UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea triennale **INGEGNERIA GESTIONALE (L-8)**

PREVENZIONE DELL'INVECCHIAMENTO DEGLI IMPIANTI PRODUTTIVI: ASSET INTEGRITY MANAGEMENT E SAFETY INTELLIGENCE

PREVENTION OF AGEING PRODUCTION PLANTS:
ASSET INTEGRITY MANAGEMENT AND SAFETY INTELLIGENCE

Tesi di Laurea di:

Monica Marconi Sciarroni

Relatore:

Prof. **Maurizio Bevilacqua**

Correlatrice:

Ing. **Sara Antomarioni**

Anno Accademico 2020 / 2021

SOMMARIO

INTRODUZIONE

Nel periodo storico attuale, caratterizzato dalla costante evoluzione del settore dell'industria in seguito alla rapida crescita economica sostenuta dalle innovazioni tecnologiche, è fondamentale gestire bene gli impianti, ancora di più se facenti parte dei cosiddetti "impianti ad alto rischio di incidente rilevante" in relazione al fenomeno di invecchiamento. Maggiore attenzione dovrebbe essere rivolta soprattutto verso le industrie operanti da decenni sul mercato i cui impianti sono composti da macchinari con oltre quarant'anni di vita.

La prima cosa da chiarire riguarda il termine "**invecchiamento**" riferito agli impianti produttivi, che non fa riferimento semplicemente al tempo trascorso dalla data di realizzazione degli strumenti, di collaudo o di messa in servizio delle apparecchiature, ma è **legato alla loro condizione e a come essa cambia nel corso del tempo**.
Lo stato di degrado deriva per lo più da fenomeni di danneggiamento che possono determinare un aumento della probabilità di guasto durante la sua vita. Questi meccanismi di danno possono determinarne l'invecchiamento, anche precoce, se non opportunamente rilevati, controllati e monitorati, provocando un effetto potenziale negativo in termini di funzionalità, disponibilità, affidabilità e sicurezza.

Si dovrebbe porre attenzione anche alla gestione delle apparecchiature elettriche, dei sistemi di controllo e delle apparecchiature strumentali, insieme alla corretta esecuzione delle attività di taratura e test in accordo con i piani emessi.

Una delle tante conseguenze per la disattenzione di questi accorgimenti è l'aumento del rischio di guasti che si è dimostrato ricoprire un fattore determinante in molti incidenti industriali.

Durante l'intervento "Ottimizzazione delle strategie manutentive delle apparecchiature datate mediante l'applicazione dell'analisi decisionale dinamica integrata", a cura di M. Demichela e G. Baldissone (Politecnico di Torino), C. Leva (Dublin Institute of Technology) e P. Agnello (Inail – Dit), si sottolinea che "l'invecchiamento degli impianti, se gestito in modo non corretto, può causare gravi incidenti".
In particolare, recenti ricerche hanno identificato che almeno la metà degli incidenti scaturiti da guasti di tipo tecnico sugli impianti sono stati essenzialmente causati da meccanismi e fenomeni di invecchiamento. Questi eventi hanno comportato un numero fortunatamente contenuto di morti, molti feriti e milioni in euro di perdite economiche, dimostrando il forte impatto dei disservizi derivanti dall'invecchiamento degli impianti sulla sicurezza e sulle performance del business.

Inoltre, l'utilizzo di attrezzature oltre il loro periodo di vita utile "riduce la competitività dell'azienda, poiché di solito queste richiedono più energia, più manutenzione e materie prime, spesso, costose". Invece l'adozione di impianti moderni permette di porre una maggiore attenzione alla sostenibilità, dovuto alla riduzione del consumo di energia, e possono aumentare la flessibilità dell'impianto per quanto riguarda la produzione, sia in termini di volumi sia di qualità.

Senza dimenticare che l'uso di impianti moderni o datati ha un evidente impatto anche sulla sicurezza dei processi industriali e degli operatori, incidendo sulle probabilità di incidenti e/o morti.

Il problema è che la presente soluzione sull'adozione di nuove tecnologie e il rinnovo degli impianti richiede elevati costi di investimento, e non tutte le imprese sono disposte a prendere queste decisioni a lungo termine, ma preferiscono utilizzare gli impianti oltre la loro vita utile. Tuttavia, per minimizzare le criticità degli impianti datati è necessario "gestire l'invecchiamento degli impianti e attrezzature anche attraverso la manutenzione".

Si vuole sottolineare che generalmente la strategia di manutenzione veniva scelta tra la manutenzione reattiva e la manutenzione preventiva, ma in questi tempi lo sviluppo tecnologico consente di sviluppare strategie manutentive con un approccio proattivo, ciò vuol dire che sono basate sulle reali condizioni delle apparecchiature. Questa recente metodologia si basa principalmente sulla stima dei valori di rischio, in cui viene proposto e discusso un approccio basato su questi valori e con l'intenzione di operare una scelta tra diverse strategie manutentive concorrenti. La metodologia proposta analizza il rischio associato alle diverse strategie manutentive in base alle possibili condizioni dell'apparecchiatura al momento di inizio delle attività di manutenzione.

La valutazione del rischio è effettuata tramite l'"**Integrated Dynamic Decision Analysis** (IDDA)". La metodologia IDDA affianca un modello logico-probabilistico ad un modello fenomenologico. Nel dettaglio, la **modellazione logico-probabilistica** procede attraverso i seguenti passaggi:
prima si effettua l'analisi funzionale del sistema e la definizione di un elenco di livelli, mediante una serie di domande e affermazioni sulla funzionalità di ciascun elemento; ogni livello rappresenta l'elemento base del modello logico, il quale nell'ottica di un albero degli eventi corrisponderebbe a un nodo; poi si procede con la costruzione di una struttura reticolare attraverso gli indirizzamenti (livelli successivi) di uscita in ogni livello; successivamente vi è la caratterizzazione di ogni livello e ogni possibile alternativa di uscita dei livelli con una stringa di testo che consente all'utente di leggere lo sviluppo logico di ogni sequenza di eventi; si prosegue con l'associazione a ciascun livello di un dato probabilistico, che rappresenta il grado previsto di probabilità di occorrenza di ogni evento analizzato e di un dato d'incertezza della probabilità di accadimento, che rappresenta la distribuzione statistica della probabilità; e infine si attua la definizione di vincoli logici e probabilistici, che consentono di tenere in considerazione le interdipendenze esistenti fra i vari eventi analizzati.

E assieme al modello logico – probabilistico viene preparato un **modello fenomenologico** che descrive il comportamento fisico del sistema. Questo modello può partecipare all'aggiornamento delle risultanze del modello logico – probabilistico al fine di avvicinare i risultati dell'analisi alla realtà, cioè, ad esempio, se dopo il guasto di un'apparecchiatura le altre apparecchiature sono in grado di compensare il guasto, o se possono comparire effetti cumulativi e divergenti portando ad eventi potenzialmente pericolosi. Inoltre, il modello fenomenologico "può fornire anche una stima delle conseguenze per ogni singola sequenza di eventi individuata in moda da ottenere una stima del rischio, la valutazione del rischio complessivo del sistema e il valore atteso delle conseguenze".

L’intervento sopracitato si conclude ricordando che in diverse realtà industriali il problema riguardo l'invecchiamento degli impianti produttivi sta diventando molto serio e può causare incidenti molto gravi, senza dimenticare le conseguenze nell’ottica economico-finanziaria.

Si è citato uno dei modi per controllare l'invecchiamento delle attrezzature, ed è quello che considera una corretta manutenzione che utilizza un approccio attraverso la stima dei dati di rischio delle diverse tecniche di manutenzione proposte. I futuri sviluppi dell’approccio proposto permetteranno poi di tenere in considerazione sempre più anche gli aspetti legati al potenziale rischio di incidente. La gestione sicura dell’invecchiamento degli impianti e delle connesse attività di gestione procedurale e operativa dell’”asset integrity” costituisce per molte aziende, ed in particolare quelle industriali, una problematica rilevante, anche a causa dell’introduzione piuttosto recente della tecnologia più avanzata negli stabilimenti industriali.

In questo ambito, un ruolo strategico è assunto dalla gestione dei processi di manutenzione delle attrezzature, non soltanto orientata ad assicurarne la continuità operativa, ma capace di garantire condizioni di sicurezza utili per evitare incidenti. Per mantenere il controllo e il mantenimento del grado di rischio a livelli accettabili è dunque necessaria una politica della sicurezza e della manutenzione finalizzata alla prevenzione.

Qui è presentata una panoramica sulle possibilità offerte dalle tecnologie attuali per controllare e monitorare l’invecchiamento degli impianti. In sintesi, bisogna focalizzare l’attenzione dapprima sui piani di monitoraggio e controllo, quale strumento di autocontrollo per il rispetto dei valori limite di emissione e il rispetto della conformità all’autorizzazione posseduta; poi sulle modalità di individuazione dei componenti critici, le tecniche di individuazione delle perdite e il monitoraggio e riparazione dei componenti; e infine ricorrere alle Best Available Techniques (BAT). In questo modo, attraverso una panoramica dei riferimenti normativi nazionali ed internazionali, si possono ottenere suggerimenti su come approcciare la problematica dell’asset integrity partendo da un’ottica di sistema di gestione, fino ad arrivare alla predisposizione di metodologie specifiche di manutenzione.

All’interno di questa realtà *capital intensive* a rischio di incidente rilevante, difatti, la cultura dell’Asset Integrity è sempre stata presente, in maniera più o meno radicata, veicolata soprattutto da aspetti di compliance normativa. Negli ultimi anni questo ambito si è arricchito con il D.lgs. 105/2015 che introduce l’obbligo di adottare piani di monitoraggio e controllo dei rischi legati all’invecchiamento di apparecchiature e impianti. Si entra nel merito dei piani che devono tenere conto dei meccanismi di deterioramento presenti, inclusi corrosione interna ed esterna, erosione, fatica termica e meccanica. La normativa quindi si aggiorna e offre uno stimolo, per i gestori, a valutare il proprio sistema di gestione dell’Asset Integrity.

Inoltre, sarebbe strategicamente limitante fare riferimento solo ad asset rilevanti dal punto di vista delle normative poiché ci sono asset che sono comunque critici semplicemente perché un guasto può portare a discontinuità nel business per perdite di produzione. Diventa fondamentale conoscere tutti gli asset critici e associare, a ciascuno, il livello di criticità legato alla continuità di business. Qui si apre un mondo legato alle strategie manutentive da

adottare sugli item critici, alle valutazioni sul ciclo di vita di queste attrezzature e ad eventuali pratiche di Life Cycle Extension. Garantire il raggiungimento degli obiettivi di produzione è un successo ma oggi assume altrettanta rilevanza anche la gestione dell'intera vita degli asset. Si può affermare che la definizione di opportuni piani di controllo e ispezione e la loro corretta implementazione rappresenta un caposaldo per la gestione del fenomeno di invecchiamento degli item

Da qui l'importanza della gestione dell'abilità di un asset a svolgere in modo efficace ed efficiente - durante tutto il suo ciclo di vita - la funzione richiesta nel rispetto della salute, sicurezza e dell'ambiente; e questo concetto è il significato dell'espressione "**Asset Integrity Management**" **(A.I.M.)** Nel settore produttivo odierno, come abbiamo visto, l'espressione A.I.M. è sempre più utilizzata e rappresenta il termine generale per la **gestione delle risorse produttive industriali**.

Al fine di aumentare la loro produttività, le imprese devono avere una manutenzione regolare delle loro strutture e attrezzature. Le stesse strutture sono caratterizzate da una crescente complessità degli aspetti organizzativi, unitamente all'estensione di operatività degli impianti e i relativi rischi per la sicurezza. Per questi motivi, l'implementazione di un sistema di gestione dell'integrità delle risorse è diventata molto importante.
La riduzione generale dei rischi tecnici, strutturali e ambientali ha effetto positivo non solo all'interno dell'azienda ma anche all'esterno, nello specifico sulla fiducia dei clienti.
A livello globale, così, l'azienda acquisisce forza in termini di qualità e sicurezza e guadagna un vantaggio competitivo sul mercato.

Questo rende chiaro il motivo per cui avere un ottimo **A.I.M. all'interno di una azienda** permetta la crescita nel campo dell'industria e della manutenzione e la sostenibilità nel proprio business aziendale. È importante quindi sottolineare l'importanza dell'adozione di metodologie adeguate per valutare **il reale stato di invecchiamento degli asset industriali**.

Gli obiettivi dell'**Asset Integrity Management** (A.I.M) sono essenzialmente quattro:

1. Definire i requisiti che gli asset devono soddisfare;
2. Progettare e costruire l'integrità nei nuovi asset;
3. Mantenere l'integrità degli asset lungo l'intero ciclo di vita dell'impianto;
4. Rilevare e correggere anomalie e i guasti durante il funzionamento degli asset.

In aggiunta al compito di verificare e assicurare le procedure e gli strumenti adeguati a garantire l'integrità e le prestazioni degli asset, ossia le risorse, ottimizzando le prestazioni durante tutto il ciclo di vita.

La gestione dell'integrità delle risorse è composta principalmente da 3 fasi.
1° fase di analisi: si esaminano i processi, le procedure e gli strumenti di gestione patrimoniale già esistenti nel periodo di servizio.
2° fase di miglioramento, si studia l'implementazione di procedure ottimizzate basate sulle raccomandazioni fornite nella fase 1.
3° fase di stabilizzazione, si definisce il supporto nella gestione delle prestazioni di queste attività.

Nel dettaglio:

FASE 1: INDAGINE SULL'INTEGRITÀ DELL'ATTIVITÀ E CONTROLLO DEL MIGLIORAMENTO (AIIIA)

È necessario effettuare una **selezione** dei dati di monitoraggio e delle condizioni di funzionamento per stilare una **valutazione dell'integrità delle attrezzature** attraverso procedure specifiche; questo permette di ottenere una **valutazione dettagliata degli elementi critici e del loro livello di rischio.** Successivamente, si eseguono **procedure di ispezione e manutenzione** per garantire una riduzione e una prevenzione ai guasti. Questo è possibile anche attuando politiche di **formazione e qualifica** per auspicare ad un miglioramento continuo**.**

Questa prima fase si conclude con la stesura di **rapporti finali completi di analisi, benchmark e lista di raccomandazioni,** con l'intento di garantire un funzionamento futuro sicuro*.* All'interno di questi documenti, si va ad analizzare l'intero ciclo di vita con l'*acquisizione dei dati* attraverso le banche dati oppure con documenti di gestione, quali ad esempio le procedure, le regole e gli standard*,* si effettua un *monitoraggio delle condizioni* e si ottiene una *diagnosi dei guasti,* conseguentemente si esprime una *valutazione dell'integrità e dell'efficienza;* tutte queste informazioni saranno poi elaborate per poter, infine, definire una *strategia di manutenzione.*

FASE 2: MIGLIORAMENTO DEL PROGRAMMA

In questa fase si attua una **ottimizzazione del processo di gestione** sulla base dei dati raccolti nella prima fase, andando a definire **programmi di ispezione basati sul rischio** precedentemente valutato. Inoltre, si definiscono le **idoneità per le procedure di assistenza** e si effettua un'**analisi dei rischi di processo.**

FASE 3: MISURA DELLE PRESTAZIONI

In questa ultima fase, si procede con **l'implementazione dei KPI:** questo è l'acronimo dell'espressione *Key Performance Indicators*, ovvero gli *indicatori chiave di performance*, che rappresentano un insieme di misure quantificabili che un'azienda utilizza per valutare le sue prestazioni nel tempo.

Si attuano **controlli delle prestazioni**, quindi del funzionamento delle risorse, con una periodicità frequente. I risultati di questi controlli contribuiscono a valutare la *gestione della manutenzione e delle parti di ricambio,* a definire *il carico di lavoro del personale,* a ottimizzare *l'efficienza lavorativa* e a migliorare *la disponibilità dei dati.*

Qui è bene considerare che le caratteristiche strutturali e l'esperienza attraverso mezzi di monitoraggio disponibili nel tempo permettono di migliorare la capacità di diagnostica delle anomalie. Si noti come l'aggiornamento e l'avanzamento delle conoscenze tecnologiche abbia un impatto notevole su questo aspetto di gestione dell'organizzazione nel mondo aziendale.

EVOLUZIONE DELL'ASSET INTEGRITY MANAGEMENT

L'**Asset Integrity Management** ha avuto un grande impatto all'interno del pensiero che sta alla base della **gestione della manutenzione**. Il settore che si occupa della gestione degli impianti è sempre più importante all'interno di un'azienda e ha avuto nel corso degli anni una sua evoluzione che può rappresentarsi in due logiche:

La prima logica si può riassumere con l'espressione "**se non è rotto, non aggiustarlo**" e questo tipo di pensiero è proprio di una tipologia di manutenzione detta "a guasto", ovvero il tipo di gestione che prevedeva di non toccare nulla finché all'interno della linea produttiva non si riscontrasse un guasto o un'anomalia che richiedesse necessariamente un intervento.

E' facile intuire che questo tipo di gestione presentava molti aspetti negativi, basti pensare che la fermata improvvisa degli impianti a causa di una rottura causava anche la fermata della produzione e questo aveva come conseguenza grosse perdite di denaro, inoltre erano necessari costi maggiori e tempestivi per avere la disponibilità di personale in grado di riparare immediatamente i danni degli impianti, infine le attività di riparazione richiedevano maggiori consumi energetici e portavano a ottenere prodotti di bassa qualità, fino al termine delle riparazioni.

La seconda logica è quella del "**se non è rotto, cerca di mantenerlo in quello stato**" e questo rappresenta il pensiero alla base delle più attuali logiche di manutenzione preventiva, le quali portano con sé numerose innovazioni in termini di approccio.
Alla base di tutto, infatti, troviamo la **programmazione**. Una revisione costante degli impianti, con una fermata preventivata permette una razionalizzazione dei costi che andranno a gravare in misura minore sui ricavi. In questo modo si ridurranno drasticamente i rischi corsi da parte dell'azienda in quanto si avrà continuamente un impianto nuovo ed efficiente. Si alzerà quindi la qualità del prodotto realizzato e con lui il valore percepito di ciò che verrà immesso sul mercato.

ADOZIONE DELL'A.I.M. ALL'INTERNO DELLE AZIENDE

Compresa la sua importanza e la sua ampia utilità, le aziende hanno adottato da molti anni strategie e azioni per la promozione dell'integrità delle risorse e della sicurezza nei processi, attraverso presentazioni e seminari per il personale interno e anche esterno.
La condivisione e l'apprendimento delle informazioni a tutti gli operatori del sistema produttivo, difatti, portano ad una riduzione delle differenze di comportamento tra le persone, soprattutto nel modo di gestire, operare e raccogliere dati.

Come è stato ribadito precedentemente, è necessario che i dati siano conformi a determinate linee guida per poter essere efficacemente utilizzati e analizzati nelle diverse fasi dell'AIM. L'uniformità di comportamento nelle varie funzioni aziendali è un cambiamento e, come tutti i cambiamenti all'interno di un'azienda, rappresenta un ostacolo ad una gestione efficace e sostenibile. È necessario, perciò, adottare un linguaggio semplice, chiaro e comprensibile alle persone coinvolte, per garantire che questa innovazione nelle attività aziendali sia adottata nella maniera più corretta possibile.

Come spiegato nella fase 1, la formazione è un requisito fondamentale affinché il team responsabile della gestione sia adeguatamente preparato per poter operare nell'ottica di un miglioramento continuo.

IMPORTANZA DELLA TECNOLOGIA

Nell'illustrare l'importanza di questa innovazione aziendale riguardo il processo di gestione, si è puntualizzato prima che il suo **sviluppo relativamente recente ha determinato la possibilità di sfruttare i**l beneficio ottenuto dalle novità sviluppate nell'ambito dell'**evoluzione tecnologica**.

La tecnologia digitale, difatti, sta assumendo un ruolo sempre più incidente per garantire una gestione che assicura all'azienda il raggiungimento degli obiettivi in termini di efficacia e di efficienza. Questo aspetto rappresenta un fattore assolutamente strategico per avere la possibilità di ottenere un vantaggio oltre che economico anche competitivo per le aziende sul mercato. Ed è proprio grazie alle nuove tecnologie digitali che è possibile il raggiungimento dei quattro obiettivi dell'A.I.M**.**

La disposizione, all'interno della realtà aziendale, di strumenti tecnologici all'avanguardia per raccogliere ed elaborare dati risulta essere essenziale e importante perché ciò permette al management di avere la conoscenza di informazioni complete e affidabili, e quindi di essere nella condizione di assumere la consapevolezza e l'impegno sull'integrità delle risorse e sulla sicurezza dei processi, e di poter prendere decisioni ben ponderate. E cosa non meno importante, la combinazione di tecnologie digitali, come per esempio IoT (Internet of Things), Big Data, Industria 4.0 etc. permette di creare un business più intelligente per aziende in cerca di maggiore produttività ed efficienza.

La progressiva informatizzazione delle aziende ha reso gli ambiti della sorveglianza e della protezione sempre più importanti, unito al fatto che oggi il business non esiste senza Internet. Il concetto di business è online e impone nuove logiche di gestione ma anche nuove visioni capaci di abbracciare sistemi sempre più complessi; la maggior parte dei processi industriali è digitale o in qualche modo passa dalle tecnologie digitali.

Prima di tutto, però, occorre spendere due parole sulle parole *safety* e *security* e sul loro significato. In Italia si parla genericamente di "sicurezza" ma la suddivisione anglosassone specifica due differenze: ***"Safety"*** è la sicurezza dei lavoratori mentre "***Security"*** è la sicurezza dei cittadini. Proteggere le persone, le aziende e le informazioni relative ad esse è parte integrante di una strategia in cui convergono sistemi di videosorveglianza ma anche di protezione da tutte le derive del cybercrime che colpisce gli utenti in azienda oppure in mobilità. Gli utenti sono tutti connessi, che agiscano in modalità privata o in modalità pubblica, che siano interni o esterni, che siano persone fisiche o entità giuridiche. In qualsiasi settore, pubblico o privato, l'informatizzazione degli strumenti di lavoro e la digitalizzazione di contenuti e applicazioni stanno portando a connettersi una quantità di oggetti crescente, come illustrano i trend di un'evoluzione gestionale che supporta un'economia sempre più digitale.

Oltre ai vantaggi funzionali associati a questa serie di oggetti che comunicano con sistemi e dispositivi, c'è un altro tema fondamentale perché **tutta l'architettura tecnologica e informativa funzioni**: la **sicurezza**. La sicurezza oggi è l'ennesimo ambito in cui la tecnologia supporta la qualità dei controlli e dei servizi associati e abbraccia in maniera organica e funzionale tutti i luoghi di attività, i mezzi d'opera e di produzione, le persone e i materiali in loro utilizzo e anche i servizi.

Uno dei problemi più grossi con la sicurezza associata all'evoluzione dell'intelligenza delle cose è un cambiamento di prospettiva della governance. Il che, in sintesi, significa sapersi occupare dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e quindi della protezione dell'integrità fisica non solo dell'hardware ma anche del software che, dal punto di vista logico-funzionale, motorizza un sistema informatico e i dati in esso contenuti o scambiati in una comunicazione con uno più utenti.

Gli oggetti connessi sono a tutti gli effetti degli elaboratori di informazioni, cioè dei computer. **Come tali vanno protetti** dalle minacce esterne della cybercriminalità organizzata, dalle anomalie di funzionamento meccaniche o applicative e dalle inadempienze degli utenti che, per ignoranza o per mala gestione, possono alterare meccanismi di funzionamento e quindi i processi associati.

La cosiddetta "***Internet of Things***" (IoT) è iniziata molti anni fa, con un progressivo processo di integrazione. Inizialmente vi era la presenza di sistemi informativi diversi e dedicati che, pian piano, hanno iniziato a comunicare tra loro per comodità e per efficienza, evitando ridondanze, discontinuità negli aggiornamenti e asincronie tra chi era più informato perché dotato di tecnologie di connessione più evolute. Il mercato dell'IoT sta generando e continuerà a generare per le aziende un valore di trilioni di dollari mentre il numero di dispositivi online crescerà in miliardi. Parallelamente, anche la criminalità informatica sta diventando sempre più sofisticata e industrializzata, connotata da un aumento delle opportunità economiche per i cybercriminali. Per semplificare al massimo la gestione della sicurezza nell'azienda distribuita e per aumentare la visibilità sulle minacce fin nei luoghi più remoti all'interno delle aziende e delle infrastrutture globali dei service provider, è necessario integrare una security in tutta la rete estesa.

Gestire la **IoT** presuppone nuove abilità e nuove competenze per chi deve integrare e amministrare i sistemi, ed è importante saper garantire innanzitutto la continuità e la sicurezza del core business, poi lo stato di efficienza e la sicurezza degli asset, unito alla salute e la continuità operativa del personale e infine affermare la responsabilità dell'impresa e dei suoi partecipanti verso il mondo esterno.

Tutto questo riguarda la security intelligence, ma il nostro interesse ora verte sulla Safety Intelligence.

La **Safety Intelligence (S.I.)** rappresenta l'insieme di tutte le varie fonti di informazioni quantitative che un'organizzazione può utilizzare per identificare e valutare varie minacce. Si occupa, quindi, di trasformare i dati e le informazioni grezze sulla sicurezza in informazioni significative e utilizzabili per la gestione della sicurezza.

Si tratta di una combinazione di analisi spaziali e temporali per offrire agli utenti una comprensione a 360 gradi degli incidenti che si sono verificati o potrebbero verificarsi in futuro. In questa maniera, riesce ad identificare schemi e anomalie che potrebbero indicare condizioni non sicure e identifica quali azioni dovrebbero essere intraprese. Ciò fornisce a manager e dirigenti una comprensione contestualizzata degli incidenti e dei problemi di sicurezza all'interno di un'organizzazione.

Il discorso precedente d'introduzione sulla IoT è stato necessaria perché oggigiorno anche **un'azienda digitale produce e gestisce una mole inverosimile di dati**. Idealmente parlando, ci sono dei dati di front end e dati di back end. Una parte di questi dati, infatti, è associata ai processi informatizzati che consentono ad aziende, organizzazioni e persone di lavorare supportarti dall'innovazione digitale. Un'altra è legata all'attività delle macchine che gestiscono questi processi: server, storage, computer, periferiche, dispositivi, router, centraline di controllo, ect. Per analizzare e capire questa mole di dati, dunque, serve una nuova intelligenza di rete e di sistema, ampliando le vision a un concetto di security in cui la gestione delle informazioni legate alla tracciabilità, al monitoraggio e al controllo fanno parte di una nuova integrazione della sicurezza di tipo nativo.

Milioni di dati a disposizione, interconnessione di sistemi governati processi e dall'ingegneria di manutenzione ci consentono un monitoraggio in tempo reale della vita degli asset. Nel campo delle attrezzature, un semplice sistema di monitoraggio, connesso con un software dinamico della gestione delle analisi RBI (e quindi al software delle Ispezioni) e coadiuvato da opportuna sensoristica, ci permette una gestione ottimale delle attività ispettive e un aggiornamento in tempo reale del fine vita degli asset. Possiamo, così, creare i digital twin dell'asset e, così facendo, siamo di fronte a una realtà in cui l'Asset Integrity si basa su un monitoraggio continuo e su manutenzione predittiva.

Mettere in sicurezza gli oggetti della IoT significa predisporre sistemi automatici di analisi che aiutino chi si occupa di governare i sistemi a ricevere le segnalazioni giuste al momento giusto, senza essere distratto dai falsi positivi e da alert a basso impatto che distolgono l'attenzione dagli eventi minacciosi e realmente pericolosi per la business continuity.

Che si tratti di Safety o di Security, la sicurezza on line e off line deve presuppore un approccio dinamico, fatto di aggiornamenti continui sia sulla sofisticazione delle minacce sia sull'evoluzione delle contromisure di protezione associate allo sviluppo di tecnologie sempre più mirate e performanti. Ma non solo: le aziende devono anche attuare una **strategia di risk management** pre e post evento disastroso.

Ogni falla alla sicurezza deve essere analizzata per verificare, in presenza di un evento negativo, se la strategia precedentemente attuata abbia retto all'impatto e, se non lo ha fatto, cosa non ha funzionato, quali e quanti danni ha prodotto, dove e cosa è necessario correggere, in che modo recuperare i danni indebitamente subiti. È evidente che l'impostazione di una strategia o la revisione di una strategia richiede l'esame di uno scenario molto vasto e multidisciplinare. È necessario, anzi, essenziale un programma di sicurezza capace di tenere conto di tutti gli aspetti.

CAPITOLO 2

2.1 L'IMPORTANZA DELLA MANUTENZIONE DEGLI ASSET

Nel 2011 fu pubblicato l'articolo "Briefing problems and lessons from ageing infrastructure" che pose la attenzione sulle sfide per la sicurezza derivanti dall'estensione del ciclo di vita degli asset, con particolare riguardo alla sicurezza del processo e alle risorse necessarie per garantire la continuità. L'autore Hackitt J. ha studiato alcuni fallimenti nella storia dell'industria ed ha esposto i princìpi di un'efficace gestione della sicurezza dei processi che sono stati sviluppati come risultato di esperienze passate.

Nel momento in cui le attrezzature che compongono l'industria energetica si avvicinano o hanno già superato la loro vita progettuale, gli amministratori devono formulare giudizi difficili sulla possibilità di continuare a far funzionare l'impianto oltre ciò che era stato originariamente previsto all'atto di installazione, per quanto tempo tale estensione della vita può essere sostenuta e come effettuare la dismissione. La decisione dell'azienda sull'opportunità di prolungare la vita di un bene è influenzata da una moltitudine di fattori. Inoltre, l'incertezza sulle tendenze economiche future rende fondamentale che le aziende prendano conto degli investimenti sostenuti richiesti per garantire la sicurezza richiesta da un impianto in fase di invecchiamento.

L'articolo prende in considerazione due eventi accaduti nel regno Unito, una grave catastrofe in un'industria petrolifera e del gas offshore in seguito ad un'esplosione sulla piattaforma Piper Alpha e poi un altro grave incidente in un impianto chimico onshore a Flixborough. Sebbene le cause che hanno innescato i due eventi potrebbero essere state diverse, c'è una somiglianza nelle circostanze. Nel primo caso, l'integrità dell'installazione è stata compromessa quando la piattaforma che era stata originariamente progettata per la produzione di petrolio è stata convertita in piattaforma del gas; nel secondo caso, il processo è stato compromesso quando un bypass non progettato è stato utilizzato per continuare a eseguire il processo durante un'interruzione del reattore. Quindi la causa principale risultò essere un programma di gestione della sicurezza insufficiente, in quanto le misure di protezione contro gli incendi e le esplosioni di quel tempo erano inadeguate.

Da questi eventi, l'Health and Safety Executive (HSE) del Regno Unito ha identificato alcuni fattori comuni tra le cause del processo di decadimento che vanno oltre l'integrità delle infrastrutture fisiche e vanno ad estendersi alla cultura dell'organizzazione.

Questi potrebbero includere misure eccessivamente semplificate e non curanti delle misure veramente importanti sul vero stato dei beni, perché spesso gli indicatori che evidenziano gli incidenti non forniscono alcuna indicazione in tempo reale sulla misura delle prestazioni o sull'integrità del processo oppure il fatto della gestione remota delle risorse dalle sale di controllo tramite solo gli schermi dei computer non evidenzia gli indicatori rivelatori di problemi meccanici.

Sebbene la tecnologia e l'automazione abbiano portato enormi vantaggi attraverso una maggiore affidabilità nel funzionamento, non è una buona attitudine credere che le cose che sono accadute in passato non possano più si verificano perché "il computer non permetterà che accada".

Si sa che l'esperienza e la conoscenza delle persone viene portata via con la loro scomparsa e così come i piani delle infrastrutture passano di mano in mano, questo può determinare una perdita delle informazioni di progettazione critiche, per esempio gli sviluppi e le innovazioni dei processi possono portare a utilizzare gli impianti per uno scopo diverso da quello per cui erano originariamente progettato. In aggiunta a questi fattori, bisogna considerare che le pressioni costanti sui tempi di consegna, sulla riduzione dei costi e sul miglioramento dei ritorni finanziari ponendo l'attenzione solo nel breve-medio termine porta a considerare le attività di ispezione come ostacoli, e questa è una scelta incosciente con un impatto drammatico sul programma di manutenzione nel lungo termine, tutto ciò a discapito dell'integrità e dell'affidabilità del processo e del business.

Prima del disastro di Texas City, l'HSE era diventato sempre più preoccupato per le condizioni degli impianti del settore petrolifero e del gas offshore, tant'è che tra il 2004 e il 2007 ha eseguito una serie di ispezioni. Queste hanno evidenziato preoccupanti considerazioni, come il fatto che il 50% degli impianti era valutato con scarsi standard di manutenzione delle strutture, che all'interno dello stabilimento ci fosse una scarsa conoscenza ed efficienza dei processi di revisione e che tra le persone una scarsa comprensione dei rischi per la sicurezza dell'impresa.

Fortunatamente la risposta del settore fu rapida e un'ulteriore revisione effettuata due anni dopo ha rilevato che l'industria offshore stava stanziando notevoli investimenti per porre rimedio ai problemi evidenziati. In particolare, la priorità data al miglioramento della leadership nella gestione dell'integrità.

L'HSE del Regno Unito sta lavorando in modo proattivo su tutta l'industria energetica per garantire che i problemi riguardo l'invecchiamento delle risorse e l'estensione della vita vengono gestiti in modo efficace. Tra le azioni portate avanti, si ricordano la campagna di sensibilizzazione per le industria offshore sulla necessità di considerare i problemi dell'invecchiamento come elementi distinti, quindi come attività specifiche all'interno del processo di gestione dell'integrità degli asset; l'obbligo di singoli soggetti ad effettuare accertamenti circa il grado di rispetto dei requisiti della normativa sulla gestione dell'invecchiamento e l'estensione della vita; l'individuazione delle carenze e l'applicazione di un adeguato programma di azioni correttive unito alla collaborazione per sviluppare un comune approccio alla gestione degli impianti obsoleti e al prolungamento della vita utile.

Il risultato di tutti questi interventi sta nel fatto che gran parte degli impianti oggi in funzione sta lavorando in sicurezza nonostante il superamento del ciclo di vita previsto al momento della costruzione, e può continuare a funzionare in sicurezza anche negli anni a venire. Tuttavia, affinché ciò accada, si ribadisce l'importanza di effettuare studi di ipotesi sulla vita di un impianto e di non effettuare tagli agli investimenti e ai programmi di manutenzione, onde evitare conseguenze catastrofiche.

2.2 IL PROGRAMMA DELL'ASSET INTEGRITY MANAGEMENT

Il valore di un programma AIM ben definito ed eseguito correttamente è stato riconosciuto in molti paesi per la garanzia dell'integrità delle risorse, la quale rappresenta un elemento critico nella sicurezza dei processi.
Tuttavia, oltre alla sicurezza della vita, l'integrità degli asset è anche fortemente connessa al business e alla sostenibilità ambientale dell'industria e dei suoi processi produttivi.
Per questo motivo, la sua gestione presenta una serie di sfide, come per esempio la distribuzione delle responsabilità per l'esecuzione del programma di integrità degli asset all'interno dell'organizzazione.
A tal proposito, la sezione 1.2 delle *Linee guida per la gestione dell'integrità degli asset* afferma che "l'AIM è un prodotto di molte attività, solitamente eseguite da molte persone..." Quindi fa capire che si tratta di un approccio che potrebbe facilmente cadere nella disorganizzazione.
Inoltre, questo programma di gestione è spesso ponderato verso l'affidabilità e la sicurezza dei processi, spesso tralasciando l'attenzione alla sostenibilità complessiva.
Questo potrebbe comportare la presenza di rischi significativi per la sicurezza "non coperti", quando in realtà dovrebbero essere affrontati nella considerazione dell'intero ciclo di vita dell'apparecchiatura.

2.2.1 Il team direttivo di gestione

La leadership del management è un elemento fondamentale per stabilire una cultura della sicurezza dei processi. Nello specifico, si elencano i ruoli e le responsabilità primarie per la leadership in AIM:

1. Stabilire la direzione e l'ambito del programma AIM a livello aziendale;
2. Garantire la qualifica delle persone che svolgono le attività e garantire strumenti adeguati e metodi efficaci nello svolgimento di esse;
3. Garantire l'esecuzione delle attività del programma AIM nei tempi e nei modi pianificati, l'acquisizione e l'analisi dei risultati e il completamento delle azioni correttive;
4. Garantire l'esecuzione di controlli appropriati all'interno della struttura per tutte le attività correlate;
5. Fornire tutte le risorse necessarie per la realizzazione delle attività.

La direzione al livello più alto di un'organizzazione ha l'oneroso e importante compito essere impegnata nell'esecuzione del programma di sicurezza del processo affinché si giunga al suo successo.
Più l'organizzazione è grande e diversificata, più le politiche aziendali hanno la probabilità, o meglio, il rischio di assumere una forma disorganizzata. D'altro canto, l'implementazione di un programma di integrità delle risorse può portare a incoerenza nell'attuazione all'interno dell'organizzazione e a incapacità di dirigere tutte le risorse necessarie.

Ecco il motivo per cui la leadership e l'organizzazione sono estremamente necessarie per assegnare efficacemente le responsabilità sopra elencate. Basti pensare che l'integrità degli asset, tra le discipline della sicurezza dei processi, è unica in quanto sono necessarie diverse aree di competenza e responsabilità per raggiungere gli obiettivi fissati.

Come possiamo vedere nella figura sottostante, le responsabilità sono suddivise tra i gruppi di operazioni, di manutenzione, di affidabilità e di ispezione, di gestione del progetto e personale addetto alla sicurezza dei processi e questo fa sì che tutti dovrebbero avere un certo livello di responsabilità nel programma AIM. Considerando un gruppo dirigente di gestione così vasto, la **comunicazione** e la **cooperazione** tra ciascuno di questi sottogruppi sono necessarie per il successo.

Figura 1. Azioni necessarie per mantenere l'affidabilità delle apparecchiature. Moyer, L., & Hedlund, M. (2019). Creating an effective asset integrity program. *Process Safety Progress*, *38*(2), e12008.

Riguardo il gruppo dirigente, questo dovrebbe essere abilitato a svolgere diverse azioni, ovvero raccomandare la politica e la pratica AIM per la propria area di responsabilità, tra cui la determinazione dell'ambito del programma; determinare il modo migliore per acquisire i dati rilevanti per le proprie attività e monitorare i progressi delle aree che richiedono maggiore attenzione e risorse; rivedere ed elaborare i risultati provenienti dal Process Safety Management (PSM) per le proprie strutture e lavorare per affrontare i risultati relativi all'integrità degli asset; monitorare lo stato generale dei processi, includendo sia uno sguardo ai dati passati sia a nuovi codici e al miglioramento continuo, e infine inviare rapporti periodici alla direzione aziendale, sempre per rispettare il discorso sulla comunicazione tra le aree.

La comunicazione tra i diversi gruppi sull'integrità delle risorse e sui problemi del ciclo di vita delle apparecchiature che potrebbero avere un impatto sulla sostenibilità delle strutture è facilitata dal fatto che si ha la rappresentanza di ciascuno dei gruppi chiave coinvolti. Inoltre, è tangibile la maggiore consapevolezza dei ruoli di ciascun gruppo, e ciò può portare a potenziali miglioramenti in termini di efficacia ed efficienza.

Il continuo monitoraggio dello stato di avanzamento del programma AIM consente al team di leadership di essere proattivo anziché reattivo nell'affrontare eventuali problemi associati alla sua implementazione.

Durante l'azione di revisione, è buona norma porsi principalmente tre domande, la prima riguarda l'andamento del programma, la seconda interroga sull'esistenza di eventuali lacune e l'ultima ragione sui nuovi cambiamenti che potrebbero essere in arrivo.
Sebbene la sicurezza svolga un ruolo fondamentale nella gestione del rischio, le attività non coperte possono rappresentare un rischio aziendale significativo con un raggio di azione eccessivamente elevato. Avere una leadership diversificata con visibilità sulla sicurezza, sul business e su altri potenziali rischi può garantire che il giusto livello di copertura sia applicato a tutte le risorse della struttura.

2.2.2 Fase iniziale del programma AIM

Un passo importante nella determinazione di un programma AIM consiste nel rendersi conto che tutte le apparecchiature non sono realizzate allo stesso modo e non possono essere gestite insieme in un unico processo AIM.

Gli asset si differenziano per i codici e gli standard di progettazione, le tecnologie e le frequenze di ispezione, le modalità di guasto e le considerazioni sulla riparazione, per questo motivo dovrebbero essere documentati sottoprocessi separati per ogni tipo di attrezzatura. Qui entrano in gioco i cosiddetti "**steward**", ossia esperti con una conoscenza dettagliata riguardo quel determinato tipo di attrezzatura.

Nello sviluppo delle procedure per il programma AIM, un approccio a più livelli può fornire il giusto livello di informazioni alle risorse giuste in tutte le parti del programma.
In sostanza, si ha questa gerarchia di procedure caratterizzata da:

- Una procedura generale, mantenuta dal gruppo dirigente della direzione; si occupa di definire l'ambito e le aspettative complessive del programma, le responsabilità del gruppo dirigente e gli strumenti standard da utilizzare.
- Una procedura dettagliata, ove gli steward del tipo di attrezzatura sono rivestiti della responsabilità delle procedure specifiche. Tali procedure dovrebbero coprire l'ambito della copertura del programma per quel tipo di apparecchiatura, le responsabilità lungo il suo ciclo di vita e le informazioni generali sui metodi e le frequenze di ispezione. Inoltre, sono responsabili dell'invio dei risultati dei controlli al team di leadership.

2.2.3 Applicazione del programma AIM al ciclo di vita completo

Ulteriore considerazione riguarda l'applicazione del programma per tutta la durata del ciclo di vita, dalla progettazione dell'attrezzatura allo smantellamento della stessa.

È facile convincersi che le prime decisioni prese in **fase di progettazione** hanno un impatto significativo sulla gestione degli asset futuri. I materiali di costruzione, le valutazioni e le specifiche di progettazione, i pezzi di ricambio delle attrezzature, le considerazioni sull'ubicazione delle strutture e altre decisioni influiscono notevolmente sulla gestione e sui costi del programma AIM. Affinché il processo di progettazione abbia successo, gli esperti in materia devono essere allineati con gli obiettivi del programma AIM.

Il processo di capitalizzazione può essere finalizzato alla riduzione dei costi ove possibile, pensando nel breve termine senza considerare l'aumento dei costi operativi e la ridotta affidabilità e operatività. Ed è qui che gli steward dovrebbero essere chiamati per definire le procedure di integrità meccanica pertinenti e fornire indicazioni durante la progettazione per garantire che gli standard siano rispettati, in aggiunta all'ideale di mantenere la coerenza tra progetti e aree operative.

La **fase operativa** del ciclo di vita è il fulcro perché richiede il massimo livello di coordinamento e comunicazione tra le organizzazioni di produzione, manutenzione, sicurezza dei processi e affidabilità. Il personale di produzione deve essere consapevole di come gestire correttamente ed efficacemente le proprie aree per aumentare i tempi di attività della struttura e ridurre i rischi.

La **fase di disattivazione**, quindi lo smantellamento, potrebbe non sembrare parte di un programma AIM, ma è particolarmente importante quando esiste la possibilità di riutilizzare l'attrezzatura.

E l'articolo si conclude, quindi, con la dimostrazione che il programma AIM può essere coinvolto in tutte le fasi dell'intero ciclo di vita del processo; e qui si ribadisce che l'ottimizzazione dei costi è fondamentale per massimizzare l'affidabilità e l'operatività. Queste due caratteristiche, poi, assumono un valore ancora più importante se durante la progettazione e la costruzione degli asset vengano consultate quelle procedure definite dagli esperti in materia. Ciò garantisce una componente fondamentale nella prevenzione degli eventi di rischio incidentale e dei conseguenti impatti sulla sicurezza e sull'ambiente.

2.3 DEFINIZIONE DI UN PROGRAMMA AIM CON UN APPOCCIO BASATO SUL RISCHIO

Le decisioni nell'ambito dell'AIM sono state intraprese sempre utilizzando approcci e metodi tradizionali basati, per esempio sull'approccio prescrittivo.

Ultimamente, però, la complessità e l'innovazione coinvolte negli asset richiedono approcci più avanzati per operare a un livello ottimale, difatti una maggiore esperienza operativa e una maggiore comprensione dei fallimenti (e delle sue conseguenze) portano alcune parti dell'industria ad adottare un approccio più informato alla pianificazione.

Gli **approcci basati sul rischio** sono utilizzati in molti settori dell'industria e, a differenza di molti altri approcci, offrono una certa **flessibilità** nella gestione dei beni pur rispettando gli stessi obiettivi. Questa flessibilità, difatti, permette di dare la giusta priorità a diversi tipi di azioni, che vengono intraprese secondo alcune misure di rischio identificate.

L'obiettivo principale è la riduzione del rischio al livello ragionevolmente più basso e nell'articolo "***A risk-based approach to asset integrity management***" viene spiegata una metodologia basata sul rischio per stimare il tempo ottimale di sostituzione o riparazione di una struttura, in un sistema comprendente un numero di componenti, entro i limiti del budget disponibile, in modo tale da massimizzare il beneficio finanziario di tutta l'azione intrapresa.

2.3.1 Definizione di rischio

La definizione generale di rischio è "una combinazione della probabilità di un evento e delle sue conseguenze, è una deviazione dal normale o previsto. Numericamente, è un prodotto della probabilità del verificarsi di un evento e della conseguenza dell'evento."

Di conseguenza, un approccio basato sul rischio va a considerare il fallimento prendendo atto dei due elementi che costituiscono il rischio: la probabilità di fallimento e la conseguenza di tale fallimento.

Laddove le due componenti di rischio, ovvero la probabilità e la conseguenza di un evento di guasto, siano espresse quantitativamente, il rischio sarà espresso in termini di "perdita attesa". La perdita attesa può essere definita quantitativamente come il prodotto delle conseguenze (C) e la probabilità (P) del suo verificarsi:

$$R = C \times P \qquad (1)$$

2.3.2 I metodi di analisi del rischio applicata all'AIM in generale

Generalmente classificati come qualitativi o quantitativi, e potrebbero esistere anche approcci intermedi caratterizzati da attributi sia qualitativi che quantitativi.

Analisi qualitativa
I risultati dell'analisi e di valutazione del rischio dipendono dal giudizio e dall'esperienza ingegneristici dell'utente. Il vantaggio principale è la possibilità di effettuare la valutazione in assenza di dati numerici dettagliati.
Questa analisi rappresenta anche il punto di partenza per attuare un'analisi quantitativa del rischio e frequentemente viene utilizzata per avere una visione totale a livello di sistema.
C'è da dire che non è un metodo molto dettagliato e fornisce solo un'ampia categorizzazione del rischio. Un esempio di analisi qualitativa è l'approccio della matrice di rischio ("risk matrix approach") dove approccio, probabilità e conseguenze del fallimento sono descritte qualitativamente in intervalli (ad es. alto, medio o basso).

Analisi quantitativa
L'aumento della complessità dei sistemi, però, ha evidenziato un difetto delle valutazioni qualitative del rischio, ossia la mancanza di perspicacia.
E qui entra in azione l'analisi quantitativa che assegna valori numerici alla probabilità e alle conseguenze del guasto.
Alcuni metodi di analisi qualitativa possono diventare quantitative attraverso la stima numerica dei valori di probabilità e conseguenza di guasto. Ciò può essere eseguito utilizzando una varietà di riferimenti come database di guasti generici o calcolati mediante analisi ingegneristiche e statistiche specifiche.

Nell'articolo in questione, si considera a scopo dimostrativo il sistema di una turbina eolica ove tra i componenti ad alto rischio è stata identificata la struttura della torre a cui, per semplicità, si farà riferimento con il termine "struttura".

Gli autori hanno descritto una metodologia per eseguire un'analisi quantitativa sulla struttura che è stata identificata come ad alto rischio e hanno evidenziato come i risultati di questa analisi alimentano la pianificazione di un processo decisionale nella gestione dell'integrità del sistema.

Il meccanismo di danno scelto per dimostrare la metodologia è la corrosione e, assumendo che il funzionamento della struttura sia business-critical, la conseguenza considerata e quantificata è, per semplicità, la perdita di produzione.

2.3.3 Esempio: modello di meccanismo di danno probabilistico quantitativo per guasto dovuto a corrosione

L'articolo illustra un semplice modello probabilistico di meccanismo di danno della struttura della torre soggetta alla corrosione generale. Per semplicità, si suppone che questo sia l'unico meccanismo di danneggiamento che causa il cedimento della struttura e che vi sia una rottura del rivestimento.

La vita residua (RL) della struttura può essere calcolata come:

$$RL = \frac{(T_c MAT)}{CR} \qquad (2)$$

dove RL è la vita residua (anni); T_c lo spessore attuale della struttura (mm); MAT lo spessore minimo ammissibile per mantenere l'integrità della struttura (mm); e CR il tasso di corrosione (mm/anno).

$$T_c = T_o CR \times t \qquad (3)$$

Se T_o è lo spessore nominale originale della struttura, allora alla fine di *t* anni:

L'affidabilità di un elemento di un sistema può essere determinata sulla base di una funzione di prestazione che, matematicamente, può essere descritta come:

$$Z = (X_1, X_2, \ldots X_n) = R - L \qquad (4)$$

dove *R* è la resistenza o forza, *L* è il carico e (X_i) sono carichi casuali rilevanti

Lo stato limite può essere definito come:

$$Z = 0 \qquad (5)$$

Di conseguenza:
$Z < 0$ => elemento è nello stato di fallimento
$Z > 0$ => elemento è nello stato di sopravvivenza.

Quando RL è 0, l'equazione di stato limite può essere espressa come:

$$RL = \frac{(T_C - MAT)}{CR} = \frac{(T_O - CR \times tMAT)}{CR} = 0$$

Dove $(T_O - CR \times tMAT)$ può essere riorganizzato in:

$$[T_O - MAT] - [CR \times t] = 0 \qquad (6)$$

dove il primo termine rappresenta la resistenza strutturale (R) e il secondo l'effetto del carico (L).

Per la definizione dei valori delle variabili, occorre fare alcune considerazioni:

- Il CR (tasso di corrosione) può essere derivato da misurazioni periodiche in servizio della perdita di metallo derivante dalla corrosione o da test di laboratorio.
- T_c (spessore attuale della struttura) è noto dalle più recenti misurazioni di spessore sulla struttura, diciamo durante l'anno di valutazione. Se non sono disponibili misurazioni recenti dello spessore, si può presumere che T_c sia uguale a T_o come specificato dal progettista comprese tolleranze, tolleranza di corrosione, ecc. e RL calcolato dall'anno di installazione.
- MAT (spessore minimo ammissibile) è calcolato dal progettista per prevenire guasti per sovraccarico, collasso, ecc., a seconda dei casi.

Tra gli strumenti di analisi statistica disponibili, gli autori hanno spiegato l'utilizzo di @RISK (di Palisade per Microsoft Excel) per descrivere in maniera probabilistica tutte le variabili indipendenti e RL viene quindi calcolato utilizzando la tecnica di simulazione Monte Carlo (MCS). In questo modo, il RL è in realtà una distribuzione di valori, in cui applicando l'equazione (2) per ogni anno, si può ottenere la probabilità annuale di guasto nel tempo.

Questa probabilità annuale di fallimento va poi a indicare la proporzione delle strutture sopravvissute l'anno precedente che si prevede fallirà entro l'anno in esame.

$$Probabilità\ annuale\ di\ fallimento\ =\ P(RL\ \leq\ 0)$$

Questa probabilità annuale di guasto (tasso di guasto) rispetto alla curva temporale viene utilizzata nella fase successiva in cui è possibile ottimizzare i tempi di un'azione (riparazione/sostituzione) in modo da ottimizzare il beneficio finanziario.

2.3.4 Ottimizzazione finanziaria basata sul rischio dell'azione di manutenzione data una tendenza ai guasti

L'invecchiamento degli impianti produttivi richiede normalmente una sostituzione ma ciò non è possibile considerando l'aumento della concorrenza, e quindi l'opzione più ragionata ricade nel prolungamento della loro vita utile. Per poter ottenere ciò, si delineano progetti di manutenzione che vengono valutati dai responsabili delle decisioni perché hanno necessità di comprendere le implicazioni anche dal punto di vista finanziario, analizzando il costo delle conseguenze di guasti. Ad ogni progetto sono associati dei costi che sostanzialmente sono investimenti effettuati con l'aspettativa di un certo ritorno finanziario, e questo rappresenta il criterio di decisione e scelta del progetto.

Analisi finanziaria: concetto di valore attuale netto (Net Present Value)
Tra le tecniche finanziarie più diffuse, in questo articolo è stata presa in considerazione la **tecnica NPV**, una forma di analisi del "flusso di cassa scontato (DCC)" ove la variabile fulcro è il VAN di un progetto che rappresenta il valore attuale (corrente) dei flussi di cassa futuri totali, ovvero al netto dei flussi di cassa sia positivi (ricavi) che negativi (costi).
Il VAN (Valore Attuale Netto, in italiano) viene calcolato come segue:

$$NPV = \sum_{t=0}^{N} (C_t) \div (1 + r)^t \qquad (8)$$

N è la vita del progetto (anni);
t la tempistica del flusso di cassa (anno);
r il tasso di interesse, o tasso di sconto;
C_t il flusso di cassa nell'anno *t*.

Analisi finanziaria: concetto di rischio misurato in termini di valori attesi (EV)

Il rischio associato a un progetto è espresso in termini di VAN utilizzando EV. L'**EV** di un evento di guasto è il prodotto della probabilità di verifica di un evento e il costo della conseguenza di tale evento. Questi due elementi sono valutati direttamente dalle analisi quantitative precedentemente illustrate.

Il VAN di un progetto con esiti incerti è la somma dell'EV di tutti i futuri flussi di cassa attualizzati, come segue:

$$NPV = \sum_{t=0}^{N} (P_t \times C_t) \div (1 + r)^t \qquad (9)$$

dove p_t è la probabilità che l'evento si verifichi al tempo *t* .

L'ottimizzazione massimizza il VAN dell'azione (riparazione/sostituzione) in esame.
Gli afflussi di cassa sono trattati come positivi e i deflussi di cassa come negativi; il denaro speso per un'azione è negativo, anche i costi delle conseguenze del fallimento dovute a un guasto (principalmente perdita di produzione che abbiamo considerato qui, per semplicità) sono anch'essi negativi; i costi di fallimento evitati grazie all'azione da intraprendere sono considerati positivi.

Considerando che il periodo di pianificazione va da $t = 0$ a $t = N$ e l'anno di valutazione è $t = 0$, il VAN di un'azione intrapresa in un qualsiasi anno $t = n$ è dato da:

$$NPV = (Valore\ attuale\ atteso\ di\ azioni\ intraprese\ nell'anno\ t = n) + (Valore\ attuale\ atteso\ di\ costi\ dovuti\ a\ interruzioni\ prima\ dell'azione) + (Valore\ attuale\ atteso\ di\ costi\ dovuti\ a\ interruzioni\ evitate\ grazie\ all'azi$$

I primi due termini dell'equazione (10) sono negativi, il terzo è positivo.

Quindi:

$$NPV = \left\{ - \left[\sum_{t=n}^{t=N} (CP_t) \div (1+r)^t \right] + \left[- \sum_{t=0}^{t=n} (p_t \times CB_t) \div (1+r)^t \right] \right\} \left\{ + \sum_{t=n+1}^{t=N} (p_t \times CB_t) \div (1+r)^t \right\} \qquad (11)$$

Nell'Equazione (11), per il VAN di un'azione intrapresa al tempo $t = n$, si può definire:
CB_t : i flussi di cassa associati alla produzione nell'anno t ;
CP_t : i flussi di cassa connessi all'attuazione del progetto nell'anno t ;
N : il periodo di pianificazione strategica del pianificatore della manutenzione;
n : l'anno in cui si propone di intraprendere l'azione;
p_t : la probabilità che l'evento (fallimento che determina la conseguenza) si verifichi nell'anno t ;
r : il tasso di interesse, cioè il costo del denaro.

L'algoritmo di ottimizzazione calcola **l'anno di intervento manutentivo** per il quale il **VAN è massimo**, subordinatamente ai vincoli previsti, tra cui si presume che il costo dell'azione includa anche il costo dei problemi di avviamento e che una volta che la struttura sia funzionante, inizi il suo ciclo di vita con un tasso di guasto relativamente molto basso.

Gli input chiave per il modello di ottimizzazione sono i seguenti:

- la probabilità annuale di guasto rispetto ai valori temporali;
- il costo conseguente al guasto (interruzione non pianificata);
- tassi di interesse e deprezzamento a seconda dei casi;
- eventuali vincoli finanziari, come il limite del budget di manutenzione annuale;
- eventuali vincoli non finanziari, ad esempio quelli sui tassi di guasto dovuti alle norme di sicurezza.

2.3.5 Applicazione del modello come ottimizzazione dell'ispezione in servizio

Nella parte conclusiva dell'articolo viene dimostrato come il modello appena descritto potrebbe essere applicato, oltre alle azioni di sostituzione, anche alle azioni ispettive, dove verrebbe considerato il costo dell'ispezione in servizio.
Considerando che tali azioni sono normalmente contabilizzate come "spese" nell'anno in cui si verificano e si tratta di costi relativamente bassi, si prevede che il modello suggerisca che l'anno di ispezione ottimale sia il primo anno del periodo di pianificazione.
Per risolvere questo problema, si considera di:

- ottimizzare la data dell'azione come se l'azione fosse sostitutiva;
- ispezionare l'attrezzatura prima di questa data di sostituzione calcolata;
- confrontare l'effettivo danno ai componenti riscontrato durante l'ispezione con le condizioni previste;
- sostituire il componente se necessario o ricalcolare una nuova data di sostituzione ottimizzata.

Nel modello di ottimizzazione appena presentato, è necessario puntualizzare che se in un sistema di strutture esiste un vincolo di bilancio che non consente di intraprendere una serie di azioni in un determinato periodo di pianificazione strategica, è possibile effettuare un'ulteriore ottimizzazione utilizzando l'approccio, e poi è stato dimostrato che l'anno ottimale di sostituzione può essere calcolato quando il VAN dell'azione di manutenzione è massimizzato.

Il modello di analisi del rischio quantitativo presentato nel documento è un notevole supporto per intraprendere decisioni nell'A.I.M in quanto implementa un approccio che porta ad una riduzione al minimo dei rischi associati ai guasti, permettendo di confluire in modo ottimale le risorse a quei componenti del sistema di asset identificati come ad alto rischio.

2.4 IMPLEMENTAZIONE DI UN PROGRAMMA AIM BASATO SUL RISCHIO

Nell'ultimo anno, Felipe A. Henao ha pubblicato un articolo intitolato "Risk-based decisions: Implementing the asset integrity program" dove ha voluto raccontare la sua esperienza nell'implementazione di tale programma, andando a chiarire gli strumenti che possono essere utilizzati per ridurre costi e tempi e delineando i passaggi fondamentali per evitare errori nell'implementazione.

L'autore ha affermato che il punto di partenza è la definizione del *framework AIM*, ossia una rappresentazione dell'incorporazione degli elementi AIM, suddivisibile in quattro raggruppamenti:

1_ Governance e leadership;

2_ Capacità organizzativa;

3_ Processi per produrre risultati allineati con gli obiettivi aziendali (RAGAGEP]);

4_ Tecnologia per assistere l'esecuzione del processo.

Cosa sono i RAGAGEP?

RAGAGEP è l'acronimo per "Recognized And Generally Accepted Good Engineering Practices", ovvero "Procedure generalmente accettate e riconosciute nella buona ingegneria", e rappresentano "**codici standard**" che sono stati ampiamente adottati dai governi federali, statali o locali e comportano che qualsiasi edificio costruito in quelle giurisdizioni deve essere costruito secondo tali codici; oppure possono rappresentare "**documenti di consenso"**, ossia documenti che riportano i requisiti in base ai quali tutta la progettazione, l'installazione e la manutenzione delle apparecchiature deve essere conforme ai tali. In sintesi, i RAGAGEP descrivono le modalità generalmente approvate per eseguire specifiche attività nell'ambito industriale.

Detto questo, poi occorre determinare la quantità di asset che dovrebbero essere coperti dal programma, la complessità o varietà dei processi industriali gestiti e il tempo necessario.

Si nota bene che l'implementazione di processi come R.B.I. richiede un ingente investimento in risorse quindi un approccio metodologico supportato da una buona strategia di implementazione è utile per consentire alle organizzazioni e ai loro dipendenti di concentrare sforzi e tempo.

L'autore ha poi analizzato i risultati di un'implementazione formale di 5 anni di un Programma AIM in una compagnia Oil & Gas, con diversità di asset, processi industriali, lingue e livelli di conoscenza, e ha fissato i punti fondamentali appresi da questa esperienza:

- Scegliere molto attentamente l'ambito di attuazione, ovvero luoghi degli impianti, dei sistemi e delle apparecchiature.
- Determinare gli elementi del programma AIM, quindi selezionare i processi di integrità degli asset seguendo RAGAGEP, ruoli e responsabilità e tecnologia di supporto;

- Progettare e implementare il framework AIM per i processi selezionati (questo è il passaggio fulcro di tutto e include una documentazione di processi e procedure);
- Definire un'autovalutazione per identificare i principali divari tra "così è" e "così dovrebbe essere" per ciascun elemento.
- Stabilire un approccio metodologico per implementare il programma AIM basato su criteri di analisi delle conseguenze;
- Definire un piano d'azione di implementazione a lungo termine (3-10 anni)
- Effettuare attività di revisione periodica per identificare i livelli di avanzamento nell'attuazione del programma AIM.

Nel primo punto si è voluto porre una particolare attenzione alla definizione dell'ambito perché l'obiettivo è quello di ridurre significativamente le risorse e i processi in gestione fino a un punto in cui il programma viene applicato rigorosamente alle apparecchiature dei processi più importanti, determinando un aumento della sua efficacia e una riduzione dei costi.

Riguardo il punto sulla definizione di un approccio metodologico, un esempio è il RIL (**Required Integrity Level**) ossia il Livello di Integrità Richiesto, progettato da un team di professionisti per determinare il livello di impatto, quindi le conseguenze, che le principali attrezzature hanno in un ambiente industriale. Questa tipologia di metodo si concretizza come un semplice screening, che aiuta a concentrare gli sforzi e stabilire un modello di implementazione che tenga conto delle strutture, dei processi o delle complessità.

I passi più importanti si identificano in 4 punti:

1) **Definizione di un modello RIL**

Come illustrato sopra, il RIL è un modello di base che può essere sviluppato internamente e dovrebbe essere basato sui criteri di tolleranza al rischio di ciascuna organizzazione. Nel processo di sviluppo è importante identificare e dimensionare i fattori legati al contesto operativo, come le sostanze pericolose, nonché i limiti massimi e i livelli di esposizione umana presenti negli impianti e nelle strutture che rientrano nell'ambito di attuazione del Programma AIM. Successivamente, la costruzione di un diagramma di flusso decisionale è utile per stabilire il livello di integrità per ciascuna apparecchiatura all'interno del processo e soprattutto per determinare l'importanza di qualsiasi apparecchiatura all'interno di un processo.

2) **Valutazione RIL**

Come esposto nell'ultimo punto, le attività di revisione sono essenziali per ottenere risultati soddisfacenti. A tale scopo, è bene identificare sezioni isolate che rappresentano circuiti e utilizzarle come input per le revisioni, meglio ancora se effettuato direttamente sul campo d'azione. Questa analisi periodica dovrebbe essere eseguita con l'utilizzo di un kit apposito che consenta di identificare le fonti dei meccanismi di guasto e le conseguenze stimate.

3) **Definizione della strategia AIM**

Al termine della identificazione del RIL dell'impianto, il passaggio successivo è stabilire l'applicazione dei processi AIM per ogni apparecchiatura classificata. Normalmente, un asset che richiede più tempo e risorse per la gestione dell'integrità, può essere incorporato con maggiore rigore nei livelli RIL più alti, richiedendo un'implementazione RAGAGEP più restrittiva, mentre gli altri livelli possono assumere la stessa come raccomandazione. In questo modo si ottiene un approccio preciso e limitato con un risultato favorevole agli obiettivi dell'organizzazione. La Figura 3 presenta un esempio di implementazione del processo AIM basato sul rischio e secondo le categorie RIL.

		AIM Strategy			
		Equipment category (ISO 14224)			
RIL	**Application**	**Mechanical**	**Rotating**	**Safety & Control**	**Electrical**
1	Shall / Must	API 580; 581 (RBI); 1160; 579 (FFS)	SAEJ1011; 1012; 1739 (RCM)	ISA 61508; 615011 (FSM); 62402 (OBE)	SAEJ1011; 1012; 1739 (RCM)
2	As necessary	API 580; 581 (RBI); 1160; 579 (FFS) / Prescriptive	SAEJ1011; 1012; 1739 (RCM) / Prescriptive	ISA 61508; 61511 (FSM); 62402 (OBE) / Prescriptive	SAEJ1011; 1012; 1739 (RCM) / Prescriptive
3	As necessary	Preventive / Corrective	Preventive / Corrective	Preventive / Corrective	Preventive / Corrective

Figura 3. Strategia di Asset Integrity Management basata sull'approccio Required Integrity Level, Henao, F. A. (2021). Risk-based decisions: Implementing the asset integrity program. *Process Safety Progress*, *40*, S24-S31.

4) **Attuazione del programma AIM**

Arrivati all'ultimo passaggio, ora si procede con la creazione di un piano d'azione completo che includa i processi RAGAGEP selezionati in conformità con la strategia AIM per ogni apparecchiatura come definito dal RIL. Si procede anche con il dettaglio di risorse, materiali, tempi e metodi di ispezione. Questa è la fase in cui il Programma AIM viene tradotto dalla carta alla pratica e inizia a determinare i primi cambiamenti all'interno delle industrie.

5) **Vantaggi dell'approccio RIL nell'attuazione dell'AIM**

L'utilizzo dell'approccio RIL per l'attuazione del Programma AIM consente all'organizzazione di soddisfare i requisiti più esigenti ma anche di svolgere operazioni in sicurezza, di utilizzare le risorse in modo efficiente e di preservare e mantenere correttamente i beni. Si ribadisce, ancora una volta, l'importanza di focalizzarsi sull'ambito di applicazione, in modo che i risultati inizino ad essere evidenti relativamente presto, soddisfacendo anche l'esigenza di mantenere il livello di rischio "più basso possibile".

Si è sottolineato più volte che per garantire una migliore implementazione del Programma AIM, è importante avvalersi dell'Enterprise Management System (E.M.S.) e delle attuali conoscenze dell'organizzazione stessa, per avere un quadro ben chiaro della localizzazione di tutti i processi e delle giuste tecnologie per garantirne l'attuazione.

2.5 LA NASCITA DELLA CULTURA DELLA SAFETY INTELLIGENCE

Nell'era dell'informazione, soprattutto nell'attuale era dei Big Data e dell'Industria 4.0, c'è una costante necessità di trovare approcci migliori per garantire che le risorse siano allocate nel modo più efficace possibile, pur mantenendo buone prestazioni di sicurezza organizzativa.

E in questa era, lo sviluppo della scienza della sicurezza è approdato nella fase della Sicurezza 4.0: si tratta della "scienza della sicurezza computazionale", una nuova tecnologia ove le attività di raccolta ed elaborazione di dati per sviluppare strategie e prendere e attuare decisioni specifiche sono stati generalmente indicati come "intelligence".
L'intelligence, quindi, svolge un ruolo sempre più cruciale in molti ambiti ed è innegabile che le informazioni sulla sicurezza sono diventati una risorsa indispensabile, necessarie per un'efficace prevenzione dei rischi per la sicurezza e un processo decisionale informato sulla sicurezza, nonché un fattore chiave di successo.

L'autore Wang B. nell'articolo "*Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework*" ha proposto un nuovo concetto e termine di informatica di sicurezza, la "**Safety Intelligence (SI)"**. Sebbene la sua definizione risalga agli anni più recenti, nel campo della scienza della sicurezza, la SI esiste da prima che fosse proposto come concetto di sicurezza ed è sempre stato ampiamente applicato alle pratiche di gestione della sicurezza.

Attualmente, ci sono numerosi professionisti che, consciamente o inconsciamente, si impegnano in varie pratiche SI, ad esempio, varie tecnologie attuali nei sistemi di informazione sulla sicurezza, big data di sicurezza e intelligenza artificiale oppure anche gli approcci, ad es. gestione della sicurezza basata sui dati e gestione della conoscenza della sicurezza.

SI può fornire vari vantaggi alla gestione della sicurezza:

- accelerare il processo decisionale in materia di sicurezza;
- accesso alle informazioni sulla sicurezza (ad es. fornitura di informazioni utili per prendere decisioni in materia di sicurezza, rendere i dati e le informazioni sulla sicurezza affidabili e speciali, aumentare la qualità delle informazioni sulla sicurezza ed evitare dati e informazioni non necessari);
- miglioramento delle prestazioni sulla sicurezza;
- ridurre e gestire il rischio per la sicurezza (ad es. identificare, analizzare, valutare e prevedere il rischio per la sicurezza e migliorare la comprensione dei rischi per la sicurezza);
- aumentare l'efficacia e l'efficienza della gestione della sicurezza (ad esempio, identificare i punti di forza, i punti deboli, le opportunità e le sfide della sicurezza; nonché valutare e migliorare l'efficienza e l'efficacia della gestione);

- promuovere la condivisione delle informazioni sulla sicurezza (come migliorare il flusso e la diffusione delle informazioni sulla sicurezza);
- risparmio di tempi e costi di gestione della sicurezza.

C'è da dire che nell'era dei big data, le organizzazioni devono affrontare il **problema del sovraccarico** di informazioni, ed è risaputo che le informazioni sulla sicurezza non hanno valore se non sono pertinenti, aggiornate e affidabili.
Questo problema è risolto grazie alla SI, che può elaborare i dati raccolti per fornire le informazioni sulla sicurezza più accurate, utili e fruibili ai responsabili della sicurezza.

Nonostante i numerosi vantaggi potenziali per la gestione della sicurezza, molte organizzazioni non hanno ancora deciso di applicare un sistema efficace basato sulla SI, questo è anche dovuto al fatto che esistono pochissimi studi e altrettante poche guide pratiche per la sua implementazione. L'ostacolo maggiore è la mancanza di un quadro universale per la SI.

Pertanto, nell'anno corrente 2021 Wang B. ha scritto il seguente articolo "*Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework* ", con l'obiettivo di presentare un quadro generale sulla SI per promuovere i suoi studi e le sue pratiche future.

2.5.1 Significato della Safety Intelligence

Il termine "intelligence" va ad indicare le attività di raccolta, analisi, interpretazione e diffusione di dati e informazioni da utilizzare per i processi decisionali nell'ambito della sicurezza organizzativa.
In pratica, la SI semplifica l'analisi dei dati e l'elaborazione delle informazioni sulla sicurezza, consentendo ai responsabili di un'organizzazione riguardo le decisioni sulla sicurezza di accedere più facilmente, comprendere, analizzare, collaborare e agire sulle informazioni utili per il processo decisionale sulla sicurezza.

Però la SI ha più significati, come spiegato di seguito:

SI come prodotto: derivante dalla raccolta, valutazione, confronto, analisi e interpretazione di tutti i dati e le informazioni disponibili relativi a uno o più aspetti della sicurezza, che hanno un significato diretto o potenziale per la gestione della sicurezza di un'organizzazione, come lo sviluppo e l'esecuzione di piani di sicurezza, politiche, decisioni e controlli sui rischi per la sicurezza. In poche parole, SI è un prodotto di dati e informazioni di sicurezza elaborati (analizzati e interpretati).

SI come processo: che produce e diffonde informazioni mediante la pianificazione, la raccolta, la lavorazione e l'analisi dei dati e delle informazioni sulla sicurezza provenienti dall'ambiente interno ed esterno di un'organizzazione.

Le fasi del processo sono i seguenti:

1) pianificazione ponendo l'attenzione sulle esigenze dei responsabili decisionali in materia di sicurezza e di altri utenti coinvolti nell'organizzazione e sulle questioni di sicurezza della massima importanza;
2) raccolta mirata di dati e informazioni sulla sicurezza da varie fonti interne o esterne dell'organizzazione;
3) ordinamento, acquisizione e archiviazione di dati e informazioni sulla sicurezza, utilizzando vari metodi e tecnologie per acquisire informazioni dai registri di gestione della sicurezza fisica ed elettronica;
4) analisi dei dati quindi la conversione in informazioni attuabili che possono essere utilizzate a supporto delle decisioni di sicurezza; questo rappresenta il passaggio fondamentale nel processo;
5) resoconto e comunicazione dei risultati del processo a coloro hanno l'autorità e la responsabilità di agire sui risultati, per aiutare l'organizzazione a raggiungere il successo nella gestione della sicurezza e quindi migliorare le prestazioni.

Il processo di SI è illustrato nella seguente figura, dimostrando che il processo è ciclico, con una serie di passaggi interconnessi.

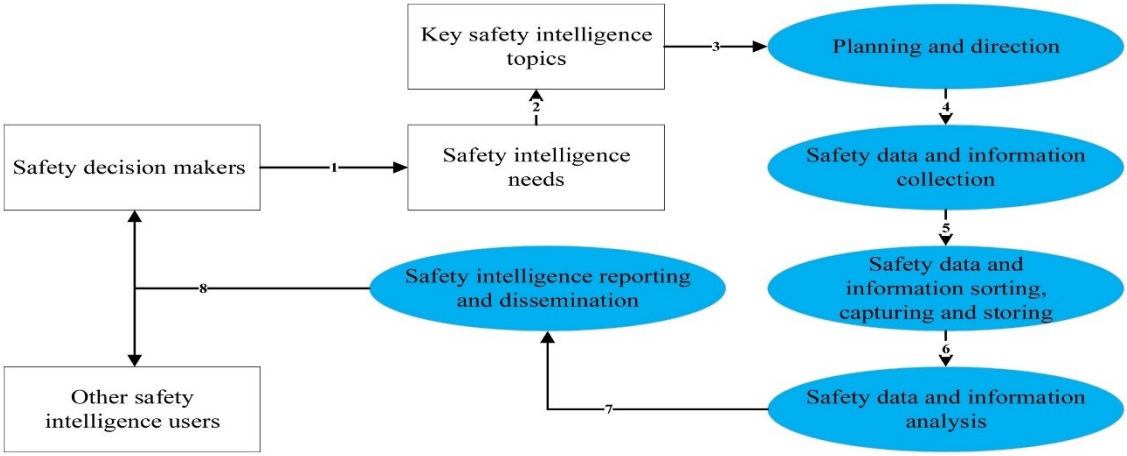


Figura 4. Il ciclo del processo di SI, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

In primo luogo, SI come processo è l'azione di sfruttare e trasformare dati sulla sicurezza frammentati in informazioni o conoscenze attuabili in un'organizzazione per aiutare a raggiungere sugli obiettivi di sicurezza. In secondo luogo, è un processo combina la memorizzazione e la raccolta di dati e informazioni sulla sicurezza con la gestione delle conoscenze sulla sicurezza per fornire input per i processi decisionali sulla sicurezza.
In terzo luogo, è un processo guidato dal software e dalla tecnologia che consente alle organizzazioni di analizzare dati grezzi da più fonti, estraendo approfondimenti che portano a decisioni di sicurezza più efficaci.
Infine, dal punto di vista della gestione della sicurezza, la SI è un processo per supportare le decisioni ben informate, che portano a un elevato livello di prestazioni di sicurezza all'interno di un'organizzazione.

SI come strumento, tecnologia e tecnica: in grado di trasformare i dati in informazioni, le informazioni in conoscenza e la conoscenza in decisioni, che permettono di migliorare la qualità e l'efficienza della gestione della sicurezza.
Per poter effettuare tutto ciò, si avvale dell'utilizzo di varie architetture e strumenti tecnologici come database, data warehousing e data mining. Pertanto, i rapidi progressi nelle tecnologie dell'informazione e l'applicazione di queste tecnologie nella gestione della sicurezza hanno ulteriormente intrapreso l'uso della SI nella gestione della sicurezza.

La SI utilizza anche una tecnologia di apprendimento automatico in grado di identificare le informazioni correlate per prevedere in modo intelligente le informazioni sulla sicurezza, rendendo così le cose più chiare per i responsabili della sicurezza dell'organizzazione. Inoltre, è capace di analizzare le cause degli incidenti e degli eventi di sicurezza ed eseguire diagnosi di sicurezza organizzativa in quanto offre un approccio basato su dati e informazioni per collegare gli obiettivi e le politiche di sicurezza strategici delle organizzazioni a procedure di sicurezza tattiche e azioni di sicurezza operativa. Ciò implica che la SI come strumento richiede molti altri strumenti originariamente sviluppati da molte discipline, come la scienza della sicurezza, la scienza dei dati, la scienza dell'informazione, l'informatica e la scienza dell'intelligenza artificiale.

SI come capacità di un'organizzazione di raccogliere ed elaborare dati e informazioni sulla sicurezza, di risolvere i problemi di sicurezza e di comprendere e prevedere rischi e cambiamenti in modo tempestivo per intraprendere azioni appropriate contro di essi.
La SI può rappresentare le seguenti capacità:

- capacità di apprendimento sulla sicurezza (ad es. acquisizione di nuove informazioni sulla sicurezza e comprensione delle ultime prove di ricerca sulla sicurezza),
- capacità di adattarsi e rimodellare l'ambiente di gestione della sicurezza di un'organizzazione,
- capacità di comprendere i fattori di gestione della sicurezza (come pericoli, incidenti, comportamenti non sicuri, cultura della sicurezza e risorse per la sicurezza) e di agire in modo appropriato dopo aver compreso;
- capacità di aggiungere più intelligenza all'attività di gestione della sicurezza delle organizzazioni.

2.5.2 Quadro teorico della Safety Intelligence

La SI mira principalmente a fornire supporto nella formulazione di un meccanismo decisionale nella gestione della sicurezza, basato sull'acquisizione di una conoscenza completa della sicurezza dell'organizzazione e dei fattori che la influenzano. È anche vero che la SI consente alle persone si tutti i livelli di un'organizzazione di accedere, interagire e analizzare dati e informazioni di sicurezza di alto valore, di identificare i rischi per la sicurezza (pericoli), di migliorare le prestazioni di sicurezza, scoprire opportunità di promozione della sicurezza e gestire la sicurezza in modo efficace, efficiente e sicuro.

Osservando la figura 4, la freccia nera indica il tradizionale ciclo di informazioni sulla sicurezza, che è "Dati sulla sicurezza → Informazioni sulla sicurezza → SI → Conoscenza sulla sicurezza".

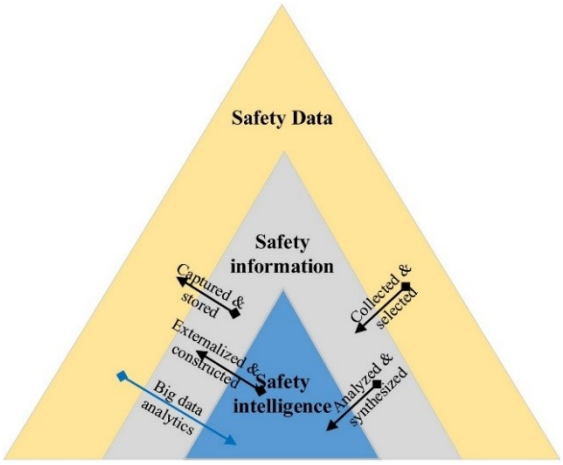


Figura 5. Interrelazioni tra dati sulla sicurezza, informazioni sulla sicurezza e SI nell'era dei big data, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

Secondo il tradizionale ciclo di informazioni sulla sicurezza, il processo di produzione sta trasformando i **dati sulla sicurezza,** ossia una raccolta di elementi di sicurezza di valore grezzo, in **informazioni sulla sicurezza**, quindi il risultato dell'analisi e dell'elaborazione dei dati in modo tale da stabilire relazioni tra gli elementi della sicurezza.
Successivamente l'altra freccia indica la trasformazione delle informazioni sulla sicurezza in **SI**, e infine in **conoscenze sulla sicurezza**.
Nell'era dei big data, i dati sulla sicurezza possono anche essere trasformati direttamente in SI mediante l'analisi dei big data. Ciò è illustrato dalla freccia blu.

I dati e le informazioni sulla sicurezza possono provenire da:
l'ambiente interno, si ottengono dati sugli investimenti, sulla sicurezza del processo provenienti da attività di monitoraggio e di ispezione e sulla sicurezza dei risultati, ossia i vari indicatori chiave delle prestazioni di sicurezza;
l'ambiente esterno si recepiscono informazioni su leggi e regolamenti nazionali sulla sicurezza, standard di sicurezza ufficiali e rapporti sugli incidenti, prove di ricerca sulla sicurezza e etc.

La figura seguente, invece, mostra il processo per ottenere i dati sulla sicurezza e il valore delle informazioni.

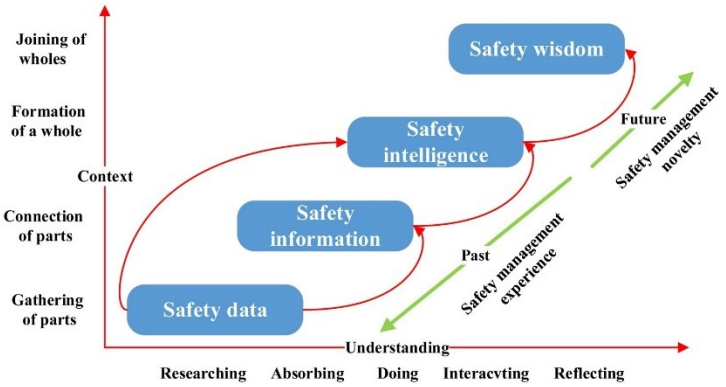


Figura 6. Raggiungimento dei dati sulla sicurezza e del valore delle informazioni nella gestione della sicurezza nell'era dei big data, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

La gestione della sicurezza è un processo decisionale in cui le decisioni vengono prese in modo continuo e sequenziale nel tempo.
A lungo termine, queste riguardano i possibili investimenti, strategie e politiche da adattare per soddisfare al meglio gli obiettivi dell'organizzazione.
A medio termine, si prendono decisioni tattiche, come ad esempio lo sviluppo di piani per ottimizzare la prevenzione quindi un aggiornamento del sistema.
A breve termine, invece, le decisioni si applicano nell'ambito operativo per assicurare un controllo quotidiano dei rischi nell'ambito del sistema di sicurezza.

Perciò la struttura di un buon sistema di gestione della sicurezza deve includere un ciclo di risoluzione dei problemi a **tre livelli: operativo, tattico e strategico**.

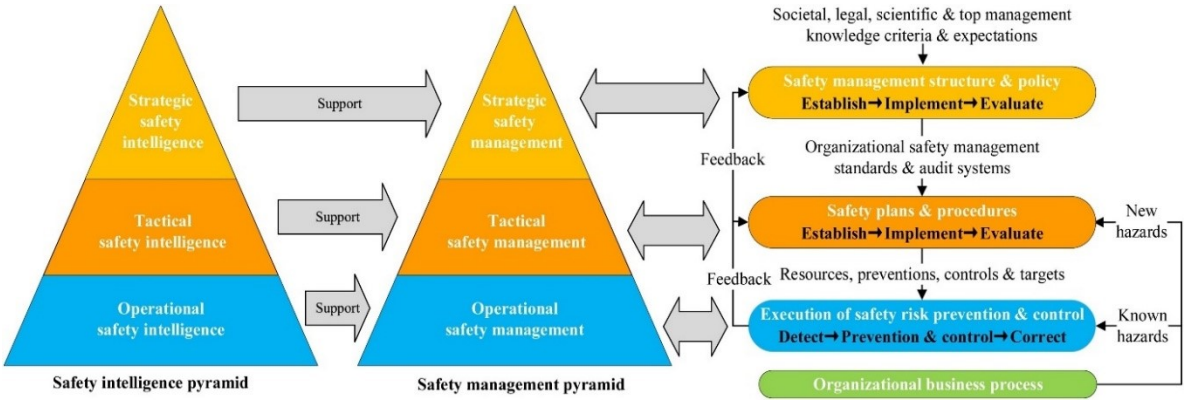


Figura 7. SI e piramide di gestione della sicurezza, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

Il **SI strategico** è progettato per aiutare i responsabili senior a comprendere il quadro generale che circonda i fattori di sicurezza; difatti si concentra sulle tendenze a lungo termine relative ai rischi, alle tecnologie o alle potenziali minacce.
Per tale motivo, si basa fortemente sulle stime della situazione, delineando così le strategie e gli investimenti ottimali per una gestione efficace.

Il **SI tattico** si concentra sui rischi e le minacce per la sicurezza, sull'identificazione dei pericoli quindi sui punti deboli, i punti di forza, le opportunità e le sfide della gestione della sicurezza; e fornisce informazioni relative a piani, procedure e tecniche di sicurezza. È una valutazione delle capacità immediate di gestione della sicurezza di un'organizzazione.

Il **SI operativo** si concentra su tutte le attività quotidiane di gestione della sicurezza,
è immediato e questo richiede che gli analisti della sicurezza abbiano accesso istantaneo ai dati e ai sistemi di raccolta delle informazioni elaborate. Infatti, questo livello differisce sia per il livello di dettaglio richiesto sia per la tempestività dei dati e delle informazioni sulla sicurezza. È da sottolineare che i tre tipi di SI si alimentano a vicenda e ciascuno ha un impatto sull'altro tipo, pertanto SI fornisce un approccio basato sui dati per collegare gli obiettivi di sicurezza strategici alle politiche di sicurezza tattiche e alle azioni di sicurezza operativa.

Unendo tutte le informazioni illustrate, l'autore Wang ha azzardato l'ipotesi di un **modello concettuale** per fornire una comprensione chiara e completa ai professionisti.

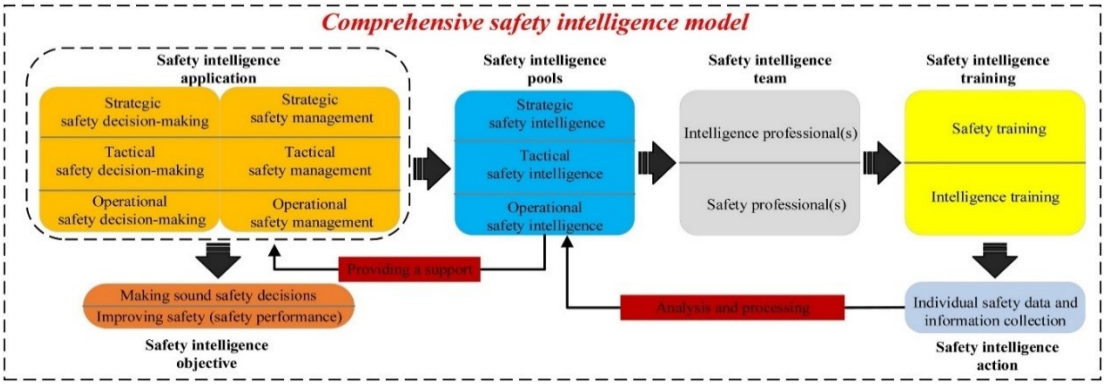


Figura 8. Modello concettuale SI proposto, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

Questo modello include sei unità:
la prima unità mostra i tre livelli di un sistema di gestione della sicurezza, quindi strategico tattico e operativo; la seconda unità indica la raccolta di dati e informazioni che possono fornire supporto ai tre livelli di gestione della sicurezza organizzativa.
La terza unità mostra il team organizzativo che dovrebbe includere professionisti dell'intelligence e della sicurezza; la quarta unità suggerisce attività di formazione (vale a dire, conoscenza di base e formazione sulle competenze per la gestione della sicurezza) per i professionisti dell'intelligence facenti parte della squadra d'organizzazione, poi c'è la quinta unità che rappresenta il piano di azione e l'ultima unità indica gli obiettivi della SI.

2.5.3 Quadro pratico della Safety Intelligence

Dopo aver delineato l'ipotesi di modello concettuale, viene ipotizzato anche un modello pratico, come si vede nella seguente figura:

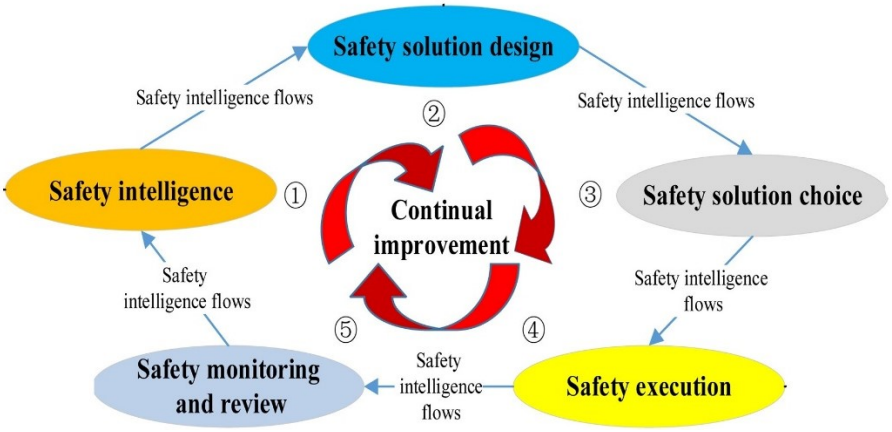


Figura 9. Modello di processo decisionale sviluppato da una prospettica di SI, Wang, B. (2021). Safety intelligence as an essential perspective for safety management in the era of Safety 4.0: From a theoretical to a practical framework. *Process Safety and Environmental Protection*, *148*, 189-199.

Osservando la figura 9, il processo decisionale può essere strutturato in cinque fasi:
una prima fase, **SI**, dove il responsabile identifica il problema di sicurezza e le sue cause, raccoglie dati relativi al problema e converte in informazioni utili e attuabili per la risoluzione dei problemi di sicurezza; si noti come le attività (i *flows*) di questa fase percorrono l'intero processo decisionale, pertanto, la sua corretta esecuzione svolge un ruolo fondamentale.
La seconda fase, **progettazione della soluzione di sicurezza**, include lo sviluppo, il riconoscimento e la comprensione delle possibili alternative di gestione della sicurezza e delle conseguenze della decisione. La terza fase è la **scelta della soluzione di sicurezza** da un insieme fattibile, in cui le alternative identificate sono limitate alla migliore opzione di utilità che porta alla scelta di un decisore in materia di sicurezza.
La quarta fase è **l'attuazione della decisione** presa nella terza fase. Nell'ultima fase si opera con il **monitoraggio e revisione** quindi dei dati e delle informazioni raccolti tramite l'attuazione della decisione sulla sicurezza e i cambiamenti dei rischi della gestione, valutando le informazioni ottenute e riutilizzando le stesse nella prima fase di un nuovo ciclo di gestione per adeguarsi e migliorare le future decisioni.

L'autore Wang si rende conto che questa proposta proviene da una prospettiva di gestione della sicurezza e quindi riconosce certamente che questo studio manca dell'analisi quantitativa e dei casi di studio necessari. A tal proposito, esorta e incoraggia il mondo industriale alla realizzazione di ricerche future per migliorare il quadro generale della SI.

2.6 CARATTERISTICHE DI UN MANAGER NELLA GESTIONE DELLA SICUREZZA

Nella sezione precedente che ha trattato la definizione di un ottimo sistema di gestione della sicurezza basato sulla tecnologia della Safety Intelligence, si è puntualizzato più volte l'importanza della formazione dei responsabili che si occupano delle questioni di sicurezza.

A tal proposito, l'articolo "*Safety intelligence: An exploration of senior managers' characteristics*" (2014) pone la sua attenzione su due studi condotti con lo scopo di identificare le caratteristiche più rilevanti dei senior manager. Queste sono state esaminate attraverso il concetto di "safety intelligence" ma il termine viene inteso come un concetto che indica la comprensione dei senior manager riguardo i problemi di sicurezza e le capacità di sviluppare e attuare politiche. Si dimostra come il modo in cui i senior manager mettono in atto le loro politiche sia fondamentale per la loro influenza sulla sicurezza e si è scoperto che la loro definizione delle politiche contribuisce in modo significativo alle percezioni del clima di sicurezza dei dipendenti e alle prestazioni di sicurezza.

L'obiettivo degli autori, Fruhen L.S., Mearns K.J., Flin R., e Kirwan B. era l'identificazione delle caratteristiche personali che determinano la capacità dei senior manager di occuparsi della gestione della sicurezza delle proprie organizzazioni.

Prima di esporre i risultati, si vuole introdurre in via generale alcune caratteristiche:

Tratti, personalità e motivazione.
Questa caratteristica è più facile spiegarla attraverso gli esempi:
un senior manager che è molto estroverso può comunicare le sue politiche di sicurezza con maggiore forza, mentre un senior manager più simpatico può essere in grado di creare un maggiore senso di fiducia e può aiutarli a mettere in atto le politiche di sicurezza in modo convincente; un senior manager coscienzioso ha maggiori probabilità di essere concentrato sui compiti e quindi possono sviluppare politiche con maggiore cautela;
un senior manager che ha poca stabilità emotiva, invece, può essere meno efficace nel controllare in modo sicuro situazioni stressanti e questo potrebbe influenzare la sua capacità di sviluppare politiche efficaci.

In sintesi, la capacità di ascoltare e apprendere dalle esperienze dei dirigenti passati può aiutarli a essere più ricettivi e a sviluppare una gamma più ampia di conoscenze sulla sicurezza e, di conseguenza, a elaborare migliori politiche di sicurezza.
Il focus normativo descrive le persone che devono essere motivate verso un obiettivo con attenzione alla promozione e alla prevenzione. L'attenzione alla promozione porta a seguire una strategia di entusiasmo e il desiderio di completare rapidamente le attività, mentre l'attenzione alla prevenzione porta a seguire una strategia di vigilanza, evitando così i rischi nell'elaborazione e nella comunicazione delle politiche di sicurezza. C'è da dire che un focus importante sulla prevenzione è più favorevole: in primo luogo, i manager potrebbero prestare maggiore attenzione ai dettagli e dedicare più tempo alle questioni di sicurezza, e poi potrebbe aiutarli a dare priorità ai problemi di sicurezza nelle loro politiche e nella comunicazione con i dipendenti.

Senza dimenticare che il tempo è di solito una risorsa limitata per i manager, perciò la quantità di tempo che trascorrono sulle questioni è stata descritta come un modo per trasmettere il loro valore personale per la sicurezza.

Abilità, problem solving e competenza sociale.
L'approccio del management ai problemi legati alla sicurezza può riflettere l'impegno dei senior manager e modella le organizzazioni e le condizioni di lavoro, e questo può anche avere un effetto immediato sullo stato di sicurezza percepito nelle organizzazioni.
Di conseguenza, la competenza sociale, vale a dire la loro capacità di interagire efficacemente con il corpo dipendente, può contribuire ad aumentare il loro supporto i modi in cui agiscono con le politiche di sicurezza.

Conoscenza.
Questa è stata descritta come uno dei principali princìpi del potere manageriale ed è correlata alle prestazioni di sicurezza ad altri livelli dell'organizzazione. La conoscenza della sicurezza può consentire ai dirigenti di comprendere le informazioni e di trarre conclusioni significative da esse e, così facendo, influenzare la loro capacità di sviluppare politiche di sicurezza efficaci.

Nello studio 1, il campione era composto da 76 senior manager (direttori e responsabili della sicurezza) che lavoravano tutti in posizioni che richiedevano loro di interagire frequentemente con l'amministratore delegato (CEO) della propria organizzazione.
Questi hanno completato un breve questionario in cui veniva chiesto le caratteristiche e i comportamenti di un amministratore delegato ideale riguardo la sua influenza sulla sicurezza. Lo studio 2, invece, ha coinvolto una decina di manager senior di ATM che coprivano varie posizioni diverse e sono stati intervistati riguardanti il loro lavoro quotidiano e il loro ambiente, concentrandosi poi sul processo decisionale in relazione alla sicurezza.
Le interviste sono un approccio più aperto alla raccolta dei dati e sono ideali per catturare i problemi nella loro complessità e interezza e le domande riguardavano l'effettivo lavoro dei senior manager sulla sicurezza.

I risultati di entrambi gli studi suggeriscono una serie di tratti, abilità e conoscenze che riecheggiano le descrizioni delle caratteristiche ritenute centrali per l'influenza manageriale su altri risultati organizzativi.

In tema di sicurezza, due caratteristiche centrali per l'influenza dei senior sulla sicurezza sono spesso la comunicazione personale e il loro coinvolgimento attivo.
Allo stesso modo, i risultati confermano la **competenza sociale** come particolarmente rilevante, e viene descritta come la tendenza a impegnarsi con gli altri e la capacità di ascoltare i suggerimenti di tutte le parti coinvolte nel sistema di gestione della sicurezza.

Lo studio 2 ha anche mostrato che la **persuasione** è altrettanto rilevante ed è probabile che li aiuti a comunicare messaggi forti riguardo alle politiche di sicurezza. Questo potrebbe essere dovuto al fatto che la sicurezza è un obiettivo astratto, per il quale gli indicatori non sono facilmente definiti, e ciò rende ancora più difficile mantenere la sicurezza come obiettivo organizzativo, richiedendo ai senior manager di essere ancora più convincenti.

Fino a poco tempo fa, la conoscenza complessiva dei senior manager è stata identificata come rilevante per la loro influenza sulle organizzazioni ma non era stata considerata come un contributo alla loro influenza sulla sicurezza. I risultati suggeriscono proprio questo, che la **comprensione teorica e pratica delle questioni di sicurezza** da parte dei senior manager e la loro conoscenza di fatti e informazioni sulla sicurezza può supportarli nell'influenzare positivamente la gestione.

Successivamente è stata identificata la caratteristica della **motivazione**, puntualizzando come la motivazione al successo sia fortemente correlata con l'influenza dei senior manager sui risultati organizzativi. E i risultati suggeriscono che questo tratto è rilevante anche per la loro influenza sulla sicurezza. Tuttavia, i risultati relativi al focus erano contraddittori:
nello Studio 1 è stato identificato il focus sulla prevenzione, mentre nello studio 2 era dominante il focus sulla promozione. È possibile che il lavoro sulle questioni di sicurezza porti i senior manager a bilanciare la cautela con il lavoro rapido.

Normalmente si pensa che la **risoluzione dei problemi** sia la parte più importante del lavoro manageriale e rilevante per la loro influenza sulla sicurezza organizzativa, ma nei due studi condotti è stata identificata come la quarta più rilevante.
Principalmente è stata indicata come la modalità con cui i senior manager comprendono i problemi e considerano le varie fonti di informazione.

La caratteristica della **personalità** era la meno frequentemente indicata pertanto non dovrebbe essere considerata centrale per la loro influenza sulla sicurezza.

Infine, è emerso da entrambi gli studi come la **leadership interpersonale** sia rilevante per la loro influenza sulla sicurezza organizzativa.
I risultati dello Studio 1 hanno suggerito che l'influenza può avvenire attraverso stili di leadership interpersonali esercitati sui loro team, ed è possibile che questa forma di influenza si riversi poi a cascata attraverso gli strati gerarchici delle organizzazioni.
È altrettanto probabile che la leadership interpersonale sia particolarmente rilevante poiché è stato precedentemente riscontrato che influenza le prestazioni aziendali.

In sintesi, si è riscontrato che l'influenza positiva dei senior manager sulla sicurezza sia evidente nella loro capacità di elaborare e attuare politiche di sicurezza, ed è particolarmente supportata dalla loro competenza sociale e conoscenza della sicurezza. Si può proporre che la competenza sociale aiuti in particolare i dirigenti nell'attuazione delle loro politiche e che la conoscenza della sicurezza sia fondamentale per lo sviluppo di queste politiche.

2.7 METODO DEL DATA-ORIENTED ASSESSMENT NELLA SAFETY INTELLIGENCE

Come si può notare anche dall'articolo precedentemente citato, le nozioni riguardo l'applicazione della safety intelligence riguardano maggiormente il settore dell'aviazione perché è uno dei settori in cui l'attenzione alla sicurezza è sempre stata massima. Solo recentemente questo concetto è stato applicato anche ai settori di produzione industriali, avendo preso consapevolezza della validità di questa tecnologia.

Per esempio, nel 2016, l'International Civil Aviation organization (ICAO) (Organizzazione per l'aviazione civile internazionale) ha reso noti i nuovi requisiti di gestione e manuali di orientamento e ha chiesto ai propri fornitori di servizi di sviluppare sistemi di gestione basati sui nuovi dati nell'aviazione civile. In questo contesto, è stato proposto il concetto di "safety intelligence", che ha fornito una nuova prospettiva per migliorare la gestione della sicurezza in futuro. In effetti, l'ICAO sostiene tutt'ora la raccolta, l'elaborazione, l'analisi, la condivisione e lo scambio di dati e informazioni sulla sicurezza perché possono essere utilizzati dalla leadership di un'organizzazione per prendere decisioni basate sui dati.

C'è da dire che l'ambito dei dati sulla sicurezza è molto ampio e le fonti di dati dovrebbero essere più mirate così che una volta migliorate la qualità e la quantità dei dati, la capacità di analisi dei dati dovrebbe essere potenziata per fornire un supporto più intelligente. Negli ultimi anni, però, si sono riscontrate difficoltà nelle attività di ispezioni di sicurezza in quanto non riescono a garantire un supporto accurato.

Una soluzione a questo problema è stata presentata nel recente articolo "Research on Data-Oriented Assessment Method for Safety Intelligence Decision", pubblicato nel 2020 con l'obiettivo di sviluppare un metodo di valutazione basato sul rischio di base da "Operation" e "Support", e introdurre la "data-oriented assessment sheet", ovvero la scheda di valutazione orientata ai dati, che contiene i principali processi operativi di tutti i dipartimenti correlati. Attraverso questo, la compagnia aerea può utilizzare il foglio di valutazione per raccogliere dati di ispezione e portare avanti l'analisi, ma anche implementare un'efficace gestione delle prestazioni di sicurezza e prendere decisioni intelligenti in materia di sicurezza.

Per poter illustrare in maniera chiara il funzionamento di questo metodo di valutazione, si prende come riferimento un articolo di studio del caso della Kunming Airlines.

2.7.1 Processo di metodo di valutazione orientato ai dati

La prima fase consiste nell' **identificare il rischio principale**: nel caso in esame un'analisi attenta e precisa dei dati di Flight Operations Quality Assurance (FOQA) su molteplici eventi, sia incidenti sia malfunzionamenti, ha selezionato l' "atterraggio pesante" come il rischio principale dell'azienda.

Poi si procede con l' **analisi e valutazione dei punti chiave:** mediante sessioni di brainstorming e analisi tecnica della cronologia dei guasti, lo studio ha individuato 6 moduli relativi all'atterraggio pesante, tra cui controllo del volo, addestramento al volo, manutenzione, spedizione, dati di volo, peso e bilanciamento, garanzia, e ogni modulo aveva i suoi punti chiave, ma il dettaglio esula dall'interesse interesse dell'argomento.

Fatto sta che successivamente si **sviluppa una scheda di valutazione della sicurezza orientata al rischio:** i dipartimenti competenti hanno studiato l'identificazione del rischio potenziale e la situazione di confronto con i benchmark e hanno sviluppato il foglio di valutazione "R.O.S.A" che sta per Risk-Oriented Safety Assessment.

Dopo il test di quel foglio sull'atterraggio pesante, lo studio ha scoperto che i dati di volo potevano essere il punto di svolta e quindi l'ultima fase consiste con l'**utilizzo del foglio di valutazione e analisi dei dati** da parte delle altre compagnie aeree. Si è dimostrato che l'implementazione di un'analisi approfondita dei dati complessivi delle operazioni di volo della flotta è utile per trovare le debolezze nell'addestramento al volo.

Infatti, nello studio del caso esaminato si legge che dopo questo processo, sono stati selezionati i principali moduli come criterio di valutazione e sono stati monitorati i dati di volo di tutti i piloti in base ad essi. Ne è risultato che l'operatività delle persone poteva essere considerata accettabile quando il valore era superiore allo standard di riferimento, e la differenza tra i valori massimo e minimo della persona poteva essere utilizzata per valutare la stabilità dell'operazione.

2.7.2 Processo decisionale di Safety Intelligence

Attraverso il processo di valutazione orientata al rischio dei dati di volo appena illustrato, lo studio ha poi identificato il gruppo di piloti più vulnerabile all'atterraggio pesante e di conseguenza ha stabilito l'addestramento sulla correzione della deviazione, l'interpretazione dell'energia dell'aeromobile e altri aspetti. In seguito a questa esperienza, la compagnia si è mobilitata per migliorare i corsi di formazione sui metodi di volo a vista e per organizzare un addestramento supplementare con il simulatore.

Queste due decisioni possono essere viste come uno dei tanti modi di migliorare il processo del decision-making tramite l'applicazione della Safety Intelligence.

ANALISI LETTERARIA

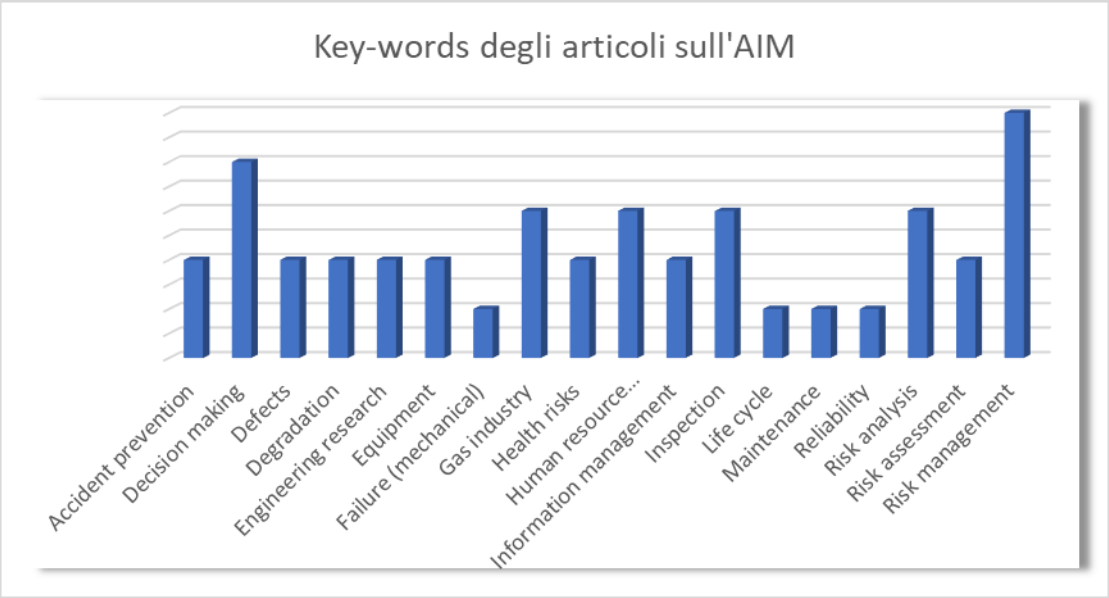
Il problema dell'invecchiamento degli impianti produttivi sussiste dall'era dello sviluppo industriale, dove le industrie hanno effettuato un radicale cambiamento nelle loro tecniche di produzione pe rispondere al ritmo della domanda del mercato. Ma solo negli ultimi decenni sono state sviluppate strategie di gestione e di prevenzione, perché la maggior parte degli impianti si è avvicinato o si sta avvicinando alla fine del ciclo di vita. Tra queste vi è l'Asset Integrity Management, la cui applicazione nelle industrie è relativamente recente. Questo dato è dimostrato anche dalle statistiche di pubblicazione di articoli a tal proposito, come evidenziato dal grafico sottostante:

Si può notare che l'anno di massima pubblicazione è stato il 2018 ma la frequenza è rimasta per lo più costante in tutti gli anni passati. Questo fatto è giustificato dalla crescente importanza che questo sistema di gestione sta assumendo nelle realtà industriali, dove la considerazione dello stato d'integrità degli impianti è mantenuta sempre alta.

Questi dati, inoltre, confermano come le aziende abbiano sempre un certo interesse nell'AIM, e questo interesse determina uno studio costante e continuo nel tempo riguardo le sue caratteristiche e i suoi metodi di implementazione. Abbiamo visto come ciò porta non solo ad un miglioramento della prevenzione di eventi catastrofici ma anche un vantaggio in termini finanziari, e questo rappresenta uno stimolo economico molto forte.

Il prossimo grafico porta all'attenzione che i numerosi studi condotti in materia trovano come aspetto più fondamentale il "**risk management**" ovvero "la gestione del rischio", inteso come rischio generale che può derivare da una disattenzione rivolta ai macchinari, alle apparecchiature, alla strumentazione presente in un impianto di produzione.

Vengono qui presentate le parole chiavi maggiormente utilizzate negli articoli:



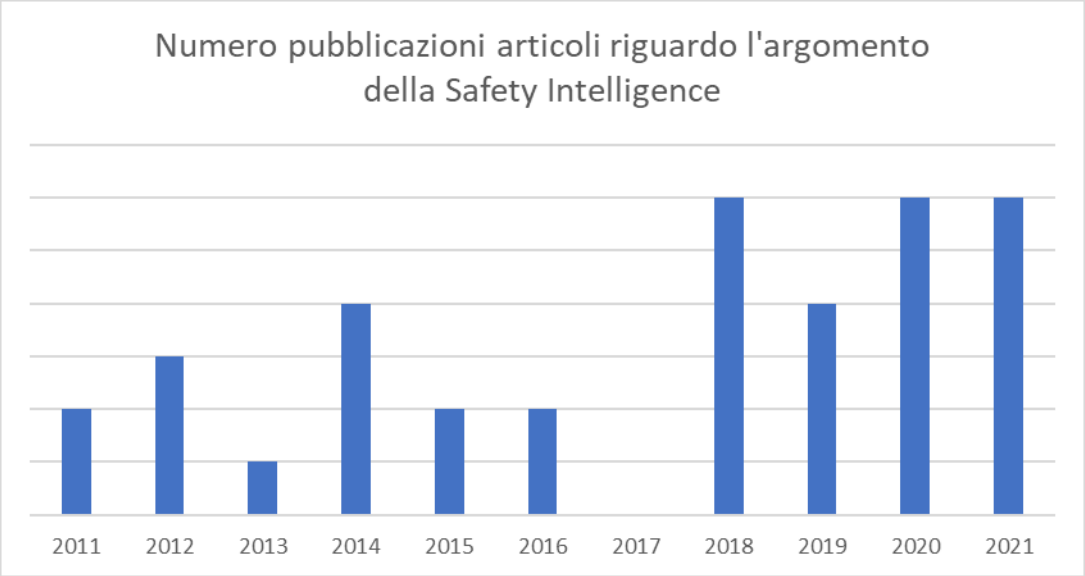
I dati suggeriscono che un altro aspetto importante risulta il "**decision-making**", ossia il processo decisionale. Questo ottiene un supporto non indifferente dall'adozione di un sistema AIM poiché la disponibilità di informazioni pertinenti alle caratteristiche degli asset permette di ponderare le decisioni e fare le scelte più adeguate.

La terza parola chiave più usata è "**inspection**", e questo va a collegarsi all'importanza ribadita più e più volte circa le attività di controllo e di ispezione, che non devono essere sottovalutate perché presentano una fase essenziale nel processo di gestione.

Una considerazione sulla parola "**gas industry**": la maggior parte degli articoli si occupa della descrizione di una situazione critica nelle industrie petrolifere o del gas proprio perché in quegli stabilimenti il problema della corrosione e del deterioramento delle attrezzature è molto delicato. L'attività industriale in questi casi si occupa di due elementi la cui gestione eseguita nel modo sbagliata potrebbe determinare conseguenze disastrose e gravissime, sia per gli stabilimenti sia per la salute umana.

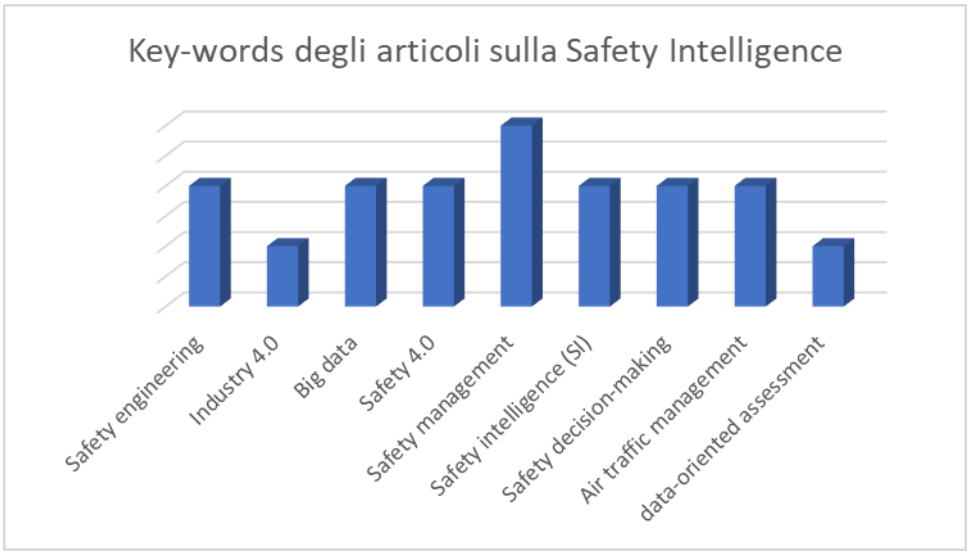
L'aspetto che viene preso poco in esame è la "**Life cycle**" e questo mette in rilievo la pratica di applicare un sistema come l'AIM a macchinari già in funzione da molto tempo, il che è assolutamente comprensibile ma nell'articolo "Creating an effective asset integrity program. *Process Safety Progress*" (Moyer, L., & Hedlund, M. (2019)) viene puntualizzato come i risultati possono essere nettamente migliori se l'implementazione avviene sin dalle prime fasi di progettazione.

Una delle tecnologie più innovative nel campo della gestione organizzativa è la Safety Intelligence. Si può affermare che questa tecnologia sia moltissimo recente, come si evidenzia anche dal grafico delle riviste che hanno trattato questo argomento nell'ultimo decennio:



Appare evidente che fino a qualche anno fa la sua potenzialità era nota ma non sufficientemente presa in considerazione; o meglio la sua applicazione era ancora molto limitata dovuta alla poca conoscenza sull'argomento. Tutt'ora viene riportato il problema riguardo la scarsità di studi pertinenti, e infatti la comunità stessa esorta i professori e gli esperti del campo ad effettuare maggiori ricerche.

Essendo un tema nuovo, il suo campo d'azione è ancora piuttosto ristretto rispetto alle sua attuali capacità, e ciò si può osservare dal seguente grafico:



La maggior parte delle parole chiavi evidenzia il fatto che la SI si sia sviluppata nell'era dell'Industria 4.0. Questo termine è stato coniato solo una decina di anni fa, ma la sua applicazione risale all'inizio della quarta rivoluzione industriale, ossia dalla nascita dell'informatica da cui poi si è affermata l'era digitale.

Caratteristica principale di questo periodo storico è l'incremento dei livelli di automazione nelle attività produttive tramite l'utilizzo di sistemi elettronici e dell'IT (Information Technology). Il fulcro di tutto ciò riguarda l'utilizzo e l'elaborazione di grandi quantità di dati per ottenere informazioni utili. I risultati dell'analisi degli studi su questo tema, difatti, hanno evidenziato i **big data** come l'aspetto cardine dello sviluppo della SI.

Il grafico, inoltre, suggerisce che il campo d'azione prediletto è quello della gestione del traffico aereo; questa informazione deriva dal fatto che quel settore richiede, anzi pretende, la massima sicurezza nei suoi processi, che nella realtà del traffico aereo si traducono nei voli effettuati ad alta quota e per lunghe distanze. E infatti è stato uno dei primi ad applicare il concetto di SI, trovando nelle sue caratteristiche la soluzione ai problemi più delicati.

Sia dal numero di articoli sia dalla quantità di parole chiavi, emerge che questo argomento non è ancora considerato a sufficienza, e quindi c'è l'urgenza di esplorarlo in tutti i suoi aspetti innovativi e i suoi ambiti di applicazione. Questa limitazione è molto ostacolante perché le possibilità e le potenzialità potrebbero portare alla creazione di nuovi sistemi di gestione ancora più efficaci ed efficienti di quelli esistenti, con un vantaggio sia dal punto di visto applicativo sia da quello economico. L'investimento nella digitalizzazione, se opportunatamente valutata, è sempre una buona scelta, e per questo motivo si vuole incentivare sempre più la ricerca sulla Safety Intelligence.

CONCLUSIONI

Negli ultimi decenni sono state effettuate numerose valutazioni dimostranti la tendenza delle infrastrutture obsolete ad essere più suscettibili alle manifestazioni di meccanismi di guasto dipendenti dal tempo. Ad oggi molte attrezzature sono state limitate nelle loro funzionalità e sono tenute sotto controllo per evitare rischi gravosi. I programmi di monitoraggio hanno il compito di identificare qualsiasi potenziale problema, che deve essere poi efficacemente e tempestivamente placato per assicurare l'integrità degli asset.

L'obiettivo principale di un Asset Integrity Management System (AIMS) è la garanzia che le risorse fisiche degli impianti di produzione siano gestite in modo affidabile, efficiente e sicuro. Con questo elaborato si è voluto dimostrare e far comprendere al mondo industriale la fondamentale importanza di effettuare regolari revisioni interne dell'AIMS. Numerosi studi hanno fatto notare che uno dei gravissimi errori commessi in modo frequente è la considerazione di queste attività come superflue, o peggio, che fanno perdere tempo e denaro, trascurando le conseguenze che si potrebbero verificare a lungo termine. Una corretta gestione della manutenzione permette di assicurare la conformità interna e l'evoluzione appropriata di tale metodo, unita alla valutazione periodica della sua efficacia nel periodo di attuazione. Si consiglia, inoltre, di iniziare a pensare con questa logica sin dalla progettazione degli asset, e non solo verso la fase finale del loro ciclo di vita.

Ultimamente, poi, si incentiva l'utilizzo di software applicativi che sfruttino al massimo le potenzialità delle nuove tecnologie esistenti nel mondo odierno. Queste consentono di avere sempre la disponibilità di un supporto informatico nel processo decisionale e, cosa ancora più importante, sono in grado di eseguire funzionalità complete di elaborazione di grandi quantità di dati per ottenere informazioni utili alla gestione.

In conclusione, alle società industriali si consiglia fortemente di prendere la decisione di effettuare un investimento iniziale sia nell'implementazione di un buon sistema di AIM, con tutti i requisiti e le peculiarità, sia nell'installazione delle strumentazioni necessarie per adottare la Safety Intelligence, tutto a favore di un ottimo vantaggio competitivo.

BIBLIOGRAFIA

Hackitt, J. (2011). Briefing: Problems and lessons from ageing energy infrastructure. *Proceedings of the Institution of Civil Engineers-Forensic Engineering*, *164*(4), 147-150.

Henao, F. A. (2021). Risk-based decisions: Implementing the asset integrity program. *Process Safety Progress*, *40*, S24-S31.

Bharadwaj, U. R., Silberschmidt, V. V., & Wintle, J. B. (2012). A risk-based approach to asset integrity management. *Journal of Quality in Maintenance Engineering*.

Moyer, L., & Hedlund, M. (2019). Creating an effective asset integrity program. *Process Safety Progress*, *38*(2), e12008.

Akanni, J., & Alonge, O. (2015, July). Effective Implementation of Risk Based Inspection (RBI) Approach in Asset Integrity Management of Oil and Gas Facilities. In *Pressure Vessels and Piping Conference* (Vol. 57021, p. V007T07A006). American Society of Mechanical Engineers.

Dutta, R., & Madi, M. (2014, January). Best Practices in Asset Integrity Management System. In *IPTC 2014: International Petroleum Technology Conference* (pp. cp-395). European Association of Geoscientists & Engineers.

Wang, B. (2021). 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*, *148*, 189-199.

Fruhen, L. S., Mearns, K. J., Flin, R., & Kirwan, B. (2014). Safety intelligence: An exploration of senior managers' characteristics. *Applied ergonomics*, *45*(4), 967-975.

Luo, M., Shen, K., Yang, K., & Li, X. (2020, October). Research on Data-Oriented Assessment Method for Safety Intelligence Decision. In *2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT* (pp. 889-892). IEEE.