

Introduzione alla norma IEC 61508 e al concetto di Safety Integrity Level (SIL)

a cura di Davide Conti, A&D AS



In data 22 Marzo 2006 si è tenuto a Milano un corso dal titolo “IEC 61508 – Metodologie di calcolo del SIL: teoria ed esempi pratici; l'utilità del Partial Stroke Test”.

Questo elaborato vuole essere un'introduzione alla norma e una illustrazione dei concetti alla base della definizione di livello di integrità del sistema di sicurezza (SIL).

Verrà, infine, fatto un accenno anche all'utilità dei test parziali (Partial Stroke Test) come metodo per ridurre i fermi impianto per scopi di manutenzione pur mantenendo un accettabile livello di sicurezza.

1 Concetti fondamentali

1.1 Sistemi di sicurezza

Si supponga di avere un **Sistema Tecnico** costituito da un serbatoio T contenente liquido destinato a raffreddare, per esempio, un reattore. La scarsità

di liquido all'interno del serbatoio stesso può portare ad un mancato raffreddamento del reattore stesso con conseguente pericolo per le persone (addetti, abitanti nelle vicinanze) e l'ambiente. In via secondaria sono da considerare anche danni all'impianto stesso.

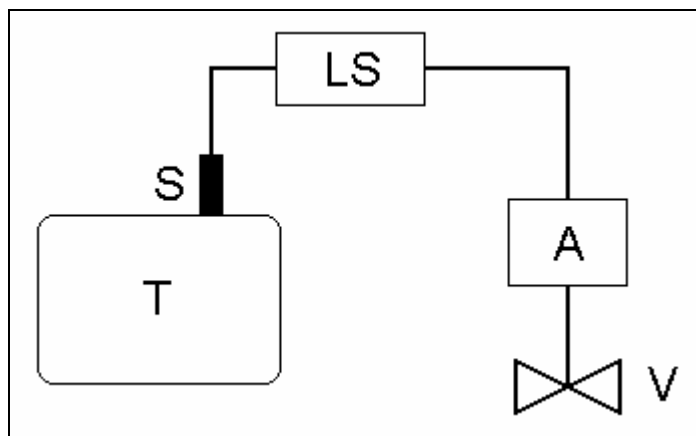


Figura 1-1: Sistema tecnico e sistema di sicurezza

Tutto ciò costituisce un **Rischio**, cioè la possibilità che si verifichi un evento con conseguenze pericolose.

Va precisato come il concetto di “rischio” sia diverso da “probabilità”: a differenza della probabilità, che esprime una misura della possibilità che si verifichi un certo evento (pericoloso), il rischio esprime la possibilità che si verifichi un determinato evento in combinazione con la gravità delle conseguenze di tale evento. Ne consegue che un evento dalle conseguenze modeste, ma fortemente probabile, può avere lo stesso livello di rischio di un evento dalle gravi conseguenze, ma con scarse probabilità di accadere. Così sebbene la folgorazione derivante da fulmine sia molto meno probabile di quella causata da corrente domestica, è ugualmente rischiosa essendo i livelli di tensione (e quindi i livelli di pericolo) molto più elevati.

Chi costruisce e gestisce il sistema tecnico deve accertare che il rischio introdotto da quest'ultimo (surriscaldamento del reattore e relative conseguenze) non sia superiore a quanto socialmente accettabile. Nel caso in cui ciò non sia verificato dovranno essere prese misure mirate a ridurre il rischio a livelli accettabili. In particolare i pericoli causati da attrezzature tecniche devono essere inferiori ai rischi esistenti in natura.

Nel caso in esempio una possibile misura di riduzione di rischio può essere l'introduzione di un sistema **ESD (Emergency Shut Down)** costituito da un sensore di livello S, un logic solver LS e una o più valvole V con i relativi attuatori A: quando il sensore rileva un livello troppo basso nel serbatoio la logica di

controllo comanda gli attuatori in modo tale che le valvole arrestino la reazione portando il sistema in condizioni di sicurezza.

L'insieme costituito dal sensore, il logic solver, gli attuatori e le relative valvole costituiscono un **Sistema Strumentale di Sicurezza** e garantiscono la **Sicurezza Funzionale** dell'impianto.

1.2 Affidabilità del sistema di sicurezza

È però ragionevole supporre che l'affidabilità del sistema non sia totale, nel senso che ogni singolo elemento può subire guasti che compromettano la funzionalità del sistema di sicurezza: errata misura del livello da parte del sensore, errore nell'elaborazione della logica di sicurezza, incollaggio delle valvole...

Si rende dunque necessario definire un **grado di affidabilità del sistema di sicurezza**. Tale grado di affidabilità dovrà essere compatibile con i livelli di rischio introdotti dal sistema tecnico: per livelli di rischio crescenti l'affidabilità del sistema di sicurezza dovrà crescere di conseguenza. In altre parole dovrà essere ridotta la probabilità di un guasto del sistema di sicurezza che possa portare l'impianto in una situazione di pericolo per mancato intervento dell'arresto di emergenza.

Nella definizione del grado di affidabilità dovrà anche rientrare la capacità del sistema di individuare eventuali guasti mediante **test (parziali o completi) e diagnostiche**: entrambi questi strumenti permettono, infatti, di rilevare in anticipo eventuali anomalie, evitando che queste ultime possano condurre ad un mancato intervento del sistema di sicurezza e quindi ad una situazione pericolosa.

2 IEC 61508 e SIL di un sistema di sicurezza

2.1 Concetto di SIL e sua scelta in relazione all'applicazione

La norma IEC 61508 definisce quattro livelli di **Safety Integrity Level (da SIL1 a SIL4)**, ciascuno dei quali definisce una misura quantitativa della necessaria riduzione del rischio e quindi il grado di affidabilità che il sistema di sicurezza deve raggiungere per poter garantire tale riduzione.

È di carattere generale, applicabile a tutti i sistemi correlati alla sicurezza indipendentemente dall'applicazione (trasporti, produzione, ...).

La norma copre tutte le fasi di vita del sistema di sicurezza, dalla fase di progetto a quella di esercizio e manutenzione fino allo smaltimento e si applica a tutti i sistemi di sicurezza in cui almeno uno dei componenti incorpori dispositivi elettrici, elettronici o elettronici programmabili.

La norma non definisce il SIL da raggiungere in funzione della specifica applicazione: questa operazione deve essere fatta mediante un'analisi di rischio del sistema tecnico in oggetto e una valutazione del rischio accettabile, come combinazione della probabilità e del livello di pericolo.

È importante ricordare, inoltre, che il SIL è relativo alla singola funzione di sicurezza e non all'intero impianto o ai singoli componenti.

All'interno di un determinato impianto esisteranno numerose funzioni di sicurezza ciascuna delle quali relativa ad un determinato pericolo a cui andrà associato un appropriato SIL. L'insieme dei componenti (e non questi ultimi presi singolarmente) di ogni sistema di sicurezza dovrà essere tale da rispettare la classe SIL da raggiungere.

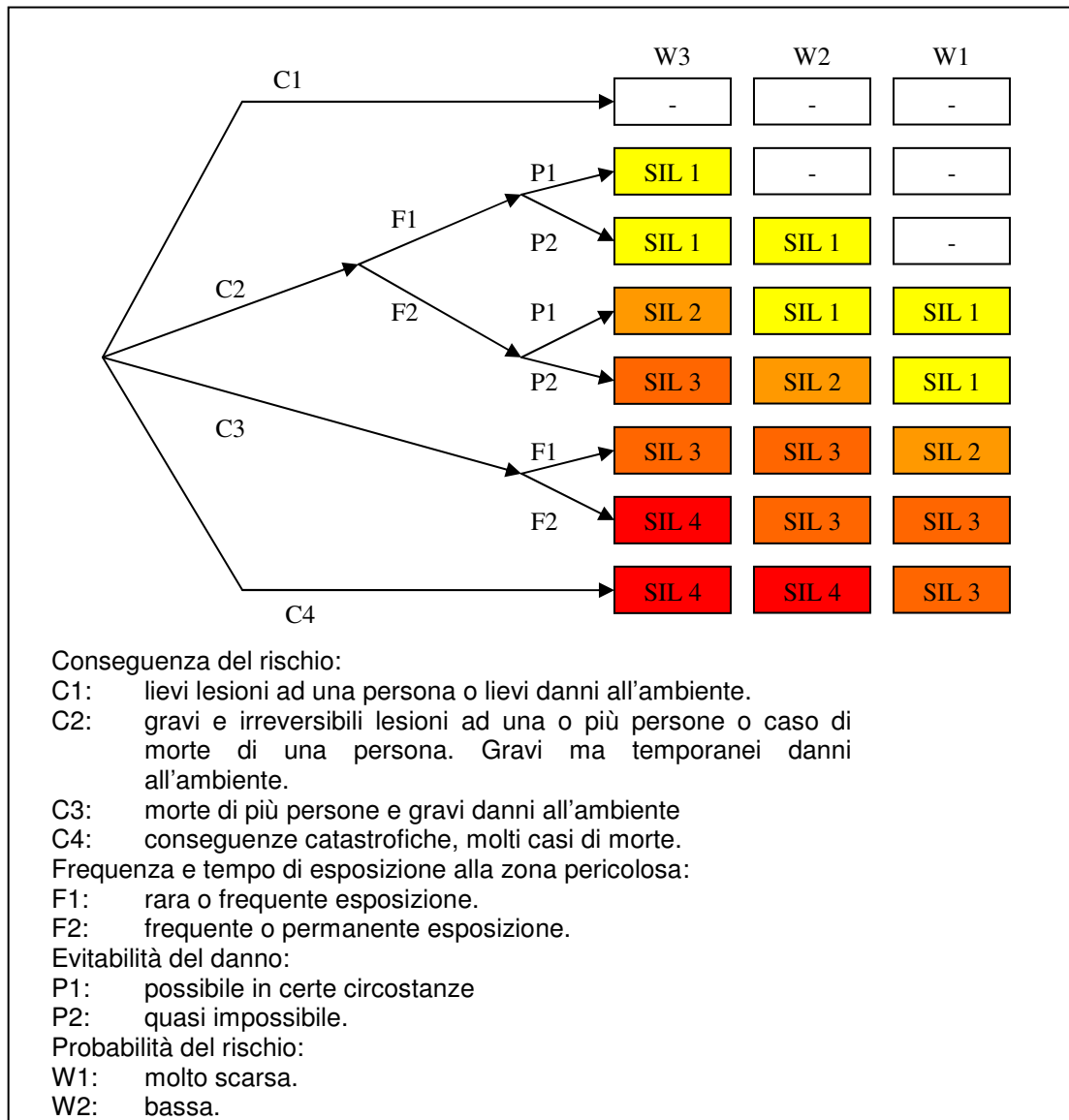


Figura 2-1: Valutazione del SIL

Un esempio di valutazione di rischio accettabile può essere la seguente.

Si può ritenere che la probabilità media che una persona muoia nel giro di un anno sia pari a 10^{-2} , ma che in ogni caso non scenda mai al di sotto di 10^{-4} .

Di conseguenza la probabilità, per una persona, di morire a causa di una installazione tecnica dovrà restare sotto tale limite. In via cautelativa si cercherà di rimanere sotto 10^{-5} .

Va da sé che per un numero maggiore di persone esposte al pericolo l'installazione dovrà essere più sicura.

Tornando all'esempio iniziale si ipotizzi quando segue:

- Massimo rischio tollerabile di morte di una persona durante l'esercizio: 10^{-5} per anno (pa)
- Guasti nell'esercizio senza protezioni: 2×10^{-1} pa
- Percentuale di guasti che causano morte senza protezioni: 10^{-2}

Definita come unitaria la conseguenza correlata alla morte di una persona il rischio legato all'esercizio dell'impianto in assenza di protezioni può essere espressa come prodotto tra il numero dei guasti in assenza di protezioni e la frazione dei guasti che causano morte, cioè 2×10^{-3} .

È possibile allora calcolare l'indice **PFD_{AVG}** (**Probability of Failure on Demand**, la probabilità che il sistema di sicurezza fallisca l'intervento in caso di necessità) tollerabile per il sistema di protezione come rapporto tra il rischio massimo tollerabile e il rischio legato al sistema non protetto, in questo caso 5×10^{-3} .

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD _{AVG})	Average Probability of Failure per Hour (PFH _{AVG})
SIL 4	$10^{-5} \leq x \leq 10^{-4}$	$10^{-9} \leq x \leq 10^{-8}$
SIL 3	$10^{-4} \leq x \leq 10^{-3}$	$10^{-8} \leq x \leq 10^{-7}$
SIL 2	$10^{-3} \leq x \leq 10^{-2}$	$10^{-7} \leq x \leq 10^{-6}$
SIL 1	$10^{-2} \leq x \leq 10^{-1}$	$10^{-6} \leq x \leq 10^{-5}$

Tabella 2-1: SIL e Probability of Failure on Demand

Dalla tabella relativa alla modalità operativa a domanda bassa si deduce che è necessario raggiungere il SIL3.

2.2 Riduzione del rischio secondo ALARP

Il livello di SIL è definito sulla base della misura in cui si intende ridurre il rischio. In linea teorica, ridotto il rischio in una certa misura, sarebbe possibile ridurlo ulteriormente, con determinati benefici, a costo di un certo sforzo tecnico ed economico. Oltre certi limiti si arriverà ad un punto in cui:

- il rischio è intollerabile: può essere giustificato solo in circostanze straordinarie.

- il rischio non è riconosciuto come accettabile ma ulteriori misure di riduzione di rischio comporterebbero uno sforzo superiore rispetto ai benefici che ne verrebbero tratti. Questa è la zona di rischio detta **ALARP (As Low As Reasonably Possible)**.
- il rischio è riconosciuto come accettabile: non sono necessarie ulteriori misure di riduzione di rischio.

Frequenza	Effetti			
	Catastrofici	Critici	Marginali	Trascurabili
Frequente	I	I	I	II
Probabile	I	I	II	III
Occasionale	I	II	III	III
Remota	II	III	III	IV
Improbabile	III	III	IV	IV
Incredibile	IV	IV	IV	IV

I Rischio intollerabile
 II Rischio non desiderabile e tollerabile solo se la riduzione dello stesso è impraticabile o se i costi sono complessivamente sproporzionati rispetto al miglioramento ottenuto
 III Rischio tollerabile se il costo per la riduzione dello stesso supera il miglioramento ottenuto
 IV Rischio trascurabile

Tabella 2-2: Rischio tollerabile, intollerabile e ALARP

3 Classificazione dei sottosistemi di sicurezza

3.1 Indici di affidabilità del sistema di sicurezza

Ciascun sistema di sicurezza (il sistema di monitoraggio del livello del liquido di raffreddamento) è costituito da vari sottosistemi (il sensore, la logica, gli attuatori) ciascuno dei quali ha una sua affidabilità. In funzione delle caratteristiche del componente è possibile determinare se può fare parte di un sistema di sicurezza con un certo SIL.

In particolare è possibile definire quattro indici quantitativi dell'affidabilità di un sottosistema di sicurezza

3.1.1 PFD_{AVG} e PFH_{AVG}

Le **Probability of Failure on Demand (PFD_{AVG})** e **Probability of Failure per Hour (PFH_{AVG})** sono le probabilità che il sistema di sicurezza fallisca l'intervento in caso di necessità; per ottenere livelli SIL elevate devono essere più basse possibile.

$$PFD_{AVG} \approx \sum \lambda_D \cdot TI_x$$

Dove: λ_D è la probabilità di guasto pericoloso.

TI_x è l'intervallo di tempo tra due test in grado di rilevare il guasto.

La scelta tra gli indici PFD_{AVG} e PFH_{AVG} dipende dalla frequenza di chiamata all'intervento della funzione di sicurezza.

Tipicamente il caso del controllo di livello è a bassa domanda (meno di un intervento all'anno). È ragionevole, infatti, supporre che esista un apposito controllo per la regolazione del livello e che la funzione di sicurezza intervenga solo nel caso in cui si verifichi un guasto per cui non sia più possibile mantenere il livello del liquido nel range consentito. Di conseguenza il sistema di sicurezza non interverrà per normali condizioni di funzionamento del sistema.

3.1.2 SFF

La **Safe Failure Fraction (SFF)** è la percentuale dei guasti sicuri oppure pericolosi ma rilevati. È complementare ai precedenti indici in quanto per livelli di SIL elevati è necessario che i guasti, oltre ad essere meno probabili possibile, siano sicuri oppure rilevabili.

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_T}$$

Dove: λ_S è la probabilità di guasto non pericoloso.

λ_{DD} è la probabilità di guasto pericoloso rilevato.

λ_T è la probabilità totale di guasto

3.1.3 HFT

La **Hardware Fault Tolerance (HFT)** è quel numero di guasti contemporanei N per cui un N+1-esimo guasto può causare una perdita della funzione di sicurezza; in pratica definisce il grado di ridondanza del sistema.

3.2 Scelta dei sottosistemi di sicurezza

Fissato il SIL della funzione di sicurezza, la scelta dei sottosistemi avverrà sulla base di un budget del SIL: a ciascun componente (sensore, valvola...) sarà assegnata una quota del PFD_{AVG} sulla base della quale verrà scelto l'esemplare più idoneo.

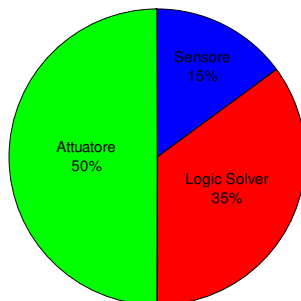


Figura 3-1: Esempio di budget del SIL

3.3 Classificazione dei sottosistemi in base al comportamento in guasto

È possibile classificare i sottosistemi di sicurezza in due classi, A e B.

3.3.1 Sottosistema di classe A

Un sottosistema appartiene alla **classe A** se:

- I modi di guasto di tutti gli elementi sono conosciuti
- Il comportamento del sottosistema in caso di guasto è definibile
- È disponibile un adeguato numero di dati che mostra che la percentuale di guasto è sufficientemente bassa

In sintesi si tratta di **sottosistemi semplici**, come valvole, contattori...

Safe Failure Fraction (SFF)	Hardware Fault Tolerance Classe A		
	N=0	N=1	N=2
$x < 60\%$	SIL1	SIL2	SIL3
$60\% \leq x < 90\%$	SIL2	SIL3	SIL4
$90\% \leq x < 99\%$	SIL3	SIL4	SIL4
$X \leq 99\%$	SIL3	SIL4	SIL4

N: il guasto N+1 può causare una perdita della funzione di sicurezza

Tabella 3-1: SIL, Safe Failure Fraction e Hardware Fault Tolerance per sottosistemi di classe A

3.3.2 Sottosistema di classe B

Un sottosistema appartiene alla **classe B** se:

- Il modo di guasto di almeno un elemento considerato non è conosciuto
- Il comportamento del sottosistema in caso di guasto non è totalmente definibile

- Non è disponibile un numero adeguato di dati che mostri che la percentuale di guasto è sufficientemente bassa

Si tratta di **sottosistemi complessi**, ad esempio logiche programmabili.

Per quest'ultimo tipo di sistema, data la parziale imprevedibilità, sono previsti requisiti di classificazione più stringenti. In particolare a parità di valori soddisfano un livello in meno.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance Classe B		
	N=0	N=1	N=2
$x < 60\%$	Non permesso	SIL1	SIL2
$60\% \leq x < 90\%$	SIL1	SIL2	SIL3
$90\% \leq x < 99\%$	SIL2	SIL3	SIL4
$X \leq 99\%$	SIL3	SIL4	SIL4

N: il guasto N+1 può causare una perdita della funzione di sicurezza

Tabella 3-2: SIL, Safe Failure Fraction e Hardware Fault Tolerance per sottosistemi di classe B

3.4 Attribuzione del SIL raggiungibile

Esempio 1: valvola per applicazione di sicurezza.

Si considerano i seguenti dati:

- Bassa domanda
- $PFD_{AVG} = 3 \times 10^{-5}$

Apparentemente la valvola potrebbe raggiungere SIL4. Considerando però che:

- HFT=0 (nessuna ridondanza)
- SFF=95%

Queste ultime condizioni riducono la prestazione della valvola a SIL3. Il SIL4 può essere raggiunto, infatti, solo in presenza di ridondanze.

Non è corretto affermare che la valvola è certificabile SIL3, in quanto tale definizione si riferisce ad una funzione di sicurezza e non ai singoli sottosistemi.

Più correttamente la valvola sarà impiegabile in sistemi di sicurezza fino a SIL3.

Anche per la valutazione del SIL raggiungibile dal singolo componente va tenuto inoltre presente che il livello di sicurezza del sottosistema dipende da tutti i suoi componenti, e quindi dalla somma delle probabilità di guasto di tutti i sottosistemi.

Esempio 2: valvola per applicazione di sicurezza.

- Bassa domanda
- $PFD_{AVG} = 8 \times 10^{-4}$
- HFT=0 (nessuna ridondanza)
- SFF=95%

Apparentemente anche in questo caso la valvola è impiegabile in funzioni di sicurezza fino a SIL3.

Va però tenuto in considerazione che il valore di PFD_{AVG} è piuttosto vicino al limite superiore consentito per tale livello. Affinché il sistema di sicurezza in cui la valvola rientra raggiunga il SIL3 sarà necessario che tutti gli altri sottosistemi abbiano PFD_{AVG} tali da rientrare nei limiti, cioè molto bassi.

Più ragionevolmente la valvola sarà impiegabile in funzioni di sicurezza fino a SIL2, in modo da consentire agli altri sottosistemi di raggiungere un livello di prestazione comparabile.

Va tenuta presente anche la classe cui appartiene il sottosistema: un sottosistema di classe B con pari caratteristiche rispetto ad un sottosistema di classe A, raggiunge un SIL più basso.

Inoltre la **ridondanza** di un elemento con un dato PFD_{AVG} , e quindi compatibile con un dato SIL, consente di ridurre il valore di probabilità di guasto; la probabilità che venga a mancare la funzione di sicurezza per guasto di due esemplari del medesimo componente, infatti, è più bassa rispetto alla probabilità che si guasti il singolo esemplare. È così possibile raggiungere un dato SIL utilizzando componenti ridondati compatibili con SIL più bassi.

Ciò non sarebbe valido per i cosiddetti guasti di modo comune, cioè guasti simultanei ad unità identiche causati dallo stesso motivo e nello stesso modo. Un modo per ridurre questa eventualità è l'attuazione della **diversità** in luogo della ridondanza, cioè l'impiego di mezzi diversi per eseguire una data funzione (ad esempio l'impiego di sensori con tecnologia diversa per una stessa funzione). Così facendo ciò che impedisce di funzionare a una certa tecnologia, presumibilmente non lo farà su una tecnologia diversa, elevando così il grado di affidabilità del sistema.

3.5 Metodi di valutazione dell'affidabilità di un sottosistema

Esistono due metodi per determinare le probabilità di guasto di un sottosistema.

3.5.1 Metodo "Proven in use"

Il metodo si basa sull'esperienza precedente di utilizzo del sottosistema in ambienti simili.

Affinché sia possibile applicare questo tipo di metodologia è necessario:

- Essere in possesso di una adeguata evidenza documentale, basata sull'uso precedente di una configurazione specifica del sottosistema (stessa applicazione o simile, in condizioni ambientali e di esercizio comparabili).
- Tutti i guasti devono essere stati formalmente registrati, analizzati e classificati, in modo da avere una ragionevole certezza di essere a conoscenza di tutte le possibili modalità di guasto.
- Il tempo operativo dell'uso precedente di una configurazione del sottosistema deve essere tale da garantire un sufficiente livello di confidenza in relazione al SIL che si intende raggiungere.

Affinché tali condizioni siano verificate è necessario, ad esempio, che i sottosistemi siano forniti direttamente agli utenti finali in modo da avere un feedback diretto in caso di guasti e malfunzionamenti.

La valutazione degli indici di affidabilità si effettua nel modo seguente:

$$\lambda_T = \frac{N^\circ \text{ guasti totali}}{\text{Ore operative totali}}$$

$$SFF = 1 - \frac{\lambda_{DU}}{\lambda_T}$$

$$PDF_{AVG} = \lambda_{DU} \cdot \frac{TI}{2} + \lambda_{DD} \cdot \frac{TI_{PS}}{2}$$

Dove: λ_{DU} è la probabilità di guasto pericoloso non rilevato dal test parziale.

TI è l'intervallo di tempo tra due test perfetti o completi, in grado di rilevare tutti i guasti.

λ_{DD} è la probabilità di guasto pericoloso rilevato dal test parziale.

TI_{PS} è l'intervallo di tempo tra due test parziali in grado di rilevare solo alcuni guasti.

È da notare come il PFD_{AVG} del sottosistema dipenda sia dalle probabilità di guasto sia dalle modalità di test (e quindi di manutenzione) del sottosistema. L'attuazione di test (parziali o completi) del sistema consente, infatti, di rilevare (ed eventualmente correggere) guasti in modo da impedire mancati funzionamenti del sistema di sicurezza.

L'utilizzo di test parziali a brevi intervalli di tempo, in particolare, consente di mantenere bassa la probabilità di guasto anche senza la necessità di effettuare test completi che, in genere, richiedono un arresto degli impianti.

3.5.2 Metodo FME(D)A

Questo tipo di metodologia si basa sull'analisi del progetto e si presta a quei sottosistemi per cui non esista uno storico di esercizio, oppure nei casi in cui si renda necessario stimare l'affidabilità o i punti deboli di un progetto.

Il sottosistema viene discretizzato in singoli componenti di cui siano note le modalità di guasto e le relative probabilità. Per ogni singola modalità di guasto ne vengono presi in considerazione gli effetti rispetto ad un elemento superiore.

Le probabilità di guasto dei singoli componenti (resistenze, condensatori, bulloni...) sono reperibili in appositi database.

3.6 Scelta del grado di indipendenza

La scelta del soggetto (o dei soggetti) preposto alla valutazione della sicurezza funzionale dipende dalle potenziali conseguenze in caso di malfunzionamento del sistema di sicurezza. In particolare, per potenziali conseguenze progressivamente più gravi, le persone preposte devono essere via via più indipendenti.

Grado di indipendenza minimo	Risultato			
	A	B	C	D
Persona indipendente	HR	HR ¹	NR	NR
Sezione indipendente	-	HR ²	HR ¹	NR
Organizzazione indipendente	-	-	HR ²	HR
A: danno esiguo. B: danno serio e duraturo a una o più persone; morte di una persona C: morte di più persone D: morte di molta gente NR: Not Recommended HR: Highly Recommended				

Tabella 3-3: Scelta dei gradi di indipendenza in funzione del risultato del rischio

Grado di indipendenza minimo	SIL			
	1	2	3	4
Persona indipendente	HR	HR ¹	NR	NR
Sezione indipendente	-	HR ²	HR ¹	NR
Organizzazione indipendente	-	-	HR ²	HR
NR: Not Recommended HR: Highly Recommended				

Tabella 3-4: Scelta del grado di indipendenza in funzione del SIL

La propensione ad HR² rispetto a HR¹ dipende da:

- Mancanza di esperienza in progetti simili;
- Maggiore grado di complessità;
- Maggiore grado di novità dei progetti;
- Maggiore grado di novità della tecnologia;
- Difettosa standardizzazione di alcuni criteri del progetto.

4 Il Partial Stroke Test

Si è accennato alla possibilità di effettuare test completi per diagnosticare la funzionalità del sistema di sicurezza. Questo genere di test, in genere, comporta un arresto dell'impianto, in quanto richiede un intervento del sistema di sicurezza. La frequente attuazione di questo genere di test comporta, ovviamente, un certo danno economico dovuto al fermo impianto.

Il Partial Stroke Test è nato nel settore dell'industria di processo come metodo per diagnosticare, senza fermata dell'impianto, alcune possibili anomalie nei componenti degli ESD, in particolare le valvole.

Un movimento parziale della sfera di chiusura, senza una chiusura completa, consente di verificare, ad esempio, possibili incollaggi delle guarnizioni, deformazioni del corpo valvola, etc.

Ciò diventa molto vantaggioso quando le valvole assumono una dimensione tecnicamente ed economicamente impegnativa, per cui una eventuale ridondanza risulterebbe uno sforzo piuttosto impegnativo. L'impiego del test parziale consente di monitorare lo "stato di salute" della valvola allungando gli intervalli di tempo tra i test completi e mantenendo nel contempo un accettabile livello di integrità del sistema di sicurezza.