SISTEMI DI RIVELAZIONE GAS : Una scelta secondo le norme

PARTE QUARTA : La nuova norma europea EN 50402 in materia di sicurezza funzionale.

Questo documento fornisce una panoramica sulla nuova normativa europea EN 50402 relativa ai sistemi fissi di monitoraggio gas, sugli aspetti connessi alla sicurezza funzionale e sui requisiti richiesti in funzione dei livelli di sicurezza. Nello specifico la normativa definisce le caratteristiche dei moduli funzionali e illustra le combinazioni che possono essere utilizzate ai fini della sicurezza. Il documento esamina anche i passaggi che hanno portato all'unificazione delle normative generiche in un'unica bozza di normativa e spiega come verranno classificati i sistemi di rivelazione gas convenzionali in base alla nuova normativa. La nuova normativa permetterà per la prima volta di utilizzare sistemi di monitoraggio gas che utilizzano tecnologie a microprocessore per applicazioni che richiedano la valutazione della sicurezza funzionale.

Nel presente documento ,che riguarda la quarta parte dell'Esagono di Sensitron,si parlera' di una Norma che, pur non essendo Direttiva ,e quindi vincolante,risulterà in ogni caso in futuro ,molto importante per quei Costruttori che vorranno offrire un prodotto sempre più sicuro e qualificato.

Introduzione

I gas combustibili utilizzati in aree pericolose vengono misurati ormai da anni mediante test di omologazione conformi a normative metrologiche (funzioni e precisione), secondo quanto previsto dalle leggi nazionali e dalle normative europee introdotte negli ultimi 10 anni. La normativa ATEX-100 a (Direttiva 94/9/CE) stabilisce che i test di omologazione delle funzioni debbano essere effettuati in tutti i paesi europei sui "sistemi di rilevazione gas con funzioni di misurazione progettati per prevenire il rischio di esplosione". I requisiti di prestazioni per la misurazione dell'ossigeno o il rilevamento di gas tossici sono definiti in altre normative ancora.

Tutte queste normative metrologiche definiscono i requisiti di prestazione standard, ma non forniscono indicazioni sulla sicurezza funzionale in caso di guasti né definiscono i requisiti che devono essere rispettati per garantire un funzionamento continuo dei sistemi in caso di guasto. I sistemi di rilevazione gas attualmente in uso hanno una struttura modulare complessa, sono controllati da microprocessori e vengono usati per applicazioni diverse con più livelli di sicurezza. Questo range applicativo complesso non era stato regolamentato da alcuna normativa in materia di sicurezza funzionale ma verrà ora disciplinato con la normativa EN 50402.

Normative esistenti

La normativa generica che disciplina la "sicurezza funzionale dei sistemi elettronici" è la EN 61508, che definisce vari requisiti di prestazione a seconda del livello di sicurezza (SIL 1 – SIL 4, Safety Integrity Level, livello di integrità di sicurezza). Questa normativa, costituita da 7 sezioni, è molto voluminosa ma anche piuttosto generica. In molti casi, la normativa fornisce solo una base teorica o suggerisce di usare complessi calcoli matematici per stimare i possibili rischi. Tutto ciò è molto stimolante da un punto di vista scientifico, ma molto poco pratico. Per la terza ipotesi necessaria per risolvere l'equazione, è più utile la creatività che la matematica pura.

La seconda normativa europea che disciplina la sicurezza funzionale dei sistemi di controllo elettronici è la EN 954-1, che specifica i requisiti generici della Direttiva Macchine in funzione delle

categorie di rischio (B (rischio minimo) e 1 – 4). Per definizione, tali categorie sono esplicitamente "non gerarchiche in termini di requisiti", ma possono comunque essere integrate in un sistema gerarchico. Le definizioni della normativa EN 954-1 sono molto più pragmatiche e in molti casi anche molto più pratiche di quelle della normativa EN 61508. Ciò nonostante, la normativa EN 954-1 disciplina adeguatamente tutti gli aspetti teorici e i limiti di sicurezza specificati nella normativa EN 61508.

Tabella 1 : normative applicabili al rilevamento gas

<table>
<tr><th></th><th>EX</th><th>TOX</th><th>02</th><th>Requisiti</th></tr>
<tr><td>Tolleranze
Condizioni ambientali
Gas interferenti</td><td>EN 61779</td><td>EN 45544</td><td>EN 50104</td><td>Unificati</td></tr>
<tr><td>EMC</td><td colspan="3">EN 50270</td><td>Unificati</td></tr>
<tr><td rowspan="2">Sicurezza funzionale dei singoli apparati
• Elaborazione segnali</td><td>EN 61779</td><td>EN 45544</td><td>EN 50104</td><td rowspan="2">Unificati</td></tr>
<tr><td>• Hardware e software</td><td colspan="3">EN 50271</td></tr>
<tr><td>Sistemi complessi
• Elaborazione combinata
• Disponibilità
• Array di sensori
• Allarmi compreso Selezione multipla</td><td colspan="3">Attualmente: interpretazione arbitraria delle normative generiche (EN 61508 Parti 1 – 7)

Ora : EN 50402</td><td>Specifici per applicazione, conformemente a
EN 61508 o
EN 954-1</td></tr>
</table>

L'obiettivo della nuova norma EN 50402

L'obiettivo della nuova norma EN 50402 è sia quello di unificare i concetti ("combinare") che quello di definire i requisiti per una famiglia di prodotti (gas combustibili, tossici o ossigeno), ovvero quello di adattare specificatamente i requisiti generici ai sistemi di rilevazione gas.

La norma apre la strada alla possibilità di approvare la sicurezza funzionale di sistemi di rilevazione gas complessi, ossia di soddisfare il requisito della Direttiva ATEX 100a che specifica che nella progettazione di apparecchiature, di sistemi protettivi e dispositivi di sicurezza controllati da software, è indispensabile tener conto dei possibili rischi derivanti da possibili problemi di funzionamento dei programmi. Essendo applicabile a tutte le classi di prodotti usate per la rilevazione del gas, la normativa permette di specificare i requisiti dei sistemi di rilevazione gas complessi in relazione a più livelli di sicurezza funzionali, di approvarli e di integrarli nel sistema di sicurezza generale di una categoria o di un livello SIL specifici.

Negli ultimi anni gli utenti o le autorità locali hanno spesso richiesto che i livelli di sicurezza dei sistemi di rilevazione gas fossero classificati in base a quanto specificato nelle normative EN 9541, EN 61508. Sebbene in passato siano stati installati sistemi di rilevazione gas con sensori ridondanti o moduli indipendenti per i segnali in uscita, come richiesto per i sistemi di Sil-C 3, questa terminologia non era ancora in uso.
L'integrazione dei sistemi di rilevazione gas in un sistema di sicurezza globale offre la possibilità di effettuare un maggior numero di analisi dei rischi (ATEX 118a) e di gestire i rischi più efficacemente. Negli anni a venire saranno sempre più numerosi i sistemi di rilevazione gas specifici per applicazione.

Si ringrazia in questo il Dr. Wenker, noto esperto internazionale in materia di rilevazione gas, consulente e uno dei "padri" della presente norma EN 50402, per i suggerimenti, definizioni ed elenco delle norme in materia.

Classificazione delle applicazioni in base ai SIL-C, ai livelli SIL e alle Categorie
La normativa EN 50402 fornisce alcune indicazioni di massima su come integrare un sistema di rilevazione gas di SIL-C specifico in un sistema di sicurezza generale, conformemente a quanto indicato nella normativa EN 61508 (SIL) o EN 954-1 (Categoria).

Tuttavia, la normativa non fornisce indicazioni sul livello di sicurezza più idoneo alle singole applicazioni. In altre parole, la decisione se configurare il sistema di rilevazione gas di una raffineria come SIL-C 1, 2 e 3 spetta all'utente o alle autorità locali. Se un'applicazione specifica è associata a un SIL-C fisso, sarà possibile consultare la normativa per informazioni sulla tipologia di sistema di rilevazione gas più idonea.

La Sicurezza Funzionale secondo i SIL nella rivelazione gas
Lo scopo della sicurezza funzionale è quello di supervisionare il comportamento di un sistema in caso di guasti. La struttura di un sistema deve considerare tutti i possibili tipi di guasti che possono aver luogo in qualsiasi parte del sistema stesso. Le normative per la Sicurezza Funzionale definiscono dei livelli gerarchici di sicurezza da SIL 1 a SIL 4 e propongono suggerimenti su come evitare guasti (in fase di sviluppo) e su come creare delle tolleranze ai guasti (fault tolerance) nei sistemi di sicurezza.

Le Normative Generiche (Generic Standard) per la sicurezza funzionale IEC = EN 61508, che definiscono i requisiti da SIL 1 a SIL 4, sono impiegate nella sicurezza dei sistemi di controllo processi e rientrano nella Direttiva Macchine Europea.
Negli ultimi anni, vi è stata una crescente richiesta per portare a livelli SIL anche i sistemi di rivelazione gas. Poiché i "Generic Standard" sono per l'appunto molto generici, molto lunghi (divisi in 7 parti con oltre 1000 pagine) e molto complicati, lo specifico comitato CENELEC per la rivelazione gas decise di specificare i requisiti per la sicurezza funzionale di un sistema di rivelazione gas in uno standard Europeo dedicato, EN 50402, che è stato ora accettato dagli stati membri del CENELEC (votazione terminata il 31 Giugno 2005).

Questo standard si rivolge ai costruttori di apparati. La conformità allo standard farà parte dei test sui prototipi presentati presso i laboratori accreditati. In molti casi i requisiti potranno essere raggiunti se accompagnati da documentazione e argomentazioni tecniche dettagliate.

Nel caso dei singoli sensori, il fabbricante potrebbe non possedere tutti i requisiti utili o necessari a presentare una documentazione dettagliata, e non sarà quindi in grado di elevare il grado di SIL.

La filosofia di base dell'EN 50402
La EN50402 vuole essere una normativa per famiglie di prodotto per la rivelazione gas.
Ogni costruttore ha elaborato sistemi di rivelazione gas complessi e profondamente differenti nella loro struttura fisica (componenti hardware) - per es. sistemi che concentrano l'intelligenza del sistema in grosse centrali di controllo, sistemi misti con unità centrali e ulteriori sotto unità decentralizzate o sistemi completamente decentralizzati – così da non rendere possibile l'elaborazione di una definizione uniforme per uno standard che sia rappresentativo di tutti i tipi di sistemi.
Per tale motivo la EN 50402 divide i sistemi in moduli funzionali e specifica i requisiti di ogni singolo modulo. Questi moduli funzionali possono essere diversi nella loro struttura fisica (componenti).

Per ogni singolo modulo verrà valutata la capacità SIL (SIL-capability) secondo la specifica rispondenza allo standard. In seguito, si valuterà la specifica funzione di sicurezza, una combinazione specifica di moduli tra moduli d'ingresso (quelli a contatto con il gas) e moduli d'uscita (es. relè per l'azionamento di attuatori), e la capacità SIL verrà valutata in base a questa funzione. L'intera funzione di sicurezza – come in una catena di moduli – otterrà il livello di sicurezza della parte più debole della catena.

Moduli funzionali: i sistemi di rilevazione gas sono divisi in unità o moduli funzionali, poiché non possono essere genericamente classificati come apparati singoli. I componenti hardware, costituiti dai singoli componenti, possono differire significativamente. La bozza esamina i moduli in base alle funzioni che svolgono all'interno del sistema di rilevazione gas. A seconda delle caratteristiche costruttive, i moduli funzionali possono appartenere a categorie di componenti hardware diversi. La bozza descrive le seguenti unità funzionali:

- Campionamento gas (4 moduli distinti)
- Sensore (sensore e relativo circuito)
- Trasmissione segnali (2 moduli distinti)
- Ingressi a unità di controllo (5 moduli distinti, compresa alimentazione)
- Elaborazione dei segnali nell'unità di controllo (5 moduli distinti compreso le situazioni straordinarie)
- Uscite a unità di controllo (5 moduli distinti con indicatore opzionale)

Fault tolerance: la stima dei rischi viene effettuata confrontando la percentuale di guasti rilevanti ai fini della sicurezza con il totale dei guasti, relativamente ai requisiti di ridondanza stabiliti nella normativa EN 61508. I rischi sono suddivisi in rischi relativi a moduli semplici (guasti con caratteristiche prevedibili) e complessi (ad esempio microprocessore). Le probabilità di guasto sono state formulate tenendo conto delle esperienze passate con i sistemi di rilevazione gas nonché degli usi pratici della normativa EN 954-1 nell'ambito della direttiva macchine.

SIL-C di sistemi: i sistemi complessi comprendono alcuni moduli funzionali. Dopo aver stabilito la categoria SIL-C di ciascun modulo funzionale durante la fase di pre-test, è necessario stabilire la categoria SIL-C dell'intero sistema di rilevazione gas. Solo la funzione di sicurezza del sistema

viene presa in considerazione per tale determinazione, quale traguardo dalla rivelazione del gas agli output del sistema.
In altre parole, la resistenza della catena di sicurezza è pari a quella dell'anello più debole. La normativa spiega anche come combinare i moduli per poterli validare come catena o come configurarli in parallelo per ottenere un SIL-C specifico. Combinazioni diverse dei moduli, ad esempio basate su ridondanza, consentono di ottenere TIPI diversi per ciascuna funzione di sicurezza del sistema di rilevazione gas. Pertanto, sistemi di rilevazione gas con caratteristiche analoghe possono essere costituite da TIPI diversi a seconda della funzione di sicurezza usata.

Determinazione pratica del SIL.

La capacità SIL di un modulo si determina dalla combinazione di due termini tecnici:

la tolleranza guasti hardware (HFT, hardware fault tolerance) e il tasso di sicurezza (SFF, safe failure franction).

Tolleranza guasti hardware HFT.

Per HFT s'intendono le caratteristiche fisiche del modulo.

HFT = 0 Hardware singolo. Un singolo guasto potrebbe portare ad uno stato di non sicurezza

HFT = 1 Hardware ridondante. Nel caso di un guasto isolato in una catena hardware, una seconda unità continuerà a funzionare.

HFT = 2 Hardware triplo. Nel caso di un guasto isolato in una catena hardware, il sistema resta ridondante.
Nel caso di due guasti in diverse catene hardware, la terza unità continuerà a funzionare.

Restrizione:
Esiste una importante restrizione nei sistemi ridondanti qualora le catene ridondanti utilizzino hardware e software identici. Il SIL risultante da HFT 1 verrà raggiunto solo se i cosiddetti "guasti comuni" potranno essere esclusi. Un guasto comune danneggerà entrambe le catene ridondanti nello stesso modo. Un tipico esempio può essere quello di due pellistori ridondanti, entrambi avvelenati dalla presenza di silicone.

Una soluzione, spesso costosa tuttavia, per evitare tale restrizione è quella di usare hardware diversi, es. un pellistore ed un infrarosso. Due pellistori diversi non si comporterebbero in modo differente in caso di avvelenamento, mentre due tipi di celle elettrochimiche (per esempio un tipo standard ed uno appositamente modificato) potrebbero essere diverse, qualora il fabbricante di sensori fosse in grado di fornire la documentazione necessaria richiesta dai laboratori di certificazione.

Entrambi i punti, la restrizione e le diversità verranno riprese e discusse in questa trattazione per l'uso di sensori.

Tasso di sicurezza (SFF)
Per la valutazione dell'SFF si devono calcolare i vari tipi di guasti possibili.

Il totale dei guasti è la somma di 4 differenti tipologie di guasto:

- i guasti non pericolosi rilevati
- i guasti pericolosi rilevati
- i guasti non pericolosi non rilevati
- i guasti pericolosi non rilevati

L'SFF è la somma dei primi tre casi in percentuale sui guasti totali (considerando che il costruttore debba aver cura che guasti pericolosi rilevati non portino a situazioni di pericolo, dato che qualsiasi azione correttiva verrà presa dopo la rivelazione del guasto).

Tutti i moduli funzionali possono essere divisi in unità più piccole chiamate elementi. Allo stesso modo la capacità SIL sarà determinata per ogni singolo elemento separatamente. Il che significa che con una adeguata separazione degli elementi si potrebbe arrivare a determinare la capacità SIL del puro sensore (senza elettronica). Ovviamente il sensore potrà raggiungere questa capacità SIL se usato con un'elettronica idonea e in condizioni ambientali specifiche, ma di tutto questo si potrà discutere nella spiegazione delle condizioni di SIL.

Secondo la loro complessità i moduli possono essere classificati come "semplici" o "complessi". Nella EN50402 alcune tabelle aiutano a determinare la capacità SIL per entrambe le classificazioni. Inoltre, l'approccio della IEC 61511-1 viene spesso utilizzato per una pratica gestione di moduli semplici. Una parte importante dell'approccio della IEC 61511 è il termine "provato in uso" (proven in use) che, nel caso dell'esempio del sensore già riportato, significa che ci sono esperienze di uso pratico di almeno un anno.

Approccio di base della normativa EN 50402
L'approccio di base della bozza della nuova normativa è quello di fornire una descrizione univoca di sistemi di rilevazione gas complessi, che possono essere costituiti da componenti hardware diversi a seconda dei produttori. I sistemi di rilevazione gas sono specificatamente divisi in "moduli funzionali". Per ciascun modulo vengono specificati requisiti dettagliati, suddivisi per tipo di livello:SIL-C 1 – SIL-C 2.

SIL-C 1: i sistemi che appartengono a questo livello devono essere approvati con i metodi definiti nella normativa EN 61779 o in altre normative metrologiche. Gli interventi di manutenzione devono essere eseguiti conformemente a quanto indicato dal produttore. La sicurezza funzionale delle uscite allarmi e dell'alimentazione, e le procedure per l'elaborazione e la trasmissione dei dati devono essere conformi ai requisiti di altre normative metrologiche. Questi sistemi prevedono anche che venga eseguito un controllo di plausibilità sui dati immessi dall'utente; ad esempio prevedono la possibilità di impostare gli allarmi in un range di misurazione specifico.
Tutte le apparecchiature devono essere disposte in modo che l'eventuale interruzione dell'alimentazione o guasto consenta il passaggio immediato a una condizione di sicurezza. La procedura di sicurezza viene attivata manualmente o automaticamente in risposta a una condizione di allarme.

SIL-C 2: oltre alle caratteristiche dei sistemi di SIL-C 1, questi sistemi dispongono anche di funzioni diagnostiche hardware o software utilizzabili sia in fase di avvio che a richiesta dell'utente. La manutenzione deve includere il controllo di tutti i componenti critici ai fini della sicurezza.
A seconda delle applicazioni, è possibile anche che siano applicabili anche altre procedure operative; ad esempio riduzione degli intervalli di calibrazione per i sistemi utilizzati in condizioni ambientali gravose. Le funzioni operative speciali, attivate automaticamente in normali condizioni di funzionamento del sistema di rilevazione gas, vengono terminate e arrestate automaticamente. Le impostazioni dei parametri possono essere controllate mentre il sistema è in funzione.

SIL-C 3: oltre alle caratteristiche dei sistemi di SIL-C 2, questi sistemi prevedono che tutti i componenti del sistema di rilevazione gas connessi alla sicurezza, compresi i segnali di uscita, siano progettati n modo che un unico guasto non possa compromettere la funzione di sicurezza controllata dal componente in questione. Nei casi in cui ciò è possibile, questi sistemi devono consentire anche il rilevamento di guasti singoli.

NOTA 1: per soddisfare questo requisito, viene usato un livello di fault tolerance 1 (ridondanza).

NOTA 2: (EN 954-1: 6.2.4): il requisito relativo al rilevamento dei singoli guasti non significa che vengano rilevati tutti i guasti. Di conseguenza, l'accumulo di allarmi non rilevati può generare un segnale di uscita non previsto e provocare situazioni pericolose. Alcuni esempi tipici di misure pratiche che possono essere adottate per rilevare gli errori sono la gestione controllata dei contatti a relé o il monitoraggio delle uscite elettriche ridondanti.

SIL-C 4: oltre alle caratteristiche dei sistemi di SIL-C 3, questi sistemi devono essere in grado di rilevare tutte le condizioni di guasto. In caso di impossibilità di rilevare il guasto, è ammesso l'eventuale accumulo di guasti non rilevati, a condizione che ciò non comprometta le funzioni di sicurezza.

NOTA: l'analisi dei guasti può essere generalmente limitata ad una combinazione di tre guasti indipendenti.

Importanza del SIL e della EN 50402 in Europa e fuori dall'Europa
Gli standard generici IEC 61508 e IEC 61511-1 sono assolutamente identici agli standard Europei EN 60508 e EN 61511-1. In teoria questo significa che le specifiche riguardanti i SIL dovrebbero essere utilizzate in tutto il mondo nello stesso modo.

In generale l'interesse per i SIL è di primaria importanza nell'Industria Chimica dove le specifiche SIL sono già note poiché impiegate per il controllo dei processi. Molte joint ventures di industrie chimiche europee in Asia richiedono di avere sistemi rispondenti ai criteri di SIL.

Le specifiche SIL saranno discusse secondo i seguenti standard di sicurezza funzionale, EN 50402, IEC 61508 e IEC 61511-1. La EN 50402 e' da considerarsi l'unico Standard Europeo per i sistemi di rilevazione gas.

G.Frigo-Sensitron srl
www.sensitron.it

Nuova Sede dal 01/01/2006

Viale della Repubblica 48
20010 CORNAREDO (MILAN-ITALY)
Tel +39 02 93548155
Fax +39 02 93548089
Email: sales@sensitron.it
Web. www.sensitron.it