

ASPETTI DI SICUREZZA DEI ROBOT INDUSTRIALI

Ing. Pietro Balbino, ISPESL, Direttore Dipartimento di Torino, Corso Turati 11/C, 10128 TORINO
ispesl.torino@tiscali.it

0. SOMMARIO

Il lavoro si articola in una introduzione, due capitoli e le conclusioni.

Nel primo capitolo vengono esaminate la norma europea UNI EN 775, con osservazioni critiche sul suo pratico utilizzo, e la norma statunitense ANSI/RIA R15.06-1999, con particolare riguardo alle soluzioni pragmatiche che dà ai problemi.

Nel secondo capitolo viene stabilito un confronto tra le impostazioni delle due norme, al fine di formulare proposte migliorative della normativa europea nel senso di una maggiore fruibilità.

1. INTRODUZIONE

Scopo del lavoro è quello di effettuare una disamina con elementi di confronto per quanto possibile tra la normativa europea e la normativa statunitense in tema di sicurezza dei robot industriali. Il confronto è chiaramente concettuale, non potendosi approfondire tutti gli aspetti tecnici specifici.

Vengono quindi esaminati i criteri di sicurezza disponibili nelle due normative relativamente alla progettazione, alla realizzazione ed all'esercizio dei robot nei vari modi di funzionamento.

Si ritiene che le osservazioni formulate possano contribuire, nei loro limiti, a fornire indicazioni per un miglioramento della normativa europea che, come si vedrà nel seguito, non ha sinora prodotto in materia una norma unica alla quale si possa fare un rapido riferimento. Tale normativa contiene rimandi ad altre norme, ma l'utilizzo complessivo non è immediato per i non addetti ai lavori. La norma statunitense che viene esaminata offre invece una visione d'insieme dei problemi, ai quali dà risposte, seppure di massima.

2. NORME

2.1. Norma UNI EN 775 “ Robot industriali di manipolazione – Sicurezza”

2.1.1. Definizioni

Si riporta la definizione di “robot industriale di manipolazione”. E' un “manipolatore a molteplici gradi di libertà, comandato automaticamente, riprogrammabile, multiscopo, fisso o mobile, destinato ad applicazioni di automazione industriale”.

Nelle definizioni viene individuato il “sistema robotico” che comprende il robot (hardware e software) costituito dal manipolatore, dall'alimentazione di potenza e dal sistema di comando, dal dispositivo di estremità, dagli equipaggiamenti, dai dispositivi e sensori e dalle interfacce di comunicazione necessarie per il funzionamento del robot.

Le definizioni riguardano componenti del robot, stati e modi di funzionamento, comandi, blocchi, dispositivi, funzioni di persone, protezioni, spazi e procedure.

E' interessante la definizione di “dispositivo di interblocco (di protezione)”. E' un “montaggio che interconnette un riparo(i) o dispositivo(i) al comando del robot e/o al sistema di alimentazione del robot e dell'equipaggiamento allo stesso associato”.

Vengono inoltre definiti gli spazi di movimento del robot: spazio ristretto (definito dai limitatori di corsa)-spazio massimo-spazio protetto. Le definizioni sono corredate da una figura esemplificativa, che non appare sufficiente ad illustrarle compiutamente.

Un'altra definizione importante riguarda l' “unità portatile di addestramento”. E' “un'unità tenuta manualmente, collegata al sistema di comando, con la quale si può programmare (o muovere) un robot”.

2.1.2. Considerazioni generali

Vengono riassunti nelle generalità i principali problemi di sicurezza dei robot.

I movimenti dei robot industriali sono ad alta energia; è da considerare inoltre la variabilità e l'imprevedibilità dei movimenti del braccio del robot.

Il problema più grave, che sarà affrontato dal punto di vista progettuale esaminando nel seguito le norme statunitensi ANSI/RIA R15.06-1999 (Approved American National Standard/Robotic Industries Association), è quello della presenza di personale all'interno dello spazio ristretto, o meglio dello spazio massimo. Altro problema è quello dell'interazione fra più robot.

Vengono dettati criteri di massima in tema di analisi di sicurezza, per individuare le sorgenti di pericolo, per valutare l'entità del rischio e per adottare una strategia di sicurezza per la selezione dei provvedimenti

necessari. In particolare viene richiesto di definire i compiti richiesti per le applicazioni prevedibili, di identificare le fonti di pericolo compresi i modi di guasto e rottura per ogni compito, di valutare e accertare i rischi, di considerare le strategie di sicurezza che minimizzano i rischi, di selezionare i metodi di messa in sicurezza e di valutare i livelli di sicurezza complessiva raggiunti.

Non viene però sviluppato direttamente nella norma un criterio e un metodo che consenta di stabilire le modalità di effettuazione dell'analisi di sicurezza, della valutazione dei risultati e dei provvedimenti presi, che stabilisca cioè se i provvedimenti assunti hanno ridotto il rischio nella misura che si ritiene sufficiente. In tema di valutazione dell'entità del rischio vengono fornite indicazioni generali che non esauriscono certamente le problematiche in essere. Tuttavia i criteri di effettuazione dell'analisi di rischio sono definiti da norme più generali, come la EN 1050 (Sicurezza del macchinario-Principi per la valutazione del rischio) e le EN 292-1 (Sicurezza del macchinario-Concetti fondamentali, principi generali di progettazione-Terminologia, metodologia di base) e EN 292-2 (Sicurezza del macchinario-Concetti fondamentali, principi generali di progettazione-Specifiche e principi tecnici).

In particolare riveste interesse la norma UNI EN 954-1 (Sicurezza del macchinario-Parti dei sistemi di comando legate alla sicurezza-Principi generali per la progettazione), nella quale, a conferma di quanto sopra indicato, vengono indicate le norme a cui riferirsi per effettuare l'analisi del pericolo sulla macchina (EN 292-1 e EN 1050) e per effettuare la valutazione del rischio sulla macchina (EN 292-1 e EN 1050). Relativamente alle misure da adottare per la riduzione del rischio, sia attraverso la progettazione che mediante la protezione, viene indicata la norma EN 292-2.

2.1.3. Progettazione e costruzione del robot. Messa in sicurezza del sistema robotico.

Il progetto del robot deve essere compatibile con la predisposizione di mezzi per la limitazione dello spazio di movimento, che consistono principalmente in fermi meccanici; metodi alternativi possono essere adottati solo se si consegue lo stesso livello di sicurezza dei fermi meccanici.

Vengono considerati gli aspetti che riguardano il comando del robot e del sistema robotico. Viene evidenziata la necessità di fornire mezzi per il rilascio controllato dell'energia immagazzinata, che può comparire in accumulatori di fluidi in pressione, in condensatori, molle, contrappesi e volani.

Il sistema robotico deve essere compatibile con le condizioni ambientali. Deve tenersi conto delle miscele esplosive, della corrosione, dell'umidità, della temperatura, della polvere e delle interferenze. L'interruzione del funzionamento non deve creare condizioni di pericolo; dopo l'intervento dell'arresto d'emergenza, gli interventi di ripristino e di riavviamento devono avvenire all'esterno dello spazio ristretto.

Per quanto riguarda le protezioni, vengono presi in considerazione i ripari fissi e i ripari interbloccati. I primi devono evitare l'accesso allo spazio protetto, tranne che da aperture dotate di interblocco, o di rilevazione di presenza. Per i secondi l'interblocco deve impedire il funzionamento automatico del sistema robotico fino a che gli stessi non siano stati chiusi. La chiusura di un riparo non deve provocare il riavviamento automatico del robot, che deve invece avvenire a seguito di azione deliberata. Nel caso che l'accesso avvenga attraverso una porta interbloccata, deve essere previsto un dispositivo che eviti la chiusura involontaria della porta.

Per quanto riguarda i dispositivi rilevatori di presenza, gli stessi non devono poter essere elusi; non devono essere influenzati dalle condizioni ambientali; il campo sensibile, quando viene riattivato per la ripresa del movimento del robot, non deve fungere da comando di riavviamento automatico. Sono previsti mezzi di allarme, che non essendo sostitutivi delle protezioni, devono essere chiaramente avvertibili senza ambiguità.

Dopo aver elencato le condizioni nelle quali il funzionamento automatico del robot può essere consentito, vengono date prescrizioni di sicurezza relative alla fase di programmazione, nel corso della quale il programmatore, unica persona nello spazio protetto, deve avere tutto sotto comando, compreso il movimento di eventuali altri equipaggiamenti. Si inizia a velocità ridotta. Successivamente ci si porta alla velocità di funzionamento. Un altro aspetto importante è la localizzazione del guasto del sistema robotico, quando si manifesta: effettuandola all'interno dello spazio protetto, il movimento del robot deve avvenire tramite un dispositivo di abilitazione.

La manutenzione deve essere effettuata, per quanto possibile, dall'esterno dello spazio protetto. Quando avviene all'interno dello spazio protetto, devono essere prese opportune precauzioni. Deve essere disinserita la sorgente di energia, con avviso su apposito cartello. Il personale all'interno dello spazio protetto per operazioni di manutenzione deve avere il comando totale del robot.

2.1.4. Installazione, messa in servizio e prova funzionale

Ai fini dell'installazione si deve considerare come guida addizionale la norma ISO 9946 "Robot industriali di manipolazione - Presentazione delle caratteristiche". Un aspetto importante dell'installazione del sistema robotico è la sua messa in sicurezza, che deve essere effettuata tenendo conto dell'analisi dei

pericoli individuati e della valutazione dell'entità dei relativi rischi. Le procedure di messa in servizio e di prova funzionale si applicano anche nel caso che al robot o al sistema robotico vengano apportate modifiche. Per quanto riguarda la messa in servizio, lo spazio ristretto deve in ogni caso essere definito e delimitato, anche con mezzi provvisori. Non può essere presente personale nello spazio ristretto prima che siano funzionanti le protezioni.

Prima di applicare potenza sono previste verifiche che riguardano il corretto montaggio del robot, la corretta effettuazione dei collegamenti elettrici ed il corretto collegamento delle "utilities" e dell'equipaggiamento periferico, l'installazione dei dispositivi di fine corsa e dei mezzi di protezione, l'illuminazione, il rumore e il microclima. Dopo l'applicazione della potenza è previsto di verificare il corretto funzionamento dei dispositivi di avvio, di arresto e di comando e dei relativi circuiti, il corretto movimento degli assi del robot nei limiti prefissati, la possibilità di scollegare e isolare le sorgenti esterne di alimentazione, il corretto funzionamento degli equipaggiamenti di addestramento, la conformità di funzionamento delle protezioni e degli interblocchi. Deve inoltre essere verificato che a velocità ridotta il robot funzioni in modo appropriato con capacità di manipolazione; lo stesso deve essere verificato nel funzionamento a velocità e carico nominale.

2.1.5. Elementi di miglioramento della UNI EN 775 .

L'esame della UNI EN 775 ne evidenzia i possibili elementi di miglioramento.

Un elemento di miglioramento consiste nella esemplificazione delle soluzioni tecnologiche necessarie per conseguire i livelli di sicurezza desiderati.

Un altro elemento che evidenzia la necessità di miglioramento è la conduzione di una analisi di rischio specifica per il tipo di prodotto, di immediato utilizzo e che non costringa a faticosi "incroci" con altre normative o regole tecniche.

Nei paragrafi seguenti verranno esaminate le norme europee che colmano queste lacune, ma dalle conclusioni emergerà la necessità di un'unica norma sull'argomento.

2.2. Altre norme di interesse ricollegabili alla UNI EN 775

2.2.1. UNI EN 954-1 e prEN ISO 13849-1:2002

La norma UNI EN 775 (settembre 1994) deriva dalla norma internazionale ISO 10218:1992 "Robot industriali di manipolazione – Sicurezza". In aggiunta ai requisiti dati nella ISO 10218:1992, per la sicurezza dei robot industriali di manipolazione si applicano, come già evidenziato, le norme UNI EN 292/1 e UNI/EN 292/2.

Una norma di interesse ricollegabile alla UNI EN 775 è la già citata UNI EN 954-1, del dicembre 1998: "Sicurezza del macchinario-Parti dei sistemi di comando legate alla sicurezza-Principi generali per la progettazione". Tale norma è riferita alle macchine in generale, ma i concetti sono chiaramente applicabili ai robot e ai sistemi robotici. E' posteriore alla UNI EN 775, ma i riferimenti tecnici sono interessanti perché coprono alcuni spazi che invece sono ben evidenziati nella norma statunitense ANSI/RIA R15.06 – 1999 che sarà successivamente esaminata. Della UNI EN 954-1 si riportano per brevità tre definizioni.

Parte di un sistema di comando legata alla sicurezza: " Parte(i) o sotto-insieme(i) di un sistema di comando che risponde a segnali di ingresso e genera segnali di uscita legati alla sicurezza. Le parti combinate di un sistema di comando legate alla sicurezza iniziano nei punti in cui i segnali legati alla sicurezza vengono generati e finiscono all'uscita degli elementi di comando di potenza. Ciò include anche i sistemi di sorveglianza".

Categoria: "Classificazione delle parti di un sistema di comando legate alla sicurezza in relazione alla loro resistenza ai guasti e al loro conseguente comportamento in condizioni di guasto, ottenuto mediante la disposizione strutturale delle parti e/o la loro affidabilità".

Sicurezza dei sistemi di comando: "Capacità delle parti di un sistema di comando legate alla sicurezza di espletare le loro funzioni di sicurezza per un dato tempo, secondo la loro categoria specificata".

Proseguendo nell'esame della UNI EN 954-1, è utile soffermarsi sul capitolo riguardante le "categorie" come sopra definite. Il concetto base della norma è la resistenza ai guasti. In tema di riduzione del rischio viene specificato che più la riduzione del rischio dipende dalle parti del sistema di comando legate alla sicurezza, maggiore è la capacità di resistenza ai guasti richiesta a tali parti. Le vie per ottenere una maggiore capacità di resistenza ai guasti sono l'affidabilità dei componenti e dei sistemi e l'adeguatezza della struttura delle suddette parti.

La norma riporta un elenco di requisiti, situazioni e di tipiche funzioni di sicurezza che possono essere realizzate dalle parti del sistema di comando legate alla sicurezza: funzione di arresto – funzione di arresto di emergenza – riarmo manuale – avviamento e riavviamento – tempo di risposta – parametri legati alla

sicurezza – funzione di comando locale – inibizione – sospensione manuale delle funzioni di sicurezza – oscillazioni, interruzioni e ripristino delle fonti di energia.

Le parti dei sistemi di comando legate alla sicurezza devono essere conformi ai requisiti di una o più delle cinque categorie sotto specificate.

Categoria B: - le parti dei sistemi di comando legate alla sicurezza devono, come minimo, essere progettate, costruite, scelte, montate e combinate in conformità alle norme relative, utilizzando i principi di sicurezza di base per la specifica applicazione, in modo che possano sopportare le sollecitazioni di funzionamento previste ed altre influenze esterne correlate.

Categoria 1: - si devono applicare i requisiti della categoria B. Le parti dei sistemi di comando legate alla sicurezza devono essere progettate e costruite utilizzando componenti e principi di sicurezza ben collaudati.

Categoria 2: - si devono applicare i requisiti della categoria B e l'uso dei principi di sicurezza ben collaudati. Inoltre le parti dei sistemi di comando legate alla sicurezza devono essere progettate in modo che le loro funzioni vengano verificate ad opportuni intervalli dal sistema di comando della macchina.

Categoria 3: - si devono applicare i requisiti della categoria B e l'uso dei principi di sicurezza ben collaudati. Inoltre le parti dei sistemi di comando legate alla sicurezza devono essere progettate in modo che un singolo guasto in una qualsiasi di tali parti non porti alla perdita della funzione di sicurezza.

Categoria 4: - si devono applicare i requisiti della categoria B e l'uso dei principi di sicurezza ben collaudati. Inoltre le parti dei sistemi di comando legate alla sicurezza devono essere progettate in modo che un singolo guasto in una qualsiasi di queste parti legate alla sicurezza non porti ad una perdita della funzione di sicurezza e il singolo guasto venga rilevato in corrispondenza o prima della successiva richiesta delle funzioni di sicurezza.

Nell'Appendice B alla norma viene indicato un metodo basato sulla norma UNI EN 1050 "Sicurezza del macchinario – Principi per la valutazione del rischio". Non vengono effettuate valutazioni quantitative del rischio; viene valutato invece il contributo alla riduzione del rischio portato dalle parti del sistema di comando legate alla sicurezza. Riferendosi alla UNI EN 1050 ed alla terminologia mutuata da ANSI/RIA, utile per un confronto, viene considerata nella norma UNI EN 954-1 la Severità (S2 danno grave – S1 danno leggero), la Frequenza (F2 esposizione frequente – F1 esposizione non frequente) e la Evitabilità (P2 non probabile – P1 probabile). In tal modo si può determinare la categoria i cui requisiti devono essere rispettati affinché sia realizzata una efficace resistenza ai guasti ed una significativa riduzione del rischio.

Il metodo è sintetizzato nella Figura 1 sotto riportata, dalla quale, seguendo il percorso severità/frequenza/evitabilità, si giunge alla categoria da adottare e cioè alle soluzioni tecnologiche e di affidabilità per contrastare il rischio connesso al percorso seguito.

Le categorie preferite da adottarsi sono indicate con un cerchio grande annerito. Il cerchio piccolo annerito indica la scelta di una categoria meno impegnativa: la sua scelta al posto del cerchio grande annerito, che individua la categoria da adottarsi, comporta misure aggiuntive, quali il sovradimensionamento o l'uso di tecniche per l'esclusione dei guasti. Il cerchio grande vuoto indica l'adozione di categoria superiore a quella da adottarsi. Nei ragionamenti condotti deve tenersi conto che la norma UNI EN 954-1 è riferita al macchinario in generale. Tuttavia la sua pertinenza, oltre che essere evidente, è avvalorata dalla citazione della norma EN 775 nella bibliografia.

Dall'esame della UNI EN 775 risultano evidenti le osservazioni formulate che la individuano come norma generale che richiede per la sua applicazione la conoscenza di altre norme, tra le quali quelle citate e brevemente esaminate. Sarebbe utile, per gli aspetti applicativi, una norma più esaustiva che includesse in sé, citandoli ed inglobandoli organicamente, i contenuti delle altre norme di pertinenza.

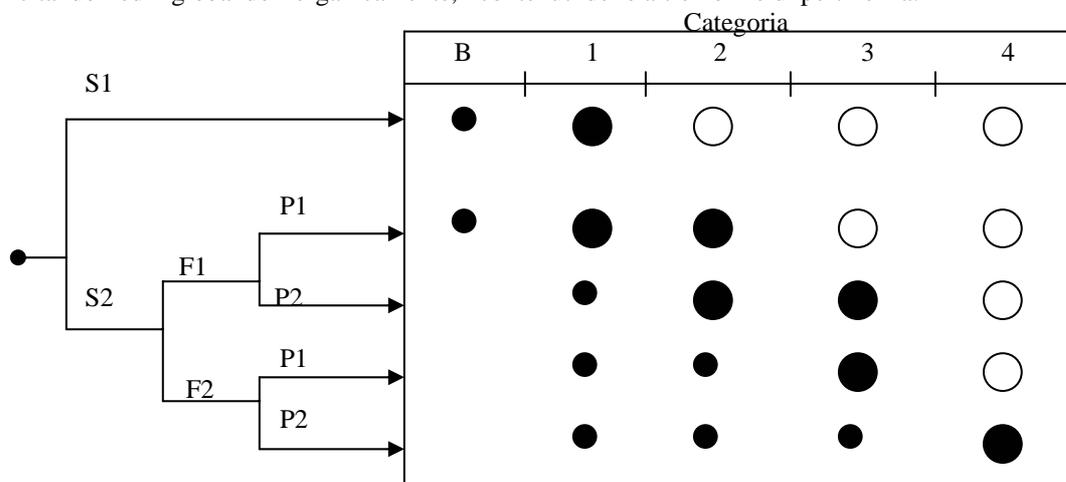


Figura 1 – Possibile scelta delle categorie

Una importante evoluzione della UNI EN 954-1 è lo standard che risulta dalla sua revisione, la prEN ISO 13849-1:2002, che ne porta la stessa denominazione, ma con una novità fondamentale.

L'analisi di rischio non viene più effettuata in base a criteri deterministici, bensì probabilistici.

Tali criteri vengono introdotti fino dalle definizioni e riguardano (non esaustivamente):

- rischio e rischio residuo: definizioni note;
- $MTTF_d$ – tempo medio al guasto “pericoloso”: valore medio del tempo di funzionamento nel quale ci si attende che un singolo canale del sistema abbia un guasto pericoloso;
- T_M – tempo di missione: periodo di tempo che copre l'uso atteso di un SRP/CS;
- SRP/CS – Safety- Related Part of a Control System: parte di un sistema di comando legata alla sicurezza;
- λ_d – tasso di guasto “pericoloso”: frazione di tutti i successivi elementi che si guastano con pericolo per unità di tempo; per elementi con tasso di guasto costante, $MTTF_d$ è il reciproco di λ_d .
- DC – copertura diagnostica – $DC = \frac{\sum \lambda_{da}}{\sum \lambda_d}$: frazione della probabilità dei guasti pericolosi rivelati rispetto alla totalità dei guasti pericolosi;
- CCF – guasti con causa comune: guasti di elementi differenti che derivano da un singolo evento. Questi guasti non sono conseguenze l'uno dell'altro.

I criteri affidabilistici introdotti si ritrovano nelle specifiche delle categorie.

Categoria B: - nei sistemi di categoria B non c'è copertura diagnostica e il tempo medio al guasto è da basso a medio. In tali strutture (sistemi a canale singolo) la considerazione dei guasti con causa comune non è rilevante.

Categoria 1: - nei sistemi di categoria 1 non c'è copertura diagnostica e il tempo medio al guasto è alto. In tali strutture (sistemi a canale singolo) la considerazione dei guasti con causa comune non è rilevante. In nota viene evidenziato che il tempo medio al guasto in categoria 1 è più alto che in categoria B. Di conseguenza la perdita della funzione di sicurezza è meno probabile.

Categoria 2: - la copertura diagnostica di tutte le parti dei sistemi di comando legate alla sicurezza comprese le funzioni di prova è da bassa a media. Nei sistemi di categoria 2 il tempo medio al guasto è da basso ad alto, perché dipende dal livello di prestazione richiesto. Nella categoria 2 devono essere adottate misure contro i guasti con causa comune.

Categoria 3: - la copertura diagnostica di tutte le parti dei sistemi di comando legate alla sicurezza comprese le funzioni di prova è da bassa a media. Nei sistemi di categoria 3 il tempo medio al guasto di ciascuno dei canali ridondanti è da basso ad alto, perché dipende dal livello di prestazione richiesto. In categoria 3 devono essere adottate misure contro i guasti con causa comune. In nota viene evidenziato che quando si verifica un singolo guasto la funzione di sicurezza viene sempre assicurata, ma che l'accumulo di avarie non rivelate può condurre alla perdita della funzione di sicurezza.

Categoria 4: - la copertura diagnostica di tutte le parti dei sistemi di comando legate alla sicurezza comprese le funzioni di prova è alta, comprendendo anche l'accumulo di avarie. Nei sistemi di categoria 4 il tempo medio al guasto di ciascuno dei canali ridondanti è alto. In categoria 4 devono essere adottate misure contro i guasti con causa comune. In nota viene specificato che i guasti devono essere rivelati in tempo per prevenire la perdita della funzione di sicurezza.

Dopo avere indicato le caratteristiche affidabilistiche delle categorie nella prEN in esame, ci si chiede quali architetture di sistema possano essere conformi ai requisiti delle categorie stesse. Una risposta viene dall'Annesso B, informativo e di carattere generale, nel quale le architetture vengono specificate.

Le architetture indicate hanno inizio nei punti in cui partono i segnali relativi alla sicurezza, e terminano all'uscita degli elementi di controllo di potenza. E' da chiarire che nelle figure l'elemento indicato come “sensore” può rappresentare, per esempio, delle barriere luminose, come pure circuiti di ingresso di elementi facenti parte della logica di controllo o interruttori di ingresso di contattori. Analogamente il termine “attuatori” può rappresentare per esempio il segnale di uscita di un dispositivo di interruzione.

Per ogni categoria viene indicato uno schema, che si riporta nelle figure 2, 3, 4, 5 e 6. Le lettere hanno i seguenti significati:

- I: Dispositivo di ingresso, per esempio Sensore
- L: Logica di controllo
- O: Dispositivo di uscita, per esempio Attuatore
- TE: Dispositivo per test

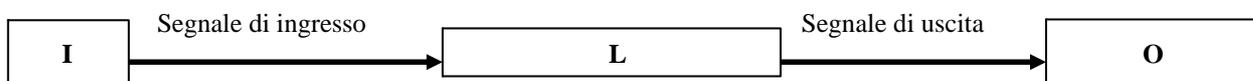


Figura 2 – Architettura stabilita per la categoria B

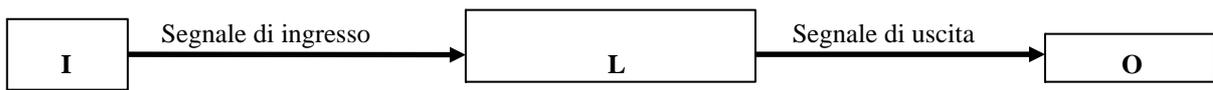


Figura 3 – Architettura stabilita per la categoria 1

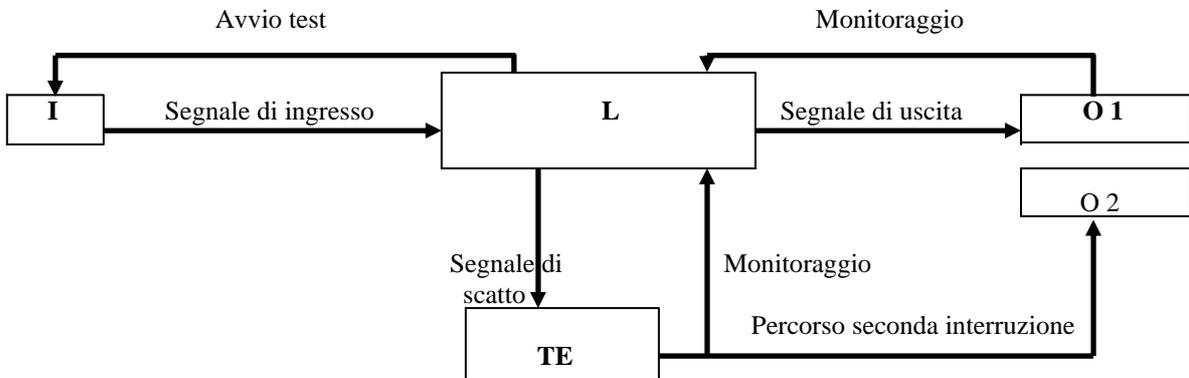


Figura 4 – Architettura stabilita per la categoria 2

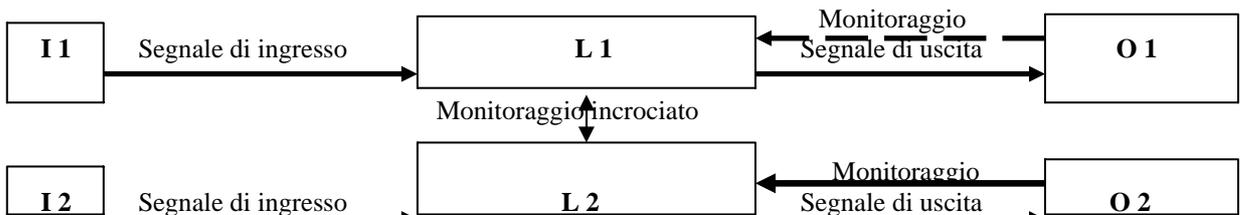


Figura 5 – Architettura stabilita per la categoria 3

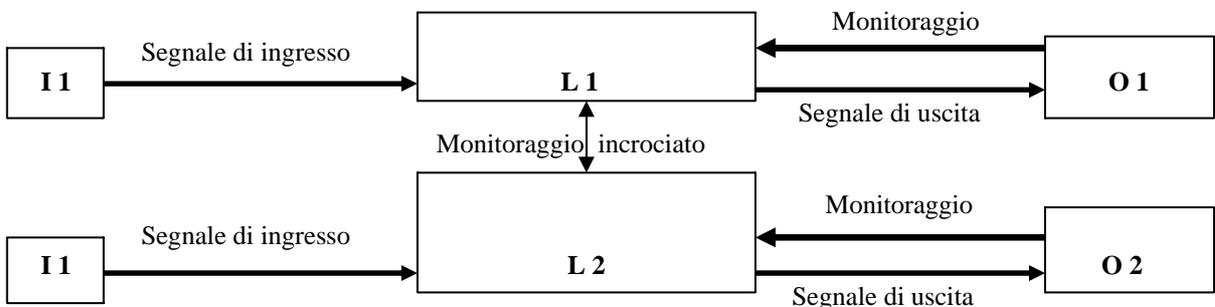


Figura 6 – Architettura stabilita per la categoria 4

2.2.2. Considerazioni conclusive sulla normativa europea.

E' auspicabile un progetto di norma che dia una chiara visione di insieme al progettista, all'installatore ed all'utilizzatore dei robot e dei sistemi robotici.

Gli elementi non mancano. Si può mantenere l'impostazione generale della UNI EN 775, completandola con gli elementi della prEN 13849-1:2002 esaminati nel paragrafo 2.2.1. del presente lavoro.

In particolare si ritiene importante mutuare la nuova impostazione che la suddetta proposta di norma dà all'analisi di rischio, introducendo dati utili per una valutazione anche quantitativa del rischio stesso, come del resto richiesto dalla UNI EN 1050 nel paragrafo 4.1 per i casi in cui il danno sia grave e comunque i dati necessari siano disponibili.

La prEN permette di determinare i livelli di prestazione richiesti e di verificarli in base ai parametri affidabilistici, essi pure determinabili; nell'ultimo annesso inoltre fornisce esempi di chiaro interesse applicativo.

Il criterio di integrazione della UNI EN 775 che si propone non vuole produrre una “summa”, bensì un testo che applichi anche al campo dei robot e dei sistemi robotici i più recenti sviluppi normativi in tema di sicurezza del macchinario.

2.2.5. Norma ANSI/RIA R15.06 – 1999. American National Standard for Industrial Robots and Robot Systems. Safety Requirements.

2.3.1. Generalità

I requisiti della norma si applicano ai robot di nuova costruzione ed ai robot ricostruiti e “migliorati”.

La costruzione comprende il progetto, le istruzioni tecniche, la costruzione vera e propria, le prove funzionali e la distribuzione di un robot industriale.

La ricostruzione comprende le nuove istruzioni tecniche o l’attività di costruzione su robot esistenti in conformità a specifiche nuove o revisionate (del costruttore originario o di altra provenienza); sono compresi i lavori di miglioramento e di modifica del robot, ad esclusione degli aggiornamenti del software.

La norma riporta le normative di riferimento:

- ANSI/NFPA 79-1997 - Standard elettrici per il macchinario industriale;
- ANSI/UL 1740-1998 - Standard di Sicurezza per i robot e gli equipaggiamenti robotici;
- OSHA 1904 - Requisiti generali per registrare e relazionare su lesioni e infermità;
- OSHA 1910.147 - Controllo delle sorgenti di energia pericolose (Blocco/Segnalazione);
- OSHA 1910.212 - Requisiti generali per tutte le macchine (Sorveglianza delle macchine);
- OSHA 1910.219 - Apparati di trasmissione della potenza meccanica.

La norma è articolata in paragrafi, il cui numero di riferimento viene riportato nel seguito.

2.3.2. Definizioni

Esaminando le definizioni, è possibile trovarvi elementi che per la loro specificità non compaiono in UNI EN 775. Se ne riportano alcune di interesse.

“Actuator” - attuatore. E’ un meccanismo usato per compiere un movimento. Può essere un meccanismo che converte energia elettrica, idraulica o pneumatica per eseguire un movimento. Può anche essere un meccanismo all’interno di un sistema di controllo (ad esempio un’asta che apre dei contatti). Può altresì essere un dispositivo (per esempio a chiave) che inizia una sequenza di blocco/sblocco.

“Attended program verification” (APV) – verifica del programma che ci si attende venga eseguito. E’ l’atto (azione) col quale una persona, all’interno dello spazio protetto, verifica i compiti programmati del robot alla velocità programmata.

“Limiting device” – dispositivo di limitazione. E’ un dispositivo che restringe lo spazio massimo, fermando o causando la fermata di ogni movimento del robot e che è indipendente dal programma di controllo e dai programmi che riguardano i compiti.

“Interlock” – interblocco. E’ un arrangiamento (sistemazione, montaggio) per mezzo del quale il funzionamento di un controllo o di un meccanismo permette, o previene, il funzionamento di un altro controllo o meccanismo. La definizione risponde ad una logica generale, mentre la definizione UNI EN, come già visto, definisce il dispositivo di interblocco come il montaggio che interconnette un riparo o un dispositivo al comando e/o al sistema di alimentazione del robot e dell’equipaggiamento ad esso associato: si tratta di una definizione meno generale ma efficace.

“Pendant” – unità portatile. E’ un dispositivo a comando manuale collegato al sistema di controllo mediante il quale il robot può essere programmato o mosso. E’ anche chiamato “teach pendant”.

“Safety rated” (riferito a componenti o sistemi) - legato alla sicurezza, testato, valutato e provato per funzionare in maniera affidabile e accettabile quando è impiegato in una funzione critica per la salute e il benessere del personale.

“Teach (Programming)” – insegnamento (programmazione). E’ la programmazione effettuata guidando manualmente il dispositivo di estremità del robot, o guidando manualmente un dispositivo meccanico di simulazione, oppure usando una unità portatile di insegnamento per muovere il robot.

“Teach mode” – modo di funzionamento “insegnamento”. E’ lo stato del sistema di controllo che permette la generazione e la memorizzazione dei dati sui punti di posizione a bassa velocità (max. 250 mm/sec.).

2.3.3. Costruzione dei robot

Vengono fornite indicazioni e prescrizioni sui requisiti generali del robot e sui pericoli per il personale dovuti ai componenti di trasmissione di potenza. Questi pericoli, come gli altri (rilascio di energia immagazzinata, interferenze etc.) devono essere evitati in sede di progettazione e di costruzione.

Sono previsti quattro livelli di prestazione per i circuiti di sicurezza:

- Livello “semplice”, realizzato mediante semplici circuiti di sicurezza progettati e costruiti con la tecnica del canale singolo;
- Livello “a singolo canale”, in cui i circuiti devono essere basati sull’hardware o sul software o sulla microprogrammazione del fabbricante (“firmware”), con componenti “safety rated”;
- Livello “a singolo canale con monitoraggio”, che include i requisiti del livello semplice. Deve permettere di effettuare prove e test ad intervalli regolari, meglio se in modo automatico. I test sulle funzioni di sicurezza devono essere effettuati alla partenza e periodicamente durante il funzionamento. Dopo la scoperta del guasto, si deve rimanere in sicurezza fino all’eliminazione.
- Livello “a controllo affidabile”, nel quale i circuiti di sicurezza siano progettati e realizzati in modo che il guasto di un singolo componente non prevenga l’azionamento dell’arresto del robot.

Durante l’impiego dell’unità portatile non deve essere possibile il funzionamento automatico del robot. Il movimento deve avvenire a bassa velocità (non maggiore di 25 cm/sec). Quando invece si deve effettuare la verifica del programma atteso (APV), e quindi si deve operare ad alta velocità, deve potersi selezionare il modo di funzionamento APV con un comando ad azione deliberata.

2.3.4. Requisiti prestazionali dei dispositivi di protezione

Vengono prese in considerazione le barriere di protezione, fisse e interbloccate, che devono essere costruite per contrastare le forze che si generano durante il funzionamento del robot e le condizioni ambientali, e non devono creare di per sé un pericolo. I dispositivi di interblocco devono avere a corredo una chiave, un pulsante o un dispositivo di messa in movimento che non siano facilmente duplicabili e non devono essere azionabili intenzionalmente senza attrezzi. I dispositivi meccanici devono avere un collegamento fisico tra la sorgente di energia relativa ad un pericolo e il meccanismo di blocco. I dispositivi elettrici, con o senza blocco di protezione, devono essere del tipo già visto “a controllo affidabile”, e dopo la rilevazione del guasto si deve prevenire il ripristino del funzionamento automatico fino a che il guasto non sia stato riparato. In alternativa i dispositivi elettrici devono essere progettati “ad apertura positiva”. Per i dispositivi a scansione di area deve essere fornito il massimo tempo di risposta, il massimo campo di protezione, il massimo campo visuale in gradi. I dispositivi basati sulla capacità a radiofrequenza devono avere una regolazione di sensibilità tale da permettere regolazioni autorizzate del campo da parte di personale qualificato. Sono previste norme per i sistemi di sicurezza a tappeto. Lo stesso per i sistemi di sicurezza a fascio singolo o multiplo. Sono regolamentati anche i sistemi di controllo a due mani, i cui controlli manuali da parte dell’operatore devono essere concepiti in modo da richiedere l’uso delle due mani entro 500 ms.

2.3.5. Installazione dei robot e dei sistemi robotici

I robot e i sistemi robotici devono essere installati secondo le specifiche del costruttore. Devono essere valutate le condizioni ambientali per assicurare che il robot sia compatibile con le condizioni di lavoro. Devono essere prese in considerazione a tal fine le miscele esplosive, la corrosione, l’umidità, la polvere, la temperatura, l’interferenza elettromagnetica, l’interferenza a radiofrequenza e le scariche elettrostatiche.

I sistemi di controllo e gli equipaggiamenti a cui si deve accedere durante il funzionamento automatico devono essere collocati al di fuori dello spazio protetto. I sistemi di controllo possono essere basati su software e su microprogrammazione (“firmware”, in cui il codice di controllo del programma predisposto dal fabbricante non può essere cambiato dall’utente), usati al posto di componenti e sistemi di sicurezza basati sull’hardware. In tal caso i dispositivi di controllo devono essere progettati in modo che ogni singolo guasto di un componente di sicurezza o della microprogrammazione porti il sistema a disinnestarsi in uno stato sicuro e non permetta il funzionamento automatico fino a che il guasto non sia stato riparato, mantenendo lo stesso grado di sicurezza dei componenti hardware.

I dispositivi di limitazione non meccanici, devono essere testati dopo l’installazione per determinare i confini dello spazio ristretto. I test devono essere effettuati alla massima velocità ed alle massime condizioni di carico in corrispondenza della completa estensione. Le prestazioni dei circuiti dei dispositivi di limitazione non meccanici devono essere del tipo “a controllo affidabile”.

I dispositivi di limitazione meccanici includono gli arresti meccanici, che sono regolati e poi resi sicuri mediante dispositivi di fissaggio. Lo spazio ristretto, definito dai dispositivi di limitazione, deve essere adeguatamente identificato. Inoltre la logica degli interblocchi di protezione deve essere tale che lo spazio ristretto venga ridefinito allorché il robot compie il proprio programma di apprendimento.

In ogni installazione deve esserci la possibilità di togliere energia al robot. Ogni sistema robotico deve avere un circuito di arresto di emergenza ed un circuito di arresto di sicurezza, del tipo a controllo affidabile. Il circuito di arresto di emergenza del sistema deve essere del tutto conforme a NFPA 79, deve prevalere su tutti gli altri controlli, provocare l'arresto di ogni movimento, togliere potenza per il movimento agli attuatori del robot e rimuovere tutte le sorgenti di energia che possono presentare un pericolo. Ogni postazione di comando con operatore del sistema robotico deve essere corredata di un dispositivo di arresto facilmente accessibile. I pulsanti per l'arresto di emergenza devono richiedere il ripristino manuale.

Quando il sistema robotico funziona in automatico, l'arresto di sicurezza può iniziare manualmente o tramite la logica di controllo. Deve essere previsto un circuito separato dal circuito di arresto di emergenza.

2.3.6. Protezione del personale. Generalità

Le principali sorgenti di pericolo sono, non esaustivamente, il movimento di componenti meccanici che causano intrappolamento o schiacciamento, l'energia immagazzinata in parti in movimento ed in componenti azionati elettricamente, pneumaticamente o da fluido, le sorgenti di energia, le atmosfere pericolose, l'interferenza elettromagnetica, elettrostatica e a radiofrequenza, gli oggetti staccati o proiettati.

Sono importanti sorgenti di pericolo gli scivolamenti, rilasci e cadute, gli errori umani nella progettazione, nello sviluppo e nella costruzione, nell'installazione e nella messa in servizio, nelle prove di funzionalità, nell'utilizzazione, nella programmazione e nella verifica dei programmi, nella messa a punto, nell'individuazione dei guasti, nella manutenzione e nelle procedure per lavorare in sicurezza.

Sono sorgenti di pericolo anche la movimentazione, le avarie o guasti dei mezzi di protezione, delle sorgenti di energia, dei circuiti di controllo, dei dispositivi e componenti, anche di input e di output, e le azioni del personale non volute ovvero deliberate.

Deve essere sviluppata una strategia per identificare e controllare i pericoli in uno dei due modi seguenti:

- installando le protezioni richieste nel paragrafo seguente (protezione del personale in assenza di valutazione del rischio) in accordo con le regole di implementazione che verranno date più avanti;
- effettuando una esauriente analisi di rischio come prescritto più avanti nel relativo paragrafo, ed installando le protezioni che ne risultano secondo le regole di implementazione di cui al punto precedente.

2.3.7. Protezione del personale. Metodo in assenza di valutazione del rischio

Le protezioni devono impedire l'accesso al pericolo, o provocare la cessazione del pericolo senza che vi sia una specifica e consapevole azione da parte del personale da proteggere.

I dispositivi di protezione devono avere circuiti di controllo del tipo "a controllo affidabile". Devono inoltre essere impiegate barriere di avvertimento e segnali di avvertimento. Deve essere prevenuto l'accesso del personale nello spazio protetto e, quando l'accesso è richiesto, deve essere arrestato, al suo ingresso, qualunque movimento dentro lo spazio protetto usando barriere interbloccate e/o dispositivi di protezione sensibili alla presenza. Il personale che svolge compiti dentro lo spazio protetto deve essere salvaguardato prevenendo che ricomincino movimenti o processi pericolosi con il personale all'interno (come può capitare chiudendo una porta aperta), prevedendo un adeguato spazio di rispetto tra protezioni e spazio ristretto, uniformandosi alle regole da seguire quando il robot è nella fase di insegnamento e limitando il suo movimento ad una velocità massima di 250mm/sec.

2.3.8. Protezione del personale. Metodo di valutazione del rischio

Quando richiesto per le nuove installazioni, deve essere effettuata una valutazione del rischio, che deve tenere conto dello stadio di sviluppo, dell'uso previsto del robot e del sistema robotico, della destrezza e dell'addestramento degli operatori, dell'esposizione a rischi addizionali e dei processi.

Sono disponibili diverse metodologie per la valutazione del rischio. E' accettabile qualunque metodo che prescriva protezioni equivalenti o più restrittive dei requisiti che si riportano di seguito.

Nella fase di valutazione del rischio si assume che le protezioni non siano installate. Nelle fasi successive vengono scelte le protezioni secondo determinati criteri, successivamente si assume che le protezioni siano installate ed infine si valida la loro scelta.

Identificazione dei compiti e dei pericoli.

Tale fase consiste nel descrivere l'applicazione e/o il processo e nel definire i limiti associati con l'uso previsto. Consiste inoltre nell'identificazione di tutti i compiti ragionevolmente prevedibili associati con il robot e il sistema robotico, e con lo stadio di sviluppo. Consiste infine nell'identificazione dei pericoli associati con ciascun compito, ad eccezione dei requisiti speciali associati con la funzione di "insegnamento".
Stima dei rischi.

Per ciascuna combinazione di compiti e di pericoli, si determina il livello di rischio adottando i fattori di Severità, di Esposizione e di Evitabilità, secondo la Tabella 1.

Fattore	Categoria		Criteri
Severità	S2	Danno grave	Normalmente irreversibile; o fatalità; oppure che richiede più di un primo soccorso
	S1	Danno leggero	Normalmente reversibile; o che richiede solo un primo soccorso
Esposizione	E2	Esposizione frequente	Tipica esposizione al pericolo per più di una volta per ora
	E1	Esposizione non frequente	Tipica esposizione al pericolo per meno di una volta al giorno/turno
Evitabilità	A2	Non probabile	Impossibilità di muoversi dal posto; o tempo di reazione inadeguato; o velocità del robot maggiore di 250 mm/sec
	A1	Probabile	Possibilità di muoversi dal posto; o tempo di avvertimento/reazione sufficiente; o velocità del robot minore di 250 mm/sec

Tabella 1 – Categorie di Severità/Esposizione/Evitabilità del pericolo

Nella Tabella 1 “Categorie di Severità, Esposizione, Evitabilità del pericolo”, al fattore Severità si assegnano due categorie di danno, grave e leggero, mentre il fattore Esposizione è correlato alla frequenza, con l’adozione di due categorie concettualmente opposte. Lo stesso discorso vale per il fattore Evitabilità, legato alla probabilità.

SEVERITA' DEL DANNO	ESPOSIZIONE	EVITABILITA'	CATEGORIA DI RIDUZIONE DEL RISCHIO
S2 Danno grave	E2 Esposizione frequente	A2 Non probabile	R1
		A1 Probabile	R2A
	E1 Esposizione non frequente	A2 Non probabile	R2B
		A1 Probabile	R2B
S1 Danno leggero (primo soccorso)	E2 Esposizione frequente	A2 Non probabile	R2C
		A1 Probabile	R3A
	E1 Esposizione non frequente	A2 Non probabile	R3B
		A1 Probabile	R4

Tabella 2 – Matrice delle decisioni per la riduzione del rischio prima della scelta delle protezioni

Determinazione della riduzione dei rischi.

Per determinare la categoria di riduzione del rischio, ci si serve, per ciascuna combinazione di compiti e di pericoli, della Tabella 2 “ Matrice delle decisioni per la riduzione del rischio prima della scelta delle protezioni”. La Tabella 2 disaggrega la Tabella 1 e la ricomponne in diverso ordine e con diversa finalità. Nella prima colonna viene collocata la Severità del danno, articolata nelle prime due righe della tabella precedente. Si parte cioè dai danni, gravi o leggeri, e se ne esamina la frequenza: da due categorie di danno derivano quattro categorie di esposizione classificate secondo frequenza, ognuna delle quali considera l’ evitabilità o meno. Il percorso logico della riduzione del rischio considera dunque come dato di base il danno in sé e per sé, ponendosi poi il problema se è frequente o infrequente e chiedendosi poi se è probabilmente evitabile o meno. Alle otto categorie di evitabilità così ottenute vengono associate sette categorie di riduzione del rischio, dato che la categoria R2B è comune alle due categorie di esposizione E1. Ci si trova così in condizione di scegliere le protezioni.

Selezione delle protezioni.

Con la Tabella 2 si è effettuata una suddivisione analitica delle situazioni di rischio che si possono presentare.. Ne deriva la Tabella 3 “Matrice di selezione delle protezioni”, nella quale alle categorie di riduzione del rischio precedentemente determinate si fanno corrispondere, singolarmente o per gruppi, le prestazioni delle protezioni più avanti esaminate e, singolarmente, le prestazioni dei circuiti.

CATEGORIA	PRESTAZIONI DELLE PROTEZIONI	PRESTAZIONI DEI CIRCUITI
R1	Eliminazione del pericolo o sua sostituzione	Controllo affidabile
R2A	Controlli di ingegneria che prevengono l’accesso al pericolo, o che	Controllo affidabile
R2B	bloccano il pericolo, come protezioni con barriere interbloccate, cortine di	Canale singolo con monitoraggio
R2C	luce, tappeti di sicurezza o altri dispositivi sensibili alla presenza	Canale singolo
R3A	Barriere non interbloccate, spazi di sicurezza, procedure ed	Canale singolo
R3B	equipaggiamenti	Semplici circuiti di sicurezza
R3C	Mezzi di avvertimento	Semplici circuiti di sicurezza

Tabella 3 – Matrice di scelta delle protezioni

Andando dalle categorie di riduzione del rischio più impegnative alle meno rilevanti, le prestazioni dei circuiti di sicurezza sono meno stringenti. Una circuiteria complessa, come quella a controllo affidabile, deve, applicando la Tabella 3, esercitare una forte azione per la riduzione del rischio. Nei circuiti a controllo affidabile il singolo guasto, se non viene scoperto quando si verifica, deve comunque essere rivelato su

richiesta della funzione di sicurezza che monitorizza il sistema. E' interessante osservare che in Tabella 3 le protezioni contro il rischio residuo devono rispondere ai requisiti delle categorie immediatamente inferiori.

Una volta scelte le protezioni, è necessario validarle.

Validazione della selezione delle protezioni.

Dopo la scelta delle protezioni e la loro installazione, bisogna ripetere la procedura di individuazione dei compiti e dei pericoli nonché la stima dei rischi per controllare se per ogni pericolo identificato è stata data protezione e se il rischio residuo è tollerabile. Per ogni combinazione di compito e di pericolo si ripete l'applicazione della Tabella 1. Poi con la Tabella 4 "Matrice di validazione della scelta delle protezioni con le protezioni installate" si rideterminano le categorie di riduzione del rischio. Questa volta la tabella parte dal fattore "Esposizione" e scambia l'ordine delle colonne. Nella sua applicazione si installano le protezioni aggiuntive per controllare il rischio residuo.

ESPOSIZIONE	EVITABILITA'	SEVERITA' DEL DANNO	CATEGORIA DI RIDUZIONE DEL RISCHIO
E2 Esposizione frequente	A2 Non probabile	S2 Danno grave	R1
		S1 Danno leggero	R2C
	A1 Probabile	S2 Danno grave	R2A
		S1 Danno leggero	R3A
E1 Esposizione non frequente	A2 Non probabile	S2 Danno grave	R2B
		S1 Danno leggero	R3A
	A1 Probabile	S2 Danno grave	R3B
		S1 Danno leggero	R4

Tabella 4 – Matrice di validazione della scelta delle protezioni con le protezioni installate

Se a questo punto la categoria di riduzione del rischio è R3 o R4, la riduzione del rischio per quella determinata combinazione di compito e di pericolo può considerarsi completata. Altrimenti si installano ancora protezioni aggiuntive e si ripete la procedura.

2.3.9. Protezione del personale. Realizzazione.

I sistemi di sicurezza debbono essere progettati in modo che in caso di guasto rimangano in uno stato di sicurezza. Le parti "safety related" dei sistemi di controllo, oltre che uniformarsi ai principi generali di sicurezza, debbono poter contrastare le sollecitazioni derivanti dal processo e da altri fattori.

Viene data una formula, che si riporta di seguito, per calcolare la minima distanza dal pericolo nel caso di dispositivi interbloccati che generano il segnale di blocco: si tiene conto del peggior tempo di fermata della macchina e di arresto del sistema di controllo, oltre che del tempo di risposta del dispositivo di protezione compresa la sua interfaccia.

$$D_s = [K \times (T_s + T_c + T_r)] + D_{pf} \quad (1)$$

Dove:

D_s = minima distanza di sicurezza fra dispositivo di protezione e pericolo

K = costante di velocità (minimo 1,6 m/sec)

T_s = peggior tempo di arresto della macchina/equipaggiamento

T_c = peggior tempo di arresto del sistema di controllo

T_r = tempo di risposta del dispositivo di protezione compresa la sua interfaccia

D_{pf} = massimo percorso verso il pericolo dentro il campo coperto dai dispositivi di protezione sensibili alla presenza.

I dispositivi di protezione devono essere integrati nei circuiti di arresto di sicurezza, uniformandosi alle prescrizioni relative al "controllo affidabile". Devono essere previste barriere e dispositivi di segnalazione, per attirare l'attenzione sull'esistenza di pericoli potenziali. Le segnalazioni visive devono essere percepite anche da una sola persona, mentre le segnalazioni acustiche devono produrre un suono ben distinguibile.

Nella ANSI/RIA vengono date regole per la protezione dell' "insegnante", che deve essere adeguatamente addestrato dall'utilizzatore, e reso edotto visivamente sull'installazione e sull'assenza di condizioni di pericolo. Devono essere effettuati test di funzionalità sull'arresto di emergenza e sui controlli di movimento comandati dall'unità portatile.

Vengono elencati i requisiti da rispettare durante una APV (Attended Program Verification) ad alta velocità, riguardanti le prestazioni dei circuiti di sicurezza, che devono essere del tipo a controllo affidabile, la selezione del modo APV ad azione deliberata e l'obbligo per il sistema robotico di non essere in funzionamento automatico. Anche l'operatore, che interagisce con il robot, deve essere protetto.

L'utilizzatore del robot deve farsi carico dell'installazione di tutte le protezioni. Una particolare attenzione deve essere posta quando l'operatore deve introdurre nel robot pezzi da lavorare

ANSI/RIA prosegue con l'esame del modo di funzionamento "Presence Sensing Device Initiation" (PSDI). PSDI è un particolare modo di impiego di un "Presence Sensing Safety Device"(PSSD) – Dispositivo di sicurezza sensibile alla presenza. PSDI è un modo di funzionamento che si ha quando un PSSD funziona ancora come dispositivo di protezione, ma è anche usato in una configurazione di controllo tale che le interruzioni dovute al PSSD sono monitorate in modo che il controllo stesso faccia partire un ciclo quando il campo sensibile è vuoto senza la necessità di premere un bottone per compiere un altro ciclo. PSDI è in sostanza un "blocco+riavvio" e può essere usato solo in produzione.

Il personale che compie operazioni di manutenzione nello spazio protetto con potenza inserita deve avere il controllo totale del robot e del sistema robotico, realizzabile con la rimozione del controllo dal modo di funzionamento automatico e con l'adozione del controllo del sistema da un solo punto. La disattivazione del sistema di abilitazione deve provocare l'arresto di tutti i movimenti pericolosi nello spazio protetto

2.3.10. Requisiti applicativi dei dispositivi di protezione

I dispositivi di protezione devono essere progettati, costruiti e collegati in modo che il personale, non accorgendosi, non possa raggiungere il pericolo. Le barriere di protezione, fisse e interbloccate, devono prevenire l'accesso al pericolo e devono essere costruite in modo da opporsi alle sollecitazioni dovute al funzionamento ed all'ambiente circostante. Ogni parte fissa deve essere rimossa con attrezzi.

Si pone l'attenzione sulle barriere di protezione interbloccate che consistono in una barriera e in un sistema di interblocco che permette l'apertura della barriera. La barriera vera e propria deve soddisfare i requisiti sopra descritti e inoltre deve essere installata ad una distanza di sicurezza ricavata dalla formula di cui alla tabella 6. Non deve aprirsi verso lo spazio protetto, non si deve chiudere da sola, né deve attivare i circuiti di interblocco. I requisiti degli interblocchi, che devono avere due gruppi di contatti, prevedono la codifica magnetica degli interruttori magnetici per ridurre la possibilità di interferenza e la loro progettazione per un funzionamento ad apertura positiva, in modo che l'attuatore dell'interruttore sia sempre collegato e il distacco dei contatti non causi funzionamenti non sicuri. La chiusura della barriera interbloccata non deve riavviare il funzionamento automatico.

2.3.11. Manutenzione e prove di avviamento dei robot e dei sistemi robotici

Per quanto riguarda la manutenzione, l'utilizzatore del robot e del sistema robotico deve organizzare un programma che ne assicuri un continuo funzionamento in sicurezza. Dopo l'installazione del robot e del sistema robotico, devono essere seguite le seguenti procedure e prove per l'avvio .

Nella realizzazione di un sistema robotico, la prevista procedura di avvio iniziale deve includere almeno quanto segue:

- prima di applicare potenza, devono essere verificati il montaggio meccanico e la stabilità, le connessioni elettriche, il collegamento delle utilities, le connessioni relative alle comunicazioni, gli equipaggiamenti periferici ed i dispositivi di limitazione che restringono lo spazio massimo (limitandolo allo spazio ristretto);
- tutto il personale deve uscire dallo spazio ristretto prima di applicare potenza;
- dopo aver applicato potenza, bisogna verificare se i circuiti/dispositivi di arresto di emergenza sono in funzione, se i movimenti degli assi sono ristretti come voluto, se il robot risponde come voluto al sistema di comando, se sono in funzione tutti i dispositivi di protezione e se è funzionale il sistema di controllo a bassa velocità.

2.3.12. Addestramento del personale per la sicurezza

L'utilizzatore deve assicurare che ogni persona che programma, svolge funzioni di "insegnamento", opera o fa manutenzione sui robot o sui sistemi robotici, compresi gli equipaggiamenti associati, sia addestrata sulle procedure di sicurezza riferite ai compiti assegnati. L'addestramento deve essere effettuato in aula e sul posto. Deve comprendere le norme di sicurezza basilari, le raccomandazioni del fornitore e le procedure passo-passo relative alle azioni per la sicurezza. Devono essere illustrate le procedure di blocco/sblocco e le procedure di emergenza.

Anche il personale addetto all' "insegnamento" deve essere addestrato. L'addestramento deve almeno comprendere il controllo a bassa velocità, le protezioni bypassate durante l'insegnamento, il funzionamento dell'unità portatile, il controllo da un singolo punto, la risposta agli eventi anormali e non previsti, i pericoli durante l'insegnamento e gli equipaggiamenti ausiliari. L'addestramento dell'operatore deve comprendere i compiti del robot ed i pericoli collegati, la risposta agli eventi anormali e non previsti e gli equipaggiamenti ausiliari. L'addestramento del personale addetto alla manutenzione deve riguardare la manutenzione

preventiva, la ricerca dei guasti e la riparazione, le prove di funzionamento, i guasti sui dispositivi di sicurezza e le operazioni di emergenza.

3. CONFRONTO TRA L'IMPOSTAZIONE DELLA UNI EN 775 E NORME COLLEGATE CON LA NORMA ANSI/RIA R15.06-1999.

Si può partire da un elemento particolare, che diventa emblematico e che riassume il problema: la nota che compare in ANSI/RIA a commento del paragrafo 4.5 "Prestazioni dei circuiti di sicurezza".

La nota recita: "Questi criteri di prestazione non devono essere confusi con le categorie europee da B a 3 come descritte in ISO/IEC DIS 13849-1, Sicurezza del macchinario-Parti dei sistemi di comando legate alla sicurezza-Parte 1: Principi generali per la progettazione (in correlazione con la EN 954-1.). I criteri sono differenti. La Commissione (*che ha approvato gli Standards della norma-nota dello scrivente*) ritiene che i criteri da 4.5.1 a 4.5.4 vanno oltre i criteri da B a 3 rispettivamente, e ritiene ancora che non sia vero l'inverso."

Per intanto è da osservare che le categorie della EN 954-1 vanno da B a 4, così come avviene nella prEN ISO 13849-1:2002. La discussione sul confronto può svilupparsi da questo elemento, tenendo conto dell'evoluzione della EN 954-1 rappresentata dalla stessa prEN ISO 13849-1:2002 "Safety of machinery-Safety related parts of control systems-Part 1:General principles for design".

Quest'ultima proposta di norma costituisce un sostanziale passo avanti rispetto alla norma precedente, con l'introduzione dell'approccio probabilistico, che supera l'impianto strettamente deterministico della ANSI/RIA. In proposito si fa un passo indietro e si torna a valutare le metodologie di analisi di rischio previste in ANSI/RIA.

La valutazione del rischio viene presa in considerazione come metodo finalizzato alla protezione del personale, da applicarsi quando richiesto per le nuove installazioni. Altrimenti vengono fornite direttamente disposizioni di protezione, anche se corredate di note importanti. Una di esse riguarda la protezione dai pericoli connessi al punto di lavoro, derivanti usualmente dal funzionamento del dispositivo di estremità, come accade per esempio nei processi di saldatura. In definitiva le protezioni, purché adeguate, sembra possano, nei casi considerati, sopperire all'assenza di una valutazione dei rischi connessi con i pericoli individuati. Dal canto suo la metodologia di valutazione del rischio, quando applicata, è apprezzabile, pragmatica, di semplice attuazione e con uno svolgimento logico. Ai fini di un confronto la si riassume, dopo averla già esaminata analiticamente.

Il metodo è senza dubbio efficace, tuttavia il suo limite è nel non poter individuare la concatenazione degli eventi che conducono al danno. L'evento dannoso viene considerato in sé e per sé, viene fronteggiato con adeguate protezioni e sicurezze circuitali, con le quali si cerca anche di prevenirlo, ma non si risale puntualmente alle cause che lo hanno determinato. E' un procedimento di sintesi a priori, preceduto da una analisi organica. In ogni caso la norma ANSI/RIA è un unicum di grande aiuto per risolvere i problemi più generali, dato che spazia sulle problematiche di installazione e di sicurezza dei robot. Tale norma rafforza la sua validità quando viene applicata nel rispetto dei punti pertinenti delle normative di riferimento citate, e soprattutto in accordo con le prescrizioni e le istruzioni del fabbricante, ma anche dell'installatore e/o integratore, che conosce le caratteristiche del sistema nel quale il robot deve svolgere i suoi compiti. E' importante anche il ruolo dell'utilizzatore, che, in quanto committente, è coinvolto nell'analisi di rischio sin dalla progettazione del robot e del sistema robotico.

Del resto anche la norma UNI EN 954-1, che non è specifica per i sistemi robotici ma riguarda più in generale il macchinario, prescrive requisiti di progettazione e di costruzione da rispettare. Tuttavia, nella preoccupazione di non perdere la funzione di sicurezza, vengono introdotti, pur se non organicamente, elementi probabilistici.

Nelle note alle specifiche delle categorie compare (categoria 1), come principio di sicurezza ben collaudato, il ridurre le probabilità di guasto mediante il sovradimensionamento dei componenti, nonché l'affermazione, solo apparentemente ovvia, che la probabilità di guasto in categoria 1 è minore di quella in categoria B.

Anche un elemento negativo per una categoria sottintende ragionamenti probabilistici. Quando si legge in nota che il comportamento dei sistemi di categoria 2 consente che il verificarsi di un guasto porti alla perdita della funzione di sicurezza nell'intervallo di tempo tra le due verifiche, viene spontaneo pensare ai guasti che non si autoevidenziano (vedi sistemi di controllo ad uscita binaria) nell'arco del tempo di missione (intervallo tra i test), la cui probabilità di verificarsi è convenzionalmente data dal tasso di guasto, supposto costante, moltiplicato per la metà dell'intervallo stesso.

Ritornando al confronto istituito nella ANSI/RIA, non è stata considerata, come rilevato, la categoria 4. Non si tratta di un aspetto di poco conto, perché in essa viene previsto che la perdita della funzione di sicurezza non si verifichi anche in presenza di un accumulo di guasti; operativamente questo si ottiene

progettando il sistema in modo che il singolo guasto venga rilevato prima della richiesta delle funzioni di sicurezza. In più, ed in accordo con i requisiti della categoria, se il rilevamento di certi guasti non è possibile, viene presa in considerazione la possibilità di ulteriori guasti; la verifica periodica dei guasti può essere interrotta quando la probabilità che si verifichino ulteriori guasti viene considerata sufficientemente bassa.

Anche prescindendo dalle valutazioni probabilistiche, pur se qualitative, è innegabile che il rispetto dei requisiti della categoria 4 supera le indicazioni del paragrafo della ANSI/RIA che riguarda il “controllo affidabile”.

Non sono però soltanto le citazioni probabilistiche ad evidenziare la funzionalità della UNI EN 954-1.

Come già rilevato, la UNI EN 954-1 è importante per la sua evoluzione in senso probabilistico e metodologico.

In essa elementi come il tempo medio al guasto e il tasso di guasto (supposto costante) di cui è reciproco, le cause comuni di guasto, la periodicità dei controlli da effettuare in determinati intervalli e la copertura diagnostica sono direttamente riconducibili all'efficienza dei componenti e dei sistemi. Inoltre permettono di standardizzare i metodi di analisi di rischio per situazioni omogenee e di stabilire elementi previsionali utili per provvedimenti di prevenzione oltre che di protezione.

Ritornando sul piano deterministico, è infine da considerare che l'evoluzione della UNI EN 954-1, la prEN ISO 13849-1:2002, presenta anche, come già riportato, le architetture basilari di sistema necessarie per soddisfare i requisiti delle categorie.

4. PROPOSTE DI MIGLIORAMENTO E CONCLUSIONI

Dall'esame delle norme e dalle considerazioni svolte emerge, così come fatto rilevare nel corso del lavoro, la necessità di poter disporre di una norma UNI EN 775 del tutto fruibile per i progettisti, gli installatori e/o integratori e gli utilizzatori e che non costringa ad un collegamento con altre norme che, pur applicabili e di grande utilità, non sono specifiche per i robot e i sistemi robotici. Si evidenzia quindi la necessità di includere nella norma i contenuti applicabili delle altre norme di pertinenza.

Si propone di dare particolare rilievo alle modalità di effettuazione dell'analisi di rischio, favorendo, data la complessità e la pericolosità delle installazioni, le metodologie semiquantitative e quantitative, che si basino però su dati affidabilistici raccolti e validati secondo procedure definite, e comunque specifici per il componente e/o il sistema in esame.

In tal modo i provvedimenti adottati per una riduzione dei rischi la più spinta possibile partono da una base che conserva elementi di soggettività solo nel caso di una scelta impropria dei dati di partenza e di una metodologia di elaborazione non congrua con l'installazione in esame. A riguardo, in linea con quanto già osservato, si ritiene utile proporre di adottare l'impostazione della prEN 13849-1:2002, nell'ultimo annesso della quale sono forniti esempi di quantificazione del tempo medio al guasto, della copertura diagnostica e del fattore di causa comune di guasto.

Da ultimo si ritiene utile corredare la UNI EN 775 di illustrazioni, tabelle ed esempi, come di fatto avviene nella norma ANSI/RIA R15.06-1999 (“Graphical aids to understanding the standard” – Annesso A).

Bibliografia

L. Sciavicco, B. Siciliano, *Robotica Industriale: Modellistica e controllo di manipolatori*. McGraw-Hill (2000)

A. Rovetta, *Fondamenti di Robotica: il rapporto uomo-macchina. Aspetti scientifici, tecnologici e tecnici della robotica*. Hoepli (1990)

UNI EN 775 – “Robot industriali di manipolazione – Sicurezza” - 1994

ANSI/RIA R.15.06-1999 – “American National Standard for Industrial Robots and Robot Systems”

UNI EN 1050 – “Sicurezza del macchinario–Principi per la valutazione del rischio” – 1998

UNI EN 954-1 – “Sicurezza del macchinario–Parti dei sistemi di comando legate alla sicurezza–Principi generali per la progettazione” – 1998

EN 292-1:1991 – “Sicurezza del macchinari–Concetti fondamentali, principi generali di progettazione–Terminologia, metodologia di base”

EN 292-2:1991 – “Sicurezza del macchinario – Concetti fondamentali, principi generali di progettazione – Specifiche e principi tecnici”

UNI EN 953 – “Ripari – Requisiti generali per la progettazione e la costruzione di ripari fissi e mobili” – 2000

PrEN ISO 13849-1:2002 – “Safety of machinery–Safety-related parts of control systems–Part 1: General principles for design” (ISO/DIS 13849-1:2002)