

SETTEMBRE 2018

Sicurezza e affidabilità del sistema di comando della macchina

Nella valutazione dei rischi richiesta dalla Direttiva Macchine 2006/42/CE è di primaria importanza l'analisi della sicurezza e affidabilità del sistema di comando della macchina in quanto diverse condizioni di pericolo potrebbero emergere da una errata progettazione del sistema di comando o da un livello di affidabilità del sistema non congruo ai rischi presenti sulla macchina. A riguardo la Direttiva Macchine 2006/42/CE definisce dei criteri di progettazione specifici per i sistemi di comando e li raccoglie all'interno dei correlati requisiti essenziali di sicurezza.

MTM Consulting s.r.l. è in grado di seguire i fabbricanti di macchine nella stesura del fascicolo tecnico e, in particolare, della valutazione dei rischi, fornendo le indicazioni più idonee per la progettazione del sistema di comando della macchina in modo che risulti sicuro e affidabile in funzione dei rischi effettivamente presenti sulla macchina. Questo studio viene effettuato con l'ausilio e le metodologie fornite dalla norma tecnica di riferimento: UNI EN ISO 13849-1: 2016.

Sicurezza e affidabilità dei sistemi di comando

La Direttiva Macchine 2006/42/CE raccoglie, in Allegato I, i requisiti essenziali di sicurezza e di tutela della salute che la macchina deve soddisfare prima di essere immessa sul mercato e/o messa in servizio da parte del fabbricante. La valutazione dei rischi richiesta dalla Direttiva Macchine deve essere funzionale a dimostrare il soddisfacimento di tutti i requisiti di sicurezza applicabili alla macchina. Di fatto, le scelte progettuali effettuate dal fabbricante devono essere il diretto risultato della valutazione dei rischi in modo che gli operatori, che avranno a che fare con la macchina in tutte le fasi di vita previste, risultino esposti solo a quei rischi residui emersi dalla valutazione stessa.

La valutazione dei rischi deve coprire anche le scelte progettuali legate all'equipaggiamento (elettrico, pneumatico e/o idraulico) del sistema di comando della macchina, in particolare per quanto attiene a quelle parti del sistema di comando legate alla sicurezza.

In particolare, il requisito 1.2.1 dell'Allegato I – “Sicurezza ed affidabilità dei sistemi di comando”-, definisce i requisiti che deve rispettare il sistema di comando della macchina in modo da evitare che si verifichino situazioni pericolose correlate ad una errata progettazione o ad un potenziale guasto dello stesso sistema. Per esempio, alcune valutazioni che è necessario effettuare:

- I sistemi di comando non devono subire influssi esterni legati all'ambiente di lavoro in cui opera la macchina: se la macchina è pensata per ambiente outdoor, i sistemi di comando devono essere progettati conformemente a questo ambiente.
- I sistemi di comando devono resistere alle sollecitazioni prevedibili: per esempio, l'intervento continuativo su un dispositivo di comando (un pulsante, per esempio) non deve portare lo stesso rapidamente a rottura, con potenziali ulteriori pericoli per l'operatore.
- Qualora il sistema di gestione e controllo della macchina presenti una condizione di avaria o guasto, non si devono mai presentare situazioni di pericolo per l'operatore: la logica di

Ragione Sociale **Via** **CAP - Città (Prov.)** **Tel.** **Fax** **eMail** **Sito** **Cap. Sociale** **C.F.-P.IVA-C.C.I.A.A.**

mtm consulting s.r.l. L. Ariosto, 10 - 20900 - Monza (MB) +39 039 2848437 +39 039 8940328 info@emtem.com www.emtem.com 12.000,00 € i.v. 02994950968
società unipersonale +39 039 2849703

funzionamento della macchina deve restare separata dalla logica di sicurezza, garantendo sempre che quest'ultima sia in grado di monitorare il corretto funzionamento della prima. Di fatto, la macchina non deve avere avviamenti inattesi, mancati arresti quando richiesti (in particolare se di emergenza), modifiche ai parametri di processo che comportino situazioni di pericolo inaspettate, comportamenti imprevedibili, ecc.

- Gli errori umani prevedibili, legati all'interazione uomo-macchina, non devono portare alla creazione di situazioni pericolose: per esempio, la gestione dell'operatore su di un software di gestione non deve comportare condizioni pericolose per l'operatore se non con intervento volontario da parte dell'operatore stesso in modo che sia effettivamente cosciente di quello che sta per abilitare.

I requisiti esposti al punto 1.2.1 dell'Allegato I si applicano a tutte le parti del sistema di comando che, in caso di un'avaria o di un guasto, possono comportare pericoli dovuti a un comportamento non richiesto o impreveduto della macchina. Le parti del sistema di comando più coinvolte sono le parti del sistema di comando legate alle funzioni di sicurezza (avvio, arresto, arresto di emergenza, ecc.). Un guasto a questi elementi di sicurezza comporterebbe un mancato intervento della corrispondente funzione di sicurezza e, di conseguenza, una potenziale situazione pericolosa per l'operatore.

La norma UNI EN ISO 13849-1: 2016

Tutti i componenti del sistema di comando sono soggetti a guasti e/o rotture, pertanto è impensabile immaginare di progettare un sistema di comando che non vada mai a guasto. È ragionevole tuttavia selezionare le parti del sistema di comando legate alla sicurezza in modo da realizzare un sistema di comando che sia sufficientemente sicuro e affidabile rispetto al risultato emerso dalla valutazione dei rischi. Le scelte progettuali (sia come componentistica adottata che come architettura) delle parti del sistema di comando legate alla sicurezza devono essere tali da garantire un livello di affidabilità (Performance Level) adeguato al risultato della valutazione dei rischi e quindi al livello di rischio effettivamente presente sulla macchina.

La norma UNI EN ISO 13849-1: 2016 presenta l'approccio probabilistico ora enunciato.

I contenuti della norma possono essere racchiusi in questi quattro passaggi sequenziali:

- Esclusione o riduzione della probabilità di guasti o avarie adottando componenti affidabili e principi di sicurezza comprovati.
- Utilizzo di componenti standardizzati con verifica delle funzioni di sicurezza da parte del sistema di comando ad intervalli regolari.
- Ridondanza degli elementi del sistema di comando in modo da non perdere la funzione di sicurezza in caso di guasto o avaria.
- Controllo automatico per il rilevamento continuo di guasti e avarie.

Questi concetti sono normalmente applicati in combinazione tra loro.

La valutazione dei rischi effettuata secondo la metodologia prevista dalla norma consente quindi di identificare un livello di affidabilità del sistema di comando che sia adeguato ai rischi presenti



sulla macchina e di scegliere la componentistica corretta per realizzare un sistema di comando con il livello di affidabilità richiesto.