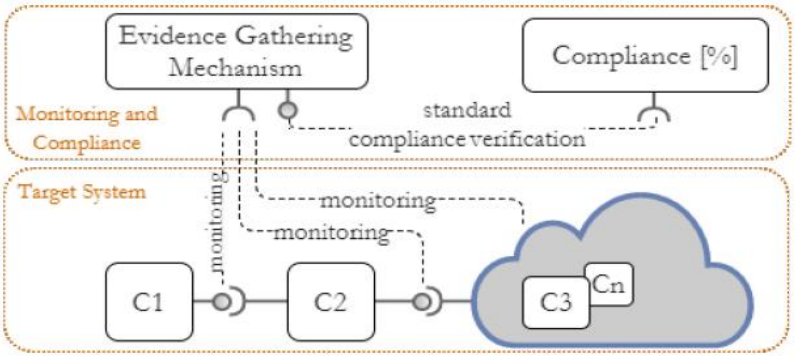

Figura 2.6 *Vista ad alto livello della verifica di conformità agli standard di sicurezza. <https://doi.org/10.1109/ICPHYS.2018.8390801.>*

La conformità agli standard rappresenta il rispetto di un determinato pacchetto di requisiti di sicurezza e protezione, individuati da metriche misurabili, sull'utilizzo e la configurazione di sistemi o di qualsiasi altro meccanismo di sicurezza o riguardante il diritto. Queste metriche misurabili dovrebbero essere imposte da meccanismi standardizzati per rendere ogni dispositivo, sistema o applicazione conforme agli standard. Per garantire la conformità agli standard e la funzionalità sicura del sistema è necessario implementare un'architettura collegabile e utilizzabile che consenta di adattarsi facilmente all'analisi e al controllo costante del sistema o dei componenti del sistema. Il quadro di monitoraggio e verifica della conformità agli standard (figura 2.7) è composto da quattro moduli principali:

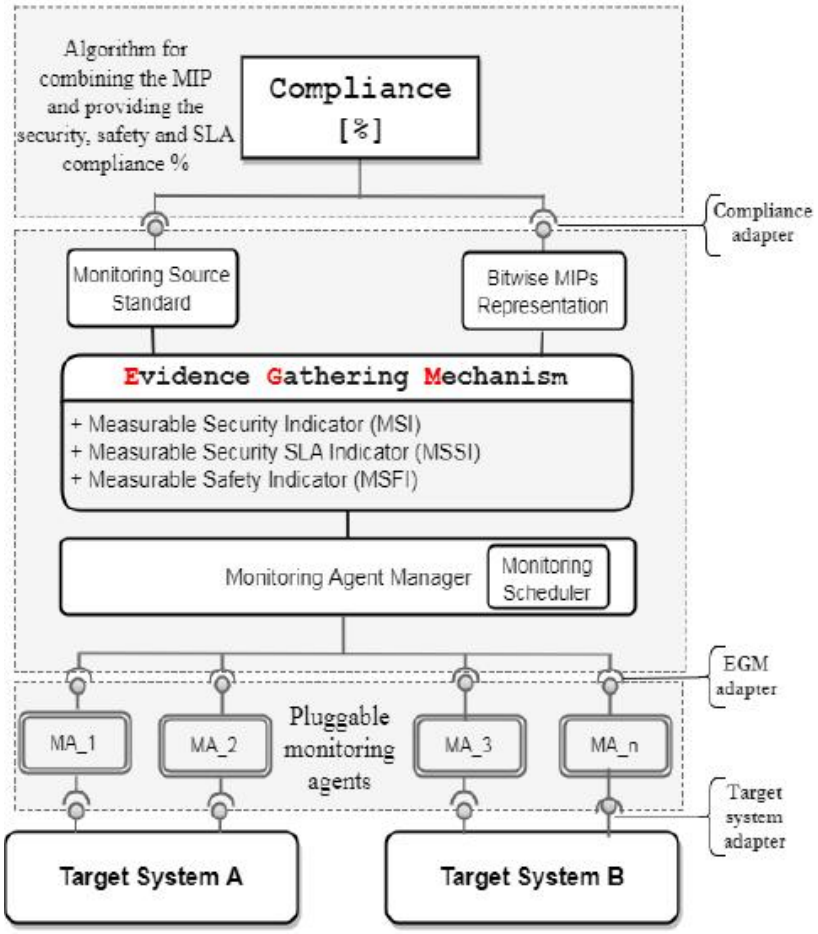

Figura 2.7 *Quadro di monitoraggio per la verifica della conformità agli standard utilizzato per misurare, aggregare, programmare, archiviare, recuperare e analizzare i dati di monitoraggio per fornire la conformità agli standard. <https://doi.org/10.1109/ICPHYS.2018.8390801.>*

1. Agenti di monitoraggio (MA): il modulo MA viene utilizzato per raccogliere dati dai target system e dovrebbe consentire l'integrazione di diversi agenti di monitoraggio collegabili da vari plug-in di strumenti di monitoraggio e script personalizzati.

2. Meccanismo di raccolta delle prove (Evidence Gathering Mechanism): Il modulo EGM è progettato per acquisire, archiviare ed analizzare la sicurezza, la protezione e le prove legali correlate. Gestisce i dati che prende in ingresso dagli agenti di monitoraggio e decide la quantità e gli specifici dati da inviare al modulo di conformità utilizzando un buffer di scrittura. Rende possibile la mappatura delle metriche misurabili e dei loro valori con gli standard per fornire

le informazioni necessarie al modulo di conformità. Il modulo EGM è sua volta costituito da:

a) Monitoring agent manager: è l'unica interfaccia tra il modulo EGM e i Monitoring agent ed è responsabile dell'organizzazione di ciascun MA in base alle configurazioni e utilizza uno "scheduler" di monitoraggio per fornire il tempo di esecuzione di ogni plug-in nel file componente.
b) Monitoring Source Standard: La sorgente di monitoraggio dello standard fornisce, per ciascuna metrica misurabile definibile, la fonte dalla quale viene estratta la linea guida/best practice. Attraverso la mappatura dei MIP allo standard specifico, il modulo di conformità può verificare se la metrica specifica è stata monitorata nel target system.
c) Bitwise MIPs Representation: il modulo di rappresentazione MIP bit per bit rappresenta ogni MIP con un numero, che può essere convertito in codice binario e letto dal computer.

3. La conformità (Compliance): si tratta di un algoritmo che combina i MIP al fine di stabilire la conformità del sistema alle linee guida e definirne il grado di sicurezza e sicurezza informatica.
4. Target System (TS): rappresenta un sistema o un componente di un sistema che verrà monitorato da plug-in di strumenti di monitoraggio o script personalizzati.

Il modulo EGM, una volta raccolti i dati di monitoraggio in una struttura a colonne basata sui MIP (MSI, MSFI, MSSI), per ciascuno di essi fornirà informazioni relative all' ID della metrica, il valore della metrica (binario) e la fonte basata sulle linee guida/best practice, ove viene estratta la metrica, come mostrato in un esempio in figura 2.8.

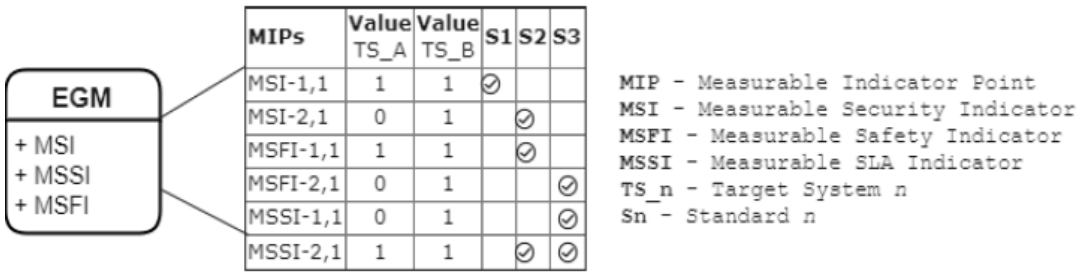

Figura 2.8 *Serie rappresentativa delle informazioni fornite dal modulo EGM al modulo COMPLIANCE. <https://doi.org/10.1109/ICPHYS.2018.8390801.>*

A questo punto, attraverso gli elementi b) e c) le informazioni vengono inviate in input al modulo Compliance, responsabile che il sistema si comporti in modo sicuro e conforme agli standard guidati dall'input fornito dal modulo EGM. Per misurare la conformità agli standard è necessario considerare una serie di MIP ed una serie di standard, poiché si tratta di coinvolgere un mix dinamico di nuove tecnologie, regolamenti e interazioni di diverse organizzazioni tuttavia, la difficoltà nell'estrarre le metriche per la sicurezza informatica, la sicurezza sul lavoro e gli standard legali è piuttosto complesso in quanto vanno considerate anche le relazioni indirette e l'affidabilità tra di loro.

Per semplicità sono stati considerati solo MSI nell'approccio alla verifica della conformità agli standard, ma questo è valido anche per MSFI ed MSSI. La figura 2.9 mostra più nel dettaglio il processo illustrato precedentemente dove ogni MSI estratto da una standard di sicurezza viene monitorato utilizzato degli agenti di monitoraggio nel componente corrispondente del sistema target. Quindi il modulo EGM invia, attraverso le sue due componenti, al modulo Compliance la sorgente da cui viene estratta la metrica e un valore binario 0 e 1, il quale, a seconda dei requisiti del sistema target specifico, assegna a ciascun MSI un peso per indicare l'importanza nell'intervallo (0,1).

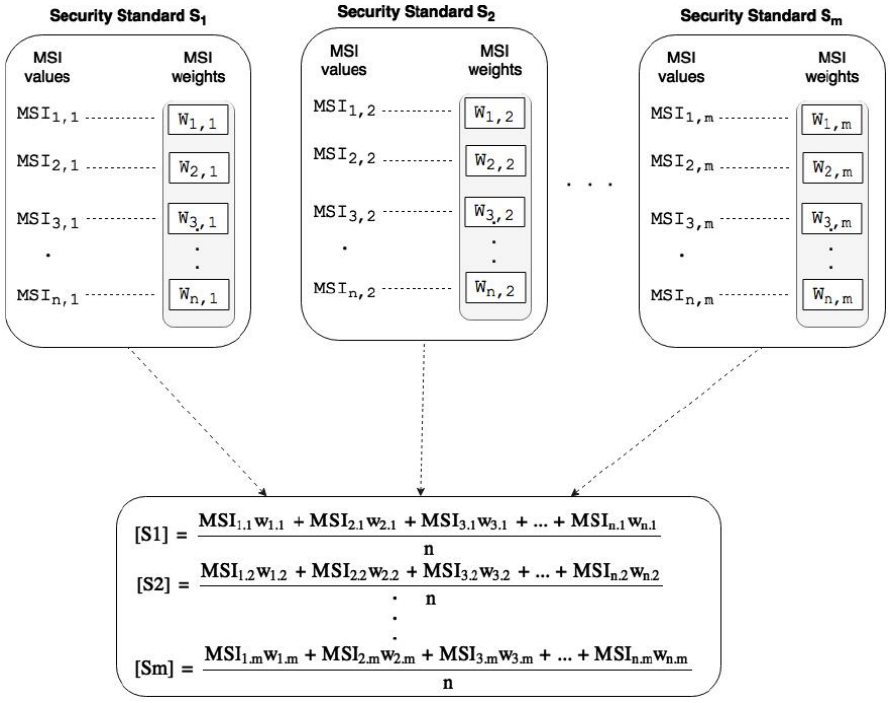

Figura 2.9 *Monitoraggio di MSI estratti dagli standard di sicurezza e raccolta nel modulo EGM. <https://doi.org/10.1109/ICPHYS.2018.8390801.>*

Una volta ottenute in ingresso le prove raccolte dal modulo EGM, il modulo Compliance verifica da subito la conformità (in percentuale) per un singolo standard di sicurezza, calcolata come il rapporto tra la somma di ciascun valore misurato MSI moltiplicato per il peso ad esso assegnato e il numero totale di metriche standard:

$$MSI_{compliance_{(j)}} = \frac{\sum_{i=1}^{n} MSI_{I,J} \times w_{i,j}}{n} \times 100 \qquad (1)$$

Dopodiché viene verificata la conformità totale come rapporto tra la somma delle conformità di ciascuno standard e il numero totale degli standard considerati:

$$MSI_{compliance_{tot}} = \frac{\sum_{i=1}^{m} compliance_{(j)}}{m} \times 100 \qquad (2)$$

Dove $MSI_{I,J}$ è il valore misurato della i-esima metrica di sicurezza e relativo al j-esimo standard, e $w_{i,j}$ è il valore del peso della i-esima metrica di sicurezza e riguardante il j-esimo standard anche in questo caso.

I valori calcolati vanno in qualche modo classificati per poter stabilire il livello di conformità raggiunto e in particolare sono stati definiti arbitrariamente quattro livelli di conformità, i quali sono caratterizzati da specifici valori dei parametri MSI, MSFI, MSSI come illustrato nella tabella 2.10.

Compliance Level	MIPs		
	MSI	MSFI	MSSI
Level 0	basic	basic	basic
Level 1	basic	basic	high
	basic	high	basic
	high	basic	basic
Level 2	basic	high	high
	high	basic	high
	high	high	basic
Level 3	high	high	high

Tabella 2.10 *Livelli di conformità arbitrari definiti sulla base dei MIPs.*
<https://doi.org/10.1109/ICPHYS.2018.8390801.>

Per dare una visione quantitativa in relazione all'equazione (2) viene definita di base la conformità nell'intervallo (0% - 50%) ed elevata la conformità nell'intervallo (50% - 100%), permettendo quindi una migliore interpretazione di ciascun livello come segue:

- Livello di conformità 0 indica che la conformità dell'intero pacchetto MIP è fondamentale
- Livello di conformità 1 indica che almeno la conformità di un gruppo MIP è elevata
- Livello di conformità 2 indica che almeno la conformità di due gruppi MIP è elevata
- Livello di conformità 3 indica che la conformità dell'intero pacchetto MIP è elevata

L'obiettivo dell'implementazione di questo quadro di monitoraggio è essenzialmente quello di garantire la cooperazione tra entità indipendenti in una realtà competitiva sempre più complessa, senza compromettere l'infrastruttura sottostante.[11]

2.2.2 Determinazione di un pacchetto di MIPs in uno scenario applicativo relativo ad una comunicazione end-to-end sicura in CPPS

Si consideri uno scenario applicativo che abbia come obiettivo quello di soddisfare i requisiti dei sistemi di controllo degli accessi per la linea di produzione e in particolare si tenga in considerazione la norma IEC 62443-3-3 (Reti di comunicazione industriale – sicurezza della rete e del sistema – Requisiti di sicurezza del sistema e livelli di sicurezza) la quale fornisce i requisiti fondamentali del sistema di controllo tecnico per l'automazione industriale e la capacità del sistema di controllo, dove sono stati selezionati tre MSI per sottolineare come ciascuno di essi viene documentato e monitorato. Oltre alla precedente norma teniamo in considerazione anche la norma sulla sicurezza funzionale IEC 61508-3 discussa nel paragrafo 2.2 e che rappresenta uno standard generale, adattabile a tutti i contesti aziendali, indipendentemente dal dominio specifico preso in considerazione.

Consideriamo quindi il caso applicativo in figura 2.11 che rappresenta una comunicazione con protocollo end-to-end[26] sicura in CPPS.

Per fornire la gestione dei dispositivi come servizio, è necessario che i dati vengano trasmessi tra i dispositivi M1, M2 ed M3, elaborati ed inviati ad un cloud privato per ulteriori elaborazioni ed analisi. Il protocollo utilizzato per la comunicazione tra i dispositivi periferici, i componenti IIOT, e il backend cloud è il protocollo MQTT[27] Nel nostro caso, avendo a disposizione un dispositivo legacy (apparecchiatura obsoleta o non più in produzione) per poter stabilire una connessione con il gateway IIOT è necessario dotarsi di un traduttore per trasporre il protocollo del dispositivo in MQTT. In tale scenario, con diversi componenti CPPS decentralizzati, i report sulle condizioni per l'intero sistema sono fondamentali;

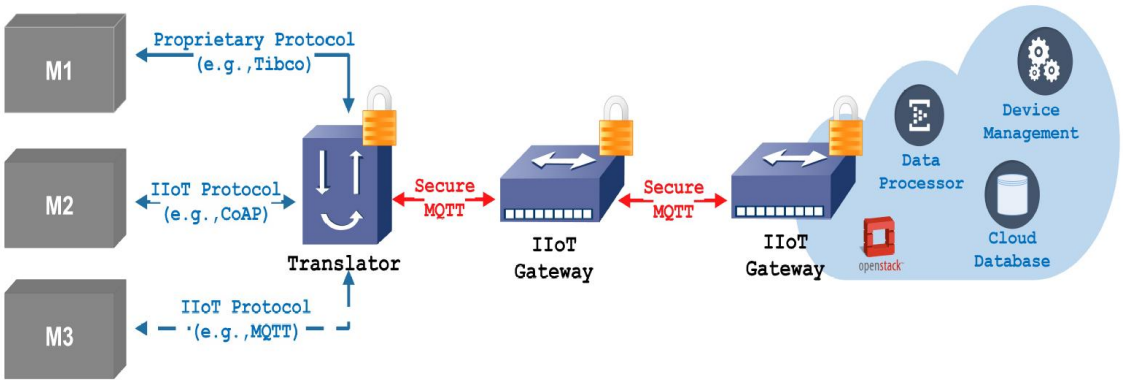

Figura 2.11 *Comunicazione end-to-end sicura in Cyber Physical Production Systems (CPPS). <https://doi.org/10.1109/ICPHYS.2018.8390801.>*

conseguentemente, molteplici elementi possono essere monitorati a tale scopo, inclusi i devices industriali. Una volta identificati i requisiti e valutato se le linee guida/best practices rispettano o meno il requisito specifico, il passo successivo è quello di

[26] *Un protocollo end-to-end "afferma che, se si hanno due applicazioni che comunicano tramite una rete, tutte le funzioni e le operazioni specifiche richieste da tali applicazioni, come il controllo di errori, devono essere realizzate ed eseguite in modo completo nei nodi terminali (end point) e non nei nodi intermedi della rete" <https://it.wikipedia.org/wiki/End-to-end>*

[27] *MQTT "è un protocollo ISO che ha l'obiettivo di abilitare la comunicazione tra le macchine in maniera efficiente e in particolare quello di minimizzare il traffico sulle reti e richiedere poche risorse ai dispositivi per la sua gestione" <https://www.internet4things.it/iot-library/mqtt-cose-e-come-funziona-il-protocollo-alla-base-delliot/>*

identificare i punti indicatori misurabili (MIPs). Definiamo quindi una serie di MSI ed MSFI rappresentativi (tabella 2.12), estratti dagli standard di sicurezza e protezione sopra elencati; in particolare, come discusso nel paragrafo 2.2.1, per ogni MIP verrà fornito l'ID, la fonte, la definizione in base agli standard, le possibili soluzioni di monitoraggio e un valore di monitoraggio.

MSI – 1.1: Identificazione e autenticazione sicure	- Fonte: IEC 62443-3-3 - Definizione: il client e il server si identificano a vicenda e garantiscono la propria identità tramite un accesso sicuro - Plug-in di monitoraggio: Può essere monitorato con l'agente di monitoraggio NAGIOS, che controlla la configurazione del protocollo utilizzato per assicurarsi che utilizzi un protocollo di comunicazione sicuro - Valore di monitoraggio: vero/falso
MSI – 2.1: Forza dell'autenticazione basata su password	- Fonte: IEC 62443-3-3 - Definizione: il sistema deve essere configurabile fornendo un grado di complessità come lunghezza minima, varietà di caratteri e rotazione della password - Plug-in di monitoraggio: Può essere implementato eseguendo controlli PAM (pluggable authentication module) per verificare se è abilitata una lunghezza o una complessità minima delle password e la rotazione delle password - Valore di monitoraggio: vero/falso
MSI – 3.1: controllo della sessione simultanea	- Fonte: IEC 62443-3-3 - Definizione: il sistema limiterà il numero massimo di sessioni simultanee per account di sistema o tipo di sistema - Plug-in di monitoraggio: sviluppare uno script che controlli una configurazione sshd_config o pam_limits - Valore di monitoraggio: vero/falso

MSFI – 1.2: Architettura temporizzata	- Fonte: IEC 61508-3 - Definizione: assicurarsi che il sistema sia conforme ai requisiti di temporizzazione di sicurezza - Plug-in di monitoraggio: può essere controllato tramite NAGIOS, inviando il pacchetto di prova al sistema e controllando se il tempo di risposta rientra nei parametri consentiti - Valore di monitoraggio: tempo di risposta
MSFI – 2.2: Tecniche e misure per il rilevamento degli errori	- Fonte: IEC 61508-3 - Definizione: assicurarsi che le modifiche apportate al sistema siano protette da errori - Plug-in di monitoraggio: verificare che le modifiche de sistema richiedano una password

Tabella 2.12 *Definizione dei MIPs di monitoraggio rappresentativi del caso di studio.*

Da qui il sistema si evolve esattamente come specificato nel paragrafo 2.2.1, quindi gli agenti di monitoraggio, definiti per ogni MIP, raccoglieranno dati dal sistema di comunicazione end-to-end sicura in CPPS e forniranno all'EGM le informazioni necessarie in relazione al soddisfacimento o meno della metrica. Il modulo compliance mappa la metrica con lo standard corrispondente e calcola la conformità sulla base dell'equazione (2), il cui risultato verrà impiegato per stabilire il livello di conformità del sistema.

3. Analisi del rischio e implementazione di sistemi di gestione della sicurezza per applicazioni "Industry 4.0"

3.1 Safety intelligence come modello di gestione dei dati e delle informazioni sulla sicurezza

La costante necessità che sta spingendo le imprese a cercare nuovi e migliori approcci per garantire che le risorse sulla sicurezza siano allocate nel modo più efficace ed efficiente possibile, è alla base di una rinnovata considerazione nei confronti delle informazioni sulla sicurezza, ma soprattutto riguardo il percorso che devono seguire in modo da arrivare integralmente ai soggetti competenti nella prevenzione dei rischi e protezione dai pericoli per cose e persone. Tuttavia la qualità delle informazioni sulla sicurezza deve essere elevata per garantire che gli obiettivi preposti possano essere raggiunti con il minor dispendio di energie fisiche ed economiche. Per questi motivi, è stato proposto un nuovo concetto per la sicurezza denominato Safety Intelligence[28] (SI): Safety Intelligence è definita come una serie di informazioni sulla sicurezza, utilizzabili e attuabili, derivanti da un processo sistematico per l'elaborazione dei dati e delle informazioni sulla sicurezza. "SI" permette ai decisori in materia di sicurezza di prendere decisioni, essendo totalmente informati su un'ampia gamma di contesti organizzativi grazie all'integrazione di dati e informazioni interni ed esterni.

Per poter creare una struttura teorica del SI è necessario partire dalle basi di questo modello; in particolare la figura 3.1 mostra le interrelazioni esistenti tra i dati sulla sicurezza, che sono una raccolta di elementi o fatti di sicurezza utilizzabili per effettuare calcoli o misurazioni ma non collocati in un contesto dal quale si possa dedurre qualche significato, le informazioni sulla sicurezza, che rappresentano il risultato della raccolta e l'organizzazione dei dati sulla sicurezza in modo tale da stabilire relazioni tra gli elementi dei dati di sicurezza, fornendo così, un chiaro contesto e significato. Infine la Safety Intelligence, che sottolinea l'elaborazione delle informazioni sulla sicurezza, la

[28] *L'Intelligence è un'espressione che trova le sue radici in ambito militare ma la sua applicazione si estende a tutte le organizzazioni e negli studi relativi all'intelligenza artificiale, diventa un termine ombrello che include usi, strumenti, infrastrutture e pratiche per consentire l'accesso e l'analisi dei dati e delle informazioni per migliorare le prestazioni organizzative e il processo decisionale*

cui qualità è fondamentale per il processo decisionale delle organizzazioni in materia di sicurezza.

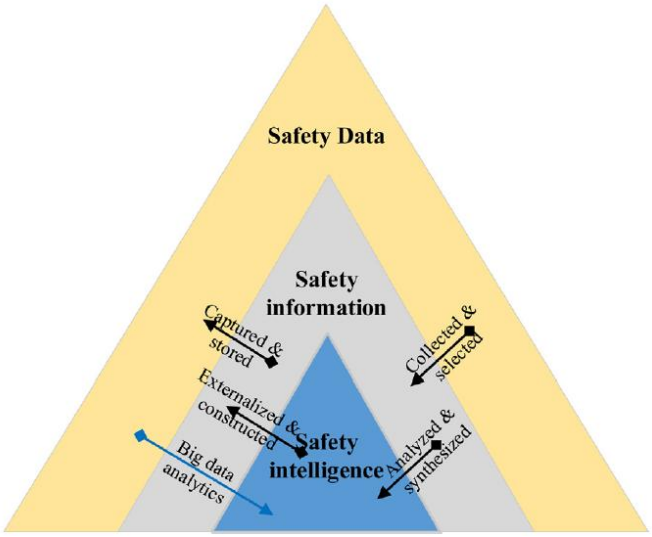

Figura 3.1 *Interrelazioni dei dati sulla sicurezza, informazioni sulla sicurezza e SI nell'era dei Big Data. <https://doi.org/10.1016/j.psep.2020.10.008.>*

La relazione gerarchica tra i dati sulla sicurezza e le informazioni sulla stessa indica rispettivamente che la qualità dei primi è un prerequisito, ma non è garanzia per la qualità delle seconde. Tuttavia si può prescindere da questi livelli gerarchici, considerando che nell'era dei Big Data, è usuale che i dati sulla sicurezza vengano trasformati direttamente in SI dall'analisi dei Big Data stessi, che permettono di avere un quadro complessivo dovuto sia ad azione esterne (leggi, regolamenti nazionali sulla sicurezza, standard di sicurezza ufficiali ecc.) che ad azioni interne (dati e informazioni del monitoraggio e ispezione della sicurezza, indicatori chiave delle prestazioni di sicurezza ecc.).

Se da un lato i responsabili della sicurezza dovranno prendere una serie di decisioni di sicurezza interconnesse tra loro e successive nel tempo, anche attraverso la programmazione di piani di sicurezza, di prevenzione e controllo dei rischi nel tempo, dall'altro lato è necessario definire i modi specifici per eseguire i piani strategici di sicurezza sviluppati. Nel dettaglio attraverso il modello Safety Intelligence, si è in grado di organizzare un buon sistema di gestione della sicurezza, il quale include tre livelli di risoluzione dei problemi, ciascuno dei quali utilizzerà i proprio strumenti e lavorerà

all'interno di dinamiche temporali differenti, che possono andare da alcuni giorni a diversi anni. Come si può evincere dalla figura 3.2, l'estremità superiore della prima piramide indica che il primo livello riguarda il SI strategico, il quale si concentra sulle tendenze a lungo termine in materia di rischi per la sicurezza, tecnologie per la sicurezza, cultura della sicurezza o potenziali minacce alla sicurezza per un'organizzazione. Questa attività prevede che venga effettuata una stima della sicurezza, anticipando così quella organizzativa futura e la gestione della medesima sulla base delle azioni di gestione passate o delle capacità di sicurezza attese.

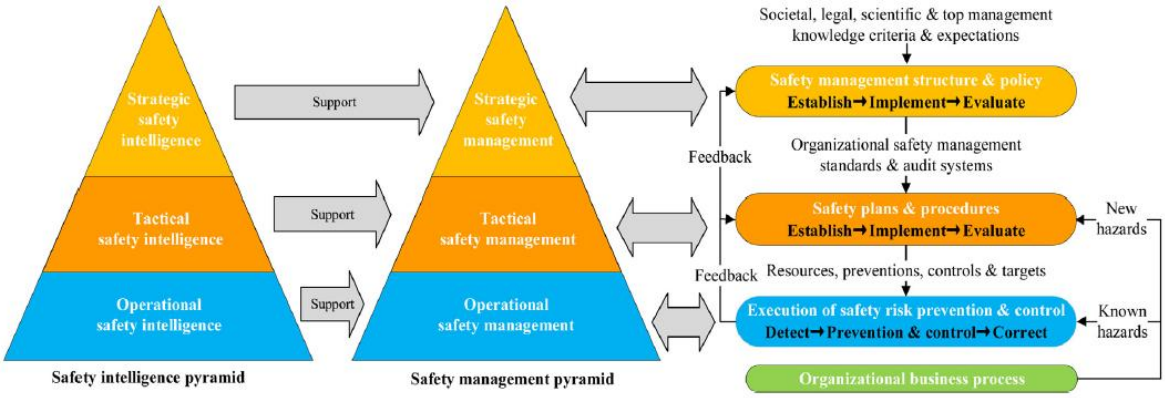

Figura 3.2 *Costruzione dei tre livelli di Safety intelligence utilizzati dai responsabili di gestione della sicurezza. <https://doi.org/10.1016/j.psep.2020.10.008.>*

È evidente che coloro che comporranno il team di gestione della sicurezza strategica, dovranno nutrire profonda esperienza in materia di sicurezza ed essere in grado di fornire notevoli intuizioni sulla gestione della sicurezza di un ambiente particolarmente dinamico. L'attività SI tattica si concentra invece sui rischi e le minacce per la sicurezza cercando di rispondere alle domande su "cosa e quando", fornendo informazioni sui piani, le procedure e le tecniche per la sicurezza. Un'efficace valutazione tattica del rischio per la sicurezza insieme ad un'adeguata analisi della gestione della sicurezza di un'organizzazione, consentono a coloro che hanno il controllo diretto sui rischi per la sicurezza, di allocare risorse cruciali in compiti critici al fine di alleviare i rischi e di adottare nei momenti più opportuni i piani di sicurezza stilati a tal riguardo.

Infine il SI operativo si concentra su tutte le attività di gestione dei rischi per la sicurezza quotidiana delle organizzazioni; si tratta quindi di operare in un intervallo di tempo che va dai secondi, in casi di pericoli imminenti, ai giorni in caso di piani di

sicurezza settimanali. Il SI operativo differisce principalmente dal SI strategico e tattico sia per scopi di gestione e promozione della sicurezza, sia per il livello di dettaglio richiesto, che per la tempestività dei dati e delle informazioni sulla sicurezza. Il SI operativo può comportare l'accesso a un sistema di transazione direttamente o tramite un data warehouse di sicurezza, che viene aggiornato quasi in tempo reale più volte durante il giorno. Il SI strategico e tattico per scopi di gestione e promozione della sicurezza può anche verificarsi quasi in tempo reale; tuttavia, possono anche essere basati su informazioni e sicurezza settimanali, mensili o annuali. Nel frattempo, i tre tipi di SI si nutrono a vicenda e ciascuno ha un impatto sull'altro tipo. Il SI strategico guida i requisiti per il SI tattico, che guida i requisiti per il SI operativo. Pertanto, SI fornisce un approccio basato sui dati per collegare gli obiettivi di sicurezza strategici delle organizzazioni a politiche di sicurezza tattiche e azioni di sicurezza operativa. Certamente, un'operazione riuscita può cambiare il quadro tattico del SI e numerose operazioni riuscite possono cambiare le prospettive strategiche di sicurezza.
Si arriva quindi a definire il modello SI concettuale che presenta sei unità (figura 3.3):

1. La prima unità mostra diversi livelli di gestione della sicurezza organizzativa (processo decisionale in materia di sicurezza) analizzati in precedenza.
2. La seconda unità indica i pool Safety Intelligence in cui tutti i dati e le informazioni sulla sicurezza raccolti vengono trasferiti. Questi pool vengono mappati secondo i tre livelli di gestione della sicurezza organizzativa.
3. La terza unità mostra il team SI organizzativo il quale dovrebbe prevedere professionisti di intelligence e della sicurezza.
4. La quarta unità è relativa al modo in cui il team SI organizzativo può contribuire alle pratiche o attività SI dell'organizzazione. Infatti, i professionisti dell'intelligence, molto spesso non hanno competenze e conoscenze in materia di sicurezza, così come i professionisti della sicurezza non dispongono di sufficienti conoscenze e competenze in materia di intelligence. Entrambi i team dovrebbero ricevere formazione relativamente alle materie che non posseggono nel loro bagaglio tecnico ed esperienziale.
5. La quinta unità del modello è relativa al SI action, ovvero una raccolta di dati e informazioni sulla sicurezza per produrre Safety intelligence
6. L'ultimo livello indica gli obiettivi SI. [13]

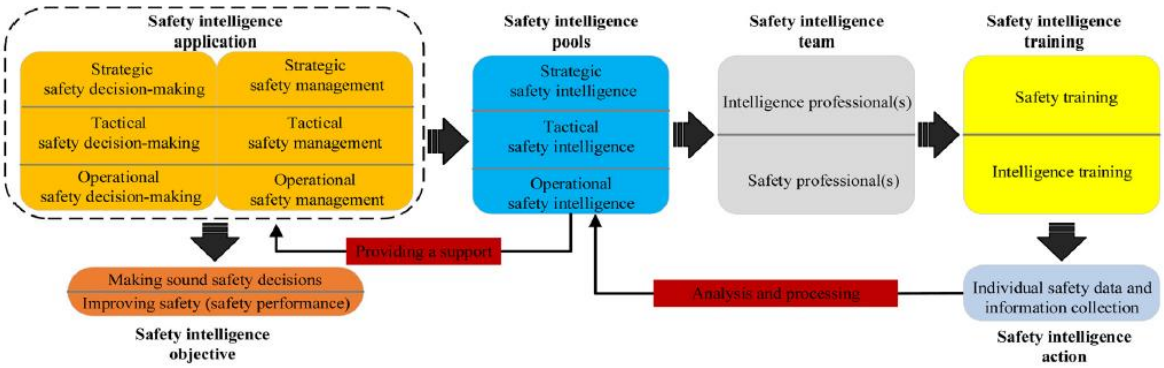

Figura 3.3 *Modello concettuale SI. <https://doi.org/10.1016/j.psep.2020.10.008.>*

3.2 Aspetti introduttivi dell'analisi del rischio

[9] evidenzia come il ciclo di vita sulla sicurezza e il rischio sia un processo molto complesso da analizzare nella sua interezza, la cui analisi di ciascuna fase è fondamentale nella riuscita di un qualsiasi progetto aziendale. In particolare questo paragrafo è focalizzato sull'analisi della prima fase del ciclo vita (Figura 3.4), che rappresenta la fase strategica e che sottolinea come "le questioni relative alla sicurezza e al rischio ambientali sono rilevanti nella fase strategica dei progetti e possono contribuire in modo determinante al rischio aziendale complessivo di un progetto. Questa fase iniziale fornisce approfondimenti sui rischi per la sicurezza associati al sistema ingegnerizzato, ai processi di costruzione e all'ubicazione del sito e permette di avere una visione di alto livello dei rischi ambientali e di sicurezza associati alle sostanze e ai processi coinvolti. Valutare questi rischi nelle prime fasi di un progetto, offre le migliori opportunità per impiegare un design intrinsecamente più sicuro."

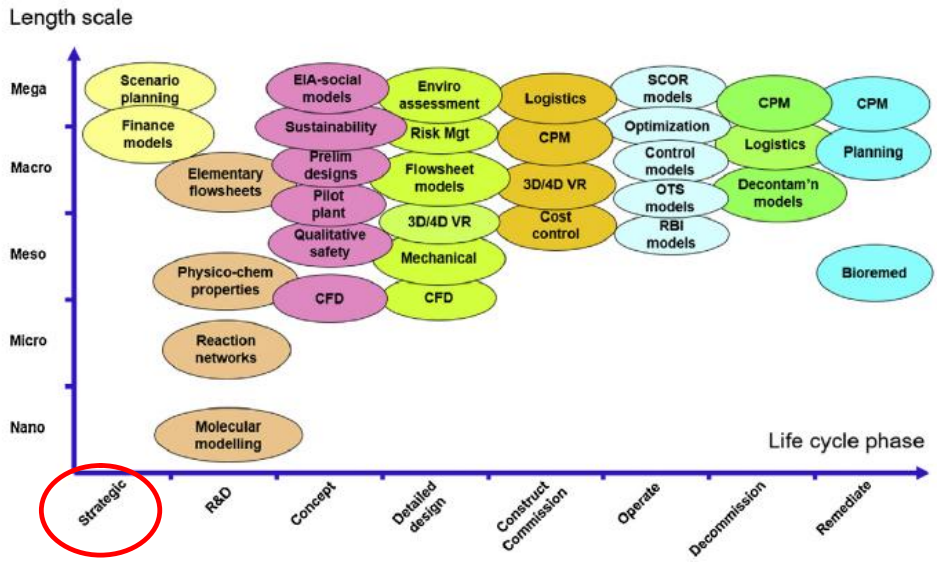

Figura 3.4 *Fasi del ciclo di vita del Process Safety. <https://doi.org/10.1016/j.psep.2019.10.021.>*

La gestione del rischio è una delle nove aree di conoscenza sottolineate dal Project Management Institute (PMI) ed è probabilmente l'aspetto più difficile del progetto, in quanto vanno considerati sistematicamente tutti i rischi relativi allo stesso, agli attori e agli attuali controlli per i rischi e le valutazioni che devono essere formulate sull'adeguatezza o meno di tali controlli. La gestione del rischio è diventata negli ultimi anni sia un fattore competitivo ma altresì anche un requisito legale che va oltre il solo obbligo morale di proteggere l'intera realtà aziendale e i propri dipendenti da eventuali pericoli.[6]

Ancor prima di entrare nel dettaglio, potremmo identificare come fase zero, l'aumento della conoscenza delle problematiche legate alla sicurezza a tutti i livelli manageriali, poiché molto spesso, soprattutto in Italia, la consapevolezza delle imprese del comparto manifatturiero e dei settori che si stanno affacciando all' industria 4.0, rispetto alla sicurezza informatica, strettamente legata alla sicurezza degli oggetti e delle persone che fanno parte dell'impresa, è relativamente bassa, mentre le minacce continuano a moltiplicarsi e ad evolversi. Per proteggere la propria azienda nel migliore dei modi, è fondamentale adottare un modello "security by design" , consistente nel progettare un'infrastruttura che prenda in considerazione le questioni rilevanti della sicurezza, ponendo particolare riguardo all'analisi e valutazione dei rischi, in modo da contemplare una revisione periodica delle scelte compiute. Così facendo, è possibile

individuare eventuali contromisure da mettere in campo.[29] È chiaro che in ambienti di lavoro molto articolati si può operare preventivamente attraverso la realizzazione di un framework di gestione del rischio di progetto basato sulle tecnologie dell'industria 4.0, in modo da porre dei paletti per la creazione di un sistema sicuro e preparato ad affrontare problematiche legate a tutti i possibili scenari di rischio.

3.2.1 Sviluppo di un framwork di Project Risk Management

Lo sviluppo di un adeguato framework per la gestione del rischio ha come prima fase lo studio del campo di applicazione e la determinazione di tutti i possibili rischi associati al progetto che si sta considerando, ciascuno dei quali viene indicato con un codice di rischio (R1,R2,….). Successivamente occorre mappare le categorie di rischio con i rischi poc'anzi identificati, tenendo conto che ogni tipologia di progetto può presentare maggiore rilevanza per determinate categorie di rischio e meno per altre. Quanto osservato in questi primi due passaggi è mostrato a titolo esemplificativo nelle tabelle 3.5 e 3.6.

codice	rischio
R1	Problemi tecnici
R2	Dettagli e specifiche di progettazione pochi chiari
R3	Mancanza di strumenti e processi semplificati
R4	Procedure complesse per ottenere approvazioni
R5	Ritardo nel completamento del progetto
R6	Rischio ambientale
R7	Mancanza di disponibilità di materiali e attrezzature
R8	Restrizione all'importazione/esportazione
R9	Cambiamenti delle leggi che regolano il settore

Tabella 3.5 *Identificazione dei rischi associati al progetto.*

[29] *<https://www.isipc.it/cuber-sicurezza-e-industria-4-0-i-rischi-e-come-affrontarli/>*

Categorie di rischio	rischio
Operativo	R1, R3, R4, R5
Tecnico	R7
Ambientale	R6
Di progettazione	R2
Rischio Finanziario	R8
Rischio politico	R9

Tabella 3.6 *Mappatura delle categorie di rischio con i rischi identificati.*

Successivamente i rischi vengono mappati nuovamente (figura 3.7), ma in questo caso con le tecnologie abilitanti dell'industria 4.0 (paragrafo 1.2), indicando con la lettera Y la circostanza in cui la tecnologia considerata aiuta a monitorare il rischio associato e con la lettera N il caso contrario.

	Industry 4.0 technologies							
Risk	Augmented reality	Big data	Cloud computing cybersecurity	Internet of Things	System integration	Additives manufacturing	Simulation	Autonomous robot
R1	Y	Y	Y	Y	Y	Y	Y	Y
R2	Y	Y	N	N	Y	N	Y	N
R3	N	Y	N	N	Y	N	Y	N
R4	N	N	Y	N	Y	N	N	N
R5	N	Y	Y	Y	Y	N	Y	Y
R6	Y	Y	Y	Y	Y	N	Y	N
R7	N	Y	Y	Y	Y	N	Y	N
R8	N	Y	Y	Y	Y	N	Y	Y
R9	Y	Y	Y	Y	Y	Y	Y	Y

Figura 3.7 *Mappatura dei rischi sulla base delle tecnologie abilitanti di industry 4.0. <https://doi.org/10.1108/BIJ-03-2019-0123.>*

Anche le tecnologie abilitanti devono essere mappate a loro volta con il processo PRM sottolineando con particolare attenzione gli step del PRM che riguardano: l'identificazione del rischio (passaggi precedenti), il risk assessment, la prioritizzazione del rischio, la risposta dello stesso e il monitoraggio.

Secondo [12], per implementare il framework PRM, è più conveniente utilizzare la tecnologia IoT (internet of things) perché è quella che ne racchiude altre come Big data,

cloud computing, simulazione, integrazione orizzontale e verticale. A seconda dell'ambito in cui si svilupperà il progetto possiamo considerare uno ad uno gli elementi di maggior interesse per la valutazione complessiva dei rischi e associare ad essi un numero relativamente basso di parametri, per non complicare troppo lo studio, che ci permettono di valutare i rischi, possibili cause della riduzione del tasso di successo del progetto. Ora, sempre a titolo di esempio, si riporta in figura 3.8 un framework PRM basato su IoT, tenendo conto che in un processo di valutazione del rischio vanno considerati molteplici attori, dal top management ai lavoratori. Inoltre, come già ampiamente discusso nei paragrafi iniziali, le realtà che hanno convertito i loro stabilimenti in vere e proprie fabbriche digitali, sono dotate di sensori, attuatori, sistemi computazionali con avanzamento integrato e applicazioni digitali intelligenti per connettere vari oggetti presenti in loco, i quali sviluppano reti digitali di oggetti nella rete locale e globale. Questa è costituita dai livelli Hardware (sensori, tag, tablet, smartphone ecc.), di comunicazione (GPS, rete geografica, IP, tecnologie WI-FI ecc.) e middleware che è essenziale per il cloud computing, l'analisi e il calcolo secondo i requisiti dell'archiviazione.

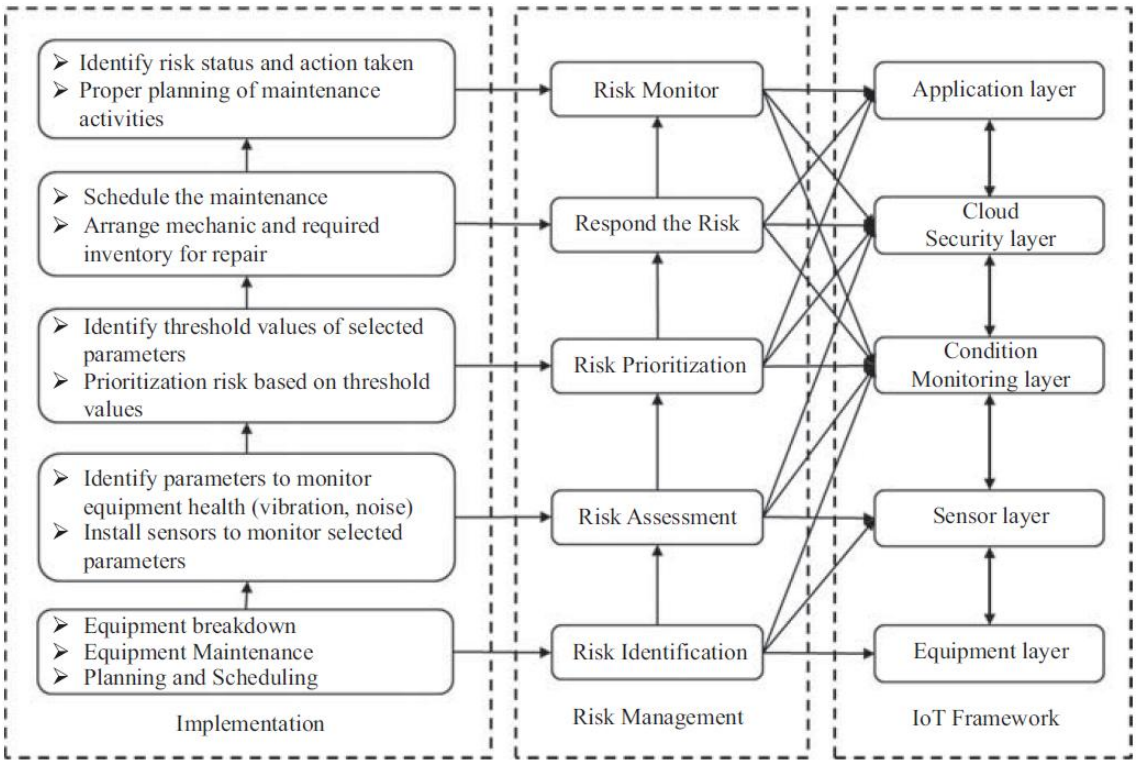

Figura 3.8 *Framework PRM basato su Internet of things. <https://doi.org/10.1108/BIJ-03-2019-0123.>*

Il processo IoT inizia con il livello dell'apparecchiatura considerata (equipment layer) che aiuta a identificare i diversi strumenti associati al progetto, proseguendo con il livello del sensore e il livello del monitoraggio che permettono di identificare il rischio connesso allo specifico elemento critico del progetto da analizzare. Termina con il livello dell'applicazione (application layer), il quale supporta il monitoraggio dell'attrezzatura relativamente ai parametri che sono stati precedentemente selezionati (es. Vibrazioni, rumori, consumi di carburante, ecc.). La cosa più importante è l'integrazione del IoT con il processo PRM per monitorare il rischio associato al progetto.

Dopodiché si passa alla definizione dei dettagli del rischio associato all'elemento critico considerato; in particolare questa fase consiste nel mettere in corrispondenza le categorie identificate precedentemente con i rischi associati all'elemento critico e i parametri selezionati per valutare l'entità di questi. Tale correlazione viene effettuata attraverso l'inserimento di determinati codici di rischio (tabella 3.9) che per semplicità vengono evidenziati con la lettera iniziale della categoria corrispondente, seguita da una numerazione progressiva per ciascuna. Tale associazione lettera-numero sarà fondamentale nelle successive fasi.

Categoria di rischio	Codice di rischio	Rischio associata alla variabile considerata	Parametri che aiutano ad identificare i rischi
Rischio Fisico	P-1 P-2	- Improvvisa rottura dell'attrezzatura(P-1) - Danno critico al componente di un'attrezzatura (P-2)	Vibrazioni Rumori
Rischio Finanziario	F-1 F-2	- Ritardo di un progetto a causa del guasto dell'attrezzatura - Aumento dei costi di manutenzione	Vibrazioni Rumori

Rischio Operativo	O-1 O-2	- Furto di carburante - Aumento del livello di vibrazione dell'attrezzatura	Consumo di carburante Vibrazioni Rumori
Rischio Ambientale	E-1 E-2	- Aumento di emissioni di CO_2 - Aumento del livello di rumore	Vibrazioni Rumori
Rischio Tecnico	T-1 T-2	- Incertezza nell'attrezzatura - Indisponibilità dell'attrezzatura	Vibrazioni Rumori

Tabella 3.9 *Rischio associato all'elemento critico del progetto.*

In questa fase del PRM si procede con la raccolta dati, di cui abbiamo discusso nel paragrafo 3.1 e che dovranno essere opportunamente gestiti e organizzati in modo da essere utilizzabili per prendere delle decisioni consone ai rischi individuati. In ogni caso devono essere considerate le attrezzature o apparecchiature che riguardano l'elemento critico considerato e sviluppare un foglio di controllo in cui sono raccolti i dati più importanti relativi ai parametri considerati nella tabella precedente. I dati sulle vibrazioni, rumori e consumo di carburante ad esempio possono essere raccolti dai sensori presenti nelle attrezzature e nelle altre zone interessate dello stabilimento al fine di raccoglierli in un file e renderli disponibili sulla rete locale. Di seguito i dati vengono archiviati nel cloud in maniera sicura in modo da poter essere condivisi con i responsabili di progetti i quali li utilizzeranno per prendere le decisioni in materia di sicurezza. Si arriva quindi ad una delle fasi più importanti che riguarda la vera e propria valutazione del rischio. In questa istanza si può applicare il metodo quantitativo quando si hanno a disposizione un numero sufficientemente elevato di dati per poter identificare il rischio critico derivante dal progetto. Qualora i dati non siano disponibili o siano insufficienti per poter applicare il metodo quantitativo si opterà per un approccio qualitativo che è esattamente quello che verrà analizzato in questa trattazione.

Un team di esperti dovrà esaminare tutte le informazioni ricavate nelle fasi precedenti e stabilire innanzitutto delle fasce di impatto del rischio, che possono andare da basso

rischio a rischio elevato, e delle fasce di probabilità del rischio, dove anche in questo caso si può andare da bassa probabilità ad elevata probabilità di rischio. Per valutare il grado di impatto e le probabilità di rischio si utilizzano i diversi livelli del framework IoT presentato in precedenza; in questo caso saranno fondamentali gli apporti dei livelli del sensore, per identificare correttamente la gravosità dei parametri su una certa attrezzatura, il livello di monitoraggio delle condizioni, per valutare se ci sono scostamenti essenziali delle condizioni di lavoro imposte come indice e il livello del cloud computing, fondamentale per i responsabili di progetto per avere a disposizione tutte le informazioni sui rischi e poter prendere le opportune decisioni.

Al termine di questa fase viene generata una matrice di valutazione del rischio (figura 3.10), che anche in questo caso è riportata solo a titolo di esempio ma potrebbe essere implementata per qualunque tipologia di progetto semplicemente adattandola alle specifiche relative, dove possiamo osservare come l'improvvisa rottura o incertezza dell'attrezzatura, rendano elevati sia l'impatto che le probabilità del rischio delle categorie di pericolo fisico e tecnico come era prevedibile aspettarsi, soprattutto in caso di studi riguardanti l'evoluzione di progetti in cantieri o stabilimenti che trattano materiali pesanti o tossici.

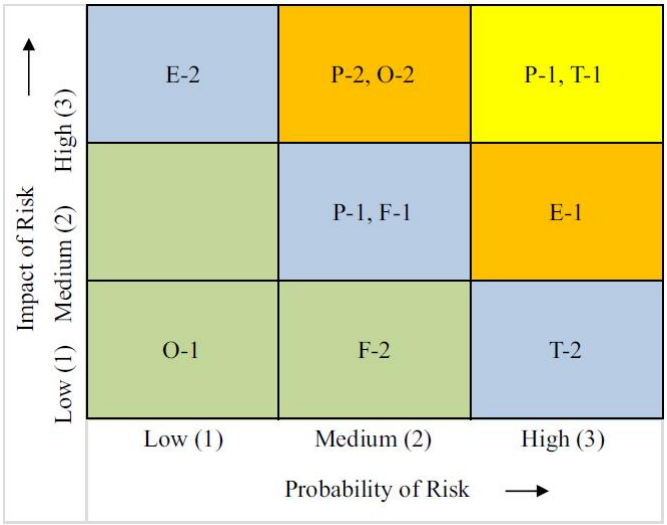

Figura 3.10 *Matrice di valutazione del rischio. <https://doi.org/10.1108/BIJ-03-2019-0123.>*

Superata la fase di risk assessment si procede con la fase di risk prioritization, nella quale viene applicato il metodo Analyitical Hierarchy Process (AHP), il quale permette

anche di confrontare le diverse alternative tra loro. AHP "è una tecnica di supporto alle decisioni multicriterio sviluppata negli anni settanta dal matematico iracheno naturalizzato statunitense Thomas L. Saaty.

La metodologia consente di confrontare più alternative in relazione ad una pluralità di criteri, di tipo quantitativo o qualitativo, ricavando una valutazione globale per ciascuna di esse. Ciò permette di:

- ordinare le alternative secondo un asse di preferenza;
- selezionare l'alternativa globalmente migliore;
- assegnare le alternative a sottoinsiemi predefiniti.

I punti di forza principali sono il confronto a coppie delle alternative decisionali e la separazione fra importanza del criterio e impatto sulla decisione."[30]

In figura 3.11 è mostrato un tipico esempio di come possono essere rappresentati i vari pesi calcolati per ciascun rischio e confrontati tra loro. Notiamo come il rischio T-1 ha ricevuto il peso massimo e conseguentemente tutti gli altri codici di rischio hanno ottenuto pesi coerenti con l'applicazione del metodo AHP. Ciò ci porta a definire quelle che sono le principali componenti di rischio coinvolte nell'elemento critico analizzato, che godranno di priorità di trattamento rispetto alle altre e che nella successiva fase saranno soggette a delle azioni di risposta per essere mitigate ed eventualmente eliminarle del tutto.

[30] *<https://it.wikipedia.org/wiki/Analytic_Hierarchy_Process>*

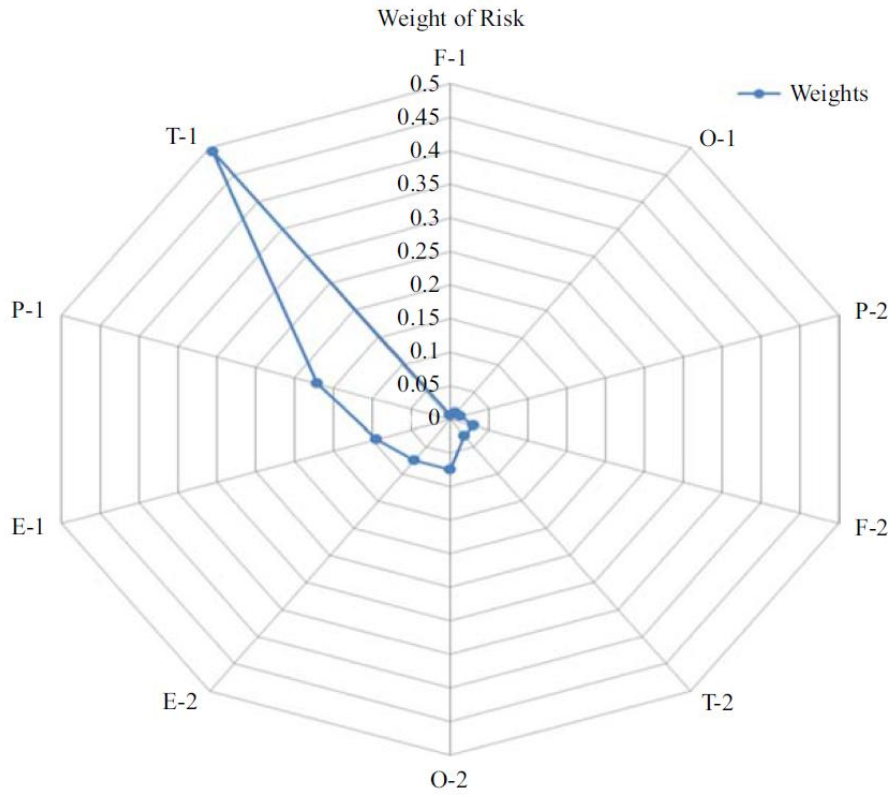

Figura 3.11 *Diagramma Radiale che rappresenta i pesi per ciascun codice di rischio e ne consente il confronto. <https://doi.org/10.1108/BIJ-03-2019-0123.>*

Una volta identificati i rischi prioritari, occorre studiare dei metodi di risposta a tali problematiche che permettono di ridurre sia l'impatto del rischio che le probabilità del pericolo stesso e in alcuni casi di eliminarli.[12]

In particolare, dall'analisi dei pericoli o attraverso l'esame delle norme (paragrafo 2.2) che regolano la sicurezza negli ambienti industry 4.0, o di quelle relative al funzionamento dei macchinari, vengono definiti i safety requirements che vanno implementati in un gemello digitale e che dovrebbero essere associati a contratti di sicurezza supportati da una o più prove relative ai "safety cases" affrontati, in modo da garantire la sicurezza dinamica dell'ambiente industry 4.0.[13]

La tabella 3.12, sviluppata sulla base di analisi dei rischi effettuate sul campo e attraverso l'ausilio delle tecnologie abilitanti poste in antitesi con le norme standard relative al campo applicativo, mostra un esempio di risposta alle criticità.

Sr. no.	Risk	Response
1	Uncertainty in equipment	Develop a system for real-time monitoring of equipment performance Monitor the equipment parameters (fuel consumption, noise and vibration) on real time Monitor the equipment maintenance activities intensively
2	Sudden break down of equipment	Develop a mechanism to monitor performance parameters of equipment Perform and check schedule maintenance activities
3	Increase in CO_2 emission	Develop a system for real-time monitoring of fuel consumption and CO_2 emission
4	Increase in noise level	Monitor noise and vibration level of equipment
5	Increase in vibration level of equipment	Monitor noise and vibration level of equipment

Tabella 3.12 *Esempio di Risposte prodotte per affrontare alcuni rischi critici di progetto.* *<https://doi.org/10.1108/BIJ-03-2019-0123.>*

L'ultima fase del PRM è, in realtà, una fase che non si esaurisce immediatamente ma è continuativa in un processo di valutazione dei rischi aziendali e di progetto: si tratta della fase di monitoraggio dei rischi dove, i dati in tempo reale, vengono confrontati con il limite superiore e inferiore dei parametri selezionati al fine di controllare il rischio coinvolto nel progetto. Inoltre, effettuando il controllo dell'intero processo di gestione del rischio, si cerca di identificare quelli che possono essere i rischi emergenti, studiando quindi i metodi per gestirli. Dunque, ad esempio, sono stati impostati dei range quantitativi (qualora sia stata effettuata una modellazione quantitativa) entro i quali si devono trovare i parametri analizzati (es. livello di rumore non deve superare una certa soglia di decibel). Qualora si verifichi il superamento di questi range, verranno applicate le soluzioni preposte alla riduzione o all'eliminazione della problematica creatasi. [12]

3.3 Fase operativa del Safety Management System

A valle della "filiera" del sistema di sicurezza, i responsabili sono chiamati a recepire tutte le informazioni sui rischi di progetto ed operare attraverso l'ausilio delle tecnologie abilitanti per raggiungere gli obiettivi di sicurezza prefissati. Per ottenere e migliorare la gestione della sicurezza, si propone di seguire un modello che analizza quattro aspetti fondamentali identificati da Teaching (insegnamento), Ergonomics (ergonomia),

Communication (comunicazione), Human Values (valori umani), le cui iniziali sono il risultato della denominazione del modello "TECH"[15]:

La fase di insegnamento è alla base di qualunque attività in quanto si è registrato che più dell'85% degli infortuni sul lavoro sono causati principalmente da comportamenti che causano situazioni di pericolo da parte del personale. Abbiamo visto come gli operatori si trovano ad essere più motivati in un contesto lavorativo se coinvolti nell'obiettivo principale dell'organizzazione e questo può influire positivamente, se il messaggio viene trasmesso, o negativamente, se i lavoratori non si sentono parte integrante dell'impresa. Quindi il comportamento può essere indirizzato principalmente fornendo consulenza e formazioni adeguate su come il loro modello comportamentale possa influire sull'ambiente sicuro dell'organizzazione. In particolare, la prima attività da svolgere in qualunque industria è garantire che le persone che lavorano siano formate all'adeguata conoscenza delle pratiche operative standard e sicure, insieme ai vari pericoli coinvolti in una determinata attrezzatura/processo.

In questo step intermedio, l'adozione di sistemi di realtà virtuale nei principali luoghi di lavoro, permetteranno al personale, ma anche a visitatori esterni, di comprendere a fondo il processo e le varie precauzioni di sicurezza che devono essere seguite prima di operare o avvicinarsi alle attrezzature. Agli operatori devono essere forniti tutti i dati utili sull'intero processo di cui sono responsabili; se attraverso l'evoluzione della tecnologia fornire dati è divenuta una pratica più semplice rispetto al passato, interpretarli è, in termini di sicurezza, diventata la vera competenza. Ecco quindi come la formazione di base e avanzata, sui pericoli che potrebbero verificarsi qualora accadessero determinati eventi, si potrebbe realizzare attraverso i cosiddetti moduli di formazione online. Essi devono essere sviluppati in dettaglio su tutti i processi coinvolti in un particolare luogo di lavoro e i dipendenti devono essere aggiornati con i programmi di formazione basati sui loro livelli di QI. Ulteriori strumenti di insegnamento riguardano le schede informative intelligenti che recuperano i dati dal server centrale e aggiornano i dipendenti sulle varie precauzioni e istruzioni di sicurezza durante il lavoro in officina, al fine di trasmettere le informazioni nel più breve tempo possibile. I sistemi di monitoraggio online per la sicurezza possono essere rafforzati attraverso le tecnologie, permettendo il controllo dello stato dei vari componenti (es. i dati di ricarica delle batterie degli AGV, le date di ultimo utilizzo, i luoghi principali in

cui vengono utilizzati gli estintori ecc.) e se necessario l'avvio di azioni correttive necessarie. Infine sistemi di telecamere Thermo-vision possono essere installate in tutti gli impianti critici e soprattutto in aree non presidiate per il monitoraggio e la comunicazione di eventuali anomalie ai responsabile in modo da prevenire guasti o incidenti molto gravi. Quando si parla di ergonomia, si fa riferimento generalmente alla scienza di progettare il lavoro per adattarsi alle capacità dei lavoratori migliorandone il benessere. Un luogo di lavoro che presenta cattive condizioni di lavoro, può causare ulteriore stress sui lavoratori, specialmente se questi sono impegnati in delle linee di produzione o assemblaggio totalmente manuali, i cui tempi di esecuzione delle attività devono essere strettamente rispettati, comportando quindi la riduzione della loro produttività che influenzerà negativamente l'andamento degli obiettivi aziendali. L'aspetto ergonomico è dunque fondamentale in qualsiasi tipo di contesto lavorativo; volendo amplificare il valore di questo concetto, basti pensare al caso di un'industria siderurgica: le operazioni che devono essere effettuate dagli operatori all'interno degli stabilimenti sono molteplici e vanno dalla movimentazione di materiali, saldatura dei materiali, controllo di qualità e arrivano fino alla progettazione computerizzata delle strutture in acciaio. Questi impieghi richiedono una grande varietà di posture e movimenti da parte dei lavoratori i quali devono essere assistiti dalla tecnologia, che sotto forma di automazione, può eliminare numerosi rischi ergonomici per i lavoratori. Le principali soluzioni innovative possono riguardare l'implementazione di "Ekso Vests" o "Ekso skeletons" (figura 3.13) per supportare attività ripetitive e che si svolgono prevalentemente con le braccia poste al di sopra del capo, richiedendo uno sforzo fisico maggiore. Si tratta di Giubbotti che supportano il peso delle braccia dei lavoratori e li aiutano a svolgere compiti che vanno dall'altezza del torace alla testa. Sono molto leggeri, poco ingombranti e consentono libertà di movimento in qualunque direzione.

Figura 3.13 *Ekso vest. <https://www.digitalengineering247.com/article/exoskeletons-on-the-move>*

Questa soluzione copre molte aree di applicazione oltre quella citata, che possono riguardare il montaggio automobilistico, in particolare per i marchi di lusso dove alcune attività di assemblaggio vengono effettuate manualmente, oppure ad esempio la manutenzione di impianti elettrici, soprattutto se si tratta di operare in impianti in altezza che portano le condizioni di lavoro ad un maggiore stress psico-fisico per l'operatore.

Altre soluzioni per migliorare l'ergonomia vanno dai "tappetini ergonomici" che consentono di limitare il tempo che l'operatore deve trascorrere in piedi, fino all'introduzione di droni di monitoraggio ed ispezione nelle aree in cui l'accesso dell'uomo e sfavorevole o sconsigliato. Quest'ultima soluzione è particolarmente interessante non solo per limitare l'ingresso in zone che possono mettere in pericolo l'incolumità dell'uomo ma anche per avere risultati migliori nel processo in se, grazie alla possibilità di utilizzo a distanze molto ravvicinate dall'attrezzatura operativa. Infine, quando si tratta di monitorare superfici in rapida rotazione, lo stroboscopio può essere una soluzione adeguata per ridurre ulteriormente il rischio derivante da azioni sbagliate da parte dei dipendenti preposti a effettuare il controllo.

Il terzo aspetto da tenere presente è la comunicazione che deve essere utilizzato dai manager come strumento per raggiungere il duplice obiettivo relativo alla produttività e alla sicurezza. La tecnologia deve essere sviluppata e gestita per evitare in ogni modo che le informazioni relative ai processi e alla sicurezza vengano mal comunicate o addirittura perdute a causa di problemi di comunicazione. Le principali soluzioni innovative a tal proposito riguardano l'utilizzo di un'app mobile denominata "SPA-SPOT, POST and ACT", la quale permette la visualizzazione da parte di tutti i diretti interessati, delle informazioni in tempo reale e di conseguenza crea la possibilità di effettuare eventuali azioni correttive senza perdite di tempo. Oltretutto, questa piattaforma consente di identificare i lavoratori e lo stato di avanzamento delle relative mansioni in modo che il top management possa avere in qualunque istante la situazione sotto controllo. L'elemento più importante dell'utilizzo di questo strumento è la prevenzione di incidenti mortali durante operazioni di fine manutenzione che possono avvenire a causa di una mancata o errata comunicazione dell'accensione dell'alimentazione. Questa grave problematica può essere risolta attraverso l'elaborazione di un sistema di autorizzazione di accesso alla linea che deve essere comunicato attraverso un dispositivo mobile da parte del manutentore, il quale, una volta terminata l'operazione di manutenzione, rilascia il permesso di accendere l'alimentazione. Un altro strumento, più comune, in ambienti industry 4.0 è rappresentato dall'identificazione con tecnologia RFID (Radio-frequency) il quale dovrebbe essere applicato, oltre che per la movimentazione degli AGV, anche negli estintori, permettendo la rilevazione delle posizioni e dello stato di "salute" in tempo reale.

L'ultimo elemento del modello riguarda i valori umani. Molte aziende dichiarano la sicurezza come elemento di massima priorità ma non la definiscono un valore fondamentale. È molto importante invece che i valori guidino le persone su ciò che è positivo e su ciò che non lo è in modo da renderli più stabili e che abbiano un impatto più sostenibile sulla sicurezza. Le soluzioni che vengono portate a tal proposito riguardano elmetti protettivi intelligenti, i quali possono sostenere gli ingegneri attraverso l'ausilio di telecamere, sensori di gas pericolosi e accelerometri. Sono dotati inoltre della tecnologia Geofencing che fornisce un sistema di localizzazione all'interno

dell'impianto e rileva se il datore di lavoro si trova in un'area nota per essere pericolosa, segnalandolo attraverso segnale acustico o altri metodi a seconda del livello di sofisticatezza. I sistemi biometrici vanno introdotti in tutte le gru, carrelli elevatori, apparecchiature rotanti ad alta velocità e veicoli pesanti in generale per garantire che il personale autorizzato ed esperto li utilizzi solo attraverso il consenso della direzione, evitando così incidenti causati da personale non autorizzato che utilizza un'apparecchiatura senza alcuna conoscenza in merito al funzionamento.

Le uscite e i percorsi d'emergenza sono progettati principalmente per proteggere i dipendenti nel caso di eventuali incidenti imprevisti e devono essere portati sotto la "sorveglianza CCTV[31]", in modo da poter eseguire un'ispezione periodica di tutti i percorsi all'inizio di ogni turno da un singolo punto, avviando immediatamente un'azione correttiva. Da ultimo la marcatura del pavimento è il processo di utilizzo di segnali visivi come linee, forme e segni sulla pavimentazione, per rendere più facile la navigazione in uno spazio per le persone. La segnaletica orizzontale viene solitamente realizzata utilizzando vernice o prodotti adesivi i quali, a causa delle condizioni di lavoro industriali avverse, si usurano e diventano meno visibili in un breve periodo. Questa problematica può essere risolta adottando segnalazioni luminose di sicurezza che posso accendersi in presenza di persone e possono offrire una soluzione unica. Tali illuminazioni agiscono come un importante segnale di attenzione per i soggetti e sono di grande utilità nelle aree in cui la luce scarseggia e di conseguenza il personale non è in grado di rilevare il percorso sicuro.[15]

[31] *Telecamere di sorveglianza a circuito chiuso.*

3.3.1 Il software W-ARTEMYS applicato al caso Parmalat e GEA Procomac

In [16] viene proposto uno strumento tecnologico per aumentare la sicurezza dei dipendenti durante le operazioni sulle macchine attraverso la gestione all'interno di W-ARTEMYS, di tutte le informazioni provenienti dai manuali delle macchine e consentendo all'operatore di utilizzare il software su un dispositivo mobile, abbinato ad una soluzione di realtà aumentata. Il software W-ARTEMYS prende in considerazione 5 tra le tecnologie abilitanti dell'industria 4.0 come segue:

- I Big Data vengono estrapolati dai server aziendali, elaborati e inviati sotto la veste di informazioni al dispositivo mobile, che comunicherà le anomalie e consentirà una rapida risposta da parte dell'operatore o del responsabile.
- L'utilizzo di simulazioni 3D, create digitalmente o ricostruite attraverso prove sul campo, aiuteranno l'operatore a svolgere tutte le attività in modo sicuro e veloce.
- L'internet of things viene utilizzato per collegare il database ottenuto dalla macchina, allo smartphone e alla ricerca della procedura desiderata; con un QR code ed eventualmente con dei chip integrati nei componenti, sarà possibile identificare in modo rapido e preciso le informazioni desiderate.
- La sicurezza informatica è di fondamentale importanza quando il software verrà installato su un server esterno all'azienda. Lo scambio dati tra i server deve essere completamente protetto da possibili attacchi esterni e anche nel caso in cui il software venga installato internamente, la natura wireless dei dispositivi utilizzati richiede la progettazione sicura della rete WI-FI. Inoltre, per garantire la sicurezza del sistema, il software raccoglierà soltanto i dati da un database situato in un server mirror[32], evitando uno scambio diretto di informazioni con le macchine.
- Il cloud è alla base della progettazione del supporto digitale trattato. Le informazioni non verranno salvate localmente sul dispositivo utilizzato, ma di

[32] *I server mirror sono la copia esatta dei server "madre" sui quali vengono caricate le versioni originali dei file e ospitano un contenuto digitale replicato diverse volte con una tecnica mirroring web, in modo da renderlo disponibile online. <https://www.fastweb.it/internet/mirroring-web-cos-e-e-come-funziona/>*

volta in volta verranno scaricate solo le informazioni richieste; in questo modo i dispositivi mobili utilizzati dagli operatori saranno liberi da problemi di memoria e oltretutto i file esistenti potranno essere continuamente aggiornati semplicemente sostituendo quelli caricati nel server cloud.

Il passo conclusivo nello sviluppo di W-ARTEMYS è l'implementazione della realtà aumentata, al fine di utilizzare il dispositivo come supporto per risolvere procedure più complesse. Il funzionamento del software si basa inizialmente sull'esecuzione di un login amministratore, il quale consente di lavorare sul "back end"[33] del software, ad esempio permettendo la modifica della posizione dei file o l'inserimento di nuovi e di un login utente, utile per navigare all'interno dell'app, cercare un file specifico e visualizzarlo. Il software ha un'architettura ad albero, dove ogni decisione porta a scelte successive, fino al livello finale. La versione attualmente sviluppata del software presenta quattro livelli, i quali includono cartelle i cui nomi sono stati selezionati per comprendere al meglio il relativo contenuto e riconoscere rapidamente il livello in cui si trovano:

1. Livello 0: è il livello che riflette il desktop di un pc e permette di creare e posizionare su di esso un insieme infinito di "oggetti principali". Per ogni oggetto si consiglia di aggiungere una descrizione, in modo da illustrarne il contenuto. Allo stesso modo, i contenuti appropriato dovrebbero essere condivisi con l'assistente vocale il quale ne migliorerà l'esperienza utente. Una volta completata la descrizione e assegnati un'immagine di riferimento e un colore, è possibile caricare l'oggetto principale sull'applicazione e renderlo visibile all'utente. Per ogni oggetto principale è stato creato un QR code ed è possibile utilizzarlo per recuperare più rapidamente le relative informazioni. La selezione di un elemento tra quelli creati permette di accedervi e di conseguenza entrare in quello che andremo a definire "livello 1".
2. Livello 1: in questo livello è possibile inserire una serie di cartelle (sezioni) e collegarle all'oggetto principale di livello 0. Contemporaneamente, all'interno di

[33] *Nel campo della progettazione software e sviluppo software il front end è la parte di un sistema software che gestisce l'interazione con l'utente o con sistemi esterni che producono dati di ingresso (es. interfaccia utente con un form), il back end è invece la parte che elabora i dati generati dal front end. <https://it.wikipedia.org/wiki/Front-end_e_back-end>*

un oggetto principale possono essere inseriti anche dei file di tipo diverso come foto, video, audio, documenti 3D e pdf. La creazione di una nuova sezione richiede quasi gli stessi passaggi dell'oggetto principale, con la differenza che la descrizione richiesta a questo livello è limitata al titolo e alle parole chiave.

3. Livello 2: si tratta del contenuto delle sezioni create nel precedente livello e inoltre include un ulteriore set di cartelle chiamate "aggregati" i quali consentono di concentrarsi su un elemento specifico. Il livello 2 è l'ultimo livello in cui l'utente può creare cartelle. Per ogni aggregato creato va inserita una descrizione completa, insieme ad elementi utili all'assistente vocale e anche in questo caso è possibile creare un QR code e utilizzarlo per accedere direttamente ad un aggregato e alle relative informazioni.
4. Livello 3: In questo livello non è consentito creare ulteriori cartelle ma possono essere aggiunti soltanto file.

Per valutare le potenzialità del software e identificarne possibili problematiche nella sua implementazione, si è deciso di verificarne il suo utilizzo su una macchina reale. L'applicazione è stata pianificata su un monoblocco di riempimento, prodotto da GEA Procomac e installato nel sito Parmalat di Collecchio. Per organizzare al meglio la struttura della web-app è stata necessaria la collaborazione di entrambe le attività. I file all'interno del software vengono creati sulla base dei manuali utente e delle informazioni ricevute dal personale tecnico delle due aziende.

Passando al sistema, il blocco di riempimento asettico in esame è costituito da 5 macchine (analizzate in tabella 3.14), che trattano contenitori sotto forma di bottiglie di plastica di diverse dimensioni.

Sterilizzatore per bottiglie	Le bottiglie vengono portate alla macchina tramite cinghie ad aria. Qui una serie di pinze afferrano le bottiglie e le ruotano sugli ugelli, fissati sopra una giostra rotante. Durante la rotazione, gli ugelli spruzzano una soluzione sterilizzante all'interno delle bottiglie
Sciacquatrice	è simile alla macchina precedente, con la principale differenza che in questo caso viene utilizzata acqua sterile per rimuovere ogni traccia di fluido lasciato dal processo di sterilizzazione
Sterilizzatore capsule	Proprio come le bottiglie, anche le capsule devono essere perfettamente sterilizzate prima di entrare nel monoblocco
Filler	È il cuore del monoblocco: qui le bottiglie vengono riempite con il prodotto prima di essere tappate. L'intero processo deve essere eseguito in un ambiente totalmente asettico
Tappatore	Una volta completato il riempimento, le bottiglie vengono spostate su questa macchina. I morsetti sulla giostra rotante della macchina tappatrice afferrano e sostengono i contenitori mentre le teste tappatrici, comandate da motori brushless, avvitano la capsula con la corretta coppia di serraggio. Al termine della procedura le bottiglie tappate escono dal monoblocco

Tabella 3.14 *Funzioni delle 5 macchine che costituiscono il blocco di riempimento.*

Oltre alle cinque macchine sono necessari anche sistemi ausiliari per il corretto funzionamento del sistema: L'unidox che prepara l'acido peracetico e il perossido di ossigeno necessari per il monoblocco di riempimento, l'Unitherm che ha una funzione simile alla macchina precedente sebbene il suo compito principale sia quello di fornire acqua sterile all'impianto e l'Uniflux che è il sistema responsabile del trattamento e della sterilizzazione dell'aria compressa. All'interno della web-app W-ARTEMYS, il primo passo è stato quello di scegliere un'adeguata suddivisione dei compiti nel sistema, aiutando così i dipendenti nella ricerca dei file desiderati:

al livello 0 sono stati posizionati 8 oggetti principali; quattro di loro hanno una suddivisione articolata mentre i restanti quattro forniscono semplici informazioni di supporto e di conseguenza incorporano ulteriori sezioni sotto di loro. Successivamente, per mantenere ordinata la suddivisione negli oggetti principali, sono state create un massimo di cinque sezioni.

A livello di aggregati, invece, è stata realizzata una scomposizione più complessa, per consentire all'operatore di scegliere con precisione l'argomento desiderato, evitando informazioni fuorvianti. Questa decisione è stata presa anche in modo tale che fosse preferibile creare un file in modo mirato su ogni rischio presente in ogni piccola operazione e oltretutto per la necessità di caricare piccoli file. Infatti, la natura cloud del software richiede il download continuo del file richiesto da parte dei dipendenti, il che è coerente con quanto stabilito.

Come mostrato in figura 3.15 la struttura W-ARTEMYS è piuttosto articolata ed in particolare il primo livello presenta le seguenti sezioni:

- Documentazione generale: contiene documenti generali sulle diverse parti della macchina;
- Cambio formato: le operazioni di cambio formato coinvolgono diverse sezioni del monoblocco di riempimento;
- Inconvenienti degli allarmi e procedure di ripristino: Attraverso l'acquisizione del database aziendale sarà possibile visualizzare in tempo reale un allarme del monoblocco; se necessario, l'operatore incaricato potrà richiamare la relativa procedura di ripristino inserita nel software;
- Controlli meccanici periodici: le verifiche periodiche vengono eseguite e descritte dal costruttore dell'impianto (GEA procomac) al fine di garantire le corrette condizioni di funzionamento del monoblocco di riempimento. Qualunque sia l'origine delle procedure, le verifiche meccaniche vengono eseguite in base al numero di ore di lavoro dell'impianto; gli aggregati sono stati quindi suddivisi in modo tale che al loro interno siano caricati dei file relativi alle specifiche attività di manutenzione da eseguire;
- Controlli elettrici periodici: il principio di base è identico alla sezione precedente. I controlli meccanici ed elettrici sono stati distinti perché possono comportare diverse tipologie di pericolo e necessitano di tecnici specializzati.

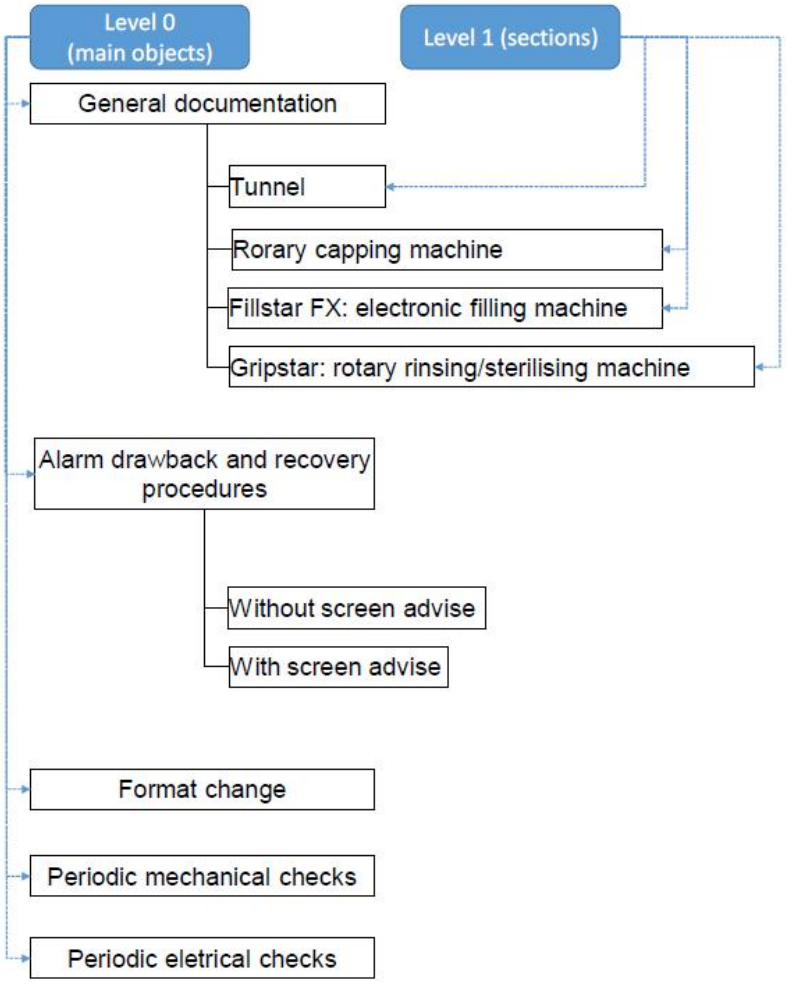

Figura 3.15 *Livello 0 (oggetti principali) e livello 1 (sezioni) del software W-ARTEMYS applicato al caso Parmalat e GEA Procomac. <https://doi.org/10.1109/ICE.2019.8792814.>*

Costruendo la struttura a quattro livelli (figura 3.16), sono state rilevate alcune difficoltà durante la navigazione nella struttura del software. Infatti, la struttura a quattro livelli non sarebbe stata adatta a rappresentare idoneamente un impianto più complesso. Non a caso in presenza di impianti molto articolati potrebbe rendersi necessaria la creazione di un quinto livello che individua un'ulteriore suddivisione dell'impianto in funzione delle diverse macchine. Per fare una valutazione oculata del software che si vuole sviluppare occorre fare uno studio completo in quanto il valore dell'investimento potrebbe crescere sensibilmente.

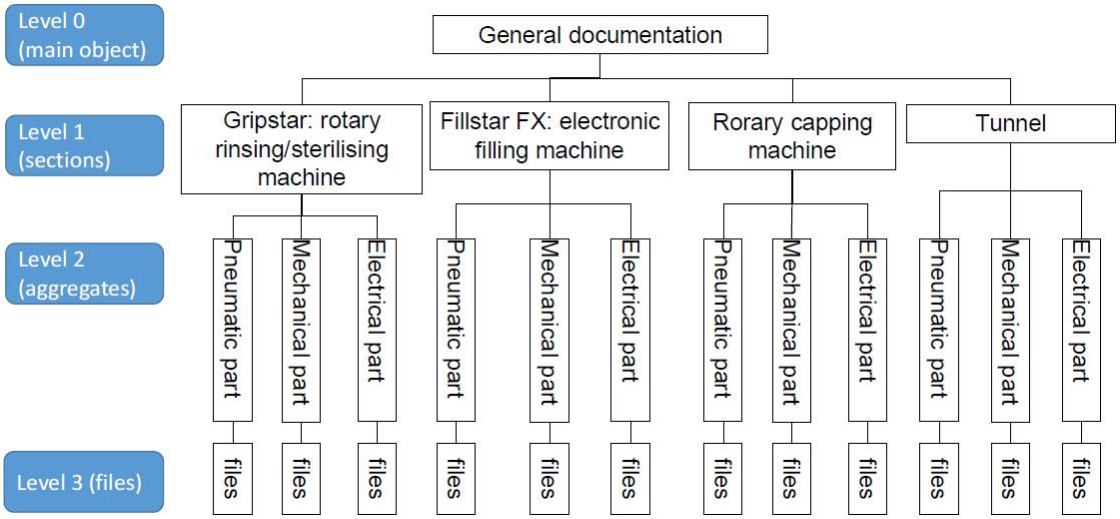

Figura 3.16 *Esempio di scomposizione dei livelli della web-app W-ARTEMYS con oggetto principale "documentazione generale"nel caso studio. <https://doi.org/10.1109/ICE.2019.8792814.>*

Tornando al caso di studio, un'ulteriore problematica è stata rappresentata dalla possibilità di inserimento dei file nel primo e nel terzo livello. Durante l'incontro con GEA Procomac, per alcuni argomenti, si è deciso di creare un solo oggetto principale e sezioni dove mettere i relativi file. Questa situazione è stata realizzata con un oggetto principale originariamente chiamato "Allarmi e problemi comuni" (e attualmente sostituito da "Ritiri di allarme e procedure di ripristino") che avrebbe dovuto tenere conto di tutti gli allarmi visualizzati dalla macchina e di alcuni dei problemi che possono verificarsi durante il funzionamento della macchina. La struttura inizialmente ipotizzata per questo oggetto principale (Figura 3.17, parte superiore) comprendeva allarmi e guasti come sezioni di livello 1. Quindi, all'interno di ogni elemento di allarme/ guasto, sarebbero stati posizionati i file dettagliati. Questa struttura, tuttavia, non era consona con la struttura a 4 livelli della piattaforma W-Artemys e in particolare non soddisfaceva i requisiti del livello 3, dove è possibile caricare solo file. Per ovviare a questo problema è stato aggiunto un ulteriore livello di sezioni, contenente allarmi "di tipo XXX", raggruppando ciascuna categoria di allarmi (o anomalie) con caratteristiche simili. La figura 3.17 mostra la soluzione descritta per consentire il corretto caricamento dei file nel livello 3 del sistema.

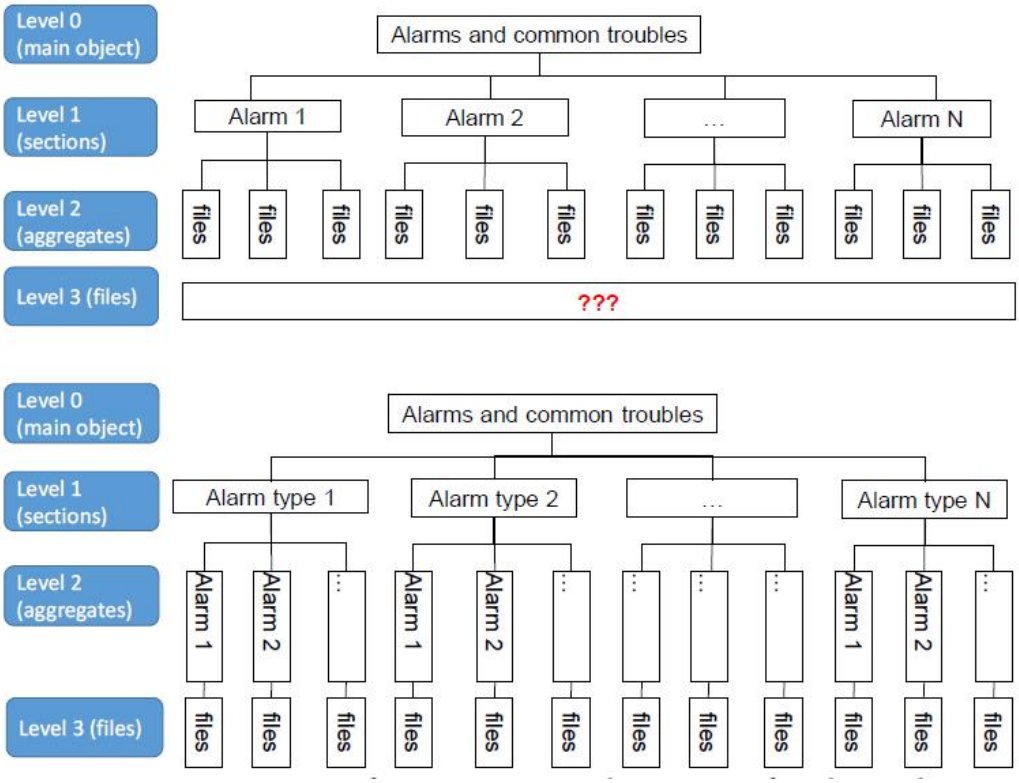

Figura 3.17 *Confronto di due architetture di sistema per l'oggetto principale "allarmi e guasti comuni". <https://doi.org/10.1109/ICE.2019.8792814.>*

3.3.2 Il digital twin OTS per la simulazione del sistema di sicurezza

L'effettiva implementazione della fase finale del ciclo di vita della sicurezza (paragrafo 3.1) può essere realizzata attraverso l'utilizzo di un gemello digitale, ossia una rappresentazione virtuale di un'entità fisica o di un sistema anche complesso, il quale integrando alcune tecnologie dell'industria 4.0, replica fedelmente il comportamento del sistema fisico che sta analizzando, apprendendone le dinamiche di funzionamento e proponendo variazioni, nel nostro caso in ambito di sicurezza (ma è funzionale per molteplici dinamiche), rispetto ai possibili scostamenti indesiderati del sistema dalle condizioni di sicurezza instaurate attraverso l'implementazione delle tecniche e degli strumenti discussi. Si è evidenziato come la sicurezza di un ambiente industry 4.0, seppur concernente tecnologie altamente digitalizzate, sia ancora focalizzata ampiamente sul comportamento degli attori che operano nell'intero complesso produttivo aziendale; tale circostanza rende essenziale l'impiego di un simulatore dinamico OTS (Operator Training Simulator) che è rivolto a operatori di impianto,

quadristi, supervisori di processo con l'obiettivo di addestrare gli utenti ad acquisire familiarità con il sistema di controllo, intervenire prontamente nel caso in cui si verifichino malfunzionamenti di apparecchiature di impianto e sperimentare condizioni di funzionamento dell'impianto che normalmente rimangono in esplorate. Un OTS in linea di principio dovrebbe rappresentare con buona approssimazione il comportamento dell'impianto reale, riprodurre fedelmente l'interfaccia operatore e rappresentare l'intervento dei sistemi di emergenza e di sicurezza. La riproduzione più o meno fedele del comportamento dinamico del processo dipende dalla complessità e accuratezza dei modelli matematici che vengono utilizzati. In relazione all'uso che se ne deve fare, il simulatore può fornire una semplice rappresentazione degli andamenti generali del processo o può descrivere dettagliatamente il sistema sia in termini di ampiezza delle risposte che di costanti di tempo. In genere i sistemi di simulazione si basano su bilanci di materia e di energia e su altre formulazioni matematiche che descrivono la dinamica del processo. I modelli matematici dei processi e delle apparecchiature sono parametrizzati in modo da tener conto della variabilità delle caratteristiche fisico-chimiche e della geometria delle diverse sezioni dell'impianto. La sintonizzazione dei parametri consente di adattare i modelli all'impianto specifico che si desidera simulare. Teoricamente è possibile rendere la risposta dei modelli sempre più prossima a quella dell'impianto reale, sia sintonizzando opportunamente i parametri di tuning, che aumentando la complessità dei modelli stessi. D'altra parte è necessario trovare il giusto compromesso tra accuratezza del modello e costi di sviluppo e manutenzione.
L'addestramento degli operatori ad affrontare condizioni insolite garantisce, oltre che un maggior livello di sicurezza, anche una riduzione dei blocchi di impianto e delle perturbazioni al sistema; la maggiore continuità di esercizio che ne consegue si traduce in risparmi economici che contribuiscono a ripagare in tempi brevi il costo del sistema di simulazione.

Il simulatore è realizzato mediante l'utilizzo di modelli matematici a principi primi, ossia bilanci di materia e di energia applicati alle singole apparecchiature e corredato di espressioni empiriche che contribuiscono a descrivere la dinamica del processo. Per garantire un'adeguata flessibilità al sistema di simulazione, esso è concepito in maniera modulare dove ogni modulo rappresenta una singola apparecchiatura e i singoli moduli

vengono assemblati per rappresentare l'impianto che si desidera simulare. La calibrazione/tuning dei parametri avviene mediante un confronto con dati reali di impianto e la sintonizzazione, che rappresenta uno degli aspetti più critici e per tal motivo sono stati sviluppati recentemente dei metodi di sintonizzazione automatica, riguarda l'interazione tra i diversi parametri del sistema di simulazione, che permette di stabilire quanto fedelmente si è in grado di rappresentare il sistema.
Un buon simulatore, oltre che rappresentare il comportamento dinamico del processo deve anche riprodurre con sufficiente fedeltà l'intervento dei sistemi di emergenza e di sicurezza e, soprattutto, l'interfaccia operatore. Per questo motivo si ritiene che la soluzione più efficace per la costruzione di un OTS si debba basare sull'utilizzo delle stesse piattaforme DCS standard utilizzate per il controllo dell'impianto.

Il sistema di simulazione così concepito tipicamente necessita di una o due stazioni operatore e di moduli di controllo (hardware DCS in modalità simulazione). Non sono ovviamente necessari dispositivi di I/O. Sull'hardware individuato vengono replicati tutti i punti di controllo che si desiderano simulare, con la configurazione degli allarmi e delle pagine grafiche che vengono utilizzate dagli operatori in sala controllo.
Lo sviluppo di un simulatore su una piattaforma DCS prevede le seguenti fasi:

- acquisizione delle configurazioni dei punti esistenti, dei loop di controllo di base e del sistema di allarmi relativi all'impianto che si desidera simulare;
- caricamento delle configurazioni acquisite su una piattaforma DCS in modalità simulazione;
- implementazione dei modelli matematici;
- sintonizzazione dei loop di controllo;
- sintonizzazione dei parametri dei modelli;
- trascrizione sul sistema di simulazione delle logiche di blocco normalmente residenti in dispositivi esterni (PLC).

Nella costruzione dei modelli si utilizzano esclusivamente i blocchi standard di controllo e gli strumenti di configurazione o i linguaggi di programmazione e controllo caratteristici di ciascuna piattaforma DCS.

Il requisito della fedeltà dell'interfaccia operatore viene risolto in maniera naturale con l'uso di hardware DCS standard e con il caricamento delle stesse interfacce grafiche presenti nelle stazioni DCS della sala controllo. In questo modo, chi utilizza il simulatore si trova davanti un sistema che è praticamente la fotocopia di quello reale, con la possibilità di operare con le pagine grafiche, i gruppi operativi, le pagine di dettaglio dei punti, le pagine allarmi, le storicizzazioni dei trend delle variabili di processo e tutto ciò che utilizza normalmente nella gestione dell'impianto.[34]

[34] *<http://www.wrange.it/simulatore>*

Conclusioni

Questo elaborato si poneva come scopo quello di fornire degli strumenti teorici e pratici per la gestione di situazioni di pericolo in ambienti innovativi che contemplano l'utilizzo delle tecnologie 4.0. Una volta analizzato lo stato dell'arte dell'industry 4.0 in relazione alla capacità delle imprese di recepire questi cambiamenti sia a livello tecnico sia a livello di sostenibilità economica, sono stati evidenziati gli standard normativi come punto di partenza per un'analisi più approfondita delle dinamiche di sicurezza. Sono stati considerati in primo luogo gli attori che possono influenzare le scelte dei top management e come questi possono reagire trovandosi di fronte a scenari completamente nuovi nell'ottica di un'integrazione verticale, mettendolo successivamente in relazione con il comportamento dell'intero contesto imprenditoriale di fronte alle possibili dinamiche esterne che influenzano il business, nell'ottica di un'integrazione orizzontale. Poste le basi per un'analisi più approfondita, si è stati in grado di valutare il ciclo di vita della gestione della sicurezza, monitorandolo e caratterizzandolo in tutti i suoi aspetti a partire dall'analisi della gestione dei dati, passando per la realizzazione di un framework di project risk managment con il quale si è potuto constatare come le informazioni in mano ai decisori, se di elevata qualità, possono portare alla definizione di una strategia di gestione del rischio efficace e applicabile in qualsiasi contesto, fino ad arrivare alla fase operativa del "process safety" dove sono state proposte diverse soluzioni per rispondere alle problematiche di sicurezza evidenziate. Fra i possibili sviluppi di questo lavoro vi è la possibilità di portare nuove strutture per la valutazione dei rischi di progetti che possano tener conto anche di fattori puramente emotivi, sia da parte dei decisori sia da parte degli operatori, che possono influenzare criticamente le scelte, creando nuove situazioni di pericolo da fronteggiare attraverso nuove scoperte tecnologiche. Esse, negli anni a venire, subiranno un notevole sviluppo, in quanto si è solo agli inizi della rivoluzione dell'industria 4.0.

Bibliografia

[1] *Adel Badria, Bryan Boudreau-Trudelc, Ahmed Saâdeddine Souissid, Occupational health and safety in the industry 4.0 era: A cause for major concern?, in "Safety Science" n. 109, november 2018, pp. 403-411, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2018.06.012.*

[2] *Disseminazione della cultura della sicurezza e salute del lavoro, Prof. Alberto Martinetti,Torino,2018, https://research.utwente.nl/files/30603033/Martinetti_24052018_rel2.pdf*

[3] *Mark P. Taylor, Peter Boxall, John J.J. Chen, Xun Xu, Angela Liew, Adebayo Adeniji, 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, in "Computers & Industrial Engineering" n. 139, january 2020, 105486, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2018.10.047.*

[4] *C. Digmayer and E. Jakobs, "Developing Safety Cultures for Industry 4.0. New Challenges for Professional Communication," 2019 IEEE International Professional Communication Conference (ProComm), Aachen, Germany, 2019, pp. 218-225, https://doi.org/10.1109/ProComm.2019.00045.*

[5] *G. Vignali et al., "Development of a 4.0 industry application for increasing occupational safety: guidelines for a correct approach," 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne Sophia-Antipolis, France, 2019, pp. 1-6, https://doi.org/10.1109/ICE.2019.8792814.*

[6] *Jiri Tupa, Jan Simota, Frantisek Steiner, Aspects of Risk Management Implementation for Industry 4.0, in "Procedia Manufacturing", Volume 11, 2017, Pages 1223-1230, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2017.07.248*

[7] *Behzad Esmaeilian, Joe Sarkis, Kemper Lewis, Sara Behdad, Blockchain for the future of sustainable supply chain management in Industry 4.0, in "Resources, Conservation and Recycling, Volume 163, 2020, 105064, ISSN 0921-3449, https://doi.org/10.1016/j.resconrec.2020.105064.*

[8] *Md. Abdul Moktadir, Syed Mithun Ali, Simonov Kusi-Sarpong, Md. Aftab Ali Shaikh, Assessing challenges for implementing Industry 4.0: Implications for process safety and environmental protection, in "Process Safety and Environmental Protection", Volume 117, 2018, Pages 730-741, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2018.04.020.*

[9] *John Lee, Ian Cameron, Maureen Hassall,Improving process safety: What roles for Digitalization and Industry 4.0?, in "Process Safety and Environmental Protection", Volume 132, 2019, Pages 325-339, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2019.10.021.*

[10] *V. Kharchenko, S. Dotsenko, O. Illiashenko and S. Kamenskyi, Integrated Cyber Safety & Security Management System: Industry 4.0 Issue, 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), Leeds, United Kingdom, 2019, pp. 197-201, https://doi.org/10.1109/DESSERT.2019.8770010.*

[11] *A. Bicaku, C. Schmittner, M. Tauber and J. Delsing, Monitoring Industry 4.0 applications for security and safety standard compliance, 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, 2018, pp. 749-754, https://doi.org/10.1109/ICPHYS.2018.8390801.*

[12] *Rane, S.B., Potdar, P.R. and Rane, S. (2019), Development of Project Risk Management framework based on Industry 4.0 technologies, in "Benchmarking: An International Journal", Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/BIJ-03-2019-0123.*

[13] *Bing Wang, Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework, Process Safety and Environmental Protection, Volume 148, 2021, Pages 189-199, ISSN 0957-5820, https://doi.org/10.1016/j.psep.2020.10.008.*

[14] *Muhammad Atif Javed, Faiz Ul Muram, Hans Hansson, Sasikumar Punnekkat, Henrik Thane, Towards dynamic safety assurance for Industry 4.0, in "Journal of Systems Architecture", 2020, 101914, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2020.101914.*

[15] *R. Satish, K. Murugabhoopathy, N. Rajendhiran, V. Vijayan, Technology strategy for improved safety management in steel industry, in "Materials Today: Proceedings", 2020, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2020.01.224.*

[16] *G. Vignali* et al*., "Development of a 4.0 industry application for increasing occupational safety: guidelines for a correct approach,"* 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Valbonne Sophia-Antipolis, France, 2019, pp. 1-6, https://doi.org/10.1109/ICE.2019.8792814.*

Sitografia

https://research.utwente.nl/files/30603033/Martinetti_24052018_rel2.pdf

https://www.bcg.com/it-it/capabilities/operations/embracing-industry-4.0-rediscovering-growth

https://blog.osservatori.net/it_it/cos-e-internet-of-things

https://it.wikipedia.org/wiki/Big_data

https://it.wikipedia.org/wiki/Dataset

https://www.sas.com/it_it/insights/big-data/what-is-big-data.html

https://ricomincioda4.fondirigenti.it/le-potenzialita-della-simulazione-avanzata-nellindustria-4-0/

https://www.industry4business.it/connected-enterprise/connected-factory/realta-aumentata-che-cose-e-come-funziona/

https://it.wikipedia.org/wiki/Cloud_computing

https://it.wikipedia.org/wiki/Produzione_additiva

https://www.internet4things.it/iot-library/che-cose-il-3d-printing-e-come-si-colloca-nellambito-industry-4-0-e-iot/

https://www.ip4fvg.it/focus-tecnologie-abilitanti-integrazione-orizzontale-e-verticale/

https://mynext.it/2018/09/integrazione-verticale-e-orizzontale-dei-sistemi-cosa-significa/

https://quattropuntozero.confartigianato.it/wp-content/uploads/2017/11/Guida-pratica-Confartigianato-Industria-4.0-versione-estesa-web.pdf

https://www.focusindustria40.com/robotica-collaborativa/

https://www.industriequattropuntozero.it/2020/06/19/i-robot-mobili-autonomi-nellindustria-dei-beni-di-largo-consumo/

http://www.key-4.com/la-sicurezza-nellindustria-4-0/

https://www.agendadigitale.eu/industry-4-0/industry-4-0-tutti-gli-standard-e-i-modelli-di-riferimento/

https://ceimagazine.ceinorme.it/ceifocus/il-background-tecnologico-e-normativo-di-industria-4-0/

https://www.cybersecurity360.it/legal/lo-standard-iec-62443-4-2-per-la-cyber-security-industriale-le-linee-guida/

https://it.wikipedia.org/wiki/ISO/IEC_27000-series

https://en.wikipedia.org/wiki/IEC_61511

https://en.wikipedia.org/wiki/MTTFd

https://en.wikipedia.org/wiki/ISO_13849

https://www.pilz.com/it-IT/support/knowhow/law-standards-norms/functional-safety/en-iso-13849-1

https://it.wikipedia.org/wiki/End-to-end

https://www.internet4things.it/iot-library/mqtt-cose-e-come-funziona-il-protocollo-alla-base-delliot/

https://www.isipc.it/cuber-sicurezza-e-industria-4-0-i-rischi-e-come-affrontarli/

https://it.wikipedia.org/wiki/Analytic_Hierarchy_Process

https://www.digitalengineering247.com/article/exoskeletons-on-the-move

http://www.wrange.it/simulatore

https://www.fastweb.it/internet/mirroring-web-cos-e-e-come-funziona/

https://it.wikipedia.org/wiki/Front-end_e_back-end

Ringraziamenti

Tornando indietro con la mente di due anni, pensare di essere qua a scrivere questo breve omaggio alla mia carriera accademica e a coloro che mi hanno accompagnato era soltanto un sogno distante anni luce. Non nego che se potessi tornare indietro rivedrei le mie scelte, ma questo non cancella i bei momenti trascorsi nella mia precedente esperienza, i quali hanno arricchito il mio bagaglio culturale e mi hanno permesso di conoscere delle persone con le quali ho condiviso gran parte del mio percorso e che, nonostante tutto, ringrazio con affetto. La mia risalita inizia con la testa piena di insicurezze e con la paura di aver fatto di nuovo la scelta sbagliata. Cambiare nuovamente abitudini, percorrere centinaia di chilometri ogni settimana, lasciare i miei coinquilini con i quali ho trascorso tre anni bellissimi e passare metà della settimana in totale solitudine; mi tormentavo di domande senza avere nessun tipo di risposta o certezza. Per questi motivi sento di dedicare una parte importante di questo traguardo alla mia fidanzata Martina. Grazie perché mi hai dato il coraggio di riprendere il percorso al quale sapevi io tenessi più di molte altre cose, affrontandolo insieme a me come se ti riguardasse direttamente. Grazie perché oltre a questo mi hai trasmesso ogni singolo giorno la forza per affrontare le nuove difficoltà e per superare tutti gli ostacoli che da solo, probabilmente, non sarei stato in grado di oltrepassare. Grazie per aver sempre creduto in me, anche quando tutto sembrava perduto e anche quando, in quel giorno di metà settembre, mi hai accompagnato a Fermo sperando che la tua presenza mi avrebbe convinto a non abbandonare tutto. Così è stato. Senza di te non ce l'avrei mai fatta e questo traguardo appartiene anche a te. Un ringraziamento particolare va anche ai miei genitori. Mi hanno dato la possibilità di studiare, di vivere delle città diverse e di appassionarmi, insegnandomi quel senso di responsabilità da portare con me nella vita di tutti i giorni e accettando incondizionatamente i miei errori rinnovandomi il sostegno di cui necessitavo per poter arrivare al traguardo. Un doveroso ringraziamento va anche ai miei compagni di percorso, Cristina e Davide; insieme abbiamo condiviso tante ore di studio, esami, progetti, arrabbiature e soddisfazioni per i risultati ottenuti. Ho trovato due persone leali che mi hanno trasmesso la giusta dose di spensieratezza e per questo mi ritengo fortunato, perché anche grazie a loro ho potuto trascorrere questi anni con una ritrovata voglia di affrontare il percorso accademico. Ora

che le nostre strade si sono separate, a loro va i miei migliori auguri per il loro futuro professionale. Ci tengo a ringraziare anche il Prof. Bevilacqua che mi ha permesso di approfondire tematiche riguardanti un ambito di notevole interesse sia per il presente ma soprattutto per il futuro. Per concludere torno a dedicare questo traguardo a me stesso, per la perseveranza nel tentare di raggiungere ad ogni costo l'obiettivo e per aver utilizzato i fallimenti come basi per la costruzione di questo successo.