SVILUPPO DI UNA VALUTAZIONE DINAMICA DEL RISCHIO E RELATIVE CONSEGUENZE PER LA SALUTE E SICUREZZA SUL LAVORO

INTRODUZIONE

La valutazione del rischio è la pietra angolare dell'approccio europeo alla salute e sicurezza sul lavoro (SSL) (EU-OSHA, 2020). I datori di lavoro degli Stati membri sono tenuti a svolgere una valutazione del rischio sul luogo di lavoro che consenta l'individuazione, la valutazione e la gestione dei rischi per la sicurezza e la salute durante il lavoro (articolo 9, paragrafo 1, lettera a) della direttiva quadro 89/391/CEE sulla sicurezza e la salute). Tuttavia, dalla terza edizione dell'Indagine europea fra le imprese sui rischi nuovi ed emergenti (ESENER) del 2019 è emerso che il rapporto effettivo dei luoghi di lavoro che svolgono una valutazione del rischio varia regolarmente tra il 42 % circa e il 94 % per i vari Stati membri dell'UE (EU-OSHA, 2020). Non è così facile spiegare queste differenze, tuttavia l'indagine ESENER mostra che in Europa esiste una correlazione positiva tra le dimensioni del luogo di lavoro e il livello di conformità: quanto più grandi sono i luoghi di lavoro, tanto più alta è la probabilità di condurre una valutazione del rischio che viene regolarmente rivista e convalidata. Spesso le PMI sono più difficili da raggiungere (EU-OSHA, 2020) e alcune non hanno mai effettuato una valutazione del rischio a causa della mancanza di competenze, risorse o comprensione. Si tratta di un fenomeno preoccupante, non solo da un punto di vista normativo, ma anche per i lavoratori.

Un modo per sostenere le imprese nello svolgimento delle valutazioni del rischio è quello di offrire strumenti tradizionali ed elettronici adeguati di facile utilizzo, che possono favorire il processo di valutazione. L'idea è che strumenti facilmente accessibili diano risultati rapidamente con sufficiente rigore. L'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), ad esempio, ha messo a punto una serie di strumenti interattivi online per la valutazione del rischio denominati OiRA (https://OiRAproject.eu/en). Gli strumenti OiRA possono essere applicati per un insieme di realtà e attività diverse e sono attualmente utilizzati da migliaia di imprese in tutta l'UE (EU-OSHA, 2021a). A livello nazionale sono stati sviluppati diversi strumenti supplementari, quali:

- BeSmart.ie: https://www.besmart.ie/,
- Rie.nl: https://www.rie.nl/,
- Prevencion10.es: https://www.prevencion10.es/.

Inoltre, è stata sviluppata una serie di strumenti digitali di supporto incentrati su rischi specifici, che possono essere utilizzati per fornire dati efficaci quando si effettua una valutazione del rischio, quali:

- rumore: https://www.av.se/en/health-and-safety/noise/mata-ljud-och-buller/noise-exposure-app/,
- sostanze chimiche: https://www.seirich.fr/seirich-web/index.xhtml.

Con il diffondersi di tali strumenti digitali si è creata quanto meno una certa fiducia nel fatto che siano efficaci nel fornire sostegno nei luoghi di lavoro in Europa. Insieme allo sviluppo della tecnologia di monitoraggio, dei sensori e dell'intelligenza artificiale (IA) a uso della salute e della sicurezza, questo è un buon momento per prendere in considerazione il futuro delle tecnologie digitali di valutazione del rischio. Il presente documento esamina il modo in cui i settori commerciali e industriali stanno avanzando verso la fase successiva della valutazione del rischio. In effetti, i loro progressi saranno così profondi da meritare un termine proprio: valutazione dinamica del rischio.

Il presente documento fornisce approfondimenti sulla valutazione dinamica del rischio rispondendo alle domande riportate di seguito.

1. Che cos'è la valutazione dinamica del rischio e come si differenzia dalla nostra attuale comprensione della valutazione del rischio?

2. Quali sono i vantaggi della valutazione dinamica del rischio per la salute e sicurezza sul lavoro (SSL) e quali sono i punti di partenza ragionevoli per il suo sviluppo?
3. Quali sono gli effetti indesiderati della valutazione dinamica del rischio per la SSL e come potrebbero essere ridotti?
4. Quali sarebbero gli effetti della valutazione dinamica del rischio su datori di lavoro, dipendenti, esperti di SSL e responsabili politici?

Per rispondere a queste domande, il presente documento affronta la questione da due prospettive. La prima si basa su un approccio aziendale alla gestione dei rischi di McKinsey (Jain *et al.*, 2020). Questa prospettiva fornisce un senso di urgenza e spiega perché viene aggiunto l'aggettivo «dinamica» alla valutazione del rischio.

La seconda prospettiva considera le industrie della sicurezza dei processi all'avanguardia nei metodi di valutazione dinamica del rischio. Queste industrie hanno avvertito la necessità di operare un cambiamento dopo gli incidenti di rilievo dei primi anni 2000 e hanno ritenuto che considerare più dinamico il rischio fosse un modo per cercare di migliorare la valutazione e la prevenzione del rischio.

Ma prima di affrontare tale argomento, questo documento collegherà i concetti fondamentali sui rischi e la valutazione del rischio, per comprendere gli aspetti principali della valutazione dinamica del rischio.

Collegamento dei concetti fondamentali

Al fine di trarre vantaggio dalle pratiche e dalle considerazioni applicate in altri ambiti, che trattano il rischio da una prospettiva diversa, è necessario un quadro di comprensione sufficientemente ampio; in particolare, deve essere spiegata la relazione tra i concetti di rischio, gestione, valutazione, barriera e SSL per facilitare la discussione sulla «valutazione dinamica del rischio».

Poiché la direttiva quadro (direttiva quadro 89/391/CEE) non definisce il rischio, in questo documento viene fatto riferimento alle norme ISO e in particolare a quelle ISO 31000 e ISO 45001 per una definizione ampia e adatta all'ambito della SSL: i rischi per la SSL sono la combinazione della probabilità che uno o più eventi pericolosi o esposizioni si verifichino in relazione al lavoro e della gravità di lesioni e malattie che possono essere causati dall'evento o dalle esposizioni.

Le norme ISO offrono una prospettiva internazionale sulla definizione di rischio che è utile nella presente discussione e, aspetto significativo, introducono le condizioni organizzative, i compiti, i metodi e le responsabilità più ampi che le organizzazioni possono scegliere di applicare per garantire il controllo dei rischi. Ciò contribuisce a definire la **«gestione del rischio»** come una vasta raccolta di caratteristiche e strumenti organizzativi, la maggior parte dei quali non sono esclusivi dell'ambito del rischio. Elementi come la comunicazione, la leadership, il coinvolgimento delle parti interessate, la progettazione e la competenza sono importanti per la gestione del rischio ma anche rilevanti in altri ambiti (quali la gestione finanziaria e la produttività). La **«valutazione del rischio»** è un processo esclusivo della gestione del rischio. Il suo ruolo nel sistema è quello di chiarire esattamente quali rischi sono prevalenti in uno specifico spazio di lavoro, quanto sono gravi in relazione ad altri rischi e come cambiano nel tempo. La valutazione può includere anche l'effetto previsto delle misure di protezione. L'obiettivo della valutazione è fornire prove a sostegno delle decisioni in merito all'opportunità di affrontare il rischio e alla modalità da adottare. Ciò si riferisce alle responsabilità dei datori di lavoro di decidere in merito alle misure di protezione per il loro personale e di fornire le attrezzature e la formazione necessarie.

In linea di principio, le norme ISO prevedono che la gestione e la valutazione dei rischi siano concetti «**dinamici**». La norma ISO 45001 propone il ciclo Plan-Do-Check-Act (PDCA) per gestire la dinamica. Anche la direttiva quadro (89/391/CEE) riconosce i processi dinamici: l'articolo 6, paragrafo 1, indica che i datori di lavoro devono adeguare le misure necessarie per la protezione della salute e della sicurezza in caso di mutamenti di circostanze e mirare a migliorarle. Naturalmente, la frequenza dell'adeguamento non è definita rigorosamente.

In sintesi, la gestione del rischio è il concetto più ampio che riguarda molti aspetti degli sforzi delle organizzazioni volti a eliminare o ridurre qualunque tipo di rischio. La gestione della SSL (rischi) è

incentrata sul controllo dei rischi professionali. La valutazione del rischio è un processo specifico all'interno della gestione del rischio destinato a esaminare il rischio e ad agevolare decisioni sistematiche circa le misure di prevenzione. È in questo quadro che deve essere inteso il concetto di valutazione dinamica del rischio; il vero elemento di differenziazione è l'aggiunta del termine «dinamico». Perché quindi diversi attori introducono il concetto di rischio «dinamico»?

Prospettive sul rischio dinamico

La prima prospettiva proviene dall'ambiente aziendale che si occupa della necessità di cambiamento. Nonostante le ovvie differenze rispetto al campo della SSL, le implicazioni sono rilevanti. Una recente relazione ricavata da una prospettiva di consulenza aziendale spiega perché i metodi relativi al rischio devono cambiare e perché devono diventare molto più dinamici (Jain *et al.*, 2020). L'argomentazione prende spunto dal fatto che il mondo delle imprese è cambiato in modo sostanziale: la rivoluzione digitale, i cambiamenti climatici, lo spostamento delle forze geopolitiche e le aspettative mutevoli delle parti interessate richiedono che le organizzazioni **diventino più flessibili, rispondano più rapidamente e acquisiscano maggiore efficienza**. La relazione suggerisce che la gestione dei rischi deve cambiare nei seguenti ambiti:

- individuazione iperdinamica del rischio per stare al passo con un ambiente aziendale in rapida evoluzione;
- valutazione del rischio e processo decisionale dinamici per affrontare i rapidi mutamenti nelle richieste del mercato, nella responsabilità sociale e nel lavoro; e
- decisione dinamica in merito ai controlli sui rischi e alle misure di prevenzione appropriati.

Se si parte dall'ultimo punto - il processo decisionale dinamico sui controlli sui rischi - lo si può associare al concetto di **resilienza**: le organizzazioni devono essere resilienti ai rapidi cambiamenti (tecnologici) delle imprese e attuare o rimuovere i controlli in modo rapido ed efficiente. Un drammatico esempio legato alla SSL è stato la distribuzione urgente di mascherine facciali o l'adattamento alle pratiche di lavoro a distanza (da casa) nell'ambito delle contromisure per la pandemia di COVID-19. Gli esperti di SSL hanno dovuto affrontare in tempi brevissimi i problemi legati alla sicurezza delle mascherine facciali e dei luoghi di lavoro domestici. La velocità con cui si verificano questi cambiamenti non richiede solo valutazioni rapide dei rischi, ma anche strutture di gestione nuove o migliori; una delle più comuni è una maggiore interazione con le parti interessate, i responsabili delle decisioni e i legislatori, senza trascurare l'apprendimento in merito ai rischi legati al COVID-19. L'introduzione di queste misure di sicurezza per la SSL è avvenuta a una velocità molto elevata, spesso scavalcando o aggirando i processi standard di SSL. I processi di governance basati sui comitati possono richiedere molto tempo per portare a una decisione e sono necessari modi più efficaci per prendere decisioni al fine di mitigare i rischi in modo rapido ed efficiente (Jain *et al.*, 2020).

Il secondo punto che riguarda la valutazione dinamica del rischio si riferisce ai rapidi e fondamentali cambiamenti nelle attività che le organizzazioni devono affrontare e che al giorno d'oggi sono numerosi. Tornando all'esempio degli esperti di SSL nella crisi COVID-19, le organizzazioni hanno dovuto valutare e decidere molto rapidamente quali membri del personale fossero fondamentali per l'attività (e avrebbero dovuto lavorare in sede) e quali avrebbero potuto lavorare a casa.

Ciò rinvia al primo punto: individuazione iperdinamica dei rischi per stare al passo con un ambiente in rapido mutamento. Una componente chiave è che le organizzazioni, ma in particolare quelle che operano in mercati volatili, devono anticipare, valutare e osservare le minacce sulla base di informazioni interne ed esterne incerte. Tornando ancora una volta alla SSL nella crisi COVID-19, i rischi per la sicurezza non si limitavano all'esposizione al virus, ma riguardavano anche i disturbi muscoloscheletrici per le persone che lavoravano a casa, i problemi di salute mentale legati all'autoisolamento e i rischi associati alle mascherine facciali. Oltre a ciò, esiste anche la necessità di prevedere il rischio futuro: come si evolverà il rischio nel tempo e cosa è possibile fare ora per attenuarne gli effetti?

In generale, l'individuazione e la valutazione del rischio e la gestione delle misure di prevenzione devono diventare più reattive e flessibili (Jain *et al.*, 2020). Inoltre, secondo la stessa relazione, esistono cinque soluzioni per agevolare il cambiamento.

La prima è quella di **elevare la gestione del rischio nelle imprese** a uno strumento più centrale per sostenere il processo decisionale strategico. Insieme alla seconda soluzione (stabilire **pratiche agili** per comprendere rapidamente la natura del rischio) ciò significa che le valutazioni del rischio devono essere effettuate più rapidamente, su una gamma più ampia di rischi e con un livello di qualità più alto. Per gli esperti in materia di SSL ne consegue che le informazioni principali sui rischi professionali devono essere prontamente disponibili per le valutazioni del rischio, essere in linea con le informazioni principali provenienti da altri ambiti di rischio e gli esperti in materia di SSL devono proporre rapidamente soluzioni creative per la SSL e applicarle prontamente.

La terza soluzione consiste nel **digitalizzare la valutazione e la gestione del rischio**. I dati sui rischi relativi alla SSL devono essere molto più accessibili e devono essere analizzati più velocemente; inoltre dovrebbero fluire prontamente in un profilo di rischio consolidato insieme ad altri rischi (come i rischi finanziari e i rischi dei processi), con il supporto della tecnologia. Tali dati possono provenire da sistemi di dati sulla SSL come gli strumenti elettronici descritti nell'Introduzione; ma, allo stesso modo, potrebbero essere utili sistemi di segnalazione degli incidenti e fonti esterne di dati sulla SSL: banche dati del settore industriale, dati degli uffici di statistica, dati sulla salute pubblica e altri dati di monitoraggio.

La quarta soluzione è che i **professionisti della SSL e i gestori del rischio devono essere meglio preparati alle nuove realtà della digitalizzazione e alle dinamiche aziendali** attuali, per quanto riguarda l'urgente necessità e le crescenti possibilità delle tecnologie di monitoraggio e della raccolta di dati tramite l'Internet delle cose e altro ancora. Per stare al passo con le realtà di un mondo digitalizzato, la loro formazione deve essere modernizzata per includere l'analisi dei dati e ampliare il loro orizzonte per comprendere il rischio in ambiti più diversificati. Allo stesso tempo, è necessario sviluppare capacità di leadership più potenti insieme ad altre competenze non tecniche, per dirigere squadre multidisciplinari e acquisire conoscenze rilevanti da colleghi e parti interessate.

La quinta soluzione, facilmente comprensibile da parte degli esperti di SSL, consiste nello sviluppo di una **solida cultura del rischio, in cui gli esperti di sicurezza e dei rischi siano in prima linea**, i dirigenti siano tenuti a rendere conto del raggiungimento di una sana cultura del rischio e i dipendenti siano pienamente coinvolti. Questa prospettiva aziendale sembra trascurare il fatto che questa soluzione ha suscitato a lungo l'interesse degli esperti di SSL.

È facile capire come questo approccio sia interessante per le grandi organizzazioni, soprattutto per quelle in settori ad alto rischio; non sorprende che le grandi industrie chimiche siano state tra le prime a occuparsi di gestione dinamica del rischio. Per le organizzazioni più piccole, che spesso sembrano procedere più lentamente rispetto all'attuazione di strumenti di valutazione del rischio (cfr. anche l'Introduzione), tali soluzioni potrebbero essere molto utili, anche se tendono a essere troppo costose. A questo proposito, le associazioni settoriali o le associazioni industriali potrebbero avere dimensioni sufficienti per sviluppare soluzioni digitali di SSL per i loro settori. Per le PMI, dovrebbero essere sviluppate soluzioni nazionali di SSL digitalizzate più avanzate, anche quale fase successiva o a livello di UE OiRAproject.eu.

Il presente documento sceglie una prospettiva unica dal punto di vista delle imprese per spiegare che le idee sul rischio stanno cambiando. Questa visione è condivisa da altri leader aziendali (Kaul *et al.*, 2018; Terblanche & O'Donnell, 2018), anche se hanno sviluppato prospettive proprie. Ciò che li accomuna è che le analisi dei rischi devono essere svolte molto più rapidamente, sulla base di dati, e rispondere a cambiamenti improvvisi e rilevanti nell'organizzazione.

Nella SSL, in quanto ambito di lavoro relativamente autonomo, gli strumenti digitali si stanno diffondendo sul mercato (cfr. gli esempi di strumenti elettronici nell'Introduzione), tuttavia l'esigenza di velocità sembra essere meno pressante. Allo stesso tempo, i suggerimenti relativi allo sviluppo di una cultura, all'istituzione di metodi di valutazione del rischio e alla precisazione dell'importanza delle analisi del rischio rientrano perfettamente nelle competenze degli esperti di SSL. Da questo punto di vista, si può supporre che i processi debbano essere accelerati con strumenti digitali.

La sicurezza dei processi dà un ulteriore impulso al concetto di «dinamico»

L'origine della terminologia «gestione dinamica del rischio» in relazione alla sicurezza deriva dalla sicurezza dei processi. La sicurezza dei processi riguarda in particolare la prevenzione di fuoriuscite, incendi ed esplosioni negli impianti di trasformazione chimica, per evitare che le persone subiscano infortuni sul lavoro (tramite la direttiva quadro 89/391/CEE), e nell'ambiente (direttiva Seveso 2012/18/UE, Commissione europea, 2012). Poiché il settore industriale comprende prevalentemente imprese di grandi dimensioni, finanziariamente solide che operano in un contesto ad alto rischio, non sorprende che tali aziende siano all'avanguardia nel rendere l'ambito del rischio più «dinamico». Un primo documento si riferisce direttamente all'esplosione della raffineria di Texas City del 2005. Cinque anni dopo l'incidente, Kalantarnia *et al.* (2010) hanno pubblicato un documento che utilizzava modelli matematici di rischio e registrazioni di incidenti su un periodo di 11 anni e hanno constatato che il rischio di incidenti era costantemente aumentato fino a 37 volte rispetto al rischio iniziale. Gli autori hanno unito il modello matematico ai dati creando un «modello di apprendimento» per dimostrare che il deterioramento delle attrezzature e la negligenza nella manutenzione dei sistemi avevano portato a un rischio dinamicamente crescente.

Pasman e Rogers (2014) hanno utilizzato lo stesso incidente, l'esplosione della raffineria di Texas City nel 2005, per sostenere che il controllo della sicurezza trae vantaggio dal monitoraggio costante degli indicatori di sicurezza del processo (preferibilmente gli indicatori principali). Questi autori hanno anche proposto di aggiornare i modelli matematici con i dati, sebbene in questo caso si trattasse di modelli matematici dell'impianto di trasformazione chimica.

Il disastro della Deepwater Horizon nel 2010 sembra aver accelerato l'interesse per i metodi di gestione del rischio basati sui dati, poiché negli anni successivi all'incidente sono stati scritti altri articoli (ad esempio, Khakzad *et al.* 2012, 2013; Vinnem *et al.*, 2012). Questi documenti hanno effettivamente introdotto una nuova tradizione di analisi e ottimizzazione degli approcci matematici alla valutazione del rischio. La scuola norvegese, con Vinnem, si è occupata dei sistemi di supporto alla gestione (nel caso del 2012, per comprendere i fattori che inducono il rischio al fine di pianificare attività di manutenzione più sicure) e la scuola canadese, con Khakzad e Kahn, ha concentrato le attività sul miglioramento degli strumenti di valutazione matematica.

Fino al 2016 erano stati prodotti documenti sufficienti per condurre una revisione sull'argomento (Khan *et al.*, 2016). In questo studio si fa ricorso all'espressione **valutazione dinamica del rischio** per spiegare l'aggiornamento dei modelli di rischio come compito costante, utilizzando quale obiettivo finale il collegamento automatizzato dei dati. Anche in questo caso, i modelli matematici per la valutazione del rischio svolgono un ruolo centrale. Nello stesso anno, Pitblado *et al.* (2016) ha dato forma alla correlazione tra i sistemi di dati e la gestione del rischio dinamico utilizzando i dati per aggiornare le valutazioni dei rischi con le richieste di permessi di lavoro, in modo che possano essere accettate o negate in base ai livelli di rischio target, garantendo così che il livello di rischio non superi mai un certo livello di soglia. Da quel momento in poi, il concetto di «dinamico» si è esteso ai sistemi di gestione della sicurezza digitali e i metodi si sono moltiplicati in altri ambiti di rischio.

Questi documenti mostrano come i grandi disastri abbiano spinto gli esperti di sicurezza dei processi chimici ad accelerare gli approcci dinamici al rischio. L'obiettivo di questi primi lavori era comprendere il deterioramento degli standard di sicurezza, introdurre il tempo come fattore pertinente nei metodi matematici di valutazione del rischio per valutare i livelli di rischio e ridurre al minimo il rischio sul luogo di lavoro. Si noti che questa mutata tendenza potrebbe essere rafforzata con l'aumento delle reti di sensori che misurano tutti i tipi di parametri di rischio. I metodi associati alla gestione del rischio dinamico o alla valutazione del rischio dinamico sono utilizzati oggi nel campo dell'analisi tecnica del rischio e le pubblicazioni sull'argomento sono numerose, anche se la terminologia non è necessariamente riutilizzabile.

L'importante lezione per la SSL è che gli interessi e gli incentivi per l'analisi del rischio dinamico nelle industrie di trasformazione sono simili a quelli per la SSL: controllare i sistemi in via di deterioramento, controllare i rischi per i lavoratori ed emettere giudizi ragionevoli sulla sicurezza. La principale differenza è che la sicurezza dei processi chimici necessita di analisi dettagliate di un vasto numero di sistemi tecnici, mentre la gestione della SSL non le richiede. Per questo motivo potrebbero esserci meno opportunità di eseguire valutazioni matematiche complesse nell'ambito della SSL. D'altro canto, la gestione della SSL si occupa di una complessa interazione di fattori tecnici, umani e ambientali; inoltre con lo sviluppo della tecnologia di monitoraggio, dei sensori e dell'intelligenza artificiale per l'uso della

salute e della sicurezza, sempre più dati vengono resi disponibili per la SSL. I riquadri 1 e 2 illustrano come potrebbe essere la valutazione dinamica del rischio nella gestione della SSL.

Riquadro 1. Valutazione dinamica del rischio con la matrice di rischio

La matrice di rischio trae origine dallo standard militare 882 del Dipartimento della difesa degli Stati Uniti (DoD), che ha avuto almeno cinque iterazioni (2012). Viene utilizzata, soprattutto nel campo della sicurezza, dagli esperti di SSL, nonché dai datori di lavoro e dai responsabili delle politiche per visualizzare i rischi in un formato di tabella. Se non è prescritta dai responsabili delle politiche, i datori di lavoro possono decidere di utilizzarla nella propria organizzazione.

La matrice di rischio indica la gravità sull'asse orizzontale (in quattro fasi: catastrofica, critica, minore e irrilevante) e la probabilità sull'asse verticale (in cinque fasi: elevata, medio alta, occasionale, remota, irrisoria). A ognuno dei riquadri della matrice è assegnato un livello di gravità di rischio (in cinque fasi: elevato, grave, medio, basso ed eliminato), dove ciascun livello richiede decisioni diverse per intervenire su una particolare situazione di rischio.

Questo esempio utilizza una possibile configurazione accanto a ipotetici pericoli per la SSL riguardanti un'area di stoccaggio. Qui di seguito sono elencate tre situazioni pericolose: un incendio, una collisione di carrello elevatore e un pavimento bagnato che provoca scivolamento, inciampo o cadute di persone (*slip-trip-falls*, STF).

Figura 1 – Matrice di rischio ipotetica per un magazzino

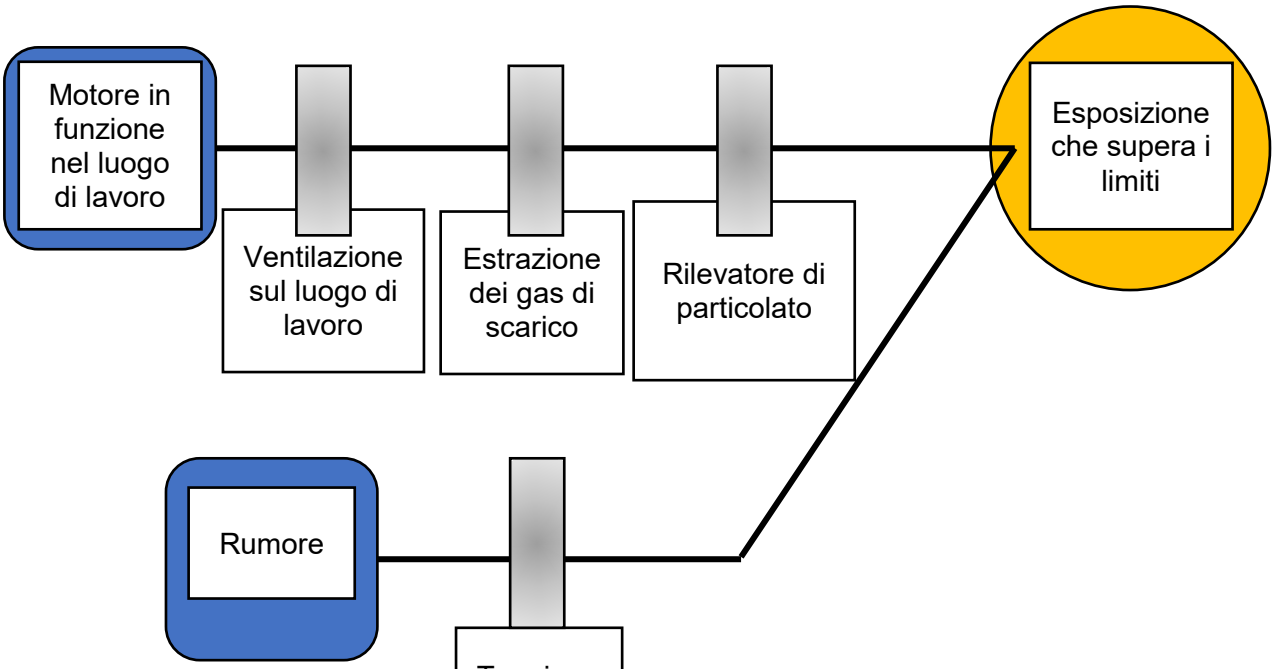
	Catastrofica	Critica	Minore		Irrilevante
Elevata					
Medio alta					
Occasionale		collisione di carrello elevatore			
Remota			pavimento bagnato - STF		
Irrisoria	incendio				

Gli esperti di SSL documentano tutte le situazioni in cui possono verificarsi i pericoli per la SSL e utilizzano elenchi di riferimento per decidere in quale riquadro della matrice di rischio rientra la situazione; tale processo può essere digitalizzato utilizzando prove digitali a sostegno della valutazione effettiva del rischio. Ciò si basa sull'idea che le prove per la selezione di un riquadro specifico nella matrice di rischio sono spesso memorizzate in formato digitale, ad esempio, nei dati relativi a incidenti che causano congedi prolungati per malattia (che la direttiva quadro impone); tuttavia per la valutazione dinamica del rischio è più interessante raccogliere i quasi incidenti, le relazioni di manutenzione e i reclami. Il collegamento di tali banche dati dovrebbe fornire informazioni più chiare sulla frequenza di incidenti relativi a pericoli specificati e, pertanto, fornire prove per il loro inserimento nel riquadro di destra della matrice di rischio. Lo stesso metodo può essere usato per monitorare ed evidenziare che un particolare rischio (ad esempio la collisione di un carrello elevatore) sta cambiando nel corso del tempo, forse perché il numero di segnalazioni di incidenti aumenta o perché vi è molto personale inesperto che lavora *in loco* in un determinato giorno. Disponendo di dati sufficienti (forniti da un'unica organizzazione, da un settore o a livello nazionale), gli algoritmi potrebbero consentire agli indicatori dinamici di monitorare tutte le situazioni pericolose.

Riquadro 2. Monitoraggio delle misure preventive

Gran parte del lavoro svolto dai professionisti della SSL riguarda il mantenimento dei livelli di sicurezza o delle misure preventive (denominate «barriere» nell'ambito della sicurezza dei processi). I BowTies offrono un metodo di monitoraggio delle misure di prevenzione in modo coerente. Questo esempio riguarda l'esposizione alla fuliggine diesel nei garage; la figura 2 mostra una parte di un ipotetico BowTie.

Figura 2 – Parte di un BowTie per l'esposizione a materiali pericolosi



Le barre grigie sono le misure di preve ere) che possono scaturire dal processo di valutazione del rischio da cui si evince che i contr ssari per mantenere i rischi a livelli accettabili. La valutazione del rischio stessa può ess lotta con metodi orientati ai dati come quelli descritti nel riquadro 1, tuttavia in questa sede vie a l'attenzione sull'integrazione con i dati provenienti dalle misure di prevenzione. In questo tore di particolato è un sistema di monitoraggio costante che conta la massa di particolato per centimetro cubo ogni minuto. È collegato a un sistema digitale per leggere le misurazioni effettuate. In questo esempio, i dati per calcolare l'esposizione accumulata sono indicatori della qualità dell'aria; con l'impostazione delle soglie adeguate, la qualità può essere visualizzata come un semaforo (rosso, giallo, verde). Analogamente, la velocità del flusso di ventilazione e il numero di attivazioni di scarico vengono monitorati e, in questo modo, si raccolgono informazioni sullo stato di tale misura di prevenzione. Tuttavia ciò che rende davvero «dinamico» l'uso di questi flussi di dati è che possono essere utilizzati per monitorare le condizioni e le prestazioni delle misure di prevenzione quasi in tempo reale, il che consente interventi in tempo reale che vanno oltre la funzione degli allarmi.

Se da questo e da altri rilevatori si possono raccogliere dati sufficienti, il livello di esposizione (e di rischio) potrebbe essere previsto, ad esempio, sulla base degli agenti atmosferici, del carico di lavoro o del tipo di auto testata. Analogamente, tali dati possono essere utilizzati per calcolare il livello di esposizione dei lavoratori e per prevedere gli effetti a lungo termine sulla salute. I monitor di rilevamento personali, che stanno diventando più economici, offrono inoltre fonti di dati interessanti per la valutazione dinamica del rischio e la gestione del rischio, che vanno oltre gli allarmi.

Discussione

L'obiettivo del presente documento è spiegare le nuove conoscenze riguardanti la «valutazione dinamica del rischio» e ciò che potrebbero significare per la SSL nonché comprendere se è possibile, e in che modo, attingere dall'esperienza di coloro che l'hanno acquisita per primi. Senza dubbio la gestione dei rischi è dinamica per natura; la direttiva quadro (89/391/CEE) e la norma ISO 45001 lo dimostrano chiaramente. Chi opera nel settore della SSL non può sorprendersi del fatto che la gestione, le valutazioni e i controlli dei rischi debbano essere aggiornati quando si scoprono nuove conoscenze, si verificano incidenti gravi, cambiano le leggi o si sviluppano nuove soluzioni per migliorare la sicurezza. Ciononostante, gli sviluppi in altri ambiti incentivano a riflettere sul futuro della valutazione del rischio di SSL in un ambiente di lavoro. Questa sezione descrive le questioni più urgenti.

Valutazione dinamica del rischio come visione per il futuro

La prospettiva dei rischi aziendali mostra che dobbiamo essere più dinamici in quanto il mondo è più dinamico. L'attività commerciale sta diventando più rapida e il rischio stesso è più dinamico rispetto al passato. Questa tendenza affonda le sue radici nella digitalizzazione, che accelera le operazioni commerciali e il processo decisionale. Il messaggio rivolto agli esperti di SSL è che i loro processi devono essere più veloci, più flessibili e basati su sistemi di prove digitali.

I punti di vista della sicurezza dei processi sostengono i punti di vista delle attività commerciali, ma adottano un approccio più pratico. Questi settori hanno elaborato metodi per sostenere la valutazione e la gestione dinamiche del rischio.

Tale visione del futuro non è priva di controversie per gli esperti in materia di SSL. Quando la complessità dei sistemi aumenta, è possibile che gli esperti di SSL si trovino a fare i conti con l'automazione e la digitalizzazione mentre la posta in gioco è la sicurezza (EU-OSHA, 2018). Considerata la presenza di strumenti elettronici sul mercato, sembra che il settore della SSL debba adattarsi a fare spazio al processo di digitalizzazione; tuttavia ogni aspetto di tale processo dovrà essere attentamente esaminato prima di poter essere applicato.

Benefici

I punti di vista della sicurezza dell'attività commerciale e dei processi dimostrano i vantaggi della valutazione dinamica del rischio, riducendoli tuttavia ad alcuni benefici fondamentali. Oltre a rendere la valutazione del rischio più accessibile ai datori di lavoro (e alle PMI) in Europa, potrebbero aiutare le aziende a sviluppare (meglio) le proprie capacità di adattamento alle dinamiche in rapida evoluzione dell'attività commerciale o della tecnologia. Ciò conferisce alle organizzazioni una migliore capacità di rispondere ai mutamenti nei processi aziendali e ai rischi di SSL a essi associati.

Un ulteriore beneficio consiste nel fatto che il sistema digitale offre rigidità alla valutazione e alla gestione dei rischi. Una volta fissate le soglie, programmati i compiti e pianificate le ispezioni, l'esecuzione è rigida e le deviazioni vengono rilevate facilmente. Ciò contribuisce a rendere coerenti e rilevabili i controlli del rischio (misure di prevenzione). Inoltre, la digitalizzazione aumenta la velocità del processo riducendo al minimo lo sforzo umano.

I sistemi digitalizzati costringono anche a metodi coerenti per la raccolta dei dati. Quando compaiono molte opzioni di dati per il rilevamento di segnali deboli, le connessioni tra i fattori di rischio che rimanevano nascoste nel funzionamento normale ottengono visibilità. Inoltre, quando si raccolgono grandi quantità di dati, può essere possibile effettuare alcune previsioni di rischio, ma ciò dipende in larga misura dalla qualità dei dati. Le analisi potrebbero essere svolte da terzi (ossia non dai datori di lavoro), approfittando dei progressi tecnologici (quali algoritmi estremamente sofisticati, Big Data, processori potenti ecc.) in modo da poter fornire valutazioni di alta qualità con uno sforzo minimo.

Con l'introduzione dei sistemi digitali, aumentano anche le possibilità di creare collegamenti diretti con altri sistemi digitali che potrebbero contenere informazioni pertinenti. Le tabelle di servizio, le previsioni meteorologiche, le relazioni di manutenzione, il software per la gestione dei permessi di lavoro e il software di audit potrebbero fornire informazioni utili per fondare la valutazione del rischio su una base di conoscenza molto più ampia rispetto a prima.

Svantaggi

Esistono al contempo degli svantaggi significativi. Alcuni processi essenziali per la SSL non possono essere prontamente digitalizzati. La cultura della sicurezza è uno di questi: notoriamente difficile da misurare e ancor più ardua da influenzare, l'evoluzione della cultura della sicurezza rimane fondamentalmente uno sforzo umano. Lo stesso vale per la leadership; l'abilità di un responsabile della SSL di guidare la propria organizzazione verso l'eccellenza nell'ambito della sicurezza è uno sforzo fondamentalmente umano. La comunicazione e la fiducia hanno caratteristiche simili, ma in questo caso i social media possono essere d'aiuto. Riconoscendo l'importanza di queste capacità umane, gli esperti di SSL possono utilizzare i sistemi di dati per personalizzare i propri interventi in modo più mirato su questioni specifiche di SSL. Se i sistemi di dati mostrano che l'uso delle mascherine facciali sta peggiorando, possono intervenire su quella questione specifica piuttosto che concentrarsi sul miglioramento della cultura della sicurezza. L'intervento stesso, tuttavia, richiede un tocco umano.

Un altro svantaggio (che i fautori della digitalizzazione non pubblicizzano) può essere il costo. Non tutte le organizzazioni, in particolare le PMI, possono avere l'intenzione o la possibilità di investire in programmi software dedicati alla SSL. Ciò costituisce una sfida per gli sviluppatori di software: devono sviluppare sistemi che rendano la fornitura di SSL efficace ed efficiente per un gruppo di utenti. Allo stesso tempo, devono dimostrare di utilizzare i dati in modo affidabile e di proteggerli correttamente. Sebbene le organizzazioni intensifichino la gestione dei rischi affinché questa assuma un ruolo più centrale, e finanzino i sistemi di dati di conseguenza, come suggerisce la relazione menzionata in precedenza (Jain *et al.*, 2020), ciò non significa necessariamente che le preoccupazioni relative alla SSL diventino più centrali per l'organizzazione. Un altro modo per ovviare alle limitazioni dei costi è che le organizzazioni collaborino in associazioni di categoria o forse a livello nazionale. Tale modalità potrebbe comportare problemi di armonizzazione, ma offrire anche opportunità di imparare dagli incidenti di sicurezza degli altri.

Un'ulteriore complicazione è che la legislazione in materia di SSL tende a cambiare lentamente: i regolamenti sulla SSL possono sopravvivere per anni e a volte anche per decenni: ad esempio, la direttiva quadro 89/391/CEE è in vigore da più di 30 anni. Ciò non sorprende del tutto, perché gli atteggiamenti giuridici di base relativi a infortuni e decessi connessi al lavoro non cambiano rapidamente. Per i dipendenti, questo può essere effettivamente accettabile; nel loro caso non importa molto se ad avere ripercussioni sulla loro salute è un tornio del XIX secolo o un robot futuristico. Ma per le soluzioni software che possono cambiare da un giorno all'altro, potrebbero rivelarsi utili alcune linee guida (ad esempio definizioni o testi legali leggibili da una macchina).

Esiste poi una questione culturale. Non tutti gli esperti di SSL accolgono con favore la digitalizzazione del loro lavoro, in quanto aumenta la distanza dalle persone e dalle relative preoccupazioni (nell'ambito della SSL). Con i sistemi digitali, i dati sono più facilmente disponibili, il che comporta decisioni sui rischi migliori e più rapide, ma si trascorre più tempo a lavorare con i computer piuttosto che con le persone. Le società di consulenza suggeriscono effettivamente che la gestione dei rischi assuma un ruolo più centrale nelle aziende, non solo come dipartimento specializzato ma al centro dei processi decisionali nelle organizzazioni. Anche se non si intendono di gestione del rischio nell'ambito della SSL, è sicuramente un'opportunità di aggiornamento per gli esperti di SSL. Tuttavia questo significa inevitabilmente il miglioramento del livello delle competenze del personale addetto alla SSL per affrontare i moderni sistemi digitalizzati, progetti agili e molta più responsabilità.

Per i responsabili delle decisioni politiche, specialmente a livello nazionale o internazionale, è difficile comprendere cosa cambierebbe a breve termine. Da una prospettiva più lontana dai processi primari, la digitalizzazione non ha un effetto così significativo sui requisiti di salute e sicurezza sul lavoro o sui sistemi che effettuano il monitoraggio delle prestazioni. Dal punto di vista dei responsabili delle politiche, si potrebbe valutare la digitalizzazione dei loro sistemi di monitoraggio per stare al passo con le dinamiche accelerate della SSL. Inoltre, va tenuto in considerazione in che modo i dati relativi alla SSL non rispettano la privacy, come in molti ambiti politici in tutta Europa.

Un accenno all'intelligenza artificiale

Al giorno d'oggi, qualsiasi progresso raggiunto nel campo della digitalizzazione suscita automaticamente discussioni sull'intelligenza artificiale. Una volta eseguita la raccolta dei dati, è sempre interessante applicare gli algoritmi di apprendimento per prevedere i rischi. Tuttavia l'IA apre una discussione completamente nuova e l'EU-OSHA non è sola ad affrontare le complicazioni dell'IA sul luogo di lavoro (EU-OSHA, 2018): l'Organizzazione internazionale del lavoro (OIL) ha affrontato la questione nella sua relazione «Negotiating the algorithm» (Negoziare l'algoritmo) (De Stefano, 2018); la Commissione elettrotecnica internazionale (IEC) ha pubblicato «Safety in the future» (La sicurezza in futuro) (IEC, 2020); e un approccio più generico all'IA è stato pubblicato dalla Commissione europea nel suo Libro bianco «On artificial intelligence» (Sull'intelligenza artificiale) (Commissione europea, 2020). Appare possibile che la discussione sulla valutazione o gestione dinamica del rischio e quella sull'IA convergano in un'unica discussione.

Conclusioni e prospettive

La valutazione dinamica del rischio è un'espressione usata per indicare che la valutazione del rischio è stata digitalizzata e modernizzata per diventare più potente e riguardare dati digitali e rischi in rapida evoluzione. Uno dei principali fattori di cambiamento è rappresentato dai leader di aziende che offrono i loro servizi per la digitalizzazione diffusa in tutta la società. I progressi scientifici nelle industrie di trasformazione hanno già consentito lo sviluppo di metodologie per attuare valutazioni dinamiche del rischio, anche se per i propri scopi specifici. Per il settore della SSL, l'analisi dinamica del rischio funge da promemoria per ribadire la necessità di modernizzazione.

I **vantaggi** evidenti per la valutazione dinamica del rischio sono l'agilità in un ambiente di lavoro dinamico, la gestione di problemi di valutazione del rischio complessi e complicati, la velocità e la coerenza. Gli **svantaggi** sono gli stessi di qualsiasi sistema TIC: la carenza in termini di competenze, la dipendenza dalle competenze TIC, la sicurezza informatica e i costi. Nonostante gli svantaggi, sono stati sviluppati diversi strumenti digitali di valutazione dei rischi, il che suggerisce che gli esperti di SSL stanno avanzando lungo il percorso della digitalizzazione in varie zone d'Europa.

Le conseguenze per le diverse parti interessate della SSL sono varie. A essere maggiormente colpiti sono **gli esperti in materia di SSL** poiché dovranno aggiungere diverse competenze digitali al loro repertorio. Dovranno comprendere quali dati entrano nel sistema e ciò che rappresentano in termini di contenuti di sicurezza, e capire quando si verificano problemi. Inoltre, fanno parte con tutta probabilità degli artefici dei nuovi sistemi e collaborano con gli esperti di TI. I **datori di lavoro** sono probabilmente molto coinvolti in quanto decidono in merito agli investimenti ma non hanno la necessità di conoscere i dettagli con precisione. **Inoltre**, sono principalmente colpiti a causa del loro ruolo di primo piano nel progetto di trasformazione e del divario di competenze e del loro controllo dei costi. I dipendenti sono molto probabilmente utenti, per cui dovranno lavorare con questi sistemi senza tuttavia avere la necessità di conoscerli in maniera approfondita. Ciononostante, i dipendenti in quanto utenti finali devono essere coinvolti per sviluppare e affrontare le esigenze degli utenti, le questioni di privacy e altre preoccupazioni che potrebbero eventualmente manifestare.

È possibile che i **responsabili delle politiche** non debbano fare molto nel prossimo futuro, a parte sottolineare che esistono rischi associati all'uso dei dati personali. Inoltre, sono solitamente coinvolti quando aumentano i livelli di prestazione o quando devono essere approvate soluzioni specifiche. Il loro ruolo in futuro potrebbe essere quello di armonizzare gli sforzi, individuare migliori prassi e operare in formato digitale.

In conclusione, da una prospettiva di SSL, le valutazioni dinamiche del rischio rappresentano una spinta verso valutazioni del rischio digitalizzate per affrontare il rischio dinamico con maggiore rapidità rispetto al passato. L'esperienza maturata in altri ambiti suggerisce che l'approccio è efficace e, di conseguenza, la valutazione del rischio della SSL potrebbe non avere altra scelta che seguirne l'esempio. Considerati i diversi strumenti per la valutazione del rischio in materia di SSL disponibili in Europa (quali OiRA, BeSafe e RIE), il cammino verso il futuro digitale è già avviato, tuttavia il motivo propulsore è diverso; mentre le piattaforme SSL si concentrano sul raggiungimento di percentuali più

elevate di luoghi di lavoro che eseguono valutazioni del rischio obbligatorie, la valutazione dinamica del rischio si concentra su prestazioni più veloci. Si noti che non vi è alcun obbligo giuridico fondamentale nella direttiva quadro o altrove che richieda una valutazione dei rischi effettuata con sistemi digitali; l'incentivo sembra essere finanziario o semplicemente il tentativo di lavorare con lo stato dell'arte.

Autore: Coen van Gulijk, TNO Healthy Living, University of Huddersfield, Delft University of Technology.

Gestione del progetto: Annick Starren, Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA)

Bibliografia e referenze

CCPS (Centro per la sicurezza dei processi chimici) (2018). *Bow ties in risk management: A concept book for process safety*. John Wiley & Sons.

De Stefano, V. (2018). *Negotiating the algorithm: Automation, artificial intelligence and labour protection*. EMPLOYMENT Working Paper No. 246. Organizzazione internazionale del lavoro (OIL). Disponibile al seguente indirizzo: https://www.ilo.org/employment/Whatwedo/Publications/working-papers/WCMS_634157/lang--en/index.htm

Direttiva 89/391/CEE del Consiglio, del 12 giugno 1989, concernente l'attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro. Disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31989L0391
Cfr. anche: https://osha.europa.eu/en/legislation/directives/the-osh-framework-directive/

Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione). Disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0042

Direttiva 96/82/CE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sul controllo dei pericoli di incidenti rilevanti connessi con determinate sostanze pericolose. Disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0018

Direttiva (UE) 2016/798 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, sulla sicurezza delle ferrovie. Disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0798

EU-OSHA (Agenzia europea per la sicurezza e la salute sul luogo di lavoro) (2018). *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025*. Relazione dell'Osservatorio europeo dei rischi. Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo. Disponibile al seguente indirizzo: https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

EU-OSHA (Agenzia europea per la sicurezza e la salute sul luogo di lavoro) (2020). *European Survey of Enterprises on New and Emerging Risks (ESENER 2019) — Background briefing*. Disponibile al seguente indirizzo: https://osha.europa.eu/en/publications/european-survey-enterprises-new-and-emerging-risks-esener-2019-background-briefing

EU-OSHA (Agenzia europea per la sicurezza e la salute sul luogo di lavoro) (2021a). *OiRA and other online risk assessment tools in national OSH strategies and legislation.* Disponibile al seguente indirizzo: https://oshwiki.eu/wiki/OiRA_and_other_online_risk_assessment_tools_in_national_OSH_strategies_and_legislation#cite_note-20

EU-OSHA (Agenzia europea per la sicurezza e la salute sul luogo di lavoro) (2021b). *Che cos'è una valutazione dei rischi?* Disponibile al seguente indirizzo: ttps://oiraproject.eu/en/what-risk-assessment

Commissione europea (2020). Libro bianco *sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* COM(2020) 65 final. Disponibile al seguente indirizzo: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Committee for Electrotechnical Standardisation (CENELEC) (2017). *Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process.* Standard No EN 50126-1:2017. Disponibile al seguente indirizzo: https://www.cenelec.eu/dyn/www/f?p=104:110:1185783283395501::::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:1257173,60236,25

IBM (2018). *IBM data risk manager*. Disponibile al seguente indirizzo: https://www.ibm.com/downloads/cas/XEMQ1MDK

IEC (International Electrotechnical Commission) (2020). *Safety in the future* [White Paper]. Disponibile al seguente indirizzo: https://www.iec.ch/basecamp/safety-future

Organizzazione internazionale per la normalizzazione (International Organisation for Standardization, ISO) (2018). *Occupational health and safety management systems — Requirements with guidance for use* (ISO Standard No 45001:2018). Disponibile al seguente indirizzo: https://www.iso.org/iso-45001-occupational-health-and-safety.html

Jain, R., Nauck, F., Poppensieker, T., & White, O. (17 novembre 2020). *Meeting the future: Dynamic risk management for uncertain times*. McKinsey & Company. Disponibile al seguente indirizzo: https://www.mckinsey.com/business-functions/risk/our-insights/meeting-the-future-dynamic-risk-management-for-uncertain-times

Kalantarnia, M., Khan, F., & Hawboldt, K. (2010). Modelling of BP Texas City refinery accident using dynamic risk assessment approach. *Process Safety and Environmental Protection*, *88*(3), 191–199. https://doi.org/10.1016/j.psep.2010.01.004

Kaul, N., Lodha, A., Countryman, T., & Patel, P. (2018). *Digitizing operational risk for improved safety performance*. Estratto il 24 marzo 2021 da: https://www.accenture.com/t20180711t081149z__w__/tw-en/_acnmedia/pdf-82/accenture-pov-digital-barrier-management.pdf

Khakzad, N., Khan, F., & Amyotte, P. (2012). Dynamic risk analysis using bow-tie approach. *Reliability Engineering & System Safety*, *104*, 36-44. https://doi.org/10.1016/j.ress.2012.04.003

Khakzad, N., Khan, F., & Amyotte, P. (2013). Quantitative risk analysis of offshore drilling operations: A Bayesian approach. *Safety Science, 57*, 108-117. https://doi.org/10.1016/j.ssci.2013.01.022

Khan, F., Hashemi, S.J., Paltrinieri, N., Amyotte, P., Cozzani, V., & Reniers, G. (2016). Dynamic risk management: A contemporary approach to process safety management. *Current Opinion in Chemical Engineering*, *14*, 9-17. http://dx.doi.org/10.1016/j.coche.2016.07.006

Pasman, H., & Rogers, W. (2014). How can we use the information provided by process safety performance indicators? Possibilities and limitations. *Journal of Loss Prevention in the Process Industries*, *30*, 197-206. https://doi.org/10.1016/j.jlp.2013.06.001

Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K., & Stokke, A. (2016). Concepts for dynamic barrier management. *Journal of Loss Prevention in the Process Industries*, *43*, 741-746. http://dx.doi.org/10.1016/j.jlp.2016.07.005

Terblanche, A., & O'Donnell, R. (2018). *Dynamic risk assessment. The power of four*. KPMG International Cooperative. Disponibile al seguente indirizzo: https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/03/dynamic-risk-assessment-for-audit-brochure.pdf

United States Department of Defense (2012, May 11). *System safety*. MIL-STD-882 E. Disponibile al seguente indirizzo: https://www.acqnotes.com/Attachments/MIL-STD-882E%20System%20Safety%205%20Nov%202012.pdf

Vinnem, J., Bye, R., Gran, B., Kongsvik, T., Nyheim, O., Okstadd, H., Seljelid, J., & Vatn, J. (2012). Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries*, *25*(2), 274-292. https://doi.org/10.1016/j.jlp.2011.11.001