Sicurezza / di Massimo Granchi, Christian Trinastich

DIRETTIVA MACCHINE 2006/42/CE: SICUREZZA E AFFIDABILITÀ DEL sistema di

Il presente articolo vuole evidenziare quanto richiede la Direttiva Macchine 2006/42/CE sul tema della sicurezza ed affidabilità, e che cosa il Fabbricante è tenuto a realizzare e inserire all'interno della valutazione dei rischi facente parte del fascicolo tecnico della macchina

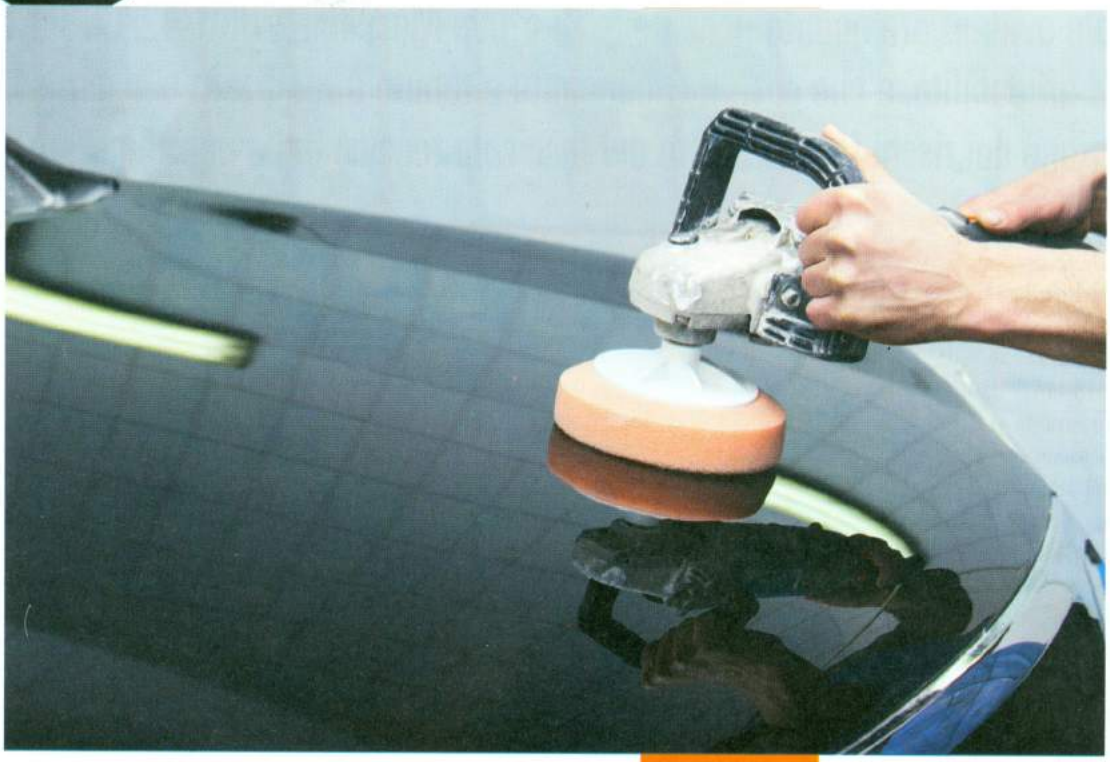
All'interno dell'Allegato I della **Direttiva Macchine 2006/42/CE** sono raccolti i requisiti essenziali di sicurezza e di tutela della salute a cui la macchina deve essere dichiarata conforme da parte del Fabbricante prima di essere immessa sul mercato e/o messa in servizio. Nello specifico, il Fabbricante è tenuto a dimostrare il soddisfacimento dei requisiti di sicurezza tramite la valutazione dei rischi, facente parte del fascicolo tecnico, e progettare e realizzare conseguentemente la macchina in funzione dei risultati ottenuti dalla valutazione dei rischi. La valutazione dei rischi è un procedimento iterativo in cui il primo passaggio è quello di evidenziare tutti i possibili pericoli e le correlate situazioni pericolose, legati all'uso della macchina in tutte le sue fasi di vita. Il passaggio successivo è la stima del rischio correlato alla situazione pericolosa, valutando quindi se quel rischio è sufficientemente basso oppure può essere ridotto adottando la metodologia di riduzione del rischio indicata dalla norma UNI EN ISO 12100: 2010. Questo processo iterativo deve essere sviluppato durante la progettazione della macchina: le scelte progettuali devono essere il diretto risultato della valutazione dei rischi in modo tale che gli operatori che avranno a che fare con la macchina siano esposti solo a quel rischio residuo emerso dalla valutazione stessa. In accordo a quanto riportato nel punto precedente, anche le scelte progettuali legate all'equipaggiamento del sistema di comando della macchina - in particolare per quanto attiene a quelle parti del sistema di comando legate alla sicurezza - devono essere il diretto risultato della valutazione dei rischi.

Sicurezza e affidabilità dei sistemi di comando

Nello specifico, 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 l'insorgere di situazioni pericolose. Infatti, la sicurezza della macchina non deriva esclusivamente dal corretto utilizzo e posizionamento di ripari (fissi e/o mobili interbloccati) e di dispositivi di protezione (per esempio, barriere di sicurezza, doppi comandi a mano, ecc.), ma anche dalla idonea progettazione del sistema di comando legato alle funzioni di sicurezza della macchina (avvio, arresto, arresto di emergenza, ecc.). Pertanto, una progettazione dei sistemi di comando della macchina che non risulti conforme a quanto richiede la direttiva nel requisito 1.2.1, potrebbe comportare il verificarsi di una serie di situazioni pericolose "indirette", dovute proprio ad un guasto e/o cattivo funzionamento di tali sistemi: per esempio, un avvio inaspettato, un mancato arresto quando richiesto, un cambiamento delle condizioni operative, un mancato funzionamento dei dispositivi di protezione, ecc. Per esempio, alcune valutazioni fondamentali che è necessario effettuare sono le seguenti:

- i sistemi di comando non devono subire influssi esterni legati all'ambiente di lavoro in cui opera la macchina: per esempio, se la macchina è pensata per ambiente outdoor, i sistemi di comando devono essere progettati conformemente a questo ambiente. Analoga considerazione è da farsi nel caso di macchine destinate a lavorare in ambiente dove è preventivabile siano presenti radiazioni elettromagnetiche esterne;
- i sistemi di comando devono resistere alle sollecitazioni di servizio: per esempio, l'intervento continuativo su un particolare dispositivo di comando non deve portare lo stesso rapidamente a rottura, con possibili ulteriori pericoli per l'operatore;
- avarie nell'hardware o nel software non devono comportare situazioni pericolose per l'operatore: in definitiva vi è la necessità di tenere separate la logica di funzionamento della macchina dalla logica di sicurezza, garantendo sempre che quest'ultima sia in

comando



grado di monitorare la prima. Di fatto, la macchina non dovrebbe mai avere avviamenti inattesi, mancati arresti quando richiesti (in particolare se di emergenza), modifiche ai parametri di processo che comportino situazioni di pericolo inaspettate, comportamenti imprevisti, 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 causare situazioni pericolose per l'operatore se non volutamente richieste dell'operatore stesso in modo che sia effettivamente cosciente di quanto sta chiedendo al sistema di comando.

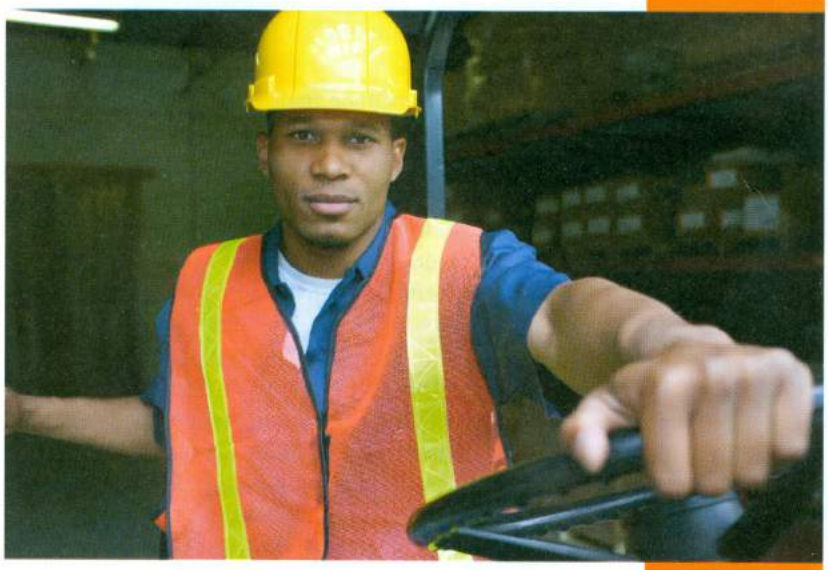
I requisiti esposti al punto 1.2.1 dell'Allegato I della Direttiva Macchine 2006/42/CE si applicano a tutte le parti del sistema di comando che, in caso di un'avaria o di un guasto, possono comportare pericoli all'operatore dovuti a un comportamento involontario o imprevisto della macchina. A riguardo, i sistemi di comando da analizzare possono utilizzare varie tecnologie o combinazioni di tecnologie quali - ad esempio - meccanica, idraulica, pneumatica, elettrica o elettronica. Le parti del sistema di comando più interessate sono, senza ombra di dubbio, le parti del sistema di comando legate alle funzioni di sicurezza quali, ad esempio, gli elementi del sistema di comando legati ai dispositivi di interblocco e/o di bloccaggio dei ripari mobili, ai dispositivi di protezione o ai dispositivi necessari ad ottenere un arresto d'emergenza. Un guasto a questi elementi del sistema di comando comporterebbe un mancato intervento della corrispondente funzione di sicurezza e, di conseguenza, una potenziale situazione pericolosa per l'operatore: il pulsante di emergenza, per esempio, è strettamente correlato alla necessità di poter arrestare in emergenza una macchina; un mancato arresto della macchina, dopo aver premuto il pulsante di emergenza, esporrebbe l'operatore a potenziali pericoli conseguenti non solo al mancato arresto degli elementi mobili pericolosi ma anche al fatto che questo mancato arresto sia del tutto inaspettato per l'operatore esponendolo, di fatto, a situazioni pericolose in origine non previste.

La norma UNI EN ISO 13849-1: 2016

Lo scopo della norma UNI EN ISO 13849-1: 2016 è quello di fornire le indicazioni per progettare le parti del sistema di comando legate alla sicurezza tali da garantire la sicurezza dell'operatore rispetto alle reali condizioni di rischio esistenti sulla macchina. Di fatto, la norma adotta un approccio probabilistico piuttosto che deterministico. Del resto, 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 o mai a rottura. E' però ragionevole pensare di poter scegliere i componenti del sistema di comando legati alla sicurezza in modo tale da realizzare un sistema che sia sufficientemente sicuro e affidabile rispetto alle condizioni di rischio da cui è necessario proteggere l'operatore, come evidenziate dalla valutazione dei rischi. In questo senso, le scelte progettuali 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 alle condizioni di pericolo realmente esistenti sulla macchina. In definitiva il fabbricante è tenuto a calcolare il Performance Level richiesto dalla condizione operativa esistente sulla macchina effettuando una specifica valutazione dei rischi in accordo allo schema fornito dalla stessa norma. Successivamente, deve scegliere sul mercato i componenti necessari ad ottenere quella architettura (per esempio, canale singolo oppure a doppio canale) necessaria per soddisfare il livello di affidabilità richiesto. Adottando la metodologia della norma è possibile realizzare quanto richiesto dalla valutazione dei rischi facendo scelte opportune per quanto riguarda i componenti adottati per progettare il sistema di comando oppure costruendo un'architettura differente (per esempio, passando dal canale singolo alla ridondanza). In definitiva, ad ogni classe di rischio ottenuta dalla valutazione dei rischi è possibile realizzare più di una soluzione che sia conforme in termini di affidabilità, eventualmente modificando i componenti scelti oppure cambiando l'architettura adottata. La norma, in questa nuova edizione, non introduce novità sostanziali rispetto alle edizioni precedenti: tuttavia, fornisce ulteriori importanti dettagli per quanto riguarda i parametri dei componenti da scegliere sul mercato - parametri che sono necessari per verificare se il livello di prestazioni del sistema di comando progettato è pari a quanto richiesto dalla valutazione dei rischi. Normalmente questi parametri sono forniti dagli stessi fornitori, in caso alternativo è necessario rifarsi alle tabelle di riferimento fornite dalla norma; in questa ultima edizione queste tabelle sono state ampliate e maggiormente dettagliate. In linea di principio, i concetti da considerare durante le scelte progettuali delle parti del sistema di comando legate alla sicurezza comprendono:

- 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 possono essere applicati anche in combinazione tra loro. Ad esempio, nella logica della ridondanza, la scelta di adottare tecnologie diverse (per esempio, elettrica e pneumatica) può essere utilizzata per evitare le avarie dovute a cause di guasto comuni. In ogni caso la scelta progettuale deve essere il risultato della valutazione dei rischi necessaria ad individuare il livello di affidabilità richiesto da parte del sistema di comando legato alla sicurezza, in funzione dell'attività pericolosa compiuta dall'operatore.

Conclusioni

Le scelte progettuali legate al sistema di comando della macchina, come evidenziato, sono parte del processo di valutazione dei rischi il cui fine è quello di dimostrare come la macchina soddisfi i requisiti essenziali di sicurezza della Direttiva Macchine 2006/42/CE. In particolare, il requisito essenziale di sicurezza 1.2.1 in Allegato I evidenzia i requisiti che deve avere il sistema di comando della macchina con particolare attenzione alle parti del sistema di comando correlate con le funzioni di sicurezza. Le indicazioni della norma UNI EN ISO 13849-1: 2016 garantiscono la presunzione di conformità alle richieste del requisito 1.2.1 della Direttiva Macchine. La norma, infatti, fornisce le indicazioni per effettuare una specifica valutazione dei rischi sulle parti del sistema di comando legate alla sicurezza con lo scopo di realizzare un sistema di comando che garantisca un'affidabilità (in merito a possibili rotture e guasti) adeguata alla reale situazione di rischio presente sulla macchina. ■