"Esperienza pratica nella applicazione delle analisi SIL (IEC 61508/61511) relative ai sistemi di sicurezza ad alta affidabilità, per uno stabilimento a rischio di incidente rilevante"

Barone D. 1, Damiani A. 1

1 Tecnologie Sicurezza Industriale S.r.l., Via P. Lomazzo 51, Milano, 20154, Italia

SOMMARIO

Scopo del lavoro è la descrizione di un'analisi SIL (Safety Integrity Level) effettuata in accordo alle norme IEC 61508 [1], IEC 61511 [2], per gli impianti di processo e gli stoccaggi presenti in uno stabilimento petrolchimico.
La valutazione del "SIL richiesto" per le funzioni di sicurezza (SIF - Safety Integrity Function) considerate, è stata effettuata utilizzando una matrice dei rischi desunta da uno standard di una multinazionale del settore petrolchimico.
Successivamente, per le stesse funzioni di sicurezza (SIF) è stato stimato il livello di SIL esistente ("SIL installato"), ovvero l'affidabilità del sistema di blocco presente, tenendo conto della strumentazione di sicurezza installata (SIS- Safety Integrity Systems).

Il confronto tra i valori di "SIL richiesto" e di "SIL installato" ha mostrato che per la gran parte delle funzioni SIF analizzate, il livello del "SIL installato" è uguale o superiore al "SIL richiesto", cioè l'affidabilità del sistema di blocco esistente è adeguato a garantire il livello di sicurezza necessario.

Per le limitate funzioni SIF che non hanno soddisfatto il suddetto requisito di SIL sono stati proposti degli adeguamenti tecnici di tipo strumentale oppure procedurale al fine di allineare i valori di "SIL installato" al "SIL richiesto".

1.0 GENERALITA'

Lo Standard internazionale IEC 61508, relativo alla sicurezza funzionale dei componenti elettrici, elettronici, ed apparecchiature elettroniche programmabili, risale alla metà degli anni 80 quando l'International Electrotechnical Committee Advisory Committee of Safety (IEC ACOS) si attivò per considerare la standardizzazione dei risultati derivanti dall'utilizzo dei sistemi elettronici programmabili. In quel tempo diversi organismi normativi proibivano per i sistemi di sicurezza critici, l'applicazione di componenti basati su software. Il lavoro iniziò all'interno del IEC SC65A/ Gruppo di Lavoro 10, su uno standard per i sistemi elettronici programmabili utilizzati nei sistemi collegati alla sicurezza. Questo gruppo si unì successivamente con il Gruppo di Lavoro 9, nel quale era in corso di approntamento uno standard per la sicurezza dei software. Il gruppo derivante trattò la sicurezza come un aspetto del sistema. Lo Standard è diviso in sette parti

Lo Standard IEC 61511 è stato sviluppato come implementazione per l'industria di processo, dello Standard IEC 61508. Lo standard presenta due concetti fondamentali per la sua applicazione: la sicurezza nel ciclo di vita ed il SIL (Safety Integrity Level). La sicurezza durante il ciclo di vita costituisce la struttura centrale la quale collega tra loro la maggior parte dei concetti di questo standard internazionale. Esso rappresenta una buona procedura di ingegneria per la progettazione dei sistemi strumentati di sicurezza (SIS: Safety Instrumented System). Nella sicurezza durante il ciclo di vita vengono valutati i rischi di processo e vengono stabilite le prestazioni della strumentazione di Sicurezza (disponibilità e riduzione del rischio). Vengono progettate ed analizzate "barriere di protezione" ed alla fine, se risulta necessaria una strumentazione di sicurezza, essa sarà progettata tenendo conto del particolare rischio di processo. I SIL sono ordini di grandezza dei livelli di riduzione dei rischi. Esistono quattro livelli SIL nello standard, come in IEC 61508, SIL 1 ha il più basso livello di riduzione dei rischi, SIL 4 il più alto, come mostrato nella tabella che segue.

Tabella 1. Livelli di SIL

Safety Integrity Level	***Probabilità di mancato intervento su domanda***
SIL 4	$\geq 10^{-5}$ e $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ e $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ e $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ e $< 10^{-1}$

Lo standard riferisce che le applicazioni dove è richiesta una sola funzione di sicurezza (SIF) con SIL 4, sono rare nell'industria di processo e dove ragionevolmente praticabile esse devono essere evitate. Lo standard riguarda principalmente la strumentazione di Sicurezza (SIS) dell'industria di processo (sensori, logiche di blocco, ed elementi finali delle strumentazione di sicurezza), inoltre, lo standard tratta la relazione tra la strumentazione di sicurezza ed altri sistemi di sicurezza, al fine della valutazione dei rischi di processo e dell'effettuazione del risk assessment.

Le analisi SIL (Safety Integrity Level) secondo IEC 61511 sono ormai applicate durante la progettazione dei nuovi impianti petrolchimici e di raffinazione, al fine di tenersi aggiornati allo stato dell'arte in materia di affidabilità dei sistemi di blocco automatico. Lo stesso approccio è utilizzato per le modifiche di impianti esistenti.

Anche per gli impianti esistenti e non soggetti a modifiche può tuttavia essere utile o necessaria una valutazione del grado di affidabilità dei sistemi di blocco automatico presenti, al fine di verificare la congruenza degli stessi allo stato dell'arte.

2.0 METODOLOGIA UTILIZZATA

Per effettuare la valutazione del livello di integrità per la Sicurezza (SIL) di un sistema di blocco automatico predisposto per la protezione di un impianto/apparecchiatura dal superamento di un parametro critico (es. altissima pressione, altissimo/bassissimo livello, altissima temperatura,,…), occorre innanzitutto individuare le funzioni di sicurezza (SIF, Safety Instrumented Function), ossia le azioni strettamente sufficienti a garantire la messa in sicurezza dell'impianto.

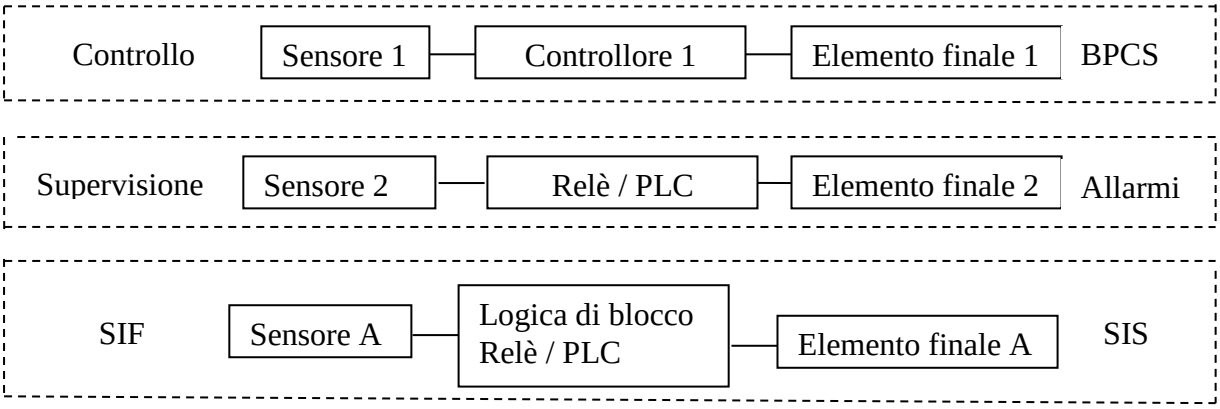
Tale selezione delle funzioni di sicurezza (SIF) può essere effettuata tenendo conto di quanto riportato nei documenti di riferimento disponibili per gli impianti/apparecchiature, quali ad esempio:

- Schemi di processo (PFD)
- P&ID di impianto
- Diagrammi Causa & Effetto dei sistemi di blocco

Per l'individuazione delle SIF può inoltre essere richiesto il supporto di personale con esperienza nelle diverse discipline come processo, sicurezza, strumentazione, esercizio.

Nella figura che segue si riporta la schematizzazione del funzionamento di un possibile assetto per le funzioni di controllo (BPCS, Basic Process Control System), di allarme (supervisione) e di blocco di sicurezza (SIF), utilizzabili nell'esercizio di impianto di processo.
Come si può notare le tre funzioni sono fisicamente indipendenti tra loro e tra esse non esistono condivisioni di dati, di informazioni, di componenti, di sistemi di supporto, di interfacce con l'operatore, né interfacce di ingegneria.

Figura 1. Funzioni di controllo, Supervisione, Blocco di Sicurezza



In questo caso la distinzione tra le tre funzioni è chiara e facilmente comprensibile, rispetto ad altri assetti in cui esistono parti condivise (es. allarmi o blocchi attivati dal controllore di processo). La totale indipendenza tra le funzioni di controllo, di allarme, e blocco, fa si che per quest'ultimo sia generalmente richiesto un SIL inferiore rispetto al caso in cui le funzioni di allarme e/o blocco sono condivise con il sistema di controllo.

In accordo alla IEC 61511, il livello di integrità per la Sicurezza SIL delle Funzioni di Sicurezza (SIF) può essere determinato utilizzando una matrice riassuntiva dei rischi (frequenze e conseguenze) riportata in Figura 2. Tale matrice è stata selezionata da uno standard di una multinazionale del settore petrolchimico.

Figura 2. Matrice dei rischi

<table>
<tr><th>Frequenza

Conseguenza</th><th>A
Quasi impossibile</th><th>B
Molto improbabile</th><th>C
Improbabile</th><th>D
Bassa Probabilità</th><th>E
Probabile</th><th>F
Frequente</th></tr>
<tr><td></td><td>$< 10^{-4}$ [yr^{-1}]</td><td>$10^{-4} – 10^{-3}$ [yr^{-1}]</td><td>$10^{-3} – 10^{-2}$ [yr^{-1}]</td><td>$10^{-2} – 0{,}1$ [yr^{-1}]</td><td>$0{,}1 – 1$ [yr^{-1}]</td><td>> 1 [yr^{-1}]</td></tr>
<tr><td>1 Sicuro</td><td colspan="5" rowspan="4">Nessun requisito SIL</td><td rowspan="5">Analisi di affidabilità. Modifiche alla progettazione dei sistemi di processo o di controllo</td></tr>
<tr><td>2 Lievemente Pericoloso</td><td>SIL 1</td></tr>
<tr><td>3 Pericoloso</td><td colspan="2">SIL 1</td><td>SIL 1</td><td>SIL 2</td></tr>
<tr><td>4 Critico</td><td colspan="2">SIL 1</td><td>SIL 2</td><td>SIL 3</td></tr>
<tr><td>5 Catastrofico</td><td>SIL 1</td><td>SIL 1</td><td>SIL 2</td><td>SIL 3</td><td>SIL 3</td></tr>
</table>

Safety Integrity Level	*Probabilità di mancato intervento su domanda*
SIL 4	$\geq 10^{-5}$ e $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ e $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ e $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ e $< 10^{-1}$

Nelle colonne della matrice (Figura 2) sono riportate le frequenze stimate per l'intervento del sistema di blocco in esame, quest'ultimo considerato come l'ultima barriera utilizzabile per la protezione dal superamento del parametro critico.

I valori delle frequenze possono essere stimati in maniera qualitativa oppure in maniera quantitativa, utilizzando metodologie come ad esempio quella degli alberi di guasto.

Nelle righe della matrice (Figura) 2 si riportano i livelli delle conseguenze del mancato intervento dei sistemi di blocco, così come definiti nella Tabella 2 che segue. Essi rappresentano gli effetti sulle persone, sull'ambiente, sugli impianti, in caso del superamento del parametro critico e mancato intervento di tutte le barriere protettive, incluso il sisma di blocco automatico oggetto della valutazione SIL. Al fine di stabilire i livelli delle conseguenze possono essere utilizzati, ove disponibili, le valutazioni degli effetti di eventuali scenari incidentali derivanti dal superamento del parametri critico.

Tabella 2. Classificazione conseguenze

Livelli	Conseguenze sulle persone	Conseguenze sull'ambiente	Conseguenze sugli impianti	
			Descrizione	Costi (€)
5 Catastrofico	Molti decessi	Danni con tempo di recupero maggiore di 5 anni	- Grandi danni agli impianti, completa distruzione dell'impianto. - Cessazione della produzione	> 10 M
4 Critico	Un decesso	Danni con tempo di recupero inferiore a 5 anni	- Grandi danni alle apparecchiature, rotture delle principali apparecchiature di processo, reattori, linee - Grandi perdite di produzione o qualità	< 10 M
3 Pericoloso	Danni permanenti	Danni con tempo di recupero inferiore a 2 anni	- Danni considerevoli alle apparecchiature, rotture, ecc. - Considerevoli perdite di produzione o qualità	< 1 M
2 Lievemente pericoloso	Trattamento medico	Danni non permanenti	- Danni minori alle apparecchiature. Incendi di estensione limitata, emissione di sostanze infiammabili, tossiche o ad alta temperatura, ecc. - Piccole perdite di produzione o qualità	< 0.1 M
1 Sicuro	Primo soccorso	Danni insignificanti	- Danni non significativi, piccoli rilasci di acqua, aria, azoto, vapore, ecc. - Nessuna perdita di produzione o qualità	< 10000

Per ciascuna funzione di sicurezza (SIF) analizzata viene elaborato un foglio di analisi SIF. Nel foglio si riporta la descrizione della funzione di sicurezza, la descrizione dello scenario stimato in caso di mancato intervento del blocco in esame, il livello di conseguenza dello scenario secondo quanto riportato in Tabella 2, la frequenza di accadimento dello scenario in occ./anno, il rischio ed il livello "SIL richiesto" per il sistema di blocco secondo la matrice dei rischi in Figura 2.

La maggior parte dei SIL di un impianto di processo sono generalmente SIL 0 ovvero SIL 1 (affidabilità $\geq 10^{-2}$ e $< 10^{-1}$) e sono realizzabili mediante una logica di blocco del tipo 1/1 cioè un sensore, una logica di blocco a relè, un attuatore costituito da elettrovalvola e valvola di intercettazione. L'intervallo di test è pari ad 1 anno.
Solo in casi di rischio particolari, come quelli connessi ai Parametri Operativi Critici (POC), possono essere richiesti SIL 2, realizzabili ad esempio mediante sensori logica 2/3 , logica di blocco a relè, attuatori in logica 1/2.

3.0 APPLICAZIONE

Per uno stabilimento petrolchimico nel quale sono presenti ca. 15 impianti di processo, 150 serbatoi di stoccaggio atmosferici, 30 serbatoi in pressione, sono state analizzate complessivamente ca. 30 funzioni di sicurezza (SIF-Safety Integrity Systems, esempio alta pressione nelle apparecchiature, alto/basso livello nei recipienti, alta temperatura nelle linee,…) presenti sia negli impianti, sia negli stoccaggi. La selezione delle funzioni di sicurezza è stata effettuata prendendo in considerazione gli scenari incidentali più gravosi contenuti nel rapporto di sicurezza.

Per ciascuna SIF è stato valutato il livello "SIL richiesto" al sistema di blocco automatico esistente, ossia l ' "affidabilità richiesta" al sistema di blocco al fine di rendere accettabili/tollerabili i rischi connessi al funzionamento dello stesso.
I risultati della valutazione del SIL richiesto sono stati riassunti in specifici fogli, come rappresentato nella Tabella 3 relativa ad una delle ca. 30 funzioni analizzate.

Tabella 3. Esempio foglio di analisi SIF

Funzione di Sicurezza: SIF 1 - Altissima temperatura combustore B 101
TT 121 A/B (logica 1/2), attivazione logica I 01 - Chiude XV 010 e 012 (gas ai bruciatori) e apre XV 011 (spurgo intermedio) - Chiude XV 027 aria di combustione
Scenario: Altissima temperatura in B 101
Possibile collasso termico combustore, danno strutturale, rilascio prodotti
Conseguenza: 4 Critico
Grandi danni alle apparecchiature (< 10 M €), possibili effetti sulle persone
Frequenza:
- Gas di processo ricco di H_2S (1 occ./anno) - Apertura impropria FC 066 (gas di combustione) (0,1 occ./anno) Totale 1,1 occ./anno Mancato intervento protezioni - Allarme di alta temperatura sul combustore proposto, indipendente ($5 \cdot 10^{-3}$) Totale $5{,}5 \cdot 10^{-3}$ occ./anno (C – Improbabile)
Rischio: 4C
Figura 2 - Matrice dei rischi
SIL: 1
Figura 2 - Matrice dei rischi
Riferimento:
P&I 0015-03, rev.01
Note:
La valutazione del SIL richiesto è stata effettuata considerando l'installazione di un allarme di alta temperatura indipendente su B 101. E' necessario rendere indipendente il blocco dal loop di regolazione della temperatura

Come si può desumere matrice riassuntiva (Figura 3), la maggior parte delle funzioni (SIF) analizzate richiede livelli di sicurezza più bassi: SIL 0 (affidabilità $\geq 10^{-1}$) oppure SIL 1 (affidabilità $\geq 10^{-2}$ e $< 10^{-1}$) come si evince dalla seguente ripartizione:

~ 30 % SIL 0;
~ 62 % SIL 1;
~ 8 % SIL 2.

Figura 3. Matrice riassuntiva Funzioni di Sicurezza (SIF) analizzate

Frequenza / **Conseguenza**	**A** **Quasi impossibile**	**B** **Molto improbabile**	**C** **Improbabile**	**D** **Bassa probabilità**	**E** **Probabile**	**F** **Frequente**
	$< 10^{-4}$ [yr^{-1}]	$10^{-4} – 10^{-3}$ [yr^{-1}]	$10^{-3} – 10^{-2}$ [yr^{-1}]	$10^{-2} – 0{,}1$ [yr^{-1}]	$0{,}1 – 1$ [yr^{-1}]	> 1 [yr^{-1}]
1 Sicuro						Analisi di affidabilità. Modifiche alla progettazione dei sistemi di processo o di controllo
2 Lievemente pericoloso			SIF 10			
3 Pericoloso	SIF 11 SIF 19 SIF 22	SIF 2	SIF 5, SIF 6 ,SIF 9 SIF 16 , SIF 21, SIF 25			
4 Critico		SIF 4 SIF 8 SIF 18	SIF 1, SIF 7, SIF 12, SIF 13, SIF 15, SIF 17 SIF 20, SIF 24, SIF 27			
5 Catastrofico	SIF 3 SIF 14		SIF 23 SIF 26			

Nessun requisito SIL

SIL 1

SIL 2

SIL 3

Il SIL 2 (affidabilità $\geq 10^{-3}$ e $< 10^{-2}$) è richiesto solamente per un numero limitato di funzioni esaminate. Non sono state individuate funzioni che richiedono livelli di sicurezza SIL 3 (affidabilità $\geq 10^{-4}$ e $< 10^{-3}$) né funzioni che richiedono livelli SIL 4 (affidabilità $\geq 10^{-5}$ e $< 10^{-4}$).

Successivamente, per ciascuna delle ca.30 funzioni di sicurezza (SIF) è stato stimato il livello di SIL esistente ("SIL installato"), ovvero l'affidabilità del sistema di blocco presente, tenendo conto della strumentazione di sicurezza installata (SIS- Safety Integrity Systems). La stima del "SIL installato" è stata effettuata sulla base dell'affidabilità dei diversi componenti che intervengono nel funzionamento del blocco automatico (elementi primari, logiche, elementi finali) utilizzando ratei di guasto desunti da letteratura specializzata di riconosciuta validità.
A titolo di esempio, nella Tabella 4 si riportano le caratteristiche strumentali della SIF 1 precedentemente descritta (Tabella 3). E' indicata l'affidabilità del blocco automatico esistente ("SIL installato") e viene effettuato un confronto tra il requisito di SIL richiesto (Tabella 3) ed il SIL installato, indicando, gli adeguamenti tecnologici per rendere compatibili i due valori di SIL (il SIL installato deve essere ≥ del SIL richiesto) .

Tabella 4. Esempio caratteristiche strumentali SIF

SIF 1	Unità di processo: Combustore B101		
1 Scenario incidentale (conseguenze, cause / incidente iniziale)			
1.1 Descrizione dell'incidente: Collasso termico bruciatore, danno strutturale			
1.2 Descrizione delle cause / dell'incidente iniziale: Aumento di pressione nel bruciatore e conseguente aumento di temperatura per eccesso di reazione			
2 Rischio (conseguenze e frequenze senza misure / dispositivi di sicurezza)			
		Conseguenze (1-5)	Frequenze (A-F)
2.1 Personale		-	-
2.2 Ambiente		-	-
2.3 Perdita di produzione, qualità, costi materiale / riparazioni		Critico 4	Improbabile C
3 Requisiti SIL			
Totale	SIL 1 ($\geq 10^{-2}$ e $< 10^{-1}$)		
Strumentazione	TT 121 A/B (logica 1/2) attivazione logica I 01		
Attuatori elettromeccanici	- Chiude XV 010 e 012 (gas ai bruciatori) e apre XV 011 (spurgo intermedio) - Chiude XV 027 aria di combustione		
Altre misure di riduzione del rischio	Allarme di alta temperatura indipendente su B 101 (proposto)		
4 Funzioni di sicurezza / misure riduzione del rischio			
4.1 Strumentazione			
4.1.1 Sensori		Funzione: Altissima temperatura combustore B 101	
	Struttura	Trasmettitori di temperatura 4 ÷ 20 mA – soglia elettronica	
	Intervallo test / controllo	1 anno	

4.1.2 Unità logica		Riferimento:
	Tipo	PLC per sicurezza
	Struttura	Fail safe
	Diagnosi	Autodiagnosi
	Affidabilità	3,5 10^{-3}
	Intervallo di test	1 anno
4.1.3 Elementi finali		Localizzazione:
	Struttura attuatori	Elettrovalvole
	Intervallo test / controllo	1 anno
4.1.4 Stima dell'affidabilità: Sensore ($4{,}19\cdot10^{-3}$) , PLC ($3{,}5\cdot10^{-3}$) , Elettrovalvola ($7{,}7\cdot10^{-3}$) , Valvola di blocco ($8\cdot10^{-3}$) . Affidabilità 1.94 10^{-2} (SIL 1)		
4.2 Sicurezza parti meccaniche		
4.3 Altre misure riduzione rischi		Allarme di alta temperatura indipendente su B101 (proposto)
5 Raccomandazioni / commenti: Per rendere congruente il SIL installato con il SIL richiesto è necessario rendere indipendente il blocco dal loop di regolazione della temperatura e installare allarme di alta temperatura (indipendente da DCS) su B101		

Dal confronto tra i valori di "SIL richiesto" e del "SIL installato" per tutte le ca. 30 funzioni SIF analizzate, è stato riscontrato che per gran parte di esse, il livello del "SIL installato" è uguale o superiore al "SIL richiesto", cioè l'affidabilità dei sistemi di blocco esistenti è adeguato a garantire il livello di sicurezza necessario.
Per le limitate SIF che non hanno soddisfatto il suddetto requisito di SIL sono stati proposti degli adeguamenti tecnici di tipo strumentale oppure procedurale al fine di allineare i due valori di SIL.

Di seguito si riassumono le tipologie degli adeguamenti proposti :

- rendere indipendente dal DCS (regolazione) le logiche di funzionamento di alcuni allarmi critici e di alcuni sistemi di blocco automatici
- installare alcuni nuovi allarmi indipendenti con soglia di intervento anticipata rispetto al blocco automatico esistente
- effettuare il test degli elementi finali di blocco con frequenza semestrale anziché annuale
- ridefinire alcune logiche di blocco esistenti, prevedendo la ridondanza degli elementi finali, in alcuni casi installando nuovi elementi finali .

4.0 CONCLUSIONI

Negli impianti di processo di nuova realizzazione e per quelli più datati oggetto di recenti revamping, la strumentazione di sicurezza presente è generalmente sufficiente a soddisfare i livelli di SIL richiesti ai sistemi di blocco. In molti casi tuttavia per ottenere i livelli di sicurezza richiesti è necessario intervenire per rendere completamente indipendenti (anche fisicamente) la seguente strumentazione: regolazione di processo (BPCS) , allarmi critici, sistemi di blocco automatico (SIS). In pochi casi è richiesta l'installazione di strumentazione aggiuntiva rispetto a quella esistente.

Per gli impianti soggetti alla normativa sul controllo dei pericoli di incidenti rilevanti è importante conoscere l'affidabilità dei sistemi di sicurezza presenti; molto spesso le analisi di affidabilità come quelle contenute negli studi SIL sono effettuate facendo uso di tassi di guasto ricavati da banche dati o da letteratura tecnica specializzata, relativi a strumenti simili a quelli installati negli impianti in esame. E' opportuno verificare, specialmente per le funzioni di sicurezza a protezione dei parametri operativi critici, la possibilità di disporre di dati di affidabilità specifici del sito, sia per gli allarmi critici, sia per i sistemi di blocco critici.
Tali valori possono essere ricavati dall'analisi delle prove (test) effettuate periodicamente da tempo sugli allarmi/blocchi critici e dalle relative schede di prova ove sono riportati i casi di mancato funzionamento su domanda.

RIFERIMENTI

1. IEC 61508 – Functional Safety of Electrical /Electronic/Programmable Electronic Safety Related System
2. IEC 61511– Functional Safety - Safety Instrumented System for the Process Industry Sector
3. ISA S.84.01 – Functional Safety - Safety Instrumented System for the Process Industry Sector