Sistemi strumentali di Sicurezza

La stima della probabilità media di guasto

Francesco Paolo Nigri
Ingegnere, Tecnologo

Il contributo, prendendo in considerazione gli effetti negativi che il tempo esercita sull'affidabilità dell'intera catena di sicurezza, spiega come calcolare la PFD_{AVE} del sistema strumentale di sicurezza, e cioè il valore medio che la probabilità istantanea di guasto PFD(t) assume nel periodo di osservazione.

Alcuni mesi or sono, la redazione di "Ambiente & Sicurezza sul Lavoro" mi chiese di sviluppare una serie di articoli riguardanti la sicurezza funzionale. Se avessi trattato l'argomento nella maniera più tradizionale, e cioè per mezzo di un'esposizione meramente analitica, il lavoro sarebbe stato praticamente inutile perché pochi lettori ne avrebbero apprezzato il contenuto.

Ho dovuto, perciò, inquadrare le diverse sfumature della sicurezza funzionale in modo più semplice, affidandomi in gran parte alle immagini, nell'ottica secondo la quale "un vedere" vale "cento sentire". Ciò nonostante, non ho potuto evitare del tutto il ricorso all'analisi matematica, senza la quale alcuni concetti, che sono alla base della sicurezza funzionale, non possono essere pienamente compresi.
Mi piace riassumere brevemente il lavoro fin qui svolto, in modo che siano più chiare le sue finalità.
Negli articoli precedenti, pubblicati nei numeri di maggio e ottobre, ho inteso dimostrare come i sistemi strumentali di sicurezza (SIS) contribuiscano efficacemente alla riduzione del rischio di processo di un impianto tecnologico.
Nel primo articolo, ho messo in evidenza la differenza fra:

1. un sistema di controllo basico del processo (Basic Process Control System, BPCS);
2. un sistema strumentale di sicurezza (Safety Instrumented System, SIS).

Entrambi i sistemi sono specificamente progettati in relazione alle esigenze del particolare impianto tecnologico nel quale devono essere inseriti. Mentre, però, il primo è un sistema sempre attivo, al quale si affida il controllo continuo delle variabili di processo, il secondo sistema resta dormiente per la maggior parte della sua vita operativa. Il SIS, infatti, è chiamato a intervenire solo nel momento in cui una delle variabili di processo sfugge al controllo del BPCS. Non occorre che un processo tecnologico sia particolarmente complicato perché le caratteristiche peculiari di un SIS risultino evidenti: un SIS può essere applicato con successo a un complesso reattore chimico oppure a un recipiente in pressione destinato al contenimento di fluidi pericolosi.
Nel primo articolo[1], ho dimostrato che la comprensione del corretto comportamento di un SIS può essere immediatamente afferrata sfruttando uno dei concetti di base della sicurezza funzionale: la probabilità di guasto su richiesta, e cioè la c.d. PFD (Probability of Failure on Demand).

Del primo articolo mi piace richiamare la tabella 1 (vedi pag. seguente) per completezza di esposizione.

1. «La sicurezza funzionale applicata agli impianti di processo: Principi di base», F.P. Nigri, in *Ambiente&Sicurezza sul Lavoro,* maggio 2019

Probability of Failure on Demand	Risk Reduction Factor	SIL
0,01 < PFD ≤ 0,1	10 ≤ RRF < 100	1
0,001 < PFD ≤ 0,01	100 ≤ RRF < 1000	2
0,0001 < PFD ≤ 0,001	1000 ≤ RRF < 10000	3

Tabella 1 - Correlazione fra PFD, RRF e SIL richiesto

Per comprendere la ragione per la quale la PFD rappresenta il concetto più importante, sebbene non unico, su cui si basa la stima del livello di affidabilità di un SIS, conviene fare un semplice esempio numerico, assumendo quale riferimento i valori di tabella 1. Se il valore della PFD è 0,01, allora è uguale a 100 il fattore di riduzione del rischio (RRF) introdotto dal SIS. Un sistema strumentale di sicurezza in grado di abbattere così pesantemente il rischio di processo, stante la validità della tabella 1, deve essere caratterizzato da un valore del SIL (Safety Integrity Level) pari a SIL2.
Nel secondo articolo[2], facendo ricorso alla c.d. "Route 1H" dell'IEC 61508, ho evidenziato i valori ottimali:
1. della frazione dei guasti sicuri (SFF);
2. della tolleranza ai guasti hardware (HFT),

che consentono ai vari componenti di un sistema strumentale:
1. sensore;
2. controllore logico programmabile;
3. attuatore finale,

di garantire, all'intera catena di sicurezza, il conseguimento di un grado di affidabilità corrispondente a SIL2.
Terminata la stesura dei primi due articoli, sono rimasto io stesso alquanto sorpreso dalla novità degli aspetti ingegneristici che ne erano scaturiti: gli articoli hanno il pregio di proiettare l'attenzione del lettore su una disciplina innovativa, la sicurezza funzionale, che presenta tecniche avveniristiche di progettazione, realizzazione e manutenzione dei sistemi di sicurezza degli impianti tecnologici.
Nel secondo articolo, ho fatto espressamente riferimento a un recipiente in pressione installato in uno stabilimento a rischio di incidente rilevante, e cioè soggetto all'applicazione della direttiva Seveso. In tale contesto, tutt'altro che raro nel nostro paese, facendo appello alla tecnica LOPA (Layers Of Protection Analysis), ho dimostrato che al sistema strumentale di sicurezza, inserito nell'impianto insieme ad altre misure di mitigazione per garantire il raggiungimento del desiderato valore di riduzione del rischio, si richiede proprio un SIL2. Il risultato conseguito, anche se significativo da un punto di vista tecnico, non è sufficiente sotto il profilo dell'affidabilità. Infatti, affermare che un sistema di sicurezza è caratterizzato da SIL2 non ha alcun significato in affidabilità. Dire, invece, che un sistema di sicurezza è caratterizzato da SIL2 dopo un anno di funzionamento ha perfettamente senso.
È necessario, pertanto, verificare che il sistema strumentale di sicurezza in esame mantenga nel tempo un livello di affidabilità cui corrisponde un SIL2, e cioè una "probabilità media di guasto su richiesta (PFD_{AVE})" non superiore a 0,01, fino al "primo test manuale di controllo" che si prevede di eseguire, a impianto fermo, dopo un intero anno solare (8760 hr). In altri termini, è giunto il momento di prendere in considerazione gli effetti negativi che il tempo esercita sull'affidabilità dell'intera catena di sicurezza. A tale scopo, non resta che calcolare la PFD_{AVE} del sistema strumentale di sicurezza, e cioè il valore medio che la probabilità istantanea di guasto PFD(t) assume nel periodo di osservazione. Questa è la finalità del terzo articolo riguardante l'applicazione della sicurezza funzionale agli impianti tecnologici.

Richiami di teoria dell'affidabilità

L'IEC 61508-6 propone equazioni semplificate per calcolare la PFD. In questa sede, si ritiene opportuno chiarire come tali equazioni siano state ricavate richiamando brevemente alcuni fondamentali concetti di Affidabilità.

2. «Sistemi strumentali di Sicurezza Riferimenti e metodi per verificare il livello di affidabilità», F.P. Nigri, in *Ambiente&Sicurezza sul Lavoro,* ottobre 2019

Nell'arco della vita operativa, nessun componente è immune da guasti. In qualsiasi momento può verificarsi un guasto che impedisce al componente di funzionare correttamente. La rapidità con la quale il componente perviene al guasto è in relazione con il c.d. "tasso di guasto λ". I fabbricanti ricavano il valore del tasso di guasto λ mediante speciali test di durata (stress test), eseguiti su un numero N sufficientemente elevato di componenti.
Si supponga che, al tempo t:
N_g componenti siano affetti da un guasto;
N_f componenti siano ancora funzionanti.

Il tasso di guasto è definito dal rapporto tra il numero di componenti guasti dopo un tempo t e il numero dei componenti ancora in funzione allo stesso tempo:

$$\lambda = \frac{N_g(t)}{t \cdot N_f(t)} \quad (1)$$

Il tasso di guasto è, dunque, una funzione del tempo:

$$\lambda = \lambda(t)$$

È possibile definire l'Affidabilità R(t) di un componente, al tempo t, utilizzando la seguente relazione:

$$R(t) = \frac{N_f(t)}{N} \quad (2)$$

dove N rappresenta il numero totale di componenti in osservazione.
La percentuale dei componenti in avaria, istante per istante, è data dalla seguente relazione:

$$F(t) = \frac{N_g(t)}{N} \quad (3)$$

Tale percentuale corrisponde alla Probabilità istantanea di guasto, che è pari al 100% nell'istante T in cui tutti i componenti cessano di funzionare (figura 1).

In altri termini:

$$N_g(t) = N$$

Per un istante di tempo t < T, risulta evidentemente che:

$$N_g(t) = N - N_f(t)$$

Per cui si ottiene:

$$F(t) = \frac{N - N_f(t)}{N} = 1 - \frac{N_f(t)}{N} \quad (4)$$

Tenendo conto della (2), si ha:

$$F(t) = 1 - R(t) \quad (5)$$

È possibile introdurre un'importante semplificazione se si accetta la costanza nel tempo del tasso di guasto, e cioè:

$$\lambda = \cos\tan te\,.$$

Ciò equivale a considerare il componente in quello stato di funzionamento che corrisponde alla sua maturità e va sotto il nome di "vita utile". Tale condizione di funzionamento, caratterizzata dal verificarsi di "guasti casuali o accidentali", segue il periodo della c.d. "mortalità infantile" e precede quello in cui predomina il cedimento per usura (figura 2). Nell'ipotesi che λ sia costante nel tempo, si dimostra che l'Affidabilità R(t) del componente ha un andamento "esponenziale negativo" in funzione del tempo:

$$R(t) = e^{-\lambda t} \quad (6)$$

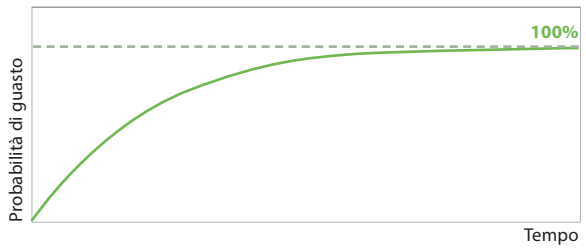

Figura 1 - Andamento nel tempo della Probabilità istantanea di guasto (Drager)

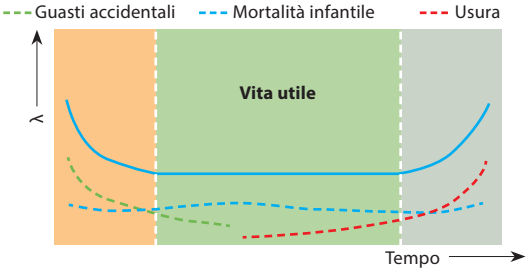

Figura 2 - Andamento del tasso di guasto λ in funzione del tempo

La dimostrazione rigorosa della validità della relazione (6) esula, per mera carenza di spazio, dalle finalità di questo lavoro. Immediata conseguenza della validità della relazione (6) consiste nel fatto che la Probabilità istantanea di guasto F(t) può essere così espressa:

$$F(t) = 1 - e^{-\lambda t} \quad (7)$$

In questo contesto, la Probabilità istantanea di guasto F(t) può essere immediatamente associata alla Probabilità di guasto su richiesta PFD(t), che è un parametro introdotto dall'IEC 61508:

$$F(t) = PFD(t) \quad (8)$$

$$PFD(t) = 1 - e^{-\lambda t} \quad (9)$$

Se si considera che l'unico guasto in grado di incidere sulla PFD(t) è quello "pericoloso non rilevato (DU)", nella (9) si può ritenere:

$\lambda = \lambda_{DU}$ = costante.

Pertanto, nel seguito, ogni volta in cui si darà cenno della PFD(t), si intenderà sempre fare riferimento alla c.d. "Probability of Dangerous Failure".

$$PFD(t) = 1 - e^{-\lambda_{DU} t} \quad (10)$$

Se si esamina attentamente l'andamento della PFD(t) riportato in figura 3, ci si accorge che si può ritenere accettabile la seguente approssimazione:

$$PFD(t) = \lambda_{DU} \cdot t \quad (11)$$

solo qualora risulti:

$$PFD(t) \leq 0{,}1 \quad (12)$$

Se si prende nuovamente in esame la tabella 1, ci si accorge, infine, che non ha senso considerare valori della PFD maggiori di 0,1. Infatti, per tali valori (PFD > 0,1), la tabella 1 non consente alcuna attribuzione del SIL. Valori di PFD maggiori di 0,1 non sono, quindi, rilevanti ai fini dei calcoli di affidabilità. Questa semplice considerazione fa comprendere che, nel caso in esame (PFD ≤ 0,1), è pienamente giustificata l'approssimazione introdotta dalla relazione (11).

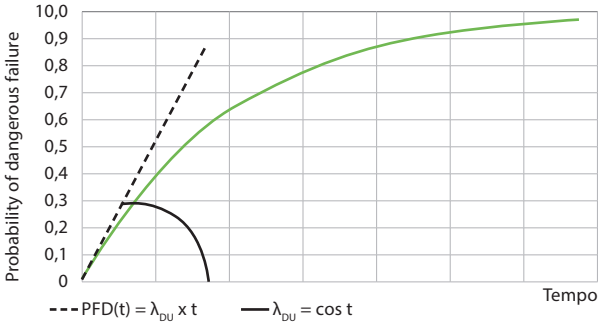

Figura 3 - Andamento semplificato (lineare) della PFD in funzione del tempo

Equazioni semplificate per il calcolo della PFD_{AVE}

L'IEC 61508-6 considera un intervallo di tempo i cui estremi corrispondono rispettivamente:

1. all'istante iniziale di osservazione (t = 0);
2. all'istante che coincide con l'inizio del primo test manuale di prova (t = T1).

L'ampiezza di tale intervallo di tempo definisce la cadenza con la quale saranno eseguite le successive prove manuali, che sono finalizzate a mettere in luce i guasti pericolosi non rilevati dalla diagnostica interna delle apparecchiature elettroniche, inserite nei sistemi di sicurezza dell'impianto. Nell'intervallo di tempo così definito, l'IEC 61508-6 procede al calcolo del valore medio (PFD_{AVE}) della probabilità istantanea di guasto PFD (t).

In termini rigorosi, la PFD_{AVE} si ricava a partire dalla seguente relazione:

$$PFD_{AVE} = \frac{1}{T1} \cdot \int_0^{T1} PFD(t) \cdot dt \quad (13)$$

Le considerazioni sviluppate nel paragrafo precedente consentono di attribuire alla probabilità istantanea di guasto PFD(t) l'espressione semplificata dettata dalla relazione (11):

$$PFD_{AVE} = \frac{1}{T1} \cdot \int_0^{T1} \lambda_{DU} \cdot t \cdot dt \quad (14)$$

Il calcolo dell'integrale definito porta al seguente risultato:

$$PFD_{AVE} = \frac{1}{T1} \cdot \frac{\lambda_{DU} \cdot T1^2}{2} \quad (15)$$

In definitiva, si ottiene:

$$PFD_{AVE} = \frac{1}{2} \cdot \lambda_{DU} \cdot T1 \quad (16)$$

Ciò significa che, mediamente, un guasto pericoloso resta "non rilevato" per un tempo la cui ampiezza è pari alla metà dell'intervallo di ampiezza T1. La relazione funzionale (16), proposta dall'IEC 61508-6 per il calcolo della PFD_{AVE}, è stata ricavata dall'estensore della norma con considerazioni analoghe a quelle appena esposte.

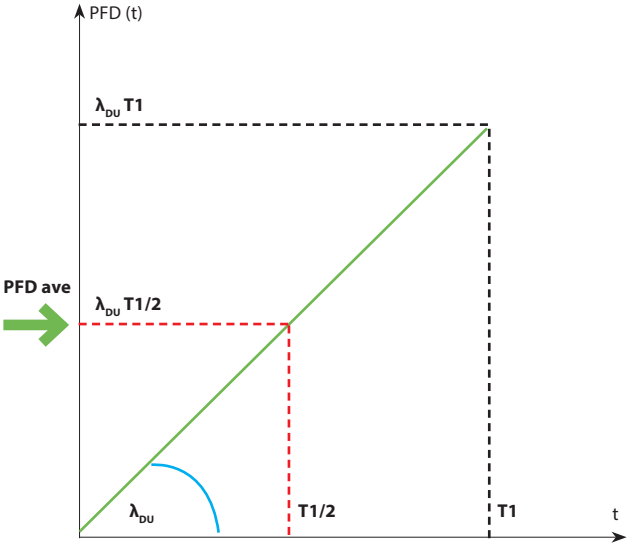

Figura 4 - Valore medio PFD_{AVE} della PFD (t) nell'intervallo [0; T1]

Se si considera, infine, che il componente necessita di riparazione, dopo che è stato rilevato il guasto pericoloso nel corso del test di prova, allora si intuisce che occorre tenere conto anche del tempo richiesto dalle operazioni di riparazione del componente. L'ampiezza di questo ulteriore intervallo di tempo, che l'IEC 61508-6 definisce "Mean Time To Restoration (MTTR)", viene assunta, per convenzione, pari a un'intera giornata lavorativa (8 hr).

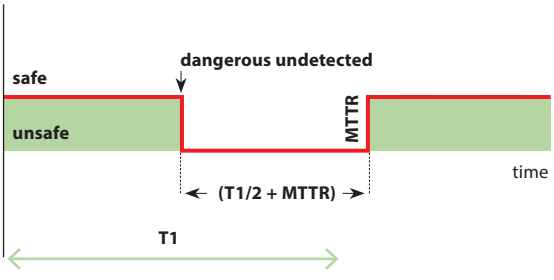

Figura 5 - Tempo medio di permanenza del componente di sicurezza nello stato "unsafe" (Drager)

Calcolo della $PFD_{AV}E$ di un sistema di sicurezza con architettura del tipo "1oo1"

La Probabilità media di guasto su richiesta di un sistema di sicurezza (SIS) con "architettura 1oo1 (senza ridondanze)" è calcolata sommando la Probabilità media di guasto su richiesta dei vari componenti:

1. sensore;
2. controllore di pressione;
3. attuatore finale.

$$PFD_{AVE,SIS} = PFD_{AVE,SENS} + PFD_{AVE,PRESS.CONTR} + PFD_{AVE,ACT} \quad (17)$$

Se si ricorda che il tasso dei guasti pericolosi λ_D equivale alla somma del tasso dei guasti pericolosi rilevati λ_{DD} e del tasso dei guasti pericolosi non rilevati λ_{DU}:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad (18)$$

allora il singolo componente (device) del sistema di sicurezza può essere riguardato come composizione logica di due elementi in serie:

1. il primo caratterizzato dal tasso di guasto λ_{DU};
2. il secondo caratterizzato dal tasso di guasto λ_{DD}.

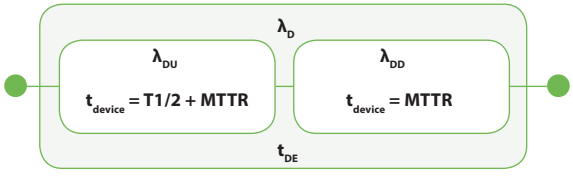

Figura 6 - "Reliability block diagram" di un componente di sicurezza (device) con "architettura 1oo1"

Ricorrendo a questo semplice artifizio concettuale e sommando i tempi di "permanenza in avaria" dei singoli "sotto-elementi" in cui il singolo componente può essere scisso, l'IEC 61508 risale facilmente al c.d. "t_{DE} (Device Equivalent mean downtime)", e cioè al tempo medio durante il quale il componente non è in grado di rispondere con successo alla richiesta di intervento dell'impianto:

$$t_{DE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (19)$$

Noto dalla (19) il valore di t_{DE}, si passa rapidamente al calcolo di PFD_{AVE} per ogni componente del sistema di sicurezza in esame:

$$PFD_{AVE} = (\lambda_{DU} + \lambda_{DD}) \cdot t_{DE} = \lambda_D \cdot t_{DE} \quad (20)$$

Per dare continuità al mio lavoro, ho ritenuto opportuno fare riferimento allo stesso sistema strumentale di sicurezza preso in esame nel numero di ottobre. I valori del tasso di guasto espressi in FIT (Failure In Time), che competono ai singoli componenti del sistema di sicurezza, sono stati ordinatamente riportati nella riga 2 della tabella 2.

device	sensor	press. controller	actuator
λ (FIT)	7700	3300	9900
λ_S (FIT)	3850	1650	4950
λ_D (FIT)	3850	1650	4950
D_C (%)	60	90	60
λ_{DD} (FIT)	2310	1485	2970
λ_{DU} (FIT)	1540	165	1980

Tabella 2 - Valori dei tassi di guasto del sistema strumentale

Nel seguito, per facilità, sono brevemente richiamati i simboli di tabella 2, che sono in linea con la simbologia adottata dall'IEC 61508:

1. $\boldsymbol{\lambda_S}$: tasso dei guasti sicuri;
2. $\boldsymbol{\lambda_D}$: tasso dei guasti pericolosi;
3. $\boldsymbol{D_C}$: copertura diagnostica (Diagnostic Coverage of dangerous failures);
4. $\boldsymbol{\lambda_{DD}}$: tasso dei guasti pericolosi rilevati dalla diagnostica interna;
5. $\boldsymbol{\lambda_{DU}}$: tasso dei guasti pericolosi non rilevati dalla diagnostica interna.

Fatto questo inciso, utilizzando la relazione (20), i valori di PFD_{AVE} dei singoli componenti del sistema di sicurezza sono stati ricavati per due differenti valori di T1:

1. T1 = 1 anno (8760 hr);
2. T1 = 6 mesi (4380 hr).

Nel primo caso (T1 = 1 anno), i valori della PFD_{AVE} sono stati riportati nell'ultima riga di tabella 3, nella quale in valori dei tassi di guasto sono espressi in hr^{-1}.

Sommando i valori della PFD_{AVE} che figurano nell'ultima riga della tabella 3, si ottiene il valore di PFD_{AVE} che compete all'intera catena di sicurezza:

$$PFD_{AVE} = 6{,}78 \cdot 10^{-3} + 7{,}36 \cdot 10^{-4} + 8{,}71 \cdot 10^{-3} = 1{,}62 \cdot 10^{-2}$$

(T1 = 1 anno)

Se il primo test manuale di prova viene effettuato dopo un anno solare (8760 hr), la Probabilità media di guasto su richiesta del sistema di sicurezza, caratterizzato da architettura del tipo 1oo1, non soddisfa il livello di affidabilità imposto dal processo, pari a SIL2. Tale conclusione è più chiara se si analizza la figura 7, che riporta l'andamento della PFD in funzione del tempo.

Nel secondo caso (T1 = 6 mesi), i valori della PFD_{AVE} sono stati riportati nell'ultima riga di tabella 4.

Sommando i valori della PFD_{AVE} che figurano nell'ultima riga della tabella 4, si ottiene il valore di PFD_{AVE} che compete all'intera catena di sicurezza:

$$PFD_{AVE} = 3{,}40 \cdot 10^{-3} + 3{,}75 \cdot 10^{-4} + 4{,}38 \cdot 10^{-3} = 8{,}15 \cdot 10^{-3}$$

(T1 = 6 mesi)

Il livello di affidabilità imposto dal processo, corrispondente a SIL2, è soddisfatto solo se il primo test manuale di prova è eseguito dopo sei mesi dalla messa in esercizio dell'impianto.

device	sensor	press. controller	actuator
voting	1oo1	1oo1	1oo1
λ_{DU} (hr^{-1})	1,54E-06	1,65E-07	1,98E-06
λ_{DD} (hr^{-1})	2,31E-06	1,49E-06	2,97E-06
λ_D (hr^{-1})	3,85E-06	1,65E-06	4,95E-06
T_1 (hr)	8760	8760	8760
MTTR (hr)	8	8	8
t_{DE} (hr)	1,76E+03	4,46E+02	1,76E+03
PFD_{AVE}	6,78E-03	7,36E-04	8,71E-03

Tabella 3 - Valori di PFD_{AVE} per T1 = 1 anno (8760 hr)

device	sensor	press. controller	actuator
voting	1oo1	1oo1	1oo1
λ_{DU} (hr^{-1})	1,54E-06	1,65E-07	1,98E-06
λ_{DD} (hr^{-1})	2,31E-06	1,49E-06	2,97E-06
λ_{D} (hr^{-1})	3,85E-06	1,65E-06	4,95E-06
T_1 (hr)	4380	4380	4380
MTTR (hr)	8	8	8
t_{DE} (hr)	8,84E+02	2,27E+02	8,84E+02
PFD_{AVE}	3,40E-03	3,75E-04	4,38E-03

Tabella 4 - Valori di PFD_{AVE} per T1 = 6 mesi (4380 hr)

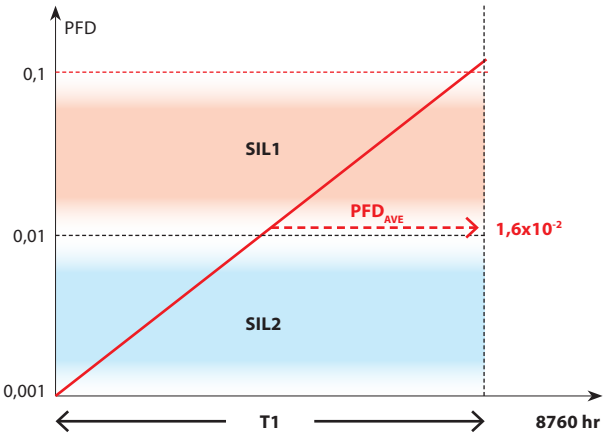

Figura 7 - PFD_{AVE} del sistema di sicurezza con architettura 1oo1 (T1 = 1 anno)

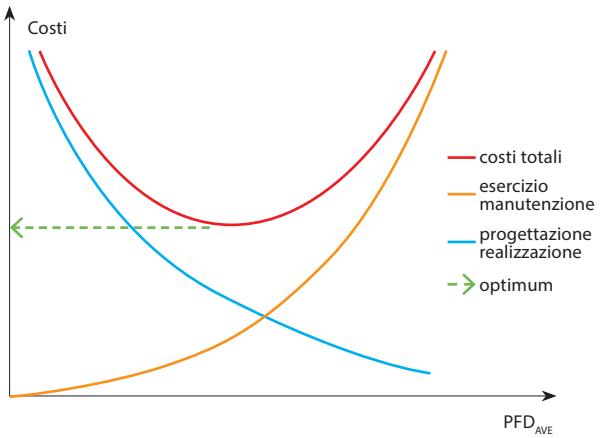

Figura 8 - Determinazione grafica dell'optimum dei costi totali di impianto

Conclusioni

L'esperienza maturata in campo impiantistico consente di affermare che, all'aumentare della PFD_{AVE}, ossia al diminuire del livello di affidabilità del sistema di sicurezza (SIL), aumentano i costi di esercizio e manutenzione, mentre diminuiscono quelli legati a progettazione e realizzazione. Al diminuire del SIL, infatti, diminuiscono i costi legati alla complessità del sistema di sicurezza che, in genere, richiedono uno sforzo progettuale e realizzativo non trascurabile.

La ricerca del c.d. "optimum dei costi totali" porta a prediligere sistemi di sicurezza i cui costi di manutenzione non siano fortemente sbilanciati, come certamente lo sono quelli di un sistema di sicurezza sul quale i test di prova manuali devono essere eseguiti con cadenza semestrale, peraltro a impianto fermo. Può risultare conveniente optare per l'adozione di un sistema di sicurezza provvisto di "canali ridondati".

Quando si introduce il concetto di "ridondanza", nel campo dell'affidabilità è inevitabile il riferimento alle c.d. "architetture MooN (**M o**ut **o**f **N**)". Un "sistema MooN" è composto da "N canali indipendenti", connessi fra loro in modo tale che almeno "M" di questi siano sufficienti per eseguire la funzione di sicurezza richiesta (SIF). Normalmente, le tipiche architetture MooN previste per i sistemi di sicurezza inseriti in impianti di processo sono le seguenti:

1. 1oo1: architettura singola senza ridondanza (votazione 1 su 1);
2. 1oo2: duplicazione parallela, corrispondente a una logica di tipo "OR" con riferimento all'algebra di Boole. ■

RINGRAZIAMENTI

L'autore esprime il più sincero ringraziamento al Prof. Pasquale Erto, che ha avuto modo di apprezzare durante il corso di "Affidabilità" erogato, nel lontano 1984, agli allievi della Facoltà di Ingegneria dell'Università degli Studi di Napoli "Federico II".