PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 17 - numero 3587 di mercoledì 15 luglio 2015

Macchine: il livello di integrità della sicurezza funzionale

Un documento si sofferma sul livello di integrità della sicurezza funzionale applicata all'industria e ai processi. L'analisi dei rischi, la sicurezza funzionale, le norme tecniche, la 'performance level' e i livelli di integrità funzionale.

Roma, 15 Lug ? Nell'ambito della **sicurezza di macchine e impianti** è necessario che l'identificazione dei pericoli e l'analisi dei rischi possano mettere in grado gli operatori preposti di identificare e partecipare alla risoluzione di alcune problematiche come "i pericoli e gli eventi pericolosi collegati alla EUC", dove per EUC si intende una parte di attrezzature, macchinari, parte di un impianto o anche l'intera installazione".
In particolare l'identificazione dei pericoli e l'analisi dei rischi "devono prendere in considerazione tutte le circostanze prevedibili ragionevoli comprese le eventuali condizioni di guasto, l'abuso e le condizioni di utilizzo ambientali estreme. L'identificazione dei pericoli e l'analisi dei rischi devono anche includere e considerare possibili errori umani e modalità anomale o rare di funzionamento dello EUC". E la **sicurezza funzionale** (e il suo corrispondente livello di integrità) è "quella frazione delle parti e dei sistemi correlati alla sicurezza della macchina da cui dipende il corretto e sicuro funzionamento in relazione a determinati stimoli generati dalle variabili controllate identificate".

A parlare in questi termini di sicurezza funzionale delle macchine è un intervento che si è tenuto al convegno SAFAP 2014 (Roma, ottobre 2014), un evento che rappresenta per gli addetti ai lavori un punto di riferimento nazionale di confronto tecnico-scientifico nel settore delle attrezzature a pressione.

Uno degli interventi, tratto dagli atti pubblicati dall'Inail, riporta indicazioni sia sulle metodologie di identificazione dei pericoli e analisi dei rischi, che sulla sicurezza funzionale con riferimento anche alle norme europee e ai concetti di funzione di sicurezza, di Performance Level (PL) e Safety Integrity Level (SIL).

Infatti nell'intervento "**SIL, PL, EPL, categorie ovvero il livello di integrità della sicurezza funzionale applicata all'industria e al processo**", a cura di P. Corbo (SILEx Engineering S.r.l.) e F.Olivieri (RINA Services S.p.A.), si presentano innanzitutto sia l'**Hazard Identification** (HAZID) che la **Hazard Analysis & Operability** (HAZOP) a cui PuntoSicuro dedicherà un futuro approfondimento.

Brevemente ricordiamo che l'identificazione del pericolo (HAZID) "deve essere eseguita per il sistema EUC e il suo sistema di controllo associato" e l'obiettivo della fase HAZID è quello di identificare il potenziale pericolo intrinseco nella EUC, senza l'implementazione delle funzioni legate alla sicurezza. Il risultato ottenuto dalla HAZID deve essere sufficientemente dettagliato in modo da consentire l'identificazione di potenziali deviazioni dai requisiti relativi al minimo SIL richiesto".
Mentre la Hazard Analysis & Operability (HAZOP) è una "tecnica strutturata e sistematica per l'analisi di sistema e la gestione dei rischi. In particolare, HAZOP viene spesso utilizzata come tecnica per identificare potenziali pericoli in un sistema e identificare i problemi di operabilità che possono portare a condizioni di funzionamento non conformi e pericolose".

Veniamo invece alla **sicurezza funzionale**.

Per chiarire il difficile concetto di sicurezza funzionale gli autori descrivono un caso specifico:
- gli operatori "che agiscono in prossimità di un pericolo generato in una macchina possono essere schermati da questo attraverso un dispositivo di protezione fisso (un pannello di chiusura fisso, una griglia fissa, barriere fisse antintrusione, ecc.):

questa soluzione è una misura di protezione che risolve la presenza di un pericolo, tuttavia questa categoria non rientra in un sistema di protezione attuato mediante il concetto di sicurezza funzionale". Infatti in questo caso, "nella misura in cui non vi sia necessità di rimuovere il dispositivo di protezione fisso durante il regime operativo della macchina, non è necessario monitorarne lo stato di chiusura";
- in altri casi può essere invece necessario "prevederne l'apertura per ragioni operative o manutentive anche con sorgente energetica non sezionata oppure con macchina in regime di 'pronto ad operare'. L'apertura deve essere monitorata affinché questa possa condurre ad uno stato sicuro. In questo caso l'interdizione dell'energia passa attraverso un sistema attivo che risponde ad uno stimolo proveniente da una variabile controllata: poiché l'apertura della protezione potrebbe portare ad un contatto con l'operatore, la macchina viene fermata oppure l'azionamento della macchina interdetto da un sistema attivo. Il sistema di controllo e attuazione così concepito deve essere sviluppato con concetti di sicurezza funzionale".

E dunque, con riferimento a quanto riportato nell'esempio, le funzioni "*Disattiva lo stato di azionamento della macchina quando una protezione mobile viene aperta*" o "*Interdici la possibilità di azionare la macchina quando una protezione mobile è aperta*" si possono definire "**Funzione di sicurezza**". E dunque la "Funzione di sicurezza" è la "sequenza degli eventi congiungenti la causa e l'effetto, sequenza che coinvolge tutte e sole le parti del sistema di controllo, inclusi il sensore o iniziatore che genera la causa e l'attuatore che genera l'effetto, ovvero tutti i dispositivi attivi coinvolti nell'attuazione dell'evento stabilito (effetto) a fronte dell'evento rilevato (causa)".
Inoltre la funzione di sicurezza deve essere "caratterizzata anche da una cifra di merito denominata '*Integrità della funzione di sicurezza*' ovvero da un'informazione che ne contraddistingua i livelli di affidabilità sistematici e casuali". E le apparecchiature destinate a realizzare l'implementazione di una o più funzioni di sicurezza sono incluse nel cosiddetto SRP/CS ovvero "Safety Related Part of a Control System" oppure nel cosiddetto SRECS "Safety-related electrical, electronic and programmable elecronic control systems for machinery".

Gli autori presentano poi le **principali norme tecniche** più significative in ambito macchine e convergenti sul tema della sicurezza funzionale:
- **EN ISO 13849-1:2008**, "la norma che, sviluppata in sede ISO, descrive gli SRP/CS attraverso le Categorie e PL ? Performance Level";
- **EN ISO 13849-2:2008**;
- **EN 62061:2005**, "la norma che, sviluppata in sede IEC, duale della EN13849-1, descrive i sistemi SRECS in termini di SIL (Safety Integrity Level);
- **EN 61508-1,2,3,4,5,6,7:2010** Functional safety of electrical/electronic/programmable electronic safety-related systems. "Queste norme coprono gli aspetti da considerare quando sistemi elettrici/elettronici o elettronici programmabili (E/E/PE) sono utilizzati per realizzare funzioni di sicurezza";
- **EN 61511-1,2,3:2004**, "queste norme forniscono i requisiti per specificare, progettare, installare, utilizzare e manutenere sistemi SIF (Safety Instrumented Systems) in modo tale che questi possano essere affidabilmente utilizzati per mantenere un processo in uno stato sicuro"; - **EN 50495:2010**.

Rimandando ad una lettura completa del documento agli atti, concludiamo riportando brevemente alcune indicazioni relative alle definizioni e ai concetti correlati alle norme presentate:
- **Performance Level** (PL): sono descritti nelle norme EN138491-1,2 e "sono classificati in 5 livelli consecutivi da "PLa", ovvero quello a minore integrità, a "PLe" ovvero quello a massima integrità. I livelli di integrità (PLa, PLb, PLc, PLd, PLe) vanno letti come fattori di riduzione del rischio e sono associati ad una probabilità oraria che la funzione di sicurezza perda di efficacia o venga meno alla sua azione. Tale probabilità non deve essere intesa come probabilità di accadimento pericoloso ma solo, come detto, come probabilità di perdita della funzione di sicurezza";
- **Safety Integrity Level** (SIL): "i livelli di integrità funzionale, in sintesi i fattori di riduzione di rischio associati all'inserzione di un sistema strumentato di sicurezza, sono 4 e fissati in particolare in SIL1, SIL2 e SIL3, SIL4 ordinatamente dal meno al più efficace in termini di integrità". L'intervento si sofferma poi sui vari parametri e grandezze correlate ai SIL. Si ricorda che le norme IEC 61508 e IEC 61511 utilizzano il concetto di livello di integrità della sicurezza;
- **Sistemi di sicurezza strumentati** (SIS): tale sistema strumentato di sicurezza "realizzato mediante loop aventi un definito livello di integrità funzionale, è fondamentale nel generare un ulteriore layer di protezione nei sistemi correlati al settore del processo industriale. Un SIS è composto in genere da una o svariate funzioni di sicurezza che contano sensori, logic solver e attuatori";
- **Funzione di sicurezza** (SIF): è dunque "una sequenza di azioni automatiche attuate a fronte di un definito evento scatenante o iniziatore, eseguite in un tempo accertato e con un livello di integrità della sicurezza specificato";
- **Equipment Protection Level** (EPL): "ovvero la sicurezza funzionale applicata al pericolo di esplosione". E allo scopo di regolamentare costruzioni destinate a luoghi caratterizzati dal pericolo di esplosione è stata sviluppata la norma EN50495:2010.

Infine l'intervento risponde ad una domanda: **il SIL è obbligatorio o volontario?**
La riposta è che "il set di norme IEC 61508 non costituisce set armonizzato a Direttive Europee. L'applicazione della IEC 61508 non è cogente ma è richiamata in varie norme e norme europee armonizzate a Direttive di Prodotto. L'uso del set IEC 61508 è raccomandato".

" SIL, PL, EPL, categorie ovvero il livello di integrità della sicurezza funzionale applicata all'industria e al processo", a cura di P. Corbo (SILEx Engineering S.r.l.) e F.Olivieri (RINA Services S.p.A.), intervento al convegno SAFAP 2014 (formato PDF, 28.36 MB).

RTM

---

www.puntosicuro.it