Suggerimenti e trucchi pratici per il calcolo del Sil

Fabrizio Gambetti

I risultati delle analisi sugli incidenti avvenuti sui sistemi di protezione elettrici/elettronici/elettronici programmabili (E/E/Pe) ha evidenziato l'importanza non solo dei guasti casuali dei componenti, ma anche degli errori di tipo sistematico che si verificano durante la progettazione. Il problema nella progettazione dei sistemi di protezione E/E/Pe, spesso deriva da un'analisi di rischio carente. Molte volte le funzioni di progetto coinvolte nello sviluppo di questi sistemi non conoscono o hanno un'idea vaga del concetto di rischio. Spesso i progettisti non hanno dimestichezza nell'uso dei differenti strumenti disponibili per assegnare il valore di Sil (Safety Integrity Level) ad una funzione di protezione, oppure sono preoccupati solo dal costo che questo tipo di analisi potrebbe richiedere. Una valutazione più accurata dell'importanza dell'analisi di rischio applicata alla funzione di protezione, potrebbe aiutare il progettista, il costruttore ed il cliente a risparmiare tempo e denaro.

Tutti concordano che il principio fondamentale alla base delle procedure Iec-61508/Iec-61511 è che i requisiti di un sistema di sicurezza strumentale (Sis) devono essere identificati attraverso un'analisi dei pericoli e di rischio dell'apparecchiatura sotto controllo (Euc, Equipment Under Control). Le procedure senza dubbio sono chiare su questo punto, la clausola 7.4 "Hazard and Risk Analysis" della Iec-61508 si può riassumere nel seguente modo:

- Determinare i pericoli e gli eventi pericolosi dell'Euc e del sistema di controllo dell'Euc (in tutte le modalità operative) per tutte le circostanze ragionevolmente prevedibili, incluse le condizioni di guasto e di uso improprio.
- Determinare la sequenza di eventi che portano agli eventi pericolosi determinati nel primo punto.
- Determinare i rischi per l'Euc associati con gli eventi pericolosi determinati al primo punto.

I requisiti di sicurezza per il Sis si fondano pertanto su un approccio sistematico (7.4.1), la probabilità di accadimento degli eventi pericolosi deve essere valutata (7.4.2.5) e le potenziali conseguenze associate con gli eventi pericolosi devono essere determinate. Si possono, inoltre, applicare tecniche di Analisi di Rischio sia qualitative sia quantitative (7.4.2.8).

Concetti legati al Rischio

Prima di affrontare il tema centrale dell'articolo è opportuno chiedersi perché molte persone trovano difficoltà nell'applicare le sopraccitate clausole dello standard e perché le domande più frequenti sono quelle relative al calcolo o all'allocazione del Sil. Probabilmente perché nessuno conosce le definizioni di rischio tollerabile o di rischio accettabile, oppure perché l'identificazione delle protezioni dell'Euc non è sempre facile anche quando tutte le informazioni di progetto sono disponibili, oppure perché la filosofia di protezione dell'Euc non è chiara, oppure... si potrebbero elencare molte altre possibili ragioni. Spesso i problemi sorgono perché non si è abituati ad analizzare il comportamento del nostro Euc in condizioni estreme. Quante volte domandando agli specialisti che cosa potrebbe succedere se il sistema di controllo o un dispositivo di sicurezza meccanico (ad esempio, una valvola di sicurezza) o una protezione elettronica si guasta la sola risposta che si ottiene è: "impossibile!!!".

Nei nostri paesi, tuttavia, ci sono leggi (ad esempio 96/82/Ec Direttiva Seveso, Osha standard-29 Cfr-1910.119, ecc.) i cui principi generali impongono di analizzare i possibili pericoli, valutarne le conseguenze ed il rischio associato; qualora il rischio sia inaccettabile, di ridurlo o rivedere i criteri di progettazione. Queste normative impongono, inoltre di documentare i risultati di questi studi in maniera ben organizzata e strutturata. Quindi è opportuno, prima di iniziare la nostra attività, conoscere il significato dei diversi termini utilizzati nel corso della analisi di rischio:

- Pericolo (Hazard): è un evento/situazione che per sua natura ha la potenzialità/possibilità di generare un danno.
- Rischio (Risk): è la misura della probabilità (o frequenza) di accadimento di uno specifico evento pericoloso associata alle conseguenze.
- Rischio Tollerabile: è la soglia di rischio, diversa da zero, accettabile per un'organizzazione. Questa soglia di rischio è necessaria per identificare il fattore di riduzione del rischio richiesto ad una funzione di protezione (Safety Instrumented Function - Sif). Il rischio tollerabile dipende da molti fatto-

F. Gambetti, Snamprogetti, Hseq (Health, Safety, Environment, & Quality)

ri, ad esempio leggi, requisiti legali, normative, procedure, linee guida industriali, persone esposte al pericolo ecc.
- Sil: il *safety integrity level* è definito come la probabilità di una *Safety Instrumented Function* di svolgere in maniera soddisfacente le funzioni di sicurezza richieste in tutte le condizioni fissate entro un fissato periodo di tempo (3.5.2 della Iec-61508 parte 4). Nella determinazione del *Safety Integrity Level* tutti i casi di guasto che portano a uno stato non sicuro dovrebbero essere tenuti in considerazione.

Innanzitutto, prima di iniziare la nostra Analisi di Rischio, è necessario conoscere il valore di Rischio Tollerabile e costruire la nostra classificazione del rischio connessa. Questo passaggio deve essere eseguito indipendentemente dal tipo di analisi effettuata (quantitativa o qualitativa) per poi poter stimare i livelli di rischio. Ad esempio nel caso di un'analisi qualitativa è opportuno fissare i valori dei parametri di sicurezza del personale, economici ed ambientali che faranno da riferimento nel corso dell'analisi.
Se la nostra analisi è qualitativa si può fare riferimento a procedure nazionali o industriali disponibili (Bs 8444, As/Nzs 4360, Nureg-0933, ecc.). Se la nostra analisi è quantitativa si possono usare ad esempio l'annesso B della Iec-61508-5 o Iec-61511-3 o Mil-Std-822 per classificare la frequenza di accadimento e la gravità delle conseguenze applicando il principio di Alarp[1].
Questo primo passo è fondamentale ed è alla base di tutta l'analisi di rischio. Nelle analisi qualitative la disponibilità delle informazioni relative ai possibili costi per fermata impianto, costi della strumentazione, costi di immagine in caso di incidente e/o ambientali, aiutano il team nell'analisi e soprattutto garantiscono la coerenza dell'analisi stessa.
Una volta che si sono fissati questi punti fondamentali, sulla base dei criteri di progetto, una classificazione del rischio potrebbe essere simile a quella riportata nella tabella sottostante tratta dalla Iec-61508-5:

Gravità della conseguenza

Frequ./Probab.	Catastrof.	Critica	Marginale	Trascurab.
Frequente	1	2	2	3
Probabile	2	2	3	4
Occasionale	2	2	3	4
Remota	3	3	4	4
Improbabile	3	3	4	4
Non credibile	4	4	4	4

La tabella sottostante, per esempio, è un'interpretazione dell'assegnazione del Sil in base alla Classe di Rischio:

Classe Rischio	Valutazione/Interpretazione	Sil
1	Intollerabile / Alto	Sil 4/Sil 3
2	Indesiderabile, Grave e tollerabile solo se è praticabile una riduzione del rischio	Sil3/ /Sil2
3	Rischio tollerabile	Sil1
4	Rischio basso o trascurabile	-

Per i diversi ricettori (persone, beni, ambiente) si possono creare differenti classificazioni connesse al rischio e diverse tabelle di assegnazione del Sil in base alla classe di rischio.
Si noti che la classificazione del rischio e l'allocazione del valore di Sil in base alla classe di Rischio è in questo caso piuttosto soggettiva!!! Mil-Std-882d per il livello di probabilità "Frequent" specifica che corrisponde a "la probabilità che avvenga spesso nella vita di un item, con una probabilità più grande di 10^{-1} nella vita", gli standard Iec non danno nessuna indicazione, ma suggeriscono solo che la classificazione deve essere sviluppata prendendo in considerazione un ampio range di fattori sociali, politici e economici.

Analisi qualitativa

Quanto detto in precedenza è solo una delle ragioni per cui le tecniche qualitative sono considerate molto soggettive e suscettibili di gravi errori; molti studi infatti, hanno ripetutamente dimostrato che gli esseri umani sono giudici piuttosto inadeguati della frequenza di accadimento di eventi che avvengono in intervalli di tempo lunghi. Tuttavia a dispetto di quanto sopra affermato, ci si aspetta che gli esperti valutino la differenza tra due eventi, la cui frequenza è inferiore a una volta in mille anni!! (più di dieci volte la vita media!). In questo tipo di analisi si devono affrontare molte trappole psicologiche che possono offuscare la capacità di giudizio umano:
- la trappola della prudenza "spinge" a stimare in maniera troppo conservativa il rischio, con il risultato di sovradimensionare il Sis, viceversa sottovalutare la frequenza di accadimento e/o le conseguenze producono il risultato opposto, quello cioè di sottodimensionare il Sis:
- l'incapacità ad analizzare passo dopo passo il comportamento del sistema, saltando subito alla conclusione. Questo comportamento ha come risultato quello di non tener conto di tutti i contributi possibili del sistema stesso, l'associazione che possiamo avere tra diversi parametri sotto controllo e le loro relazioni:
- la difficoltà ad effettuare un esercizio ripetitivo per molte ore, può essere causa di valutazioni superficiali.

Per tutte le ragioni sopra esposte, è importante ricordarsi che quando si costruisce una squadra per un'analisi qualitativa: esperienza, capacità di visione d'insieme del sistema che si sta esaminando, lealtà nell'affrontare la valutazione delle conseguenze, sono essenziali per la valutazione della sicurezza e dell'integrità. Questo è vero anche quando sono disponibili normative, procedure e linee guida di progettazione,

[1] Il principio Alarp afferma che c'è un livello di rischio intollerabile, a volte detto de manifestus risk level, sopra questo livello, il rischio non può essere giustificato. Sotto questo valore intollerabile c'è una regione Alarp o regione di tollerabilità dove un'attività è permessa se il rischio ad essa associato è tale da essere il più basso ragionevolmente praticabile. Sotto la regione Alarp c'è il livello di rischio minimo (minimum risk level) o regione ampiamente accettabile (broadly acceptable region) dove il rischio è così basso che non è considerato di per se pericoloso, in questa regione il rischio è così basso che probabilmente nessuna riduzione del rischio è efficiente da un punto di vista dei costi.

l'abilità e l'esperienza degli individui che eseguono direttamente l'analisi di rischio incide sul valore della valutazione. Il livello di dettaglio per un'analisi di probabilità, per la valutazione del SIL, può variare da una semplice stima qualitativa (basata sul giudizio ingegneristico): *what-if*, *checklists, hazard and operability* (Hazop), *failure mode and effect analysis* (Fmea), *hazard matrix* (Lopa, Soa), *Risk Graph*.
Fino ad un'analisi quantitativa che usa tecniche sofisticate di modellazione della propagazione del guasto in combinazione con dati storici: albero dei guasti (fault tree), albero degli eventi (event tree), analisi di Markov, equazioni affidabilistiche. Indipendentemente dalla tecnica usata, è mia opinione che è meglio identificare i possibili pericoli connessi con la nostra Euc e, passo dopo passo, valutare tutti i possibili contributi alla riduzione del rischio disponibili nel nostro sistema. È possibile fare questo seguendo il livello di protezione identificato come mostra l'Iec-61511-1, il ben noto "onion ring". Si tratta quindi di analizzare e assegnare i contributi di riduzione del rischio a tutte le misure protettive come: criteri di progettazione (ad esempio: sistemi di drenaggio, contenimento liquidi, distanza tra le apparecchiature ecc.); sistema base di controllo del processo; dispositivi meccanici; intervento dell'operatore; mezzi esterni per la riduzione del rischio.
Per la valutazione del Sil, è fondamentale analizzare i diversi modi di funzionamento dell'Euc, per ognuno di essi identificare le possibili cause che generano una deviazione del processo al fine di valutare il possibile comportamento dinamico dei parametri di processo coinvolti e quindi poter effettuare la relativa analisi delle conseguenze. Spesso nel corso delle analisi ci si scontra con una manifesta "ignoranza" delle possibili cause che possono condurre il sistema a situazioni di pericolo e che richiedono l'intervento della funzione di protezione, oppure sembra che possa cambiare solamente una variabile del processo in esame, quando normalmente si ha a che fare con più variabili tra loro correlate. Nell'identificazione degli scenari pericolosi è importante, cercare di comprendere per quanto possibile il comportamento dinamico della Euc, al fine di valutare il contributo che si può attribuire alla riduzione del rischio ad ogni livello di protezione presente nell'impianto, ad esempio: controllo di processo, criteri di progettazione, procedure operative, intervento degli operatori.
Gli strumenti più utilizzati per eseguire l'analisi qualitativa sono il Risk Graph e la hazard matrix (analisi dei livelli di protezione). Dal punto di vista concettuale non ci sono differenze, si tratta sempre di una analisi di rischio; la differenza è solo nel metodo per stimare le conseguenze.
L'analisi dei livelli di protezione, utilizzato soprattutto dagli americani (Lopa – layer of protection analysis), può essere definita un'analisi semi-qualitativa. L'analisi una volta identificata la causa iniziatrice e la sua frequenza di accadimento, stima il contributo di tutti i livelli di protezione indipendenti (ad esempio: valvole di sicurezza, criteri di progettazione, sistemi di controllo di processo ecc.) che contribuiscono a ridurre le conseguenze dell'evento indesiderato preso in esame. Il Risk Graph, inizialmente sviluppato da uno standard nazionale tedesco (Din/Vde 19250) segue un approccio diverso, infatti si considera la probabilità di guasto su richiesta della funzione di sicurezza (Sif) e con diversi Risk Graphs, sulla base delle conseguenze valutate, si può assegnare il Sil. Risk Graphs sono normalmente prodotti per tenere in considerazione perdite economiche, impatto ambientale ed effetti sulle persone di un incidente. La conseguenza più grave determina il Sil assegnato al Sif.

Un esempio

Un esempio pratico di assegnazione di un Sil potrebbe essere il seguente: supponiamo di avere un serbatoio a pressione atmosferica collegato ad una pompa per il trasferimento di un liquido. Sulla base di queste semplici informazioni proviamo ad identificare e quindi classificare le protezioni necessarie per le nostre apparecchiature. Delle dieci possibili deviazioni sopra riportate a cui può essere soggetta la nostra apparecchiatura è possibile assegnare un Sil, avendo a disposizione la matrice di rischio, indipendentemente dalla architettura di protezione adottata dal progettista.

EUC	Parametro	Deviaz.
Serbatoio	Livello	Alto
		Basso
	Temperatura	Alta
		Bassa
	Pressione	Alta
		Bassa
Pompa	Pressione in aspiraz.	Alta
		Bassa
	Portata	Bassa
		Alta

Supponiamo infatti di esaminare per semplicità la protezione di bassa pressione in aspirazione della pompa. Sulla base delle informazioni disponibili dal progettista possiamo assumere come frequenza di intervento della protezione un valore ad esempio occasionale. A questo punto dobbiamo identificare in caso di mancato funzionamento della protezione, le possibili conseguenze sull'apparecchiatura da proteggere, ad esempio se ipotizziamo di avere come liquido dell'acqua, la possibile conseguenza potrebbe essere il danno meccanico della pompa per cavitazione. La quantificazione della conseguenza per determinare il Sil a questo punto può essere effettuata nel seguente modo:

- Valutazione della sicurezza del personale operativo. A causa della mancata protezione il nostro personale potrebbe corre dei rischi, tuttavia a seconda della presenza e permanenza del personale in campo, delle possibili caratteristiche dell'area di processo si può effettuare una valutazione delle conseguenze per il personale. Ad esempio nel nostro caso se il personale fosse presente nell'area della pompa in caso di incidente le possibili conseguenze potrebbero essere dei danni alla salute, tuttavia se la presenza nell'area delle pompe può essere considerata limitata nell'arco della giornata a poche ore ed in ogni caso il personale può allontanarsi dall'area pericolosa, le conseguenze potrebbero essere stimate come marginali. Sulla base della frequenza attesa "occasionale" e della conseguenza stimata "marginale" la valutazione di rischio in base alla matrice sopra riportata risulta tollerabile (Sil 1).

- Valutazione del danno economico. Questo è l'aspetto più problematico, in quanto i tecnici cercano di entrare nel dettaglio delle singole voci senza sforzarsi di identificare la possibile dimensione della voce "costo" nella sua globalità, mentre, gli operativi insistono sulle problematiche relative alla tempistica di riparazione, che generalmente sono sottostimate da parte dell'ingegneria. Per esempio nel nostro caso se si rompe la pompa, a seconda del luogo, ci potrebbero essere problemi di reperimento dei pezzi di ricambio e disponibilità del personale specializzato per effettuare la riparazione, con il conseguente prolungamento dei costi di fuori servizio. Negli impianti ad alto rischio una voce da tenere in considerazione è il danno d'immagine che un incidente può avere sulla Società. Nel nostro caso, avendo una sola pompa il danno economico potrebbe essere considerato critico. Sulla base della frequenza attesa e della conseguenza stimata la valutazione di rischio sarebbe indesiderabile (Sil 2).
- Valutazione Ambientale. Nel nostro caso la fuoriuscita del liquido acqua non ha effetti sull'ambiente, ma se fosse acqua con prodotti inquinanti da trattamenti industriali l'analisi sarebbe differente. Normalmente nell'analisi dei danni ambientali si stimano gli effetti che un eventuale rilascio di prodotto può avere unicamente sull'ambiente, lasciando alla precedente voce la stima dei costi di disinquinamento ed eventuale recupero d'immagine da parte dell'azienda.

Alla fine di questa classificazione qualitativa possiamo concludere che la nostra protezione è classificata Sil 2, poiché delle tre valutazioni effettuate la più gravosa è risultata quella economica. Al momento non abbiamo nessuna informazione su come il progettista intende proteggersi dalla bassa pressione in aspirazione della pompa, quando sarà disponibile il progetto di dettaglio sarà possibile verificare quantitativamente se la probabilità di guasto su domanda della protezione rientra nel Sil assegnato.

L'ingegnere di processo in questo caso potrebbe prevedere una protezione basata sulla semplice rilevazione della pressione in aspirazione oppure prevedere una protezione per bassissimo livello, oppure entrambe. L'importante è che sulla base dell'intervallo di test previsto per la nostra protezione sia rispettato il Sil assegnato. Per fare questa verifica possiamo utilizzare le formule riportate nella parte 6 della Iec-61508, tuttavia per fare questi calcoli dobbiamo disporre di alcune informazioni specifiche relative la strumentazione che sarà installata come ad esempio:

- rateo di guasto;
- copertura diagnostica;
- percentuale di guasti comuni;
- intervallo di test;
- tempo di riparazione del guasto.

Sulla base dei dati sopra riportati e dell'architettura della nostra protezione sarà possibile determinarne la probabilità di guasto media (Pfd_{medio}). Nel caso dell'analisi quantitativa gli strumenti a disposizione dello specialista per la valutazione sono diversi, ma il problema principale è identificabile nelle cinque voci sopraelencate. Non sempre, infatti, i dati sono disponibili da parte dei costruttori dei componenti, ed in questo caso occorre utilizzare le banche dati disponibili e formulare delle ipotesi. Nel nostro caso ad esempio supponiamo che il processista abbia utilizzato un sensore di pressione che tramite la logica Esd ferma il motore della pompa.

- Supponiamo di avere la logica certificata Sil 3, assumiamo un $Pfd_{medio} = 5.5*10^{-4}$.
- Il rateo di guasto per il trasmettitore di $7,6*10^{-6}$ guasti/ora, con una copertura diagnostica del 50%, periodo di test 1 anno e tempo di riparazione di 8 ore, utilizzando la formula B.2.4.1 della Iec-61508 si ottiene un $Pfd_{medio} = 8.4*10^{-3}$.
- Il rateo di guasto per il motore della pompa $2,3*10^{-6}$ guasti/ora, con una copertura diagnostica del 90%, periodo di test 1 anno e tempo di riparazione di 8 ore, utilizzando la stessa formula della Iec-61508 si ottiene un $Pfd_{medio} = 5.1*10^{-4}$.

Sommando i tre valori di Pfd_{medio} si ottiene per la funzione di protezione il valore di Pfd_{medio} =9.5*10-3, che equivale ad un Sil 2. Se il tempo di test fosse di due anni la funzione avrebbe un Pfd_{medio} = 2.2*10-2 e quindi equivalente a Sil 1, che non soddisfa i nostri requisiti.

Conclusione

Indipendentemente dallo strumento selezionato per l'analisi di rischio, si dovrebbe sempre ricordare che un'analisi di rischio accurata del proprio sistema di protezione, aiuterà a capire sia il suo comportamento, che come la riduzione del rischio è gestita da tutti gli altri dispositivi previsti nell'impianto. L'obiettivo di questa attività non è solo quella di sviluppare i requisiti di integrità del sistema di protezione secondo le normative, ma progettare e realizzare la funzione di sicurezza richiesta sulla base di un'analisi adeguata.

Un'analisi accurata, infatti, permetterà a coloro che sviluppano il sistema di protezione di progettarlo sulla base del requisito di sicurezza e perciò offrire un'architettura appropriata per tutte le Sif identificate in tutte le condizioni operative prevedibili per l'impianto. Un'analisi accurata permetterà agli utenti di ottimizzare il costo del ciclo di vita del sistema con un Sis progettato anche sulla base dei loro requisiti di operazione e di manutenzione.

Riferimenti

[1] *Guidelines for Safe Automation in Chemical Process*, American Institute of Chemical Engineers, 1993, ISBN 0-8169-0554-1.

[2] Paul Gruhn, Harry Cheddie, *Safety Shutdown Systems: Design, Analysis, and Justification*, Instrument Society of America, ISBN 1-55617-665-1.

[3] Marszal, Scharpf, *Safety Integrity Level Selection. Systematic Methods Including Layer of Protection Analysis*, Instrument Society of America, ISBN 1-55617-777-1.

[4] "Standard Practice for System Safety", Mil-Std-882d.

[5] Kirk Clark, "Definition and Classification of critical instrumentation and controls for compliance with Osha Standard-29 Cfr-1910.119", 2001.

[6] "Functional Safety of Electrical/Electronic/Programmable Electronic Safety Releted Systems", Iec-61508.