SIL, PL, EPL, categorie ovvero il livello di integrità della sicurezza funzionale applicata all'industria e al processo

P. Corbo*, F.Olivieri**

*SILEx Engineering S.r.l,
**RINA Services S.p.A.

Sommario

L'identificazione dei pericoli e l'analisi dei rischi devono mettere in grado tutti coloro che vi sono preposti, secondo la norma EN 61508, di identificare e partecipare alla risoluzione dei seguenti problemi:

- i pericoli e gli eventi pericolosi collegati alla EUC ovvero apparecchiatura controllata; per EUC si intende una parte di attrezzature, macchinari, parte di un impianto o anche l'intera installazione; l'EUC è considerata come fonte di pericoli e quindi è protetta da Sistemi di Sicurezza (SIS), altri sistemi di sicurezza tecnologici, misure di riduzione del rischio esterno, o una combinazione di questi sistemi) e alle apparecchiature di controllo ad essa associati;
- la sequenza di eventi che porta ai pericoli e alla manifestazione degli stessi;
- i rischi relativa alla EUC associati ai pericoli identificati;
- i requisiti per la riduzione del rischio.

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.
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 con identificazione del rischio sopra descritto.

1. Hazard Identification (HAZID)

L'identificazione del pericolo (HAZID) deve essere eseguita per il sistema EUC e il suo sistema di controllo associato. 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.
Le operazioni di HAZID devono essere effettuate con tutte le opportune considerazioni e approfondimenti riguardanti temi e casi di funzionamento e operatività come: le proprietà e lo stato fisico delle parti operate dalla macchina o dal processo; le procedure operative e di manutenzione; le varie e diverse operazioni e modalità operative concernenti l' EUC come avvio, arresto, marcia, manutenzione ordinaria, straordinaria; tutti i rischi derivanti dall'intervento umano; la novità e la complessità dell'impianto in esame; la presenza o la necessità di presenza di funzioni di protezione speciali funzionali ai pericoli individuati.
Al fine di ridurre la possibilità di omettere l'identificazione di eventuali pericoli durante l'esame della EUC, l'identificazione del pericolo deve essere eseguita da un team multidisciplinare che copra tutte le pertinenti discipline ingegneristiche, nonché sia dotato di adeguata autonomia operativa ed esperienza nei settori di installazione, funzionamento di macchina, manutenzione, dismissione.

Per una discussione dettagliata di questo argomento e per un approfondimento del quadro esposto può essere interessante consultare la norma ISO 17776 "Orientamenti in materia di strumenti e tecniche per l'identificazione e valutazione degli eventi pericolosi" che include i seguenti argomenti in ambito petrolchimico: rischi e concetti di valutazione dei rischi, metodi per l'identificazione dei pericoli e la valutazione dei rischi , scelta dei metodi, ruolo dell' esperienza e del livello decisionale, liste di controllo, codici e norme, selezione delle tecniche di analisi strutturate, gestione del rischio (Identificazione, Assessment, Riduzione del rischio), linee guida per l'utilizzo in attività specifiche, identificazione del pericolo e concetti di valutazione dei rischi, tecniche di revisione strutturate.
In altro ambito (macchine) può essere invece di interesse la consultazione della norma ISO 12100 “Sicurezza del macchinario - Principi generali di progettazione - Valutazione del rischio e riduzione del rischio” che include argomenti in ambito sicurezza macchine.
La norma specifica peraltro la terminologia di base, i principi e una metodologia per il raggiungimento della sicurezza nella progettazione del macchinario.
Essa specifica i principi per la valutazione del rischio e la riduzione del rischio per aiutare i progettisti nel raggiungere questo obiettivo che si basano sulla conoscenza e l’esperienza della progettazione, dell’utilizzo, degli incidenti, degli infortuni e dei rischi associati al macchinario. Sono indicate procedure per identificare i pericoli e stimare e valutare i rischi durante le fasi pertinenti del ciclo di vita della macchina e per eliminare i pericoli o arrivare a ridurre sufficientemente i rischi. Sono fornite linee di orientamento sulla documentazione e la verifica del processo di valutazione del rischio e di riduzione del rischio.

2. Hazard Analysis & Operability (HAZOP)

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.
HAZOP è basato su una teoria che presuppone che gli eventi di rischio sono causati da deviazioni dalla progettazione o dalle normali condizioni operative.
L'identificazione di tali deviazioni è facilitata utilizzando insiemi di "parole guida" che identificano un elenco sistematico di probabili deviazioni. Questo approccio è una caratteristica peculiare della metodologia HAZOP.
HAZOP è uno strumento di valutazione qualitativa del rischio di tipo induttivo e costituisce un approccio di tipo " bottom-up " di identificazione dei rischi.
Anche in questo caso, al fine di ridurre la possibilità di omettere l’identificazione di eventuali pericoli durante l'esame della EUC, l'identificazione delle deviazioni deve essere eseguita da un team multidisciplinare che copra tutte le pertinenti discipline ingegneristiche, nonché sia dotato di adeguata autonomia operativa ed esperienza nei settori di installazione, funzionamento di macchina, manutenzione, dismissione.
L’analisi HAZOP è facilitata utilizzando il modello descritto nella norma IEC 61882 “Hazard e Operability (HAZOP Study) - guida all'applicazione”. Lo scopo di tale norma è quello di descrivere i principi e le procedure di Hazard e Operability (HAZOP) Studies. HAZOP è ivi descritto come una tecnica strutturata e sistematica per l'esame di un sistema definito, con l'obiettivo di identificare potenziali rischi nel sistema. I pericoli in esame possono includere sia quelli rilevanti solo per l'area adiacente al sistema sia quelli con una più ampia sfera di influenza, ad esempio alcuni rischi ambientali. La norma delinea le procedure di esecuzione HAZOP individuando i potenziali problemi di interoperabilità con il sistema e, in particolare, individuando le cause dei malfunzionamenti operativi e le deviazioni di produzione che possono portare a prodotti non conformi.

3. La sicurezza funzionale

La sicurezza funzionale 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.
Per meglio chiarire il concetto di sicurezza funzionale descriviamo il seguente caso.
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 antiintrusione, 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.
In effetti, 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 taluni casi è 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.
Considerando l'esempio precedente, 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*" assumono il ruolo di "*Funzione di sicurezza*". Funzione di sicurezza è dunque 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).
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. La funzione di sicurezza, infatti, deve essere attuata da una struttura di controllo non standard ovvero affidabile con affidabilità accertata. Una funzione di sicurezza non attendibile o di cui non sia tenuta sotto controllo l'attendibilità non può svolgere funzione di sicurezza quando il livello di riduzione di rischio atteso è sostanziale e apprezzabile. Sistemi di controllo non caratterizzati da funzione di sicurezza e integrità della funzione di sicurezza vanno sotto il nome di **BPCS** ovvero *Basic Process Control Systems* (vedi EN61511, abbreviazioni e definizioni).
Di converso, 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" (vedi EN13849-1, Termini e definizioni)* oppure nel cosiddetto ***SRECS*** "Safety-related electrical, electronic and programmable elecronic control systems for machinery" (vedi EN62061, Termini e definizioni).

4. Norme Europee e Internazionali applicabili

Alcune delle norme più significative in ambito macchine, peraltro armonizzate alla Direttiva Macchine 2006/42/CE (solo le prime tre) e alla Direttiva ATEX 94/9/CE (l'ultima) e convergenti sul tema della sicurezza funzionale, sono le seguenti:

EN ISO 13849-1:2008 Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione (ISO 13849-1:2006).
È la norma che, sviluppata in sede ISO, descrive gli SRP/CS attraverso le *Categorie* e *PL – Performance Level.* Questa norma si applica a qualunque sistema sia esso di natura elettrico, meccanico, elettromeccanico, specifica i requisiti di sicurezza e fornisce linee guida sui principi di progettazione delle parti dei sistemi di comando legate alla sicurezza. Per queste parti specifica le categorie e descrive le caratteristiche delle funzioni di sicurezza. Sostituisce definitivamente, a partire dal 1 gennaio 2012, la norma superata EN954-1:1996.

EN ISO 13849-2:2008 Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 2: Validazione (ISO 13849-2:2003).
Questa norma va usata in modo congiunto alla precedente e specifica il processo di validazione, comprendente sia l'analisi che le prove, per le funzioni di sicurezza e le categorie per le parti del sistema di comando legate alla sicurezza.

EN 62061:2005 Sicurezza del macchinario - Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza (IEC 62061:2005).
È la norma che, sviluppata in sede IEC, duale della EN13849-1, descrive i sistemi SRECS in termini di SIL (Safety Integrity Level) come la EN61508, ma solo fino ad un livello di integrità funzionale SIL3 e ciononostante è applicabile alle macchine e determina risultati equivalenti. In linea di principio può essere applicata solo a sistemi elettrici.

Norme progenitrici degli argomenti trattati nei documenti sopra riportati sono le norme:

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. Lo scopo di queste norme include i principi alla base dello sviluppo dei prodotti e delle apparecchiature e della loro applicazione. Non sono norme armonizzate ad alcuna Direttiva Europea, contrariamente alle norme precedenti.

EN61511-1,2,3:2004 Functional safety - Safety instrumented systems for the process industry sector.
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. Queste norme rappresentano dunque l'applicazione delle norme EN61508 al settore dell'automazione e della sicurezza funzionale del processo.

EN50495:2010 Dispositivi di sicurezza richiesti per il funzionamento sicuro degli apparecchi in relazione al rischio di esplosione.

5. Performance Level (PL)

I performance level sono, come detto, descritti nelle norme EN138491-1,2: 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.
In ogni caso la stessa norma EN13849-1 riporta all'allegato A un grafico di rischio sintetico che associa un livello di rischio dedotto in modo qualitativo ad un predefinito livello di integrità, adeguato per ottenere la riduzione di rischio in generale accettabile per il livello di rischio totalizzato.
I parametri che conducono alla determinazione del livello di integrità sono i seguenti:

- MTTFd Mean Time to Dangerous Failure ovvero il tempo medio all'evento pericoloso
- DC Diagnostic Coverage ovvero la capacità di auto diagnostica del sistema strumentato di sicurezza
- CCF Common Cause Failures ovvero l'insieme delle condizioni di guasto di modo comune in sistemi strumentati di sicurezza di tipo ridondato

  A questi vanno affiancati concetti più complessi e specifici relativi al sistema strumentato di sicurezza :
- Structure (Architettura)
- Comportamento del sistema in caso di guasto
- Guasti sistematici
- Capacità di esecuzione della funzione di sicurezza in determinate condizioni ambientali
- Safety related software

Il concetto di Structure (Architettura) si riepiloga nelle 5 architetture predefinite e contraddistinte ordinatamente con 5 categorie: B, 1, 2, 3 e 4 dalla categoria base (B) alla categoria caratterizzata da maggiore reiezione al guasto (4).
La Categoria B è la categoria base. La presenza di un solo guasto può condurre alla perdita della funzione di sicurezza. La categoria 1 presenta la stessa limitazione ma la probabilità del guasto è ridotta attraverso la corretta selezione del design e della componentistica.
Nelle categorie 2, 3, 4 l'affidabilità del sistema strumentato di sicurezza è sotto controllo agendo sull'architettura e sull'auto diagnostica.
In particolare, la categoria 2 si basa sul fatto che è implementato un monitoraggio periodico della funzione di sicurezza (*Test diagnostico*). Nella categoria 3 e 4 si garantisce addizionalmente che anche un singolo guasto non conduca alla perdita della funzione di sicurezza. La categoria 4, infine, garantisce anche che l'accumulo di più guasti sia possibile senza perdita della funzione di scurezza.
Le caratteristiche riepilogate poco sopra devono poi confluire nella corretta selezione del livello di integrità del sistema strumentato di sicurezza ovvero il livello PL ottenuto dal sistema di controllo.
Nel diagramma precedente, estratto dalla norma EN13849-1, convergono le informazioni precedenti: con queste si opera selezionando la colonna adeguata in ascissa, sulla base della categoria, ovvero sulla base dell'architettura e sulla base della copertura diagnostica.
Il livello MTTFd del singolo canale determina il posizionamento verticale sulle colonne a bande colorate: più elevato è il livello MTTFd più alto è il Performance Level raggiungibile.
Come visibile dalla figura, un sistema in categoria 4, ad elevata copertura diagnostica e MTTFd alto matura in automatico un PLe.

6. 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.
La cifra di merito "SIL" è la sintesi opportuna delle seguenti grandezze:

- PFHd Probability of Dangerous Failure per Hour ovvero rateo orario di guasto pericoloso (perdita della funzione di sicurezza)
- PFD Probability of Dangerous Failure on demand ovvero probabilità di guasto pericoloso (perdita della funzione di sicurezza) quando la funzione di sicurezza è richiesta
- SFF Safe Failure Fraction ovvero frazione dei guasti sicuri
- DC Diagnostic Coverage ovvero fattore di copertura diagnostica
- β Common Mode Failure Ratio ovvero rateo di guasto di modo comune di architetture ridondate
- HFT Hardware Fault Tolerance ovvero livello di reiezione dell'architettura al guasto (ridondanza)
- T1 Proof Test Interval ovvero intervallo di tempo stabilito tra due test successivi completi della funzione di sicurezza
- Tid Diagnostic Test Interval ovvero intervallo di tempo stabilito tra due test successivi parziali (auto diagnostica)

In particolare, senza entrare nello specifico di ciascun parametro, è importante sottolineare la valenza dei parametri PFHd (PFD) e SFF.
Il primo rappresenta, in termini molto semplici, la probabilità oraria oppure on demand di perdita della funzione di sicurezza ed è un termine probabilistico puro che si lega alle proprietà specifiche e all'affidabilità di ogni elemento componente la funzione di sicurezza; si lega anche all'architettura di sistema ed alle proprietà e alla frequenza della diagnostica.
Il soddisfacimento del requisito relativo al PFHd e al PFD non è da solo sufficiente per poter dichiarare un SIL target raggiunto: è infatti necessario soddisfare anche il requisito relativo al secondo parametro (SFF), ovvero la frazione di guasti sicura.
Ancora in termini molto semplici, questo parametro riporta il rateo di guasto sicuri di un sottosistema o di un elemento quando raffrontato con il numero complessivo di guasti.
Tanto più elevato è il rateo SFF tanto più il sottosistema o l'elemento hanno tendenza a guastarsi in modo prevalentemente sicuro. L'uso concomitante delle due tabelle definisce il SIL raggiunto dalla funzione strumentato di sicurezza. La norma EN13849-1 riporta una tabella di corrispondenza teorica tra SIL (high/continuous mode) e PL.
In generale i Performance Level hanno unicamente una corrispondenza limitata al SIL3 e non includono eventi catastrofici, verosimilmente possibili solo nell'industria di processo, richiamanti un livello di integrità della funzione di sicurezza pari a SIL4 e non applicabili alle macchine; per questa ragione il PLe, corrispondente al livello di integrità SIL 3, è definito come il livello di performance più elevato.
Le norme IEC 61508 e IEC 61511 utilizzano il concetto di livello di integrità della sicurezza per specificare il target sistematico e probabilistico cui le funzioni implementate in termini di E / E / PE devono rispondere.
Il livello di integrità della sicurezza è una figura di merito che comunica la capacità di un sistema di controllo critico di attuare una cosiddetta funzione di sicurezza in un tempo stabilito. Lo standard definisce quattro livelli di integrità della sicurezza. Maggiore è il livello di integrità di sicurezza, minore è la probabilità che il sistema di sicurezza fallisca la chiamata svolgere le funzioni di sicurezza.
Tale figura di merito è l'interpolazione di due parametri descrittivi:

1) la probabilità di guasto on demand, PFDavg in low demand mode (o PFH per High demand mode);
2) la frazione di guasto di modo sicuro SFF.
Il primo rateo è un'informazione puramente probabilistica correlata ai ratei di guasto pericolosi rilevabili e non rilevabili, pesati attraverso riferimento a tempi di test diagnostico e test completo.
Il secondo rateo è un'informazione architetturale che descrive quanto più un'architettura è per costruzione spostata verso guasti sicuri piuttosto che pericolosi. Minimizzare la prima cifra massimizzando la seconda è l'obiettivo del miglioramento del livello di integrità della sicurezza associata a quella particolare architettura.
Bisogna sottolineare che l'integrità funzionale si riferisce all'intero loop di controllo e pertanto deve includere la probabilità di guasto dei sensori, della logica e degli elementi finali. Esprimere una figura di merito SIL di un sottosistema o di un componente ha senso solo se questa è accompagnata da informazioni relative a PFD e SFF.

7. Sistemi di sicurezza strumentati (SIS)

Il sistema strumentato di sicurezza (SIS) 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.

8. SIF: funzione di sicurezza

La funzione di sicurezza è 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.
La funzione di sicurezza è pertanto il risultato dell'azione automatica eseguita di concerto dai sensori, dal logic solver e dagli elementi finali che consiste nel raggiungimento, da parte del processo, di uno stato di sicurezza.
Una SIF può funzionare in continuo oppure on demand.

9. EPL: Equipment Protection Level ovvero la sicurezza funzionale applicata al pericolo di esplosione

Allo scopo di regolamentare costruzioni destinate a luoghi caratterizzati dal pericolo di esplosione è stata sviluppata la norma seguente di recente armonizzazione:

EN50495:2010 Dispositivi di sicurezza richiesti per il funzionamento sicuro degli apparecchi in relazione al rischio di esplosione.
Tale norma specifica infatti i requisiti per i dispositivi elettrici di sicurezza che sono usati per evitare sorgenti d'innesco potenziali di apparecchi usati in atmosfera esplosiva. Essa include inoltre dispositivi di sicurezza che sono usati fuori dalla zona con atmosfera esplosiva, per garantire il funzionamento sicuro dell'apparecchio in relazione ai pericoli di esplosione. Questa norma precisa testualmente che i dispositivi di sicurezza, la cui funzione di sicurezza non possa adeguatamente essere specificata nelle Norme esistenti della serie EN/IEC 60079, devono in aggiunta essere progettati in accordo ai requisiti in essa contenuta.
La tabella 1 in essa disponibile, relativa ai "Requisiti minimi per Livello di Integrità della Sicurezza e Tolleranza al guasto per un dispositivo di sicurezza", è il cardine del documento:

EUC Tolleranza al Guasto Hardware	2	1	0	1	0	0
Dispositivo di sicurezza						
Tolleranza al guasto hardware	-	0	1	-	0	-
Livello di integrità della sicurezza	-	SIL1	SIL2	-	SIL1	-
Apparecchio combinato						
Gruppo I, Categoria	M1			M2		-
Gruppo II, III, Categoria	1			2		3

Tabella 1 Correlazione tra categorie, EPL, HFT

Oltre ad introdurre esplicitamente il requisito di caratterizzazione SIL dei dispositivi assemblati in accordo alle prescrizioni in essa riportate, associa la categoria o il livello EPL ottenibili ad un sistema di sicurezza che agisca in modo da controllare i guasti dello EUC (Dispositivo controllato): al crescere della tolleranza al guasto dello EUC i requisiti di integrità funzionale (Livello SIL) del sistema di controllo e il livello di ridondanza (Tolleranza 1 significa un sistema 1oo2 ovvero sistema a doppio canale ridondato; tolleranza 0 significa 1oo1 ovvero un sistema a singolo canale) decrescono. Se la tolleranza al guasto è allineata alla categoria (o EPL) non sono necessari sistemi di scurezza attivi: infatti una categoria 1 (EPL=a) ha per costruzione (progettazione intrinsecamente sicura) una tolleranza pari al guasto pari a 2. Se ci adoperassimo per elevare una categoria 2 (una sola tolleranza al guasto) ad una categoria 1, dovremmo attrezzarla con un sistema di sicurezza SIL1 non ridondato; se infine ci adoperassimo per portare un dispositivo non caratterizzato in termini affidabilistici (Nessun categoria, nessun EPL definiti) verso una categoria 1 dovremmo attrezzarlo con un sistema di sicurezza doppio canale ridondato SIL2. Gli altri passaggi di categoria si deducono dalla tabella sopra riportata.

10. SIL: Obbligatorio o volontario?

Il set di norme IEC61508 non costituisce set armonizzato a Direttive Europee.
L'applicazione della IEC61508 non è cogente ma è richiamata in varie norme e norme europee armonizzate a Direttive di Prodotto. L'uso del set IEC61508 è raccomandato.

11. Bibliografia

[1] Norma ISO - EN ISO 13849-1:2008 Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione (ISO 13849-1:2006)
[2] Norma ISO - EN ISO 13849-2:2008 Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 2: Validazione (ISO 13849-2:2003)
[3] Norma IEC - EN 62061:2005 Sicurezza del macchinario - Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza (IEC 62061:2005)
[4] Norma IEC - EN61508-1,2,3,4,5,6,7:2010 Functional safety of electrical / electronic / programmable electronic safety-related systems
[5] Norma IEC - EN61511-1,2,3 :2004 Functional safety - Safety instrumented systems for the process industry sector
[6] Norma CENELEC - EN50495:2010 Dispositivi di sicurezza richiesti per il funzionamento sicuro degli apparecchi in relazione al rischio di esplosione