

## Approvazione di prodotti secondo IEC 61508 – un processo fuori rotta.

Fonte: ControlGlobal.com – Tutti i diritti in merito alla diffusione del presente scritto sono riservati agli autori.

Da un'analisi accurata appare che il processo di approvazione secondo IEC 61508 di prodotti e' andato essenzialmente fuori rotta, rendendo di fatto molte SIS ( Safety Instrumented Systems ) meno affidabili di quanto ipotizzato o desiderabile.

Di [Angela Summers](#), SIS-TECH, traduzione e note di [Dino Olivieri](#), ORI srl (Giugno 2009)

### SOMMARIO:

*A seguito di una disamina approfondita di un numero nutrito di manuali di sicurezza di prodotti certificati, appare chiaro che molti degli strumenti analizzati hanno ottenuto livelli di sicurezza funzionale (o SIL) molto piu' alti di quanto si possa supportare sulla base di solidi dati presenti nella letteratura industriale. L'appendice F.1.3 delle linee guida della CCPS (CCPS e' una sezione della AIChE, associazione americana degli ingegneri chimici, chiamata Center for Chemical Process Safety – n.d.t.) denominata "Linee Guida per Sistemi di protezione sicuri e affidabili", afferma come "una raccolta di dati su trasmettitori di pressione di vari costruttori riporti dei valori di intervallo medio di tempo tra fallimenti dannosi su domanda (MTTFD) da 3 a 10 volte migliori di quelli che sono i dati riscontrati sul campo da operatori/utilizzatori", e questi dati sono stati confermati da alcuni costruttori (3)*

*Sfortunatamente, le modifiche che sono attualmente allo studio presso il comitato della IEC 61508 non miglioreranno la situazione. Appare chiaro come il comitato sia piu' intento a prescrivere richieste addizionali piuttosto che a concentrarsi su debolezze strutturali esistenti all'interno della normativa stessa. L'unica soluzione sensata che rimane agli utilizzatori e operatori e' rifiutarsi di installare in applicazioni di sicurezza dei dispositivi che non abbiano gia' dimostrato in applicazioni similari e concrete in campo, anche se non direttamente rispondenti a funzioni di sicurezza, il loro livello di integrita' e affidabilita'. Gli utilizzatori dovrebbero fermamente richiedere che i costruttori smettano di millantare delle performance esagerate manipolando la SFF (Safe Failure Fraction, la SFF e' calcolata dal rapporto tra la somma di tutti gli errori sicuri e tutti gli errori dannosi ma riconoscibili prima che avvengano fratto la somma di tutti gli errori sicuri e di tutti gli errori dannosi non riconoscibili, n.d.t.) e spostando la responsabilita' della sicurezza sull'operatore dell'impianto quando i propri prodotti si comportano in modo non affidabile. Infine gli utilizzatori dovrebbero richiedere che i manuali di sicurezza includano delle procedure di test complete per verificare i valori pubblicizzati, in modo da rispondere alle esigenze delle normative IEC 61511 (5) e OSHA process safety management (PSM, 6).*

Analizziamo qui i diversi aspetti della questione.

### **1) Affermazioni esagerate sulla performance**

Prima dell'introduzione della IEC 61508, molti costruttori riportavano dati di failure sulla base di esperienze di campo o di test di cicli di durata accelerati. A seguito dell'approvazione della IEC 61508, si e' diffusa sempre piu' la tendenza dei costruttori di affermare la compliance alla normativa basandosi sull'analisi dei componenti in condizioni di fabbrica con delle condizioni operative ottimali. La IEC 61508 permette ai costruttori di affermare livelli di SIL basandosi su analisi predittive, senza il

compito poi di confermare queste analisi alla luce dei dati di campo acquisiti con l'esperienza diretta: in questo senso, i costruttori non fanno nulla di illecito. Bisogna però considerare che il rateo di guasti dannosi teorico, la Safe Failure Rate e la probabilità di fallimento su domanda (PFD) hanno valori molto migliori in questo tipo di analisi predittive rispetto a quanto viene poi verificato in campo. La distanza tra i valori derivanti dall'analisi teorica e la performance che viene poi riscontrata in campo nella realtà è davvero notevole (ragion per cui noi consigliamo sempre di dare più credito a valori derivanti da sistemi proven in use rispetto a quelli derivanti da analisi tipo FMEA magari riferite a sistemi che di fatto sono prototipi, n.d.t.)

Con rare eccezioni, questo tipo di analisi predittive non è in grado di fornire adeguate informazioni tali da illuminare sulla disparità che si riscontra tra i valori dichiarati dai costruttori e l'esperienza di campo degli utilizzatori, particolare rilevato dall'analisi effettuata da Thomas e altri (4) che riporta come "ci sia una mancanza di qualità e coerenza nei manuali di sicurezza". Queste analisi predittive non riportano una descrizione di quelle che sono le assunzioni in merito a installazione e configurazione dei sistemi, o alle modalità di guasto e la loro distribuzione. Al contrario, questi report forniscono delle tabelle soltanto sommarie sulla distribuzione delle classi di guasti. La questione che ne deriva è che mentre le modalità di guasto e relativi effetti sono relative ai prodotti e possono essere valutate indipendentemente dai costruttori, la classificazione dei guasti è dipendente dall'applicazione concreta.

Ci sono molti modi in cui un dispositivo può essere installato e configurato in campo, rendendo di fatto la classificazione delle modalità di guasto (guasti sicuri o non, n.d.t.) estremamente difficile per i costruttori, specialmente quando si tratta di costruttori di elementi comuni in impianto (commodity). Un costruttore non è in grado di determinare autonomamente se una modalità di guasto debba essere classificata come dannosa o sicura senza aver ottenuto prima una piena conoscenza dell'applicazione a cui il proprio dispositivo è destinato.

A titolo di esempio, in una configurazione di operazione in cicli (come ad esempio nelle valvole di blocco, servizio on-off, n.d.t.) dove una valvola solenoide controlli la fornitura di aria strumenti a un attuatore, il bruciarsi della bobina può essere classificato come guasto sicuro in un'applicazione dove l'attuatore debba comandare la valvola in chiusura per mancanza di energia, mentre sia un guasto dannoso nell'applicazione contraria. In una configurazione di operazione in continua (es: funzione di controllo, n.d.t.) tutti i guasti alle bobine di solenoidi hanno un'altra probabilità di essere guasti dannosi.

Si rimarca il fatto che agli utilizzatori dovrebbe essere data non soltanto una sintetica tabella che riassume la classificazione delle modalità di guasto, ma un dettaglio sulle modalità di guasto e i relativi effetti riferiti alla SIF. Con questi dati, gli utilizzatori potrebbero poi classificare essi stessi le modalità di guasto in rapporto alla loro specifica applicazione e calcolare delle PFD e dei valori di guasti spuri riferiti all'applicazione concretamente analizzata.

La maggioranza dei rapporti utilizzati per certificare i prodotti non definiscono concretamente lo scenario dell'applicazione per cui il prodotto è destinato, né descrivono cosa sia incluso o escluso dall'analisi. Per una serie di ragioni, escludono poi una gamma di guasti che accadono in servizio. Alcuni guasti vengono riferiti al naturale invecchiamento del prodotto e vengono esclusi dall'analisi sul ciclo di vita del prodotto. Gli impatti delle condizioni operative ambientali che portano ad esempio a occlusioni, corrosioni o interferenze elettriche, vengono considerate tematiche relative all'operazione dei sistemi e viene lasciato all'utilizzatore la responsabilità di analizzarli e stimarli. Il ristretto punto di vista sul prodotto e il suo ambiente di lavoro è la fonte primaria della disparità tra i dati pubblicati dai costruttori sulla base di studi predittivi (FMEA) e quanto poi si riscontra nella realtà, ma non è l'unico problema.

Si assiste spesso ad affermazioni assolutamente eccessive riguardanti la copertura diagnostica di elementi di campo elettronici e programmabili (PLC specialmente, ma anche elementi finali di loop di sicurezza HIPPS o ESD, n.d.t.). Pretese coperture diagnostiche sopra al 90% sono purtroppo molto comuni anche con assunzioni molto restrittive sull'effettivo campo di impiego. Il motivo è che, come sappiamo, una alta copertura diagnostica si traduca immediatamente nella possibilità di ottenere un SIL più elevato e una minore PFD. Tutto ciò ha senso soltanto nel caso in cui la diagnostica porti veramente a un'operazione in campo più sicura, e sia periodicamente comprovata la sua efficacia sulla base dell'esperienza concreta – regola che si applica a qualsiasi dispositivo di sicurezza. La diagnostica avanzata deve essere verificabile e comprovata.

Sfortunatamente, la gran parte dei sistemi di diagnostica forniti da costruttori (di elementi in funzione di sicurezza, n.d.t.) non e' in grado di essere testata in accordo ai paragrafi 11.3 (Requisiti di comportamento di un sistema in caso di scoperta di guasti) e 16.3.1.1. della IEC 61511 (test di verifica periodici devono essere effettuati sulla base di procedure scritte atte a rivelare guasti non riconoscibili che precludano al SIS la possibilita' di operare in accordo alle specifiche di sicurezza per le quali e' progettato). In aggiunta, generalmente i report generati considerando queste diagnostiche non forniscono informazioni sull'integrita' del prodotto nel caso in cui le diagnostiche stesse non siano configurate correttamente o non funzionino correttamente.

I manuali dei sistemi di sicurezza dovrebbero descrivere chiaramente i limiti di impiego e le assunzioni fatte in merito all'installazione, commissioning, configurazione, diagnostica, manutenzione e test che vengono fatti a supporto di affermazioni sul raggiungimento di determinati livelli di SIL. Senza queste informazioni e' molto difficile per gli utilizzatori rispettare il paragrafo 5.2.5.3 della IEC 61511 (che prescrive come procedure apposite debbano essere implementate per valutare la performance dei sistemi di sicurezza strumentata - SIS - in rapporto ai requisiti di sicurezza per i quali sono stati progettati) potendo quindi confrontare le assunzioni in merito all'affidabilita' dei sistemi di sicurezza in rapporto alle reali prestazioni durante il funzionamento in campo. Si rileva inoltre la necessita' che vengano incluse le modalita' di guasto ed effetto nei manuali di (operazione e, n.d.t.) manutenzione in modo tale da poter ricondurre a queste analisi i guasti che concretamente possono avvenire in campo e confrontarne gli effetti con le assunzioni contenute nelle analisi FMEA dei costruttori.

## **2. Manipolazione della SFF, rapporto di guasti sicuri.**

Il comitato della IEC 61508 ha introdotto il concetto di rapporto di guasti sicuri (o frazione sul totale) e le relative prescrizioni riguardanti la tolleranza ai guasti dell'hardware (e quindi la ridondanza sul numero degli elementi che compongono un loop di sicurezza, n.d.t.) dei sistemi di sicurezza in modo da non permettere ai costruttori di dichiarare alti livelli di SIL per sistemi non ridondati, basandosi soltanto sul calcolo matematico della PFD. Il motivo dell'introduzione delle tabelle relative alla SFF era il poter garantire una determinata tolleranza al guasto (attraverso i requisiti di ridondanza degli elementi) in una situazione generale in cui i dati usati per ottenere le PFD e le relative certificazioni apparivano (troppo, n.d.t.) ottimisti. (In pratica durante la stesura stessa della IEC 61508 era apparso subito chiaro che i costruttori di sistemi avrebbero trovato il modo di aggirarne il vero spirito e ridurre di fatto la certificazione di un determinato SIL a un calcolo astratto, senza la possibilita' di verificare in concreto che le architetture scelte per le SIF fossero rispondenti alle concrete richieste di sicurezza di impiego degli operatori, n.d.t.). Purtroppo, dato che la SFF viene calcolata comunque utilizzando gli stessi dati "inaffidabili", anche la SFF e' soggetta agli stessi errori.

In pratica, non c'e' correlazione tra la SFF e la reale sicurezza di un prodotto. Anzi, il fatto che sia piu' facile certificare secondo SIL 3 prodotti caratterizzati da un numero totale di guasti possibili alto, ma assumendo che sia possibile riconoscerli prima che avvengano dichiarando alti livelli di copertura diagnostica, rispetto alla possibilita' di certificare prodotti con un numero totale di guasti possibili basso (e quindi in assoluto piu' affidabili e preferibili, n.d.t.) ma non dotati di diagnostiche avanzate, dimostra esattamente il contrario. (e anche qui siamo di fronte a uno stravolgimento totale degli intenti della IEC 61508: un sistema progettato e costruito su solide basi ingegneristiche, magari meccanico, con positivi riscontri di campo, si vede "sorpassare" da sistemi basati su complicate architetture che prevedono software, sensori, diagnostiche avanzate, il tutto frutto di pianificazioni a tavolino, senza un qualsiasi tipo di esperienza concreta, n.d.t.).

Questo tipo di manipolazioni della SFF appare evidente dall'analisi di svariati manuali di strumenti di sicurezza. Parecchie analisi, in completo disaccordo con quello che era lo spirito della IEC 61508 e IEC 61511, hanno addirittura introdotto delle classificazione artificiose delle modalita' di guasto al fine di aumentare il valore di SFF. Contrariamente a quanto prescritto dalle citate normative (che classificano i guasti soltanto in guasti sicuri, tali cioe' da non impedire al SIS di attendere alla propria funzione di sicurezza e guasti non sicuri, n.d.t.), questi report introducono delle dubbie classificazioni di guasti quali "senza effetto", "residuali", "senza conseguenze" e "segnalazione non rilevata": tali classificazioni non sono discusse dalla IEC 61511 e non sono incluse in alcuna definizione di guasto. In alcuni di questi rapporti, queste modalita' di guasto sono definite in maniera del tutto approssimativa come "ne' sicuri ne' non". La IEC 61508 definisce un guasto come la cessazione della abilita' di un'unita' funzionale di eseguire una determinata funzione richiesta. Simili definizioni si trovano nella IEC 61511 e nelle linee guida del CCPS. Se un'unita' funzionale non ha avuto un guasto tale da portarla in un determinato stato - sicuro o pericoloso che sia - si suppone che sia ancora

funzionante, dato che non ha cessato di avere la capacita' di eseguire il suo compito. Al contrario, queste modalita' di "non-guasto" sono state fatte passare come guasti sicuri nella determinazione della SFF, di fatto accrescendone artificiosamente il valore.

La normativa IEC 61508 riconosce soltanto due modalita' di guasto, sicuri o non, quindi si deve ritenere che gli analisti considerino che qualsiasi modalita' di guasto che rappresenti una degradazione delle performance dell'elemento di sicurezza, sia essa sicura o non, debba essere considerata come un guasto sicuro. Ironicamente, sebbene questi "non guasti" siano generalmente inclusi nei calcoli della SFF, i vari rapporti raccomandano di non includerli nell'analisi dei guasti spuri.

Alcuni report definiscono la modalita' "segnalazione non rilevata" come un guasto del circuito diagnostico tale da non permettergli di comunicare un possibile guasto futuro. La semplice verita' e' che la mancanza di notifica di un guasto alla diagnostica comporta l'impossibilita' da parte dell'utilizzatore di essere in accordo al paragrafo 11.3.1. della IEC 61511, che identifica la necessita' di utilizzare test diagnostici, test di funzionamento o altre modalita' di rilevazione di guasti pericolosi. Guasti tali da compromettere la funzione di diagnostica non dovrebbero quindi essere considerati come sicuri, come invece accade da parte di analisti che sorprendentemente si rifanno alla IEC 61508 per giustificare le proprie affermazioni (e qui davvero non si capisce come possano farlo, n.d.t.).

Quando gli analisti computano queste "nuove categorie" di guasto come sicure, il prodotto ottiene una SFF piu' alta senza in realta' alcun vantaggio in termini di sicurezza reale. Questo trend e' seguito anche da costruttori di componenti meccanici, dove troviamo esempi di questi guasti "senza effetto" e per questo spesso delle SFF spesso maggiori del 60% o 90% richiesto per diminuire i requisiti architettonici di tolleranza al guasto secondo le tabelle della IEC 61508, tabelle 5 e 6. Spesso una (artificialmente, n.d.t.) alta SFF rende possibili architetture SIL 2 o 3 senza alcun requisito di ridondanza. (Secondo IEC 61511 invece, che ha un approccio piu' limitante e conservativo, la ridondanza e' comunque prescritta secondo il paragrafo 11.4.4, tabella 6, n.d.t.)

A titolo di esempio, un costruttore di valvole a globo con attuatore a diaframma affermava ottenere dei failure rate di  $9.356e-03/yr$  "senza conseguenze" a fronte di un valore di solo  $8.226e-03/yr$  computando solo i guasti sicuri e non, includendo di fatto piu' "non guasti" che il numero totale dei possibili guasti. La SFF calcolata considerando soltanto i guasti sicuri e non sicuri e' il 59.2%, il che la rende non idonea per ottenere un SIL 2 per componenti di tipo A. Considerando i guasti "senza effetto", la SFF balza all'80.9%, sufficiente ad ottenere un SIL 2. (Purtroppo le societa' di ingegneria e anche gli utilizzatori tendono a fidarsi troppo dell'asettico certificato ottenuto da questo o quel fabbricante grazie alla verifica dei dati operata da societa' di certificazione, che compiono spesso azioni ampiamente discutibili in termini di sicurezza reale e di vera analisi di cosa concretamente possa succedere a un dato elemento nel corso del suo ciclo di vita, in campo, in un'applicazione concreta. Da qui il nostro suggerimento di privilegiare sempre sistemi certificati sulla base di dati di campo, di sistemi "proven in use" al posto di risultati pompati al solo scopo di ottenere vantaggi commerciali, n.d.t.)

Tutto questo per denunciare come queste "nuove" modalita' di failure sembrano essere state create a valle dell'introduzione della IEC 61508 apposta per aumentare artificiosamente la SFF: rappresentano solo dei costrutti teorici, la vera antitesi di una solida ingegneria mirante alla sicurezza. Gli utilizzatori dovrebbero rigettare completamente (certificazioni di prodotti comprendenti, n.d.t.) tolleranze ai guasti basate su tali categorie di guasti e dovrebbero richiedere che i costruttori fossero in grado di provare concretamente le affermazioni in tematiche inerenti la sicurezza.

### **3. Tendenza a ribaltare sull'operatore la responsabilita' per l'esercizio in sicurezza di una SIF**

Svariati rapporti di certificazione SIL prevedono che le modalita' di guasto riconosciute vengano configurate per generare un allarme invece di porre lo strumento in sicurezza. Questa configurazione permette ai costruttori di componenti di dichiarare un rateo di guasti spuri molto basso e similmente un rateo di guasti dannosi non riconoscibili altrettanto basso, anche quando il prodotto di fatto non e' affidabile. Secondo i dettami della IEC 61508, un prodotto con un rateo di guasti totale alto puo' raggiungere un livello di SIL elevato soltanto quando i guasti siano riconoscibili e annunciati. Non e' prevista una penalizzazione sulla SFF per la circostanza in cui i guasti determinino una semplice segnalazione di allarme rispetto al portare l'elemento guasto in sicurezza. Ne consegue che con piu' guasti sono scoperti, maggiore e' la SFF, senza considerare il numero di accadimenti o il tempo in cui il componente si viene a trovare in condizioni di guasto, essenzialmente ribaltando la responsabilita' dell'operazione del processo sull'operatore (che deve quindi agire o gestendo questo segnale, o

prendendo delle decisioni che possono comportare dei downtime, a discapito della disponibilit  totale del sistema con ricadute pesanti in termini di produzione dell'impianto, ad esempio, n.d.t.).

La possibilit  di riconoscere un guasto significa semplicemente che l'operatore viene notificato che un componente non   pi  in grado di operare come richiesto (dalla relativa SIF, n.d.t.): il riconoscimento del guasto non riesce quindi a garantire o mantenere la sicurezza del processo. L'operatore viene messo di fronte a una seria decisione con pesanti conseguenze se decide di continuare a esercire il processo con un SIS degradato o non pi  in grado di garantire la sicurezza del processo: tale decisione deve essere supportata da adeguate misure di compensazione per continuare ad assicurare la sicurezza d'impianto e fornire il previsto fattore di riduzione di rischio sulla base del quale era stata progettato di inserire un determinato SIS. Bisogna considerare infatti come molti SIS vengono installati proprio perch  l'operatore non ha tempo sufficiente per prendere le decisioni richieste (es: HIPPS con tempo di chiusura <2", n.d.t.) o non   continuamente presente (es: sistemi di protezione di mini-piattaforme unmanned, n.d.t.) o non   in grado di garantire una risposta adeguata.

I costruttori che prescrivono la segnalazione dei guasti invece della messa in sicurezza dell'apparecchiatura guasta si espongono a sostanziali rischi, dato che semplicemente non possono avere le adeguate informazioni sull'operazione dei sistemi per poter fare simili raccomandazioni. Sfortunatamente, in quasi tutti i manuali di sicurezza analizzati si assume che ci sia un operatore sempre disponibile a intervenire e fare le veci dei sistemi di controllo di processo (BPCS) e/o dei sistema di sicurezza strumentati, in modo immediato al ricevimento di un segnale di guasto. Tali assunti sono ovviamente irrealistici e sarebbe preferibile che i costruttori si limitassero a fornire le analisi di guasto/effetto (FMEA) in modo "asettico", lasciando all'operatore valutare le reali conseguenze dei guasti analizzati sul processo e permettendogli di calcolare PFD e ratei di guasto spurio specifici per l'applicazione considerata.

#### **4. Mancanza di una corretta procedura di collaudo.**

L'utilizzatore deve validare e dimostrare periodicamente che le apparecchiature utilizzate operano secondo i requisiti di sicurezza specificati. Tale dimostrazione include la diagnostica, allarmi, operazione manuale e la sicurezza funzionale secondo IEC 61511 paragrafi 11.3, 16.2.2 e 16.3. Sfortunatamente, ben poche delle procedure di collaudo verificate rispondono ai requisiti dell'OSHA-PSM in merito all'effettuazione di test presenziati riguardanti la capacit  delle apparecchiature di rispondere alle esigenze delle funzioni di sicurezza.

La maggior parte dei manuali di sicurezza fornisce procedure di test funzionali parziali, con delle stime sulle coperture diagnostiche. Dato che non vengono fornite le modalit  di guasti e le distribuzioni di guasto, non   possibile determinare se i livelli di copertura diagnostica dichiarati siano ragionevolmente conservativi o quali guasti vengano o meno rilevati dai test funzionali. Come gi  rilevato in precedenza, le procedure di collaudo normalmente non considerano la diagnostica dei prodotti. Molti apparecchi hanno raggiunto alti livelli di SIL grazie a fattori di copertura diagnostica elevati: nonostante cio' metodologie e procedure per la verifica della diagnostica non sono fornite o discusse. (alzare il livello di copertura diagnostica dei test, aumentando la SFF, e' come abbiamo visto uno dei "trucchi" pi  frequenti, similmente all'uso del Partial Stroke Test per le valvole di blocco, dove si riesce "a tavolino" a migliorare la PFD con un fattore di 3, n.d.t.)

I manuali di sicurezza dovrebbero fornire delle procedure di test per verificare l'operativit  delle apparecchiature, incluso la diagnostica e le funzioni di allarme e trip. Test parziali e diagnostiche avanzate sono strumenti che permettono una validazione pi  frequente di un determinato sottoinsieme di modalit  di guasto, ma il loro uso non elimina il bisogno di un test funzionale completo. Fondamentalmente, devono essere verificabili tutti i livelli di protezione e quindi   necessario un test funzionale periodico al fine di verificare che non siano intervenuti guasti sistematici che abbiano compromesso la performance dei sistemi di sicurezza. Ciascun potenziale guasto non coperto da adeguati test   una condizione latente che puo' manifestarsi in qualsiasi momento del ciclo di vita dello strumento. Nessun utilizzatore dovrebbe approvare per una funzione di sicurezza uno strumento le cui modalit  di guasto non siano tutte verificabili in modo da garantire una piena operativit  e rispondenza ai requisiti di sicurezza.

#### **Passi successivi**

Un determinato processo opera in condizioni sicure quanto i componenti installati rispondano pienamente alle esigenze di operabilità, affidabilità e manutenibilità dell'utente finale. Non si può parlare di sicurezza quando si utilizzano apparecchiature non affidabili. La scarsa affidabilità delle apparecchiature accresce i costi di manutenzione, riduce la fiducia negli operatori verso l'apparecchiatura considerata e verso coloro che ne hanno curato le specifiche tecniche e da ultimo accresce il potenziale rischio di upset di processo, shutdown e in fase di avviamento. Gli utilizzatori finali devono verificare quale sia la performance di una data apparecchiatura in rapporto al loro caso concreto. A tal fine, la valutazione della certificazione sulla base di solidi dati di campo è essenziale per garantire la rispondenza ai requisiti di installazione, commissioning, collaudi e manutenzione richiesti dall'utente.

La motivazione di base dei problemi riscontrati nei manuali di sicurezza è la mancanza di conoscenza da parte dei costruttori di quali siano le reali necessità degli utilizzatori. I manuali osservati non contengono informazioni sufficienti per essere in accordo alla IEC 61511 o alle richieste dell' OSHA PSM. Per servire meglio gli utilizzatori finali, i costruttori dovrebbero compiere approfondite analisi sui propri prodotti e fornire adeguata documentazione sugli aspetti in merito all' installazione. Gli utilizzatori infatti richiedono più di una semplice tabella di numeri per poter verificare che lo scenario ipotizzato dal costruttore sia in linea con l'applicazione concreta. È responsabilità dei costruttori fornire "le informazioni fondamentali sulle cose di cui sono in controllo, permettendo agli utilizzatori di compiere le proprie valutazioni in modo efficiente e puntuale (4)". Al contrario, per la maggior parte dei componenti si fanno affermazioni (di performance, n.d.t.) esagerate basate su evidenze dubbie se non in alcuni casi sospette.

Sfortunatamente, pare che molte delle questioni qui trattate non verranno discusse in una prossima edizione della IEC 61508. Sarebbe caldamente consigliabile ai membri del comitato di prendere in considerazione seriamente modifiche alla IEC 61508 che portassero i costruttori verso prodotti sicuri e affidabili. Dovrebbe anche essere richiesto ai costruttori di fornire i dati completi delle FMEA comprensivi delle distribuzioni dei guasti, in modo da permettere agli utilizzatori di controllare le proprie modalità di guasto in relazione alle modalità definite. Dovrebbe anche essere chiesto loro di fornire i dati di campo in modo da poter verificare che le affermazioni dei costruttori trovino poi riscontro nella reale applicazione. I costruttori non dovrebbero considerare sicuro annunciare un guasto invece di forzare il componente a raggiungere il proprio stato sicuro. Essi dovrebbero inoltre riferire le modalità di guasto che possono essere riconosciute e permettere agli utilizzatori di determinare se sia appropriato o meno segnalarle con un allarme o con un trip, basandosi su una analisi di rischio compiuta sul processo. Da ultimo, i costruttori dovrebbero fornire procedure di test complete su tutte le funzionalità degli apparecchi, in modo da permettere agli utilizzatori di essere in accordo alle prescrizioni della IEC 61511 e OSHA PSM.

## Riferimenti

1. IEC 61508, Functional Safety of Electrical /Electronic/Programmable Electronic Safety Related Systems, Parts 1-7, Geneva, Switzerland (1999-2001).
2. Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, NY, (2007).
3. <http://www.emersonprocess.com/rosemount/solution/faq61508.html>
4. Thomas, Harold, David Deibert, David C. Arner, and David Weir, Air Products & Chemicals, Inc., "Safety Instrumented System Manuals-A Need to Balance Reliability and Safety," Process Safety Progress, Vol 27, No 1 (March 2008).
5. IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Geneva, Switzerland (2003).
6. OSHA, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR Part 1910." Federal Register 57, 36, Washington, DC (1992).