

4. Nuovi strumenti per la gestione della salute e sicurezza sul lavoro con i cobot¹

di Margherita Bernabei, Francesco Costantino,
Andrea Falegnami e Sara Stabile

1. Introduzione

Il termine cobot nasce dalla sintesi di *collaborative robot*, riferendosi a quelle applicazioni robotiche in cui persona e robot interagiscono fisicamente in un ambiente condiviso, senza sistemi di separazione. Se si pensa, infatti, alla tipica applicazione di robot industriali, un robot si muove a grande velocità in spazi recintati inaccessibili all'operatore (Cohen *et al.*, 2022; Gualtieri, Rauch, Vidoni, 2021; Hentout *et al.*, 2019; El Zaatari *et al.*, 2019); diversamente, i cobot operano in spazi raggiungibili dalle persone svolgendo attività solitamente a velocità piuttosto ridotte.

Le applicazioni dei cobot sono sempre maggiori grazie all'evoluzione tecnologica che ne aumenta le funzionalità e ne riduce i costi. Le categorie principali di cobot sono tre: quelli che supportano l'uomo nello studio della natura, che potremmo chiamare "cobot esplorativi", che permettono di acquisire conoscenze lì dove gli ambienti sono particolarmente ostili (profondità degli oceani, vastità dello spazio, ecc.) e quindi affiancano l'uomo sostituendolo nelle attività più rischiose per la propria incolumità o per il successo della missione esplorativa; esempi sono i sistemi robotici di identificazione mine, i ranger spaziali, i droni che seguono i ricercatori raccogliendo dati e via dicendo. La seconda categoria è quella dei "cobot per la persona" che, ad esempio, supportano gli anziani e persone con disabilità e in generale si occupano di attività di cura e educazione. La terza categoria, di nostro interesse, riguarda i "cobot produttivi", che supportano nella realizzazione di beni o erogazione servizi per l'industria o il commercio. La applicazione di questi ultimi permette di far svolgere loro attività nocive, anche solo potenzialmente, per l'operatore, in termini di ergonomia

1. Il presente contributo è frutto del lavoro realizzato nell'ambito del progetto di ricerca finanziato da Inail BRIC 2019 ID 50 - TRADARS www.tradars.it.

o carico psicologico. Inoltre, poiché le prestazioni dei sistemi robotici sono elevate, con i cobot le imprese riescono solitamente ad ottenere anche un miglioramento di produttività, con aumento di velocità e riduzione di difetti o errori (El Zaatari *et al.*, 2019; Galin, Meshcheryakov, 2019).

Nelle industrie, il livello di collaborazione tra robot e persona può essere più o meno elevato, andando da operatore e cobot che lavorano in maniera **indipendente** e su pezzi differenti, semplicemente condividendo lo spazio, al lavoro **contemporaneo** sullo stesso pezzo, alle operazioni svolte dai due soggetti in sequenza, fino al caso in cui persona e robot **si supportano** a vicenda nello svolgimento di una singola operazione (ad esempio nei casi di co-manipolazione dei pezzi).

Diverse sono le tipologie di attività manifatturiere che in diverse aziende beneficiano del supporto di cobot (El Zaatari *et al.*, 2019): la movimentazione di oggetti, soprattutto se pesanti o da posizionare con precisione; l'assemblaggio, in cui il cobot recupera pezzi da posizioni non immediatamente raggiungibili o identificabili dall'operatore, svolge alcune operazioni rischiose (ad esempio la saldatura), o semplifica alcune operazioni che altrimenti richiederebbero più operatori ma solo in alcuni momenti; il controllo, demandando al sistema robotico la verifica del rispetto delle specifiche di produzione, lavoro spesso ripetitivo e tedioso.

L'attuale livello di mercato e diffusione dei cobot colloca questa tecnologia dell'Industria 4.0 tra le più pervasive, come mostra il settore dell'*automotive*, in cui attualmente utilizzano cobot aziende come BMW, Audi, Volkswagen, Nissan e Skoda. In generale, il mercato dei cobot ha subito una flessione a inizio pandemia per poi riprendersi completamente nel 2021, grazie a un ritorno sull'investimento di circa 2-3 anni. Chiaramente le aziende hanno verificato come l'automazione non soffrisse la pandemia, portando ad una spinta che oggi fa stimare una crescita attorno al 20-30% annuo del mercato. I settori più impattati sembrano essere quelli che stanno automatizzando il confezionamento e la movimentazione flessibile dei prodotti, ad esempio l'alimentare, in cui i volumi produttivi permettono un grande risparmio. I più famosi cobot industriali sono lo YuMi di ABB, il LBR iiwa di KUKA, il Motoman di Yaskawa, ma i modelli disponibili sono sempre di più.

2. I rischi per la salute e sicurezza sul lavoro quando si implementa un cobot

La diffusione dei cobot apre la necessità di ragionare sulle capacità e competenze richieste agli operatori che si trovano ad utilizzarli, così come sui modelli formativi più adatti a garantire le condizioni di salute e

sicurezza per tali operatori. Infatti, se da un lato le aziende valutano l'introduzione dei cobot nei propri processi solitamente con una tradizionale valutazione costi-benefici e di ritorno sull'investimento richiesto, dall'altra il successo dell'introduzione di questa tecnologia dipende molto da come le persone la inseriscono nel proprio lavoro. Con questo obiettivo, i costruttori hanno lavorato da subito a garantire l'incremento dei livelli di sicurezza per i lavoratori sui rischi più evidenti (da contatto con il robot, schiacciamento, ecc.), ma non sembra siano presi in considerazione con pari attenzione i rischi afferenti alla sfera psicologica e organizzativa, di cui si parlerà nei prossimi paragrafi. La tipica proposizione commerciale narra che i cobot aumentano la salute e la sicurezza dei lavoratori (e sotto diversi punti di vista è vero), che gli operatori si interfacciano senza alcuna specifica necessità formativa con i robot collaborativi, di fatto senza ipotizzare la necessità di modelli cognitivi o formativi differenti rispetto a quanto solitamente presente in azienda. Tra i benefici legati all'introduzione dei cobot spiccano la possibilità di giungere ad una piena automatizzazione delle attività ripetitive o pericolose, esonerando così i lavoratori dalle mansioni più alienanti e rischiose; di ottenere una maggior precisione e velocità nelle lavorazioni; ma anche di rendere altamente versatile e flessibile la produzione. Contribuendo anche a livello sociale, poi, i cobot possono rendere il lavoro accessibile ai soggetti più anziani o in condizioni di disabilità. Benefici a parte, ogni percorso di digitalizzazione introduce nuovi rischi che possono impattare sulla salute e la sicurezza delle persone. Pertanto, sia il mondo della Ricerca sia le aziende del settore analizzano in modo sempre più sistematico e costante tematiche quali la *prevention through design*, l'ergonomia, il design degli ambienti di lavoro collaborativi, nonché la capacità di anticipare gli effetti delle nuove tecnologie per prevenire e gestire i rischi nuovi ed emergenti e per sostenere, attraverso processi di informazione e formazione, i lavoratori rendendoli degli "operatori 4.0" sempre più competenti, consapevoli e fiduciosi del cambiamento. L'inclusività e il coinvolgimento costante del lavoratore, oltre alla conoscenza preventiva di scenari futuri che si possono paventare quando si affronta una trasformazione digitale, vogliono minimizzarne l'impatto negativo di tale trasformazione sulle persone e, più in generale, sull'intera organizzazione.

Ma quali sono dunque pericoli e rischi specifici del lavoro con cobot? In prima battuta, si devono considerare i rischi "tradizionali", storicamente affrontati con le normative dedicate alla sicurezza delle macchine (si veda lo Standard ISO12100:2010: "Safety of machinery - General principles for design - Risk assessment and risk reduction"), vale a dire rischi di natura meccanica, elettrica, termica, chimica e biologica; ma anche rischi originati dal rumore, dalle vibrazioni e dalle radiazioni delle macchine. Molte

di queste categorie di rischi continuano a sussistere con l'utilizzo di cobot. Inoltre, elementi quali la condivisione di attività, strumenti e spazi di lavoro, e le interfacce antropomorfe delle macchine, portano inevitabilmente all'emersione di rischi nuovi ed emergenti, di natura organizzativa e psicologica. Un rischio organizzativo può derivare da procedure, metodi, criteri adottati dall'organizzazione, come ad esempio la non corretta assegnazione di obiettivi all'operatore rispetto alla durata del turno di lavoro. Invece, un rischio psicologico è riconducibile alla percezione soggettiva del lavoratore che interagisce con la macchina, come il timore di poter essere sostituito dalla stessa e l'affaticamento mentale o fisico legato alla prestazione.

Nello specifico, rischi meccanici possono derivare dal movimento di parti mobili quali i bracci dei cobot, dalla presenza di spigoli o parti taglienti, dall'insufficiente reattività delle macchine nelle attività collaborative, dall'ostruzione e/o limitazione dei sistemi di visione, ma anche dall'impossibilità, per gli operatori, di allontanarsi dai cobot. Le caratteristiche citate, vale a dire proprio le fonti di rischio, possono indurre a fenomeni di schiacciamento, taglio, impigliamento, intrappolamento, impatto e abrasione. Ulteriori tematiche emerse, tra i rischi meccanici, fanno riferimento a criticità in termini di riconoscimento e prevedibilità da parte dell'uomo delle traiettorie dei cobot e viceversa, problematica che potrebbe generare collisioni tra i soggetti interagenti e danni dovuti a sbilanciamenti e cadute. Critiche, seppure rare, risultano anche le attività di manutenzione dei cobot in altezza, laddove questi presentino consistenti dimensioni, che potrebbero essere motivo di caduta. Rischi elettrici possono emergere in presenza di interferenze elettromagnetiche tra le apparecchiature e dai conseguenti malfunzionamenti delle stesse, da eventi di interruzione di corrente o di rilascio inaspettato di energia potenziale da fonti immagazzinate, motivo di bruciature e ustioni per gli operatori. Danni che, in aggiunta, potrebbero derivare dal contatto con parti o connessioni sotto tensione. I rischi termici risultano unicamente connessi al surriscaldamento dei dispositivi, anch'esso origine di bruciature ed ustioni. Emergono anche rischi legati ad eventi di esposizione: alle vibrazioni e al rumore dei dispositivi, a radiazioni ionizzanti, sorgenti laser, agenti corrosivi o acidi provenienti dalle batterie, possibili cause di danni superficiali alla pelle, agli occhi e alle vie aeree. Dal punto di vista ergonomico, la presenza di interfacce non *user-friendly* può causare discomfort e stress lavoro-correlato, mentre le posizioni adottate durante le lavorazioni collaborative, possono portare a danni posturali. Anche i rischi organizzativi rappresentano una tematica ampia e non trascurabile. Questi, risultano legati alla presenza di attività svolte a ritmi di lavoro dettati dai cobot, causa di affaticamento, stress muscolo-scheletrico, pressione psicologica e sovraccarico fisico per i lavoratori, origine di un conseguente decremento della vigilanza. Il monitoraggio di più cobot

contemporaneamente porta ad un sovraccarico cognitivo dei lavoratori. Si potrebbe anche generare un sotto carico cognitivo e, quindi, danni dovuti al decremento della concentrazione, se si considera la diminuzione del numero di attività svolte dall'uomo, perché sostituito dalla macchina, e la diminuzione dell'attrattività del lavoro. Oggetto di attenzione sono anche le circostanze in cui i cobot vengono implementati in luoghi diversi da quelli per cui sono stati originariamente progettati. Questa tendenza, infatti, risulta pericolosa perché responsabile di danni legati a comportamenti imprevedibili delle macchine, o a collisioni legate all'inadeguatezza degli spazi di lavoro in cui si implementano i dispositivi. Tendenze di *outsourcing* in fase di costruzione, configurazione, installazione e programmazione delle macchine, decrementano notevolmente la conoscenza delle stesse che, operativamente, intensifica la possibilità che si verifichino collisioni e l'incapacità di reagire in situazioni di emergenza. Se non adeguatamente formati, i dipendenti possono temere la sopraffazione da parte dei cobot (addirittura facendo nascere la paura del licenziamento), non conoscere, e quindi prevedere, adeguatamente i comportamenti delle macchine e sviluppare una dipendenza da terzi, come ad esempio gli addetti alla riparazione. Infatti, le più attuali tendenze tecnologiche hanno introdotto macchine in grado di apprendere in modo automatico ed autonomo che, in termini di rischi, può generare comportamenti imprevedibili delle macchine stesse. La presenza di inadeguati sistemi di sicurezza informatica, da una parte le espone a cyber-attacchi, dall'altra aumenta il rischio di collisioni dirette e indirette. Per collisioni indirette pericolose si pensi alla caduta di contenitori di prodotti chimici o radioattivi. L'assenza di recinzioni, all'interno delle quali lasciare operare le macchine, può essere motivo di stress mentale per i lavoratori, paura e insicurezza. Significativi risultano essere anche i rischi di tipo psicologico, dal momento che l'interazione con i dispositivi e la riduzione del contatto tra colleghi umani può causare isolamento sociale. Talvolta, poi, si percepisce una condizione di inferiorità e subordinazione nei confronti delle macchine, più veloci dei lavoratori. Si riscontra anche un eccessivo affidamento nelle capacità dei cobot di riconoscere ed individuare l'uomo, così come di ragionare, il che aumenta il verificarsi di collisioni. Infine, l'intrinseca mutevolezza e l'imprevedibilità delle macchine, può indurre negli operatori stress psicologico, paura e insicurezza.

Implementare un cobot, non è dunque una questione banale. E forse l'eterogeneità dei rischi ai quali i lavoratori vengono esposti, nonché la natura sistemica dei nuovi processi, sempre più complessi e mutevoli, rendono obsolete e inefficaci le metodologie di analisi del rischio tradizionali. In tale ottica, ha senso fare riferimento al concetto di *Safety-II* come possibile nuova filosofia per la gestione della salute e sicurezza sul lavoro con i cobot.

3. Dal concetto di “Safety-I” al concetto di “Safety-II”

Allo scopo di perseguire il proprio obiettivo primario, qualunque organismo, biologico, sociale o tecnologico, deve necessariamente conservarsi, almeno per il tempo necessario all’ottenimento di quello stesso obiettivo primario. Per questo motivo, la definizione più diffusa e frequente di sicurezza (*Safety*) è quella di uno stato libero da danni o perdite (“freedom from harm or loss”). Va da sé che l’obiettivo perseguito da una Scienza della Sicurezza che sostiene questa visione non possa che essere la riduzione degli eventi indesiderati o, in altri termini, che meno cose possibile vadano male. Tale visione è quella che tradizionalmente è stata associata alla Scienza della Sicurezza, e inevitabilmente finisce per categorizzare la realtà in eventi positivi e negativi: se esistono cose che vanno male, devono esistere cose che vanno bene (Dekker, 2019). Lo scivolamento in una prospettiva manichea è per certi versi inevitabile, una volta accettato il presupposto di fondo. La *Safety* allora non può che essere perseguita discriminando la realtà in eventi positivi e negativi e valutandone le implicazioni potenziali. Esiste un comportamento corretto dei mezzi tecnologici, ma anche degli operatori umani. Esiste un’idea a cui la realtà deve conformarsi. Le macchine sono infallibili, almeno fintanto che ne viene garantita l’affidabilità. Gli esseri umani, d’altro canto, sono esseri imperfetti che tendono intrinsecamente a deviare da quest’idealità: sono incompetenti, distratti o semplicemente stanchi. Certo il progettista può e deve migliorare gli ambienti, l’ergonomia e l’interazione uomo-macchina al fine di ridurre il più possibile la non-conformità, ma questi è egli stesso un uomo (Woods *et al.*, 2017). L’errore, il fatto negativo da ridurre, si può annidare ovunque. La soluzione sarà quindi l’individuazione della causa, la sua rimozione, o quando non possibile, la limitazione dei suoi effetti tramite l’inserimento di barriere e/o difese, fisiche, cognitive e organizzative. Una prospettiva del genere è figlia di una concezione neopositivista della scienza, diretta discendente della tradizione analitica di stampo Cartesiano-Newtoniano che ha caratterizzato le *hard sciences* fino ai giorni nostri. Del resto, una tale posizione epistemologica ha innegabilmente funzionato a lungo, riducendo progressivamente gli eventi di danno in maniera significativa dalla nascita della *Safety Science*. Tuttavia, dalla seconda metà degli anni ’80 del XX secolo essa ha iniziato a mostrare i suoi limiti, entrando in un nuovo periodo critico del suo sviluppo. Da una parte, i suoi risultati sono entrati nella fase, per certi versi fisiologica, di *plateau*, per cui a parità di risorse impegnate i miglioramenti sono stati sempre meno significativi; dall’altra, essa ha fallito nel prevenire e contenere diversi eventi catastrofici (e.g., l’incidente di Three Mile Island, il disastro dello Space Shuttle Challenger,

quello di Černobyl', la Deepwater Horizon e l'impianto di Fukushima, tra gli altri); senza considerare che in aggiunta essa comporta una certa tendenza connaturata alla ricerca del capro espiatorio (se qualcosa è andato male, allora ci dovrà necessariamente essere un colpevole, qualcuno che ha fallito o non ha vigilato) e, soprattutto, all'*hindsight bias*, fenomeno di distorsione cognitiva dei fatti che, facendoli percepire ex-post più predicibili di quanto non fossero in realtà, rischia di invalidare qualunque analisi d'incidente (Dekker, 2012; Pollock, 2015).

Una corrente di studi relativamente recente, in seno alla *Safety Science*, la cosiddetta *Resilience Engineering* riconosce ai moderni sistemi sociotecnici lo *status* di sistemi complessi, non completamente trattabili né conoscibili, per i quali inevitabilmente falliscono gli approcci tradizionalmente adottati (Hollnagel, Woods, Leveson, 2012; Patriarca *et al.*, 2018). A partire dalla forse banale considerazione che nella loro gestione quotidiana tali sistemi vengono mantenuti entro limiti accettabili di sicurezza proprio grazie alla gestione subottimale ed estremamente variabile degli operatori umani, Erik Hollnagel – uno dei padri della *Resilience Engineering* – ha iniziato a riferirsi a tali nuove pratiche con il nome di *Safety-II*, in contrapposizione alla *Safety-I* – la visione tradizionale della *Safety* di cui si è discusso poco sopra (Hollnagel, Wears, Braithwaite, 2015).

La *Safety-II* riconosce la sicurezza come una proprietà emergente dei sistemi, nella variabilità delle performance la chiave per il loro successo, e gli esseri umani non più un elemento di debolezza, ma una risorsa necessaria per l'adattabilità, la resilienza e in definitiva la sicurezza di cose e persone. Come conseguenza la *Safety-II* abbandona il proposito di minimizzare il numero di cose che vanno male in favore della massimizzazione di quelle che vanno bene (Hollnagel, 2017).

Le differenze tra i due paradigmi (cfr. Tab. 1) in apparenza sono consistenti, e non hanno mancato di dare adito a ferventi dibattiti in seno alla *Safety Science* (Cooper, 2022; Haavik, 2021), ma bisogna sottolineare il fatto che lo stesso Hollnagel non ha mai sostenuto che la *Safety-II* fosse un approccio sostitutivo della *Safety-I*, semmai complementare. Egli suggerisce che per sistemi semplici, perlopiù caratterizzati da relazioni perfettamente intellegibili e lineari, l'approccio tradizionale sia più che sufficiente. Eppure, in sistemi complessi di media-grande scala, perseguire la sola *Safety-I*, porterebbe al fallimento. Per questo motivo, Hollnagel ed altri autori raccomandano l'impiego congiunto della *Safety-I* e della *Safety-II*.

Sono queste pratiche, ed in particolare l'aggiunta di quanto visto per la *Safety-II*, a poter costituire la base per un nuovo modello di gestione della sicurezza nei contesti digitali che richiedono organizzazione, processi, competenze e capacità particolarmente dinamiche, come quello delle appli-

Tab. 1 - Differenze tra Safety-I e Safety-II, adattato da Hollnagel (2014)

	Safety-I	Safety-II
Definizione	Ridurre al minimo le cose che vanno male	Aumentare al massimo le cose che vanno bene
Principio di gestione della sicurezza	Reattivo: rispondere quando qualcosa va storto o viene categorizzato come rischio inaccettabile	Proattivo: cercare continuamente di anticipare eventuali sviluppi ed eventi
Ruolo del fattore umano	Gli esseri umani sono visti perlopiù come debolezza o pericolo	Gli esseri umani sono visti come una risorsa necessaria per la resilienza di sistema
Investigazione degli incidenti	Gli incidenti sono causati da malfunzionamenti e <i>failure</i> . Scopo dell'investigazione è l'identificazione delle cause	Non esiste una differenza tra eventi positivi e negativi, le cose accadono semplicemente per i medesimi motivi a prescindere dal risultato finale. Lo scopo dell'investigazione è la comprensione di come le cose normalmente vadano bene come base per spiegare come occasionalmente le cose possano andare male

cazioni cobot. Si possono così far strada i concetti di resilienza ingegneristica, cui spesso si sente far riferimento, ma tramite strumenti e metodi in grado di renderla applicata nella prassi quotidiana dell'impresa.

4. La Resilience Analysis Grid come strumento innovativo per la salute e sicurezza

Per resilienza s'intende l'abilità intrinseca di un sistema di aggiustare il proprio funzionamento in presenza di disturbi o di cambiamenti imprevisti, interni o esterni a esso (Hollnagel *et al.*, 2012). Il *Resilience Analysis Grid* (RAG) è uno strumento ideato da Erik Hollnagel che si propone di valutare lo stato potenziale di resilienza di un sistema sociotecnico (Hollnagel, 2011, 2017). Il RAG è basato su una definizione operativa di resilienza che la considera come composizione di quattro abilità di base dette *corner-*

stone abilities: Rispondere (*Respond*), Monitorare (*Monitor*), Anticipare (*Anticipate*) e Imparare (*Learn*). Più in dettaglio:

- *Respond*, corrisponde a sapere cosa fare e ad avere la capacità di affrontare la situazione contingente; essere in grado di rispondere ai cambiamenti regolari e irregolari, ai disturbi e alle opportunità, sia mediante l’attuazione di una serie di risposte pronte all’uso, sia regolando il normale funzionamento del sistema.
- *Monitor*, si riferisce al sapere che cosa controllare, ovvero alla capacità per l’organizzazione di identificare le situazioni critiche e (secondo i principi della *Safety-II*) quelle di opportunità; il monitoraggio deve essere rivolto tanto verso l’esterno (l’ambiente) quanto verso il sistema stesso (le prestazioni).
- *Anticipate*, riguarda il sapere prevedere cosa avverrà, ovvero la capacità di affrontare il futuro; ad esempio, si fa riferimento all’anticipare potenziali interruzioni, nuove esigenze o vincoli, nuove opportunità o minacce, o ancora mutevoli condizioni di esercizio.
- *Learn*, corrisponde alla conoscenza di quanto è successo, ovvero alla capacità di imparare dall’esperienza; in particolare, si può far riferimento alle *lessons learned* sia derivanti da successi che da fallimenti.

Pensare la resilienza come un costrutto composto dalle *cornerstone* ne consente l’operationalizzazione, vale a dire l’adozione di un criterio operativamente fattibile per misurare un concetto altrimenti irraggiungibile, perché definito prettamente dal punto di vista teorico. L’operationalizzazione avviene relazionando o scomponendo le *cornerstone abilities* in item di valutazione. Di fatto, il RAG è uno strumento valutativo associato a un questionario, per questo motivo il termine “item” sottolinea l’appartenenza ai metodi di valutazione per scale, cui il RAG fa riferimento. Ogni item può essere valutato tramite una o più domande a esso pertinenti. Generalmente, ma non necessariamente, si dà alle risposte una struttura di misura ordinale tramite l’adozione di un’ordinaria scala Likert (e.g., Eccellente = 9; Ottimo = 7; Sufficiente = 5; Insufficiente = 3; Scarso = 1; Mancante = 0). Tipicamente, il RAG è uno strumento il cui obiettivo d’indagine è quello di valutare la resilienza di team, reparti, gruppi di persone. Le domande dovrebbero essere specifiche del contesto applicativo poiché altrimenti il questionario perderebbe in capacità diagnostica. I punteggi ottenuti rispetto alla misura di capacità delle quattro *cornerstone* costituiscono il profilo di resilienza di un sistema. Alla griglia valutativa del RAG, costituita dalle domande, si accompagna un metodo composto dalle seguenti fasi:

1. Definire e descrivere il sistema di cui si vuole valutare la resilienza; sarà opportuno includere i confini del sistema, la struttura organizzativa, le persone e le risorse coinvolte, oltre che tutte le informazioni utili

a definire l'ambito del sistema. È necessario conoscere il sistema e lo specifico dominio di applicazione. Questa fase è fondamentale per decidere quali domande proporre e come valutare le risposte.

2. Individuare e formulare un insieme di domande per ciascuna delle quattro abilità; in questa fase si formulano le domande, per ciascuna abilità, da sottoporre alle persone che lavorano nel sistema. Il metodo prevede di partire da un set iniziale e selezionare e/o rifinire e/o aggiungere le domande in modo che siano adeguate in numero e tipo.
3. Ottenere le risposte alle domande formulate al passo precedente; il questionario viene somministrato agli intervistati. Questa somministrazione non è prescritta, può avvenire: tramite intervista non strutturata; tramite intervista semi-strutturata; telematicamente, e così via.
4. Unire le valutazioni per giungere a un punteggio per ogni capacità e per le quattro abilità combinate. I dati, eventualmente stratificati secondo le dimensioni di interesse, raccolti per item, possono essere aggregati in un diagramma *Radar*, uno per *cornerstone*, sui cui assi si segnano i valori Likert. I valori possono ulteriormente essere aggregati in un unico diagramma *Radar* rappresentante il profilo di resilienza.

Il profilo di resilienza ottenuto da una sessione RAG rappresenta in maniera sintetica la capacità potenziale del sistema indagato di essere resiliente. Il RAG è uno strumento di rapida, ma soprattutto facile, valutazione dello stato di resilienza potenziale. Non avendo nessun riferimento, il RAG tradizionale assume carattere di misura relativa quando alla stessa struttura si ripropone lo stesso questionario in momenti distinti. Dal confronto dei due profili di resilienza si potrà dedurre il miglioramento o il peggioramento della performance. Da un'unica sottomissione del questionario si potranno individuare i punti di forza e di debolezza dell'organizzazione, a partire dai quali possono essere motivate una serie di azioni d'intervento. Il RAG è uno strumento che presenta il vantaggio di una semplicità realizzativa superiore a quelle di molti altri metodi della *Resilience Engineering* e probabilmente una maggiore efficacia comunicativa; dunque, si tratta di uno strumento di primo impiego atto ad aumentare la consapevolezza e il coinvolgimento dei diversi stakeholder. Per sua natura, quindi, il RAG si presta a modifiche volte a inglobare declinazioni differenti da quella di ideazione. Ciò può essere sfruttato per ampliare l'impostazione tipica dei sistemi di gestione per la sicurezza tenendo conto delle dimensioni tipiche della resilienza applicata alla salute e sicurezza sul lavoro, anche in considerazione della coabitazione tra il personale umano e quello robotico.

5. Il questionario per l'applicazione della Resilience Engineering sui cobot

Si comprende come analisi e valutazioni tradizionali dei rischi non siano più sufficienti a garantire un'implementazione sicura dei cobot. Un approccio innovativo, basato sul *Resilience Engineering*, in particolare sulla metodologia RAG di cui sopra, ha permesso di realizzare uno strumento mediante il quale le organizzazioni possono valutare il profilo di resilienza a fronte dell'implementazione dei cobot, considerando la salute e la sicurezza dei lavoratori. Come detto, gli obiettivi che la metodologia RAG si prefigge sono rappresentati dalle quattro necessità, sopra indicate come *cornerstone*, che nelle applicazioni cobot corrispondono al rispondere efficacemente ai cambiamenti sui processi interessati al lavoro collaborativo, al monitorarne gli eventi e le prestazioni utili a comprendere quanto in atto nell'interazione persona-cobot, anticipare l'accadere degli eventi con potenziale impatto sulla salute e sicurezza dei lavoratori, e infine apprendere da quanto accaduto e sperimentato con i cobot. Tali capacità sono state inserite in un questionario, poi sottomesso a diverse aziende, che ne hanno validato la significatività rispetto alla possibilità di rispondere con sicurezza alle domande e di ottenere indicazioni sui rischi nuovi o emergenti legati all'utilizzo dei cobot, nonché sulle aree di resilienza da migliorare. I contenuti del questionario rispecchiano fedelmente i risultati collezionati mediante un'analisi sistematica della letteratura, in sede di individuazione di rischi nuovi ed emergenti per la salute e sicurezza dei lavoratori. Partendo dalla capacità delle organizzazioni di *Rispondere* agli eventi, il questionario indaga la presenza e l'aggiornamento di una lista di eventi interni ed esterni all'azienda, potenzialmente critici per la salute e sicurezza del lavoratore, legati alla presenza di cobot. Se tale lista esiste, si indaga la capacità di risposte a tali eventi. Queste attività permettono di formalizzare cosa possa succedere di pericoloso e, in seguito, capire come rispondere. La modalità e la capacità di risposta, vengono valutate analizzando la presenza di *trigger* specifici per l'attivazione della risposta stessa, e la presenza di un monitoraggio del tempo che intercorre tra il verificarsi di un evento e il momento di attivazione della risposta. Si entra, così, nella sezione di *Monitoraggio*. Ivi, la struttura del questionario rispecchia le categorie di rischio presentate in precedenza. Per ogni categoria di rischio, vengono indagati principalmente tre aspetti: dapprima, se il rischio venga monitorato. Si sottolinea che con monitoraggio si intende un controllo costante, sia per verificare la bontà della valutazione del rischio, tendenzialmente realizzata in momenti sporadici, sia per intercettare in tempo reale nuovi fonti di rischio e procedure di mitigazione, eventualmente aggiornando le analisi. Qualora il rischio venga effettivamente monitorato, il questio-

nario indaga se l'organizzazione definisca degli indicatori analitici specifici e, tra questi, si distinguono indicatori di tipo *Lagging* e *Leading*. Gli indicatori *Lagging* e *Leading* sono rispettivamente rivolti alla capacità reattiva e proattiva del sistema. I primi, permettono il monitoraggio dei processi al fine di individuare misure di prestazione di quanto avvenuto. Dunque, tipicamente “in ritardo” (*Lag*) rispetto allo svolgersi degli eventi passati. I secondi, invece, permettono di riconoscere il verificarsi di *pattern* comportamentali del sistema e dell'ambiente al fine di prevedere eventi d'interesse, offrendo segnali predittivi di elementi che portano (*Lead*) a situazioni pericolose. Considerando il grande potenziale in termini di resilienza degli indicatori *Leading* il loro peso è maggiore all'interno del questionario rispetto agli indicatori *Lagging*. Ad esempio, se consideriamo il rischio legato al rumore, un indicatore *Lagging* è il numero di segnalazioni da parte del medico competente di danni all'udito, perché necessariamente successivo all'evento dannoso; un indicatore *Leading* è la misura dell'esposizione sonora degli operatori, perché permette interventi di mitigazione prima che il danno si manifesti. Tale logica viene applicata per tutte le categorie di rischio individuate. Quindi, rischi meccanici, elettrici, termici, chimici, rischi legati al rumore, alla vibrazione, alle radiazioni; infine, rischi di natura ergonomica, psicologica e organizzativa. Nella sezione del questionario rivolta alla capacità delle organizzazioni di *Apprendere*, viene introdotta una distinzione tra le situazioni di non pericolo, pericolo e danno legate ai cobot. Le prime, rappresentano momenti che non si concretizzano in un evento pericoloso ma che in qualche misura rappresentano momenti utili a fini esperienziali. Anche comprendere perché si verifichi un evento inusuale, inatteso, o con risvolto positivo inaspettato, infatti, può rappresentare un'opportunità secondo i principi della *Safety-II*, secondo i quali l'apprendimento può derivare dall'analisi di eventi positivi e negativi (*lessons learned*). In particolare, il questionario indaga come queste tre tipologie di evento vengano analizzate e quali tipologie di evidenze vengano formalizzate. Le analisi, infatti, possono essere *ad hoc*, vale a dire al verificarsi dell'evento, o avere una cadenza regolare, laddove l'organizzazione preveda momenti prefissati per passare in rassegna l'eventuale avvenimento di tali eventi. D'altra parte, le evidenze possono prevedere la formalizzazione di una conoscenza da trasferire in azienda e/o di azioni e comportamenti da modificare che, una volta trasferiti, andrebbero verificati per consolidarne l'efficacia. Ad un livello di astrazione maggiore, la formalizzazione delle evidenze può essere rivolta all'indagine di meccanismi generali, principi astratti, *pattern* ricorrenti su cui l'azienda potrebbe intervenire in maniera proattiva. Oltre a ciò, si indaga la modalità di diffusione interna delle *lessons learned* e le eventuali strategie di diffusione implementate, che possono prevedere momenti di incontri frontali o assumere caratteristiche più esperienziali, anche includendo mo-

menti di riflessione addizionale posteriori alla formazione (*follow-up*). Infine, l'oggetto della formazione può essere improntato sull'apprendimento di questioni puramente tecnologiche o includere tematiche legate anche ai nuovi processi e metodi di lavoro. Tutte questioni affrontate da tale sezione che, in ultima istanza, vuole comprendere se esista un obiettivo specifico della formazione: informare sull'utilizzo della tecnologia? Rendere i dipendenti capaci di utilizzarla? Massimizzare le abilità degli operatori rispetto a mansioni specifiche o a fronte di eventi inattesi? Si giunge, così, nell'ultima sezione del questionario: le organizzazioni sono anche in grado di *Anticipare*? Quando si analizzano soluzioni tecnologicamente evolute, quali i cobot, la capacità di anticipare richiede sia lo studio dell'evoluzione delle tecnologie stesse, sia dei processi e metodi di lavoro annessi, studio che può essere declinato su un orizzonte di breve o lungo periodo. Possono venire in ausilio, con dovuti adattamenti legati al diverso orizzonte di indagine, strumenti predittivi, simulativi ma anche logiche di *trade-off*, quali analisi costi-benefici o *SWOT analysis*. L'analisi delle norme tecniche e dell'evoluzione del mercato, invece, meglio si presta ad indagini di lungo periodo. Infine, si può anticipare un evento significativo per la salute e sicurezza delle persone anche stanziando dei *surplus* di risorse. Si possono, cioè, mettere a disposizione persone, dispositivi, materiali e tempo in misura maggiore rispetto a quanto strettamente richiesto o necessario. Quando ci si confronta con un cobot, gruppi di continuità per evitare arresti delle attrezzature inattesi e potenzialmente pericolosi, sono tra le soluzioni che potrebbero svolgere proprio questa funzione. Gli aspetti presentati, indagati in modo puntuale ma anche analizzati nel complesso, aiutano a comprendere quanto resilienti siano le organizzazioni che utilizzano applicazioni cobot. Inoltre, contribuiscono a fornire alle aziende strumenti e modalità di gestione della salute e sicurezza sul lavoro che includono anche i rischi nuovi ed emergenti che caratterizzano i processi di trasformazione digitale.

6. Alcune evidenze sull'attuale gestione della salute e sicurezza nel lavoro con cobot

Un'indagine promossa da INAIL² ha sperimentato l'utilizzo delle logiche appena riportate a livello nazionale e internazionale, presentando interessanti evidenze.

2. Progetto Bric Inail 2019 - ID 50 condotto dal Dipartimento di medicina, epidemiologia, igiene del lavoro e ambientale dell'Inail, dal Dipartimento di Ingegneria Meccanica e Aerospaziale, Università degli Studi di Roma "La Sapienza", dal Dipartimento di Giurisprudenza, economia, politica e lingue moderne, Università LUMSA e dal Dipartimento di Filosofia e scienze dell'Educazione, Università degli Studi di Torino.

L'assenza di una specifica regolamentazione tecnica rappresenta un tema fortemente critico per le aziende, che a gran voce richiedono una standardizzazione specifica, soprattutto per la gestione degli aspetti legati alla sicurezza dei cobot. Appare troppo esemplificativa, infatti, la visione che considera il cobot come una semplice evoluzione del robot, dal momento che porta a sottostimare caratteristiche distintive di queste soluzioni, quali la mobilità e l'interazione diretta con l'essere umano. Nello studio dei rischi legati all'implementazione dei cobot, le analisi si focalizzano sulle caratteristiche della macchina stessa, non considerando in modo esaustivo che un cobot può utilizzare strumenti, trasportare materiale e, in generale, intraprendere azioni che richiedono un certo grado di controllo della situazione, nonché la capacità di comunicare emergenze e domare situazioni pericolose. Se si considera, infatti, che un cobot può sostituire una persona, possiamo immaginare che, per espletare le proprie attività produttive, utilizzi strumenti di lavoro e movimenti materiale pericoloso. Se lo strumento si rompe o scivola dalle prese della macchina (rischio meccanico), così come se si verificano perdite di sostanze nocive (rischio chimico), l'uomo ha la capacità di domare la situazione, notificarla e rispondere all'emergenza, generalmente con un buon grado di reattività e consapevolezza del rischio. Il cobot, tipicamente, non possiede tali capacità. Se, quindi, non si monitorano rischi che rispecchiano la natura reale del cobot, le organizzazioni possono perdere la capacità di intervenire nelle situazioni di emergenza per i lavoratori. E questo rischio appare tangibile se si considera che solo un terzo delle organizzazioni intervistate monitora il rischio chimico legato ai cobot. Interessanti considerazioni scaturiscono anche dal fatto che, per la maggior parte delle organizzazioni, esiste un soggetto di riferimento in capo a cui attribuire la progettazione e la gestione delle tematiche legate alla sicurezza dei cobot: il fornitore. Se è vero che il costruttore è tenuto a vendere il cobot come un pacchetto prodotto-servizio, dove il servizio prevede anche valutazioni puntuali dei rischi legati alla macchina, è vero anche che è impossibile che tale valutazione tenga conto dei tanti e diversi elementi contestuali che caratterizzano la gestione dei rischi. Il livello di competenza delle persone, le interazioni con attrezzi e materiali, i sistemi di monitoraggio attivi su un processo, la vicinanza o la lontananza con altri processi e via dicendo, cambiano quando cambia l'azienda dove il cobot è implementato. La problematica si avvicina di molto al noto problema di responsabilità legale che emerge nel campo dei veicoli a guida autonoma, in ambito di trasporto civile. Se si verifica un incidente, la responsabilità è di chi progetta gli algoritmi di guida autonoma, del costruttore dell'autoveicolo che utilizza l'algoritmo, o della persona a bordo dell'autoveicolo che ha sempre la possibilità di intervenire? Analogamente, le organizza-

zioni tendono a demandare la responsabilità della valutazione dei rischi al costruttore, o quantomeno a considerare esaustiva la valutazione fornita da esso. In termini di formazione, poi, vanno considerati tutti gli aspetti riconducibili alle tematiche di *Safety-II* precedentemente presentate. Rispondere unicamente ai requisiti di legge non è sufficiente per superare le criticità identificate. Fondamentale è anche riuscire a coniugare in modo vantaggioso l'*usability* e la *learnability*: la capacità di fare propria la tecnologia, di avere familiarità e di saperla utilizzare in maniera vantaggiosa, deve corrispondere ad un'altrettanta facilità e rapidità di apprendimento della nuova tecnologia.

Come è tipico dell'innovazione, sono tanti i rischi e gli aspetti da migliorare, ma non si possono negare i promettenti benefici. In questo senso, implementare un cobot non significa solamente rendere il processo più efficiente e tecnologicamente avanzato per le fasi produttive strettamente coinvolte nell'utilizzo del cobot stesso. Ma permette, ad esempio, di effettuare analisi termografiche per identificare tempestivamente necessità di manutenzione; talvolta, poi, il cobot stesso viene implementato come una misura extra di sicurezza, per le attività che prevedono interazioni pericolose. Per i motivi evidenziati, il cobot sta sempre più assumendo la dimensione di prima tecnologia abilitante verso l'evoluzione 4.0 in ambito manifatturiero. Le potenzialità di altre tecnologie, dedicate al monitoraggio e all'analisi dei dati, sono ad oggi incorporate in queste soluzioni, e i benefici complessivi, in termini di sicurezza, efficienza e resilienza organizzativa, suggeriscono che il cobot sia forse la scelta più completa.

Bibliografia

- Cohen Y., Shraga S., Faccio M., Minto R. (2022), "Deploying cobots in Collaborative Systems: Major Considerations and Productivity Analysis", *International Journal of Production Research*, 60(6), pp. 1815-31.
- Cooper M.D. (2022), "The Emperor Has No Clothes: A Critique of Safety-II", *Safety Science*, 152, p. 105047.
- Dekker S. (2012), *Just Culture: Balancing Safety and Accountability*, Ashgate Publishing, 2nd Edition.
- Dekker S. (2019), *Foundations of Safety Science*, CRC Press, Taylor & Francis Group.
- El Zaatari S., Marei M., Li W., Usman Z. (2019), "Cobot Programming for Collaborative Industrial Tasks: An Overview", *Robotics and Autonomous Systems*, 116, pp. 162-80.
- Galin R., Meshcheryakov R. (2019), "Review on human-robot interaction during collaboration in a shared workspace", *Lecture Notes in Computer Science*, 11659, pp. 63-74.

- Gualtieri L., Palomba I., Wehrle E.J., Vidoni R. (2020), “The Opportunities and Challenges of Sme Manufacturing Automation: Safety and Ergonomics in Human-Robot Collaboration”, in Matt D.T. *et al.*, Eds., *Industry 4.0 for SMEs*, Palgrave Macmillan.
- Gualtieri L., Rauch E., Vidoni R. (2021), “Emerging Research Fields in Safety and Ergonomics in Industrial Collaborative Robotics: A Systematic Literature Review”, *Robotics and Computer-Integrated Manufacturing*, 6, 101998.
- Haavik T.K. (2021), “Debates and Politics in Safety Science”, *Reliability Engineering & System Safety*, 210, 107547.
- Hentout A., Aouache M., Maoudj A., Akli I. (2019), “Human-Robot Interaction in Industrial Collaborative Robotics: A Literature Review of the Decade 2008-2017”, *Advanced Robotics*, 33(15-16), pp. 764-99.
- Hollnagel E. (2011), “RAG - Resilience Analysis Grid”, in Hollnagel E., Paries J., Woods D.D., Wreathall J., Eds., *Resilience Engineering in Practice: A Guidebook*, Ashgate Publishing Co., Surrey, UK.
- Hollnagel E. (2014), *Safety-I and Safety-II (The Past and Future of Safety Management)*, Ashgate Publishing Co., Surrey, Farnham, UK.
- Hollnagel E. (2017), *Safety-II in Practice: Developing the Resilience Potentials*, Routledge.
- Hollnagel E., Woods D.D., Leveson N. (2012), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Aldershot, UK.
- Hollnagel E., Wears R.L., Braithwaite J. (2015), *From Safety-I to Safety-II: A White Paper*, testo disponibile al sito www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-white-papr.pdf.
- Patriarca R., Bergström J., Di Gravio G., Costantino F. (2018), “Resilience Engineering: Current Status of the Research and Future Challenges”, *Safety Science*, 102, pp. 79-100.
- Pollock R.A. (2015), “Human Error: There Is No Root Cause”, in *ASSE Professional Development Conference and Exposition 2015*.
- Rosen A., Strathdee G., Slade M., Powell R. (2000), “Threshold Assessment Grid (TAG): The Development of a Valid and Brief Scale to Assess the Severity of Mental Illness”, *Social Psychiatry and Psychiatric Epidemiology*, 35(2), pp. 78-85.
- Woods D.D., Dekker S., Cook R., Johannesen L., Sarter N. (2017), *Behind Human Error*, Ashgate Publishing Co., Aldershot, UK.