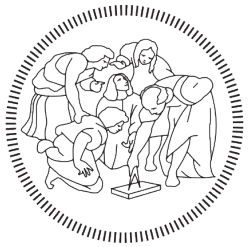


POLITECNICO
MILANO 1863

Dipartimento di Ingegneria Industriale

Corso di Laurea in Ingegneria della Prevenzione e della Sicurezza nell'Industria di Processo

Nuova Edizione della serie IEC 61508: Analisi e Metodologie per le Architetture di Sicurezza

Relatore:
Prof. Loredana Cristaldi

Referente aziendale:
Ing. Marco Tacchini

Candidata:
Lucia Matina
Matricola 252857

Anno Accademico 2025/2026

Indice

Sommario **iv**

Abstract **v**

1 Introduzione **1**
1.1 Introduzione alla Sicurezza funzionale 1
1.2 Storia della IEC 61508 1
1.3 Struttura della serie IEC 61508 2
1.4 Livello di Integrità di Sicurezza SIL 3

2 Evoluzione di PFD e PFH **5**
2.1 High Demand e Low Demand Mode 5
2.1.1 Tipologie di guasto 5
2.2 Parametri della Teoria dell'Affidabilità 6
2.2.1 SIL e Limiti di Architettura 11
2.2.2 PFD 12
2.2.3 PFH 13
2.3 Differenze tra 2010 e 2026 14
2.3.1 Modalità a Bassa Richiesta 14
2.3.2 Simulazione di Analisi Comparativa PFD 18
2.3.3 Modalità ad Alta o Continua Richiesta 21
2.4 Confronto High Demand con IEC 62061 23
2.4.1 Simulazione di Analisi Comparativa PFH 26

3 Sistemi Misti: Alta e Bassa Richiesta **30**
3.1 Cosa sono i Sistemi Misti 30
3.2 Introduzione dei Sistemi Misti nella IEC 61508 31
3.3 Altri Approcci per Sistemi Combinati 34
3.3.1 Metodo del confronto tra i tassi di guasto 34
3.3.2 Metodo secondo IEC TS 63394 35

4 Affidabilità della Funzione Diagnostica **37**
4.1 Introduzione alla Funzione Dagnostica 37
4.1.1 Ruolo della Diagnostica 37

4.2 Novità nella Nuova Edizione 38
4.2.1 Tipi di Funzioni Diagnostiche 38
4.2.2 Tassi di Guasto della Diagnostica e $DSFF$ 38
4.2.3 Requisiti Aggiuntivi per Sistemi Non Ridondanti 39
4.3 L'Importanza dell'Annex F 39
4.4 Limiti della Funzione Diagnostica 54

5 Conclusioni **56**

Elenco delle figure

2.1 Alcuni tempi caratteristici tra lo stato Up e Down di un guasto DD 8
2.2 Confronto del valore di PFD_{avg} al variare di λ, DC e K 20
2.3 Confronto del valore di PFH al variare di λ, DC e K 28

3.1 Esempio di Sistema Misto: Contattore per Alta e Bassa Richiesta 30
3.2 SIF Combinata per Modalità in Alta Richiesta, IEC 61508-6:2026 Annex B 31
3.3 SIF Combinata per Modalità in Bassa Richiesta, IEC 61508-6:2026 Annex B 32
3.4 SIF Combinata per Modalità in Alta e Bassa Richiesta, IEC 61508-6:2026 Annex B 33
3.5 Valori massimi di PFD_{avg} e PFH_D per i rispettivi SIL target . 35

4.1 Esempio IEC 61508-6:2026 Annex F.2 43
4.2 Albero dei Guasti IEC 61508-6:2026 Annex F.3 51

Elenco delle tabelle

1.1 Livelli di Integrità di Sicurezza - Misure di Riferimento, IEC61508-1 7.6.2.9 3

2.1 Livello massimo di integrità di sicurezza consentito per una funzione di sicurezza eseguita da un componente di tipo A. 11
2.2 Livello massimo di integrità di sicurezza consentito per una funzione di sicurezza eseguita da un componente di tipo B. 12
2.3 Vincoli di Architettura per un sotto-sistema B: massimo SIL raggiungibile 25
2.4 Sintesi dei possibili casi di 1oo1D 26

Sommario

La presente Tesi tratta in modo approfondito l'aggiornamento della norma IEC 61508, la quale si concentra sugli aspetti che influenzano la valutazione della sicurezza funzionale per i dispositivi elettrici, elettronici ed elettronici programmabili (E/E/PE) destinati alla sicurezza. La norma vigente, essendo redatta nel 2010, andava aggiornata con nuovi approcci che sono maturati negli anni, insieme all'evoluzione tecnologica dei dispositivi considerati.
Una prima parte del mio Lavoro è dedicata alle modifiche apportate nel calcolo della Probability of Failure on Demand (PFD) e della Probability of Failure per Hour (PFH). La norma affina questi calcoli, rendendo più specifici i valori di β, il fattore di guasto di causa comune (CCF) tra canali. Per le funzioni di sicurezza richieste in alto funzionamento (più di una volta all'anno) vengono introdotte ulteriori metodi di calcolo di PFH. Tali formulazioni tengono conto dell'eventuale intervento della diagnostica, ossia che vada o meno a spostare la funzione di sicurezza da un canale che presenta un guasto ad uno sicuro.
Per ogni architettura di sicurezza sono state analizzate nel dettaglio le modalità di aggiornamento delle formule, e vengono riportati esempi applicativi di comparazione tra la versione attuale e la futura.
Inoltre, per la funzione in alta richiesta di funzionamento, è stato confrontato il valore di PFH ottenuto usando le espressioni nella norma IEC 61508 e quelle presenti nella IEC 62061.
Un secondo aspetto approfondito nel presente documento è l'introduzione in ambito normativo delle modalità di gestione dei sistemi misti. Si tratta di architetture che integrano componenti in bassa modalità di funzionamento con parti ad alta modalità di funzionamento, tipiche delle realtà industriali. Sono stati analizzati i vari approcci affrontati o suggeriti dalla norma e sono stati confrontati tra di loro.
Infine, viene esaminato a fondo il tema delle innovazioni introdotte in ambito diagnostico. All'interno della norma vengono introdotti nuovi parametri per poter stimare l'affidabilità della funzione di diagnostica. Il calcolo dei tassi di guasto, comprensivo di guasti della funzione diagnostica, viene ripreso seguendo tre approcci: l'analisi Fault Tree, il metodo di Markov Multifase e l'uso di formule semplificative espresse nella Nuova Edizione della norma.
Nel complesso, il Lavoro offre una visione integrata delle novità adottate nella norma IEC 61508 e delle loro implementazioni nella pratica industriale per la progettazione, valutazione e gestione di sistemi E/E/PE legati alla sicurezza.

Abstract

The following thesis provides a deep analysis of the updated version of the IEC 61508 standard, which focused on functional safety assessment of electrical, electronic and programmable electronic (E/E/PE) safety-related systems.
The current edition, published in 2010, required an extensive revision to integrate new approaches and concepts that have emerged over the years, driven by the technological evolution of these devices.
The first part of my work is dedicated to the modifications introduced in the calculation of the Probability of Failure on Demand (PFD) and the Probability of Failure per Hour (PFH). The new version refines these calculations, making β factor, which stands for common cause failures between redundant channels, more specific and better aligned with realistic system behavior. For high demand rates, where the safety function is required more than once per year, the new edition includes additional PFH formulas, adapted for diagnostics that can or cannot switch from a faulty channel to a safe one.
For each safety architecture, the updated formulas have been examined in detail. Applications examples are provided to compare results between the current and future editions. Furthermore, for high demand functions, the PFH values obtained using IEC 61508 formulas have been compared with the same calculated using IEC 62061.
A second key topic is the introduction of methods for handling mixed systems, architectures that combine components operating in low and high demand, commonly found in industrial processes. Various approaches proposed by the standard have been analyzed and compared to evaluate their applicability and limitations.
Finally, the thesis examines the innovations introduced in diagnostic function evaluation. The updated IEC 61508 standard introduces new parameters aimed at estimating the reliability of diagnostic functions. The calculation of failure rates, including failure within diagnostic function, is revised through three different approaches: Fault Tree Analysis, Multi-phase Markov model, and simplified formulas provided in the standard.
Overall, this work offers an integrated overview of the new concepts introduced in the future IEC 61508 standard and their implications for the design, the assessment and management of safety-related systems.

1

Introduzione

1.1 Introduzione alla Sicurezza funzionale

La sicurezza funzionale è un concetto che nasce durante l'evoluzione industriale avvenuta nell'ultimo secolo. Prima degli anni '70, la sicurezza industriale si affidava esclusivamente a sistemi meccanici semplici: un interruttore di emergenza che chiudeva un circuito in caso di guasto. Durante quegli anni ci fu il passaggio da sistemi unicamente meccanici ai PES (Programmabe Electronic Systems), sistemi più complessi. Eventi storici come il disastro di Seveso nel 1976, dovuti in parte a errori informatici, ha portato la sicurezza ad un nuovo livello. In particolare, l'uso di sistemi di controllo elettronici ha generato nuovi rischi: le possibili anomalie nel funzionamento di sistema, oltre che nella tecnologia fisica. Il concetto di sicurezza funzionale è vasto: questa segue il macchinario dalla sua fase di assemblaggio, al funzionamento del suo sistema di controllo. Essa svolge un ruolo di prevenzione, ma anche di gestione dei possibili guasti, andando a ridurre il rischio totale di utilizzo del macchinario.
La serie di norme IEC 61508 si fa portavoce dei principi di sicurezza funzionale, e proviene dalla necessità di uniformare e standardizzare i metodi di gestione della sicurezza nelle funzioni controllo dei dispositivi industriali. Essa è il pilastro fondamentale nella progettazione di sistemi di controllo elettromeccanici ed elettronici che svolgono funzioni di sicurezza, e racchiude sia una parte tecnica che una teorica sulle metodologie da adottare per gestire al meglio tutto il ciclo di vita dei dispositivi di sicurezza.

1.2 Storia della IEC 61508

La prima edizione della IEC 61508 venne pubblicata sul finire degli anni '90, dopo la pubblicazione una serie di studi e ricerche sulla sicurezza nell'uso dei sistemi programmabili elettronici. In particolare, l'HSE (Health and Safety Executive), il quale dettava delle linee guida in cui veniva introdotto il concetto di

adattare il livello di sicurezza in base al rischio da gestire.
L'IEC raccolse tutte le intuizioni a riguardo e venne redatta la prima edizione della norma. Questa portò una novità assoluta, il concetto che tutti i sistemi di sicurezza si possono guastare, ma la probabilità di guasto doveva essere tanto più bassa quanto più alto era il rischio che il sistema di sicurezza doveva ridurre.
Nel 2010 venne redatta la Seconda Edizione, con delle aggiunte riguardo il software e i guasti ad esso connessi.
La IEC 61508 è considerata la "Norma Madre" essendo generica e da essa sono state generate altre norme settoriali. Ciascuna di queste norme ha il suo linguaggio specifico, come ad esempio la IEC 61511 per l'Industria di Processo (chimica, petrolchimica etc...); la EN 50126 che trattano la sicurezza delle caldaie; la IEC 62061 per i macchinari industriali e altre ancora.

1.3 Struttura della serie IEC 61508

La norma è composta da 7 parti, alcune delle quali sono normative e altre informative. Le parti normative espongono degli obblighi da rispettare per la conformità, e questo riguarda le prime tre parti. Tutto quello che segue è anche riportato nella norma IEC 61508 [1].
Nella Parte 1 vengono presentati i requisiti generali di sicurezza. Viene esposto un criterio di base su cui la norma si fonda: il Safety Lifecycle, ossia come la sicurezza debba accompagnare ogni stadio della vita di un sistema, dalla progettazione alla dismissione. Nei requisiti generali viene trattato il tema della competenza del personale, la documentazione necessaria di cui disporre. Viene spiegato come gestire il processo di sicurezza, compresa la pianificazione delle attività da svolgere e la valutazione del sistema di sicurezza affinché rispetti i criteri.
La parte 2 tratta i requisiti specifici della componente hardware dei sistemi E/E/PE. In questa sezione vengono visti i criteri di progettazione dei dispositivi per prevenire guasti casuali e sistematici. Vengono introdotte alcune nozioni principali per analizzare la funzione di sicurezza tra cui la Safe Failure Fraction e la ridondanza nelle architetture.
La parte 3, invece, si focalizza sul Software del dispositivo legato alla sicurezza. Questo potrebbe riscontrare errori logici, quindi guasti sistematici, i quali si vuole tentare di ridurre al minimo.
La parte 4 spiega le principali definzioni dei termini contenuti nella norma. Ad esempio, offre nel dettaglio le differenze tra "Errore" e "Guasto". Spazia su ogni argomento, dal generale al dettaglio, fornendo anche la spiegazione delle abbreviazioni.
Le ultime tre parti, invece, sono informative, ovvero non racchiudono obblighi, ma sono utili nell'applicazione pratica delle prime tre parti.
La parte 5 racchiude esempi di metodi per la determinazione dei SIL (Livelli di Integrità di Sicurezza). Vengono mostrati metodi qualitativi e quantitatvi sul calcolo del rischio, e come passare dall'analisi del rischio alla scelta del SIL.

La parte 6 fornisce delle linee guida per applicare la parte 2 e 3 della norma. In particolare, presenta esempi pratici per il calcolo dell'affidabilità del sistema a livello hardware, oltre che organizzare lo sviluppo software. Questa parte è centrale nell'applicazione tecnica della norma.
Infine, la parte 7 contiene delle tabelle che chiariscono quale tecnica e metodo usare in funzione al SIL richiesto.

1.4 Livello di Integrità di Sicurezza SIL

Il SIL è un indice utilizzato in Sicurezza Funzionale per indicare una performance legata ad una funzione di sicurezza, la quale riduce il rischio di un macchinario o di un processo ad un livello accettabile. Il SIL rappresenta la probabilità che un sistema di sicurezza SIS esegua in modo opportuno la sua funzione quando richiesta.
Ci sono quattro livelli di SIL:

- SIL 1, richiede una riduzione del rischio minima.
- SIL 2, ad un livello intermedio, è molto comune nell' industria di processo.
- SIL 3, indica un livello elevato di precauzioni da avere e di tecnologie avanzate, richiede ridondanza nelle apparecchiature.
- SIL 4, indica il livello massimo e viene usato in settori critici come ferroviario o nucleare.

Il livello di integrità totale è costituito da una componente hardware, legata ai guasti casuali, e una componente software, legata a quelli sistematici. L'integrità di sicurezza dell'hardware comprende anche il rispetto dei vincoli di architettura per lo specifico SIL.
Per identificare il livello di integrità vengono usati due parametri, in base a quanto la funzione di sicurezza è richiesta. Nel caso di bassa domanda, si valuta la probabilità di guasto su richiesta PFDavg. In caso di attivazione della funzione di sicurezza in modo frequente (più di una volta all'anno) o continuo si valuta la probabilità di guasto pericoloso all'ora PFH.

SIL	**Bassa Domanda: PFDavg**	**Alta Domanda: PFH** $[h^{-1}]$
SIL 4	$\geq 10^{-5}$	$\geq 10^{-9}$
SIL 3	$\geq 10^{-4}$	$\geq 10^{-8}$
SIL 2	$\geq 10^{-3}$	$\geq 10^{-7}$
SIL 1	$\geq 10^{-2}$	$\geq 10^{-6}$

Tabella 1.1: Livelli di Integrità di Sicurezza - Misure di Riferimento, IEC61508-1 7.6.2.9

Nella norma IEC61508-5 vengono descritti i metodi di determinazione del SIL.

Tra i metodi quantitativi abbiamo l'Analisi dell'Albero dei Guasti (FTA). Questo metodo è molto preciso ma piuttosto lento, in quanto un guasto e la sua relativa probabilità di accadimento viene combinato con altre possibili cause di guasto. Si parte dall'evento indesiderato e si procede a ritroso, usando uno schema contenente delle porte logiche (AND/OR), fino ad arrivare alla frequenza di guasto totale del sistema.
Un approccio semi-quantitativo anche molto usato è il LOPA, ossia L'Analisi degli Strati di Protezione di un dispositivo in modo da ridurre il rischio di una situazione pericolosa. Ogni strato di protezione è indipendente dagli altri, come ad esempio l'uso di sistemi di controllo e valvole elettromeccaniche di emergenza.

2

Evoluzione di PFD e PFH

2.1 High Demand e Low Demand Mode

La funzione di sicurezza opera secondo tre possibili modalità di funzionamento: a bassa domanda, alta domanda oppure in modalità continua. Nel primo caso, la funzione di sicurezza viene eseguita solo su necessità, allo scopo di portare l'EUC (Equipment Under Control), ovvero il macchinario o il processo che stiamo analizzando, ad uno stato di sicurezza predefinito, chiamato Stato Sicuro. Viene richiesta raramente, per la norma è necessario che la frequenza non superi una volta l'anno (e.g. una valvola di chiusura di emergenza). Il sistema E/E/PE (Electrical, Electronic o Programmable Electronic) legato alla sicurezza che esegue la funzione di sicurezza può non avere alcuna influenza sull'EUC o sul sistema di controllo dell'EUC fino a quando non si verifica una richiesta.
Nella modalità di funzionamento ad alta domanda, la funzione di sicurezza viene eseguita solo su richiesta e la frequenza della stessa è superiore a una volta l'anno (e.g. un interblocco installato su un accesso ad un'isola robotizzata).
Nel caso di modalità continua, la funzione di sicurezza mantiene l'EUC in uno stato sicuro come parte del normale funzionamento.

2.1.1 Tipologie di guasto

L'idea di base è che i componenti che fanno parte della funzione di sicurezza si possono guastare, come riporta il libro Functional Safety of Machinery (2023) [2]. In sicurezza funzionale, vengono distinte due categorie di guasti: guasti casuali e guasti sistematici. Questa distinzione è fondamentale poiché le due tipologie hanno differenti cause, modalità di gestione e misure di prevenzione. Nella serie di norme IEC 61508 vengono trattati entrambi, ed entrambi influenzano il Safety Integrity Level (SIL) di un sistema legato alla sicurezza.

Guasti sistematici

Prima di tutto vengono affrontati i guasti sistematici, perché questi derivano da errori nel processo di specifica, progettazione, implementazione o manutenzione del sistema di sicurezza. Per ogni fase di vita del componente, è importante seguire i principi di sicurezza di base, trattati in diverse norme, come la IEC 62061 o la ISO 13849-1. I guasti sistematici possono essere riferiti sia alla parte hardware del componente, che software. Nella IEC 61508-1 vengono esplicitati i principi generali della sicurezza funzionale, tra cui la gestione del guasti sistematici. Mentre nella parte 3 la IEC 61508 si concentra sui software dei sistemi di sicurezza. Quindi, fornisce linee guida sui requisiti per lo sviluppo, la validazione del software attraverso test e metodi formali, e suggerisce misure preventive per i guasti sistematici. Aderendo a questi requisiti, si garantisce che il software contribuisca al raggiungimento del SIL richiesto per la funzione di sicurezza.

Guasti casuali

I guasti casuali, legati alla parte hardware del componente, sono eventi aleatori che si verificano nel tempo di missione a causa dell'usura oppure di fenomeni fisici non controllabili. I guasti casuali influenzano l'integrità complessiva del sistema di sicurezza, e vengono gestiti mediante approcci statistici e regole di affidabilità. Vengono trattati nella IEC 61508-2 dove vengono definiti i criteri quantitativi per la determinazione del SIL del sistema e nella IEC 61508-6, in cui vengono esplicitati i metodi di calcolo di parametri fondamentali per definire il SIL.

2.2 Parametri della Teoria dell'Affidabilità

Per gestire i guasti casuali, essendo imprevedibili individualmente, si usa un approccio probabilistico con parametri di affidabilità. Per sistemi elettronici è valida la distribuzione esponenziale. Per cui troviamo una probabilità di guasto F entro un tempo t e un tasso di guasto λ, che per i componenti E/E/PE consideriamo costante, ovvero ipotizziamo che il componente non venga consumato significativamente con l'utilizzo.

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

Tasso Medio di Guasto λ

Il tasso medio di guasto λ indica la frequenza con cui un sistema o una sua parte si guasta nell'unità di tempo. Infatti, viene misurato come numero di guasti all'ora (h^-1), ma nella realtà si usano i FIT (Failures In Time), dove $1FIT = 10^{-9}$ guasti all'ora.
In genere, e soprattutto per componenti meccanici, il tasso di guasto non è costante. Il suo profilo nel tempo prende il nome di "Curva a vasca da bagno",

perché è ipotizzato costante nella parte centrale, ossia nella fase utile della vita del componente, mentre nelle zone iniziale e finale aumentano i guasti, dovuti alla mortalità infantile oppure all'usura verso la fine dell'esercizio.
Nella IEC 61508 i tassi di guasto vengono suddivisi in base a due criteri:

- Sicurezza: nel caso di guasto, questo mette in pericolo il sistema?
- Rilevabilità: il sistema di diagnostica riesce a individuare il guasto?

In base a come rispondono alle due funzioni, vengono distinti quattro tassi di guasto:

- λ_{SD}: tasso di guasto sicuro rilevato dalla diagnostica.
- λ_{SU}: tasso di guasto sicuro non rilevato dalla diagnostica.
- λ_{DD}: tasso di guasto pericoloso rilevato dalla diagnostica, per cui si riesce a portare il sistema in uno stato sicuro.
- λ_{DU}: tasso di guasto pericoloso non rilevato dalla diagnostica. Questo guasto verrà scoperto solo durante uno dei test manuali periodidi (Proof Test), altrimenti la funzione di sicurezza non verrà svolta quando richiesta.

Il tasso medio di guasto è la misura probabilistica dell'affidabilità hardware.
I valori di λ provengono da diverse possibili fonti. Il metodo principale per la stima del loro valore è il metodo FMEDA (Failure Modes, Effects and Diagnostic Analysis), solitamente effettuato dai costruttori del componente di sicurezza.
Nel caso in cui non fossero forniti i dati dal costruttore, si utilizzano database di applicazioni in impianti industriali reali, ad esempio EXIDA.
Un altro metodo prevede l'utilizzo di dati di campo, ossia per componenti che sono già in uso da tempo, si può fornire un quantitativo del tasso di guasto.

Tempi Medi Caratteristici di Down della Funzione di Sicurezza

La norma IEC 61508-4 definisce il Tempo Medio di Ripristino MTTR (Mean Time To Restoration) il tempo medio atteso per riportare un componente guasto a uno stato in cui può svolgere nuovamente la sua funzione richiesta.
Il MTTR comprende:
a) il tempo di rilevazione del guasto
b) il tempo di attesa logistica impiegato prima di iniziare l'intervento di riparazione
c) la riparazione effettiva
d) il tempo per effettuare controlli necessari e il tempo di riavvio del processo.

Escludendo il tempo di rilevazione del guasto (in Figura 2.1 indicato con "a"), rimane il Mean Repair Time (MRT), quindi il tempo medio della sola riparazione del componente.

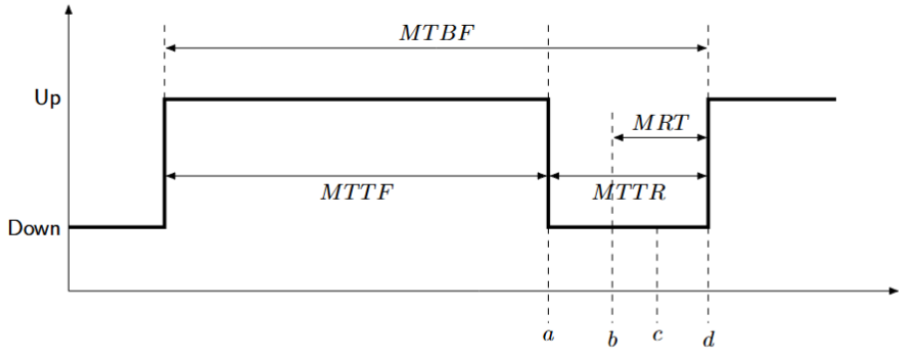


Figura 2.1: Alcuni tempi caratteristici tra lo stato Up e Down di un guasto DD

Nella figura si vede la suddivisione dell'MTTR in quattro componenti indicative principali, che includono il MRT.
Un altro parametro è il Mean Time To Failure (MTTF), il tempo medio in cui il componente si trova in uno stato funzionante prima di un guasto. Si usa per componenti non riparabili.
Invece, il Mean Time Between Failures (MTBF) si usa per dispositivi riparabili e indica il tempo medio tra un guasto e quello successivo. Da qui:

$$\text{MTBF} = \text{MTTF} + \text{MTTR}$$

Distinguiamo i guasti *DD* come pericolosi rilevabili e quelli *DU* non rilevabili dalla funzione di diagnostica. Per quelli rilevabili, la diagnostica interviene subito, e la durata del tempo di non funzionamento del sistema è relativamente breve. Quest'ultimo comprende il tempo per accorgersi del guasto e il tempo di riparazione. In questo caso si utilizza l'MTTR che viene tipicamente valutato di 5-10 ore.
Per quanto riguarda i guasti pericolosi non rilevabili, non si viene a sapere del guasto finché non viene effettuato un Proof Test. Per cui la durata del mancato funzionamento è piuttosto elevata. Segue che il tempo di riparazione è trascurabile rispetto al quello di attesa, che solitamente viene ipotizzato in mesi o anni.
Mentre l'MTTR rappresenta il tempo di rilevamento e riparazione di un guasto DD dalla diagnostica, il MDT (Mean Down Time) si riferisce all'intero periodo in cui un sistema di sicurezza non è disponibile e l'EUC rimane senza protezione dopo un guasto pericoloso non rilevabile.
Infatti, dopo il guasto e fino al Proof Test, questo non viene scoperto e quindi non può essere riparato.
Dopo il Proof Test viene considerato un tempo medio di riparazione effettiva del guasto MRT. Il MDT risulta, quindi, la somma tra il MRT e il tempo che intercorre tra il guasto e il Proof Test successivo.
Nella norma troviamo un parametro analogo al MDT, il t_{CE} (Channel Equivalent Mean Down Time), ovvero il tempo medio equivalente di downtime di

un singolo canale. Questo racchiude entrambi gli scenari visti, sia dei guasti rilevabili che non rilevabili:

$$t_{CE} = \underbrace{\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right)}_{\text{Parte Silenziosa (DU)}} + \underbrace{\frac{\lambda_{DD}}{\lambda_D} MTTR}_{\text{Parte Rilevata (DD)}}$$

$T_1/2$ è quando ipotizziamo si verifichi il guasto DU, dato che non conosciamo il periodo esatto.
Per i guasti DU, MRT è trascurabile rispetto a $T_1/2$.
Per i guasti DD, l'$MTTR$ si scompone in $T_2/2 + MRT_{DD}$, dove T_2 rappresenta l'intervallo della diagnostica. Questa componente solitamente è trascurabile rispetto al primo termine.

Copertura Diagnostica DC

I tassi di guasto si collegano, come chiarito nella norma, a due concetti chiave in ambito sicurezza funzionale: l'SFF e la DC.
La DC (Diagnostic Coverage) è la percentuale di guasti pericolosi rilevati dal sistema, rispetto a tutti i guasti pericolosi possibili. Esprime quanto efficacemente il sistema riesce a eseguire auto-diagnosi e intercettare un guasto al suo interno.

$$DC = \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}}}$$

La Copertura Diagnostica agisce direttamente sulla probabilità di guasto pericoloso, diminuendo la parte di guasti pericolosi non rilevati. Una volta rilevato il guasto pericoloso, questo potrà essere gestito, portando solitamente il sistema di sicurezza verso uno stato sicuro.
Per questo motivo, i guasti DD non contribuiscono al calcolo della probabilità di fallimento del sistema di sicurezza su richiesta, se il sistema viene gestito correttamente ed entra, appunto, in stato sicuro.
La normativa classifica il DC in quattro fasce, dalla più bassa (< 0.60) alla più alta (< 0.99). Maggiore è rischioso il sistema, più il livello di DC richiesto deve essere alto.
Nella ISO 13849-1 il DC viene collegato direttamente al livello di sicurezza di un componente. Invece nella IEC 61508 questo viene effettuato con un altro parametro, ossia la Safe Failure Fraction. Il DC è correlato ad esso, dal momento che rileva i guasti pericolosi presenti nel calcolo dell'SFF.
Nel caso di componenti elettromeccanici legati alla sicurezza, i quali non hanno una diagnostica interna, i due parametri devono coincidere $SFF = DC$.

Frazione di Guasto Sicuro SFF

L'SFF (Safe Failure Fraction) è la percentuale fra tutti i guasti possibili, di quelli non pericolosi oppure rilevati.

$$SFF = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{S}} + \lambda_D}$$

Nella pratica, questo valore può essere "manipolato" aumentando i guasti sicuri. In questo modo l'SFF aumenta, ma non la sicurezza reale.
Per questo motivo, si punta a depotenziare l'effetto degli SFF. Ad esempio, nella scorsa edizione sono stati esclusi dal calcolo i guasti che non inluenzavano la funzione di sicurezza (i No Effect Failures). Conoscendo l'SFF del sistema, la norma ci impone di valutare, insieme all'architettura fisica del sistema, il livello massimo di SIL conseguibile, come spiegato in seguito.

Fattore di Causa Comune β

Il fattore β rappresenta i Guasti provocati da una Causa Comune (CCF). Solitamente, in sicurezza, si tende a utilizzare la ridondanza per rendere più affidabile il sistema. Ma la rindondanza di un canale è efficace solo nel caso in cui ci sia indipendenza, ossia i guasti siano casuali. In alcuni casi la causa di guasto potrebbe essere per entrambi i canali la stessa, ad esempio una causa ambientale o un errore umano.
Il fattore β è una percentuale che dice di tutti i guasti che avvengono, quanti sono capaci di mettere fuori uso etrambi i canali contemporaneamente.
Per cui $\beta\lambda$ sono i guasti di causa comune, mentre $(1-\beta)\lambda$ sono i guasti indipendenti, e in quest'ultimo caso la ridondanza funziona in modo ottimale.
Questo fattore incide pesantemente sulla sicurezza, quindi sul calcolo della probabilità di guasti pericolosi quando vi è richiesta, portando anche ad abbassare il livello di SIL raggiungibile.
Per ridurre le cause comuni di guasto si seguono le procedure indicate nella parte 2 della norma IEC 61508 e poi negli Annex D della parte 6 della stessa, per il calcolo di β.

Intervallo del Test di Prova $T_{\mathbf{proof}}$

Il test di Prova Funzionale (Proof Test) è una verifica periodica che viene eseguita manualmente o automaticamente. Serve per individuare i guasti nel sistema di sicurezza che non sono stati riscontrati dalla funzione diagnostica (λ_{DU}).
Il test serve a riportare il sistema di sicurezza ad uno stato quasi pari al nuovo, assicurando che sia in grado di svolgere la sua funzione di sicurezza.
Il T_{proof}, spesso indicato come T_1, è l'Intervallo del Test di Prova, cioè il tempo trascorso tra un test di prova e un altro. Di solito viene posto pari ad un anno per i componenti che hanno una bassa richiesta. Questo parametro è usato nel calcolo della Probabilità di Fallimento su Richiesta (PFD), perché nel caso in cui il tempo tra i test fosse molto ampio, aumenterebbe il rischio che il componente si sia guastato in modo latente.

2.2.1 SIL e Limiti di Architettura

Tolleranza ai Guasti Hardware HFT

La Tolleranza ai Guasti Hardware (HFT) appare nella norma ed è un parametro fondamentale indicativo della capacità di un sistema di continuare a funzionare nonostante una o più parti dell'hardware riscontrino un guasto pericoloso.
Nel paragrafo 7.4.4.1 della IEC 61508-2 vengono definiti i criteri per stabilire questo parametro. Inoltre, viene specificato che il SIL di una funzione di sicurezza non viene determinato solo dal calcolo della probabilità di fallimento (PFD/PFH), ma anche da quanto l'architettura è robusta, quindi dall'HFT.
Nella pratica, se un sistema ha $HFT = N$, saranno necessari N + 1 guasti per far fallire la funzione di sicurezza. In questo conteggio è esclusa la diagnostica, che ha come scopo quello di rilevare i guasti e far raggiungere al sistema uno stato sicuro.
La norma inoltra afferma che il livello di SIL massimo raggiungibile viene vincolato dall'architettura, nonostante i calcoli di affidabilità affermino la possibilità di raggiungere un SIL più alto. In particolare, per elevati livelli SIL, la norma impone una tolleranza ai guasti minima.
Per determinare il SIL massimo ottenibile, si confrontano l'HFT e la SFF, ovvero la frazione di guasti non pericolosi.
Vengono distinte due tipologie di dispositivi:

- Tipo A: elementi semplici di cui sono noti i modi di guasto (es. relè e valvole). Questi non hanno necessità di elevata ridondanza.
- Tipo B: elementi più complessi contenenti logiche programmabili (es. PLC). Richiedono una maggiore ridondanza e non si conoscono del tutto le modalità di guasto.

Vincoli Architetturali

Nella norma IEC 61508-2 vengono fornite due tabelle in cui la Frazione di Guasto Sicuro SFF determina l'architettura minima hardware per sistemi di tipo A e B. Il dispositivo di sicurezza, infatti, deve essere classificato secondo queste due categorie. Nel caso in cui sia un componente di Tipo A, ossia semplice, senza processore, come l'esempio di valvole, relè, avremo:

SSF of an element	**Hardware Fault Tolerance of an element**		
	$HFT = \mathbf{0}$	$HFT = \mathbf{1}$	$HFT = \mathbf{2}$
< 0.6	SIL 1	SIL 2	SIL 3
0.6 - 0.9	SIL 2	SIL 3	SIL 4
0.9 - 0.99	SIL 3	SIL 4	SIL 4
> 0.99	SIL 3	SIL 4	SIL 4

Tabella 2.1: Livello massimo di integrità di sicurezza consentito per una funzione di sicurezza eseguita da un componente di tipo A.

Invece i dispositivi di Tipo B, ossia complessi, con microprocessori, PLC, Smart Sensors, o che hanno all'interno un software, richiedono delle considerazioni più approfondite. La norma fornisce un'altra tabella di riferimento, la 2.2.
Queste tabelle indicano il valore massimo di SIL che il componente potrà raggiungere, in base alla sua ridondanza fisica (HFT).

SSF of an element	**Hardware Fault Tolerance of an element**		
	$HFT = \mathbf{0}$	$HFT = \mathbf{1}$	$HFT = \mathbf{2}$
< 0.6	Not Allowed	SIL 1	SIL 2
0.6 - 0.9	SIL 1	SIL 2	SIL 3
0.9 - 0.99	SIL 2	SIL 3	SIL 4
> 0.99	SIL 3	SIL 4	SIL 4

Tabella 2.2: Livello massimo di integrità di sicurezza consentito per una funzione di sicurezza eseguita da un componente di tipo B.

2.2.2 PFD

Il PFD (Probability of Dangerous Failure on Demand) rappresenta la funzione di inaffidabilità $F(t)$ di un sistema di sicurezza che opera in bassa richiesta (ossia quando viene richiesta la sua funzione di sicurezza meno di una volta l'anno). Secondo la definizione nella norma IEC 61508-4, il PFD è la non disponibilità di un sistema E/E/PE legato alla sicurezza a svolgere la sua funzione specificata, quando viene richiesta dal sistema sotto controllo (EUC).
Ipotizzando un tasso di guasto costante λ, la PFD può essere così calcolata:

$$PFD(t) = 1 - e^{-\lambda t} \tag{2.1}$$

dove λ è il tasso medio di guasto pericoloso del componente, espresso in guasti per ora;
t è l'intervallo di tempo considerato, di solito il tempo trascorso dall'ultimo test di prova T_{proof}, il quale di solito è pari a un anno.
Dunque, il PFD è la misura quantitativa dell'integrità di un sistema di sicurezza in modalità di bassa richiesta. Visto che la funzione di sicurezza è richiesta raramente, la funzione istantanea può essere trascurata per valutare invece la funzione nel lungo periodo. Pertanto viene calcolato un valore di PFD medio su tutto l'intervallo in cui opera Ti, ossia l'intervallo tra due test T_{proof}.

$$PFD_{\text{avg}} = \frac{1}{T_i} \int_0^{T_i} PFD(t)\, dt \tag{2.2}$$

Nei sistemi E/E/PE a bassa domanda con componenti affidabili, ossia $\lambda \cdot t \ll 1$ (cioè la proabilità di guasto è molto piccola, tipicamente $< 0{,}1$), allora attraverso lo sviluppo in serie di Taylor:

$$e^{-\lambda t} \approx 1 - \lambda t + \frac{(\lambda t)^2}{2} - \dots$$

ottengo un'approssimazione lineare che semplifica il calcolo di $PFDavg$:

$$1 - e^{-\lambda t} \approx \lambda t \tag{2.3}$$

Per un sistema che ha un singolo canale, il $PFDavg$ è così ricavato:

$$PFD_{\text{avg}} = \frac{1}{T_i}\int_0^{T_i} PFD(t)\,dt = \frac{1}{T_i}\int_0^{T_i}\left(1-e^{-\lambda t}\right)dt \cong \frac{1}{T_i}\int_0^{T_i}\lambda t\,dt = \frac{\lambda\,T_i^2}{2\cdot T_i} = \frac{\lambda\,T_i}{2}$$

In modalità a bassa richiesta, i guasti pericolosi rilevabili λ_{DD} sono automaticamente rilevati dalla diagnostica e il processo viene fermato subito. Questi guasti non contribuiscono alla probabilità che il sistema non funzioni quando dovrebbe. Invece, i guasti pericolosi non rilevati dalla funzione diagnostica λ_{DU}, vengono scoperti solo durante il Proof Test, oppure nel caso in cui venga richiesta la funzione di sicurezza. Per questo motivo, il contributo al $PFDavg$ è determinato solo da λ_{DU}. Statisticamente, il guasto avviene a metà dell'intervallo di test, per cui la durata media in cui il sistema è in stato pericoloso è $Ti/2$.
La formula diventa:

$$PFD_{\text{avg}} = \frac{\lambda_{DU} T_i}{2} \tag{2.4}$$

2.2.3 PFH

Il PFH (Probability of Dangerous Failure per Hour) è una misura fondamentale nell'analisi di integrità della funzione di sicurezza per sistemi E/E/PE che operano in modalità ad alta richiesta o in modalità continua, ossia la funzione di sicurezza viene richiesta più di una volta l'anno, oppure deve essere attiva sempre durante il normale svolgimento delle attività.
Definito nella IEC 62061 come la frequenza media di guasti pericolosi che un sistema può sperimentare in un dato periodo di tempo (ore).

$$PFH_D = \frac{1}{T}\int_0^T w(t)\,dt$$

dove $w(t)$ è il tasso di guasto istantaneo con cui il sistema entra in uno stato di guasto pericoloso in un certo istante t. Poi viene fatta la media su tutto l'intervallo T.
Si assume nei componenti di sicurezza E/E/PE che $w(t)$ sia costante e pari al tasso dei guasti pericolosi non rilevabili λ_{DU}, otteniamo:

$$PFH_D = \frac{1}{T}\int_0^T \lambda_{\text{DU}}\,dt = \frac{1}{T}\,\lambda_{\text{DU}} T = \lambda_{\text{DU}} \tag{2.5}$$

Invece, per i componenti soggetti a invecchiamento, $w(t)$ assume un andamento variabile nel tempo, e il PFH viene calcolato come media temporale del tasso istantaneo di guasto pericoloso.
Un corretto dimensionamento del PFH, supportato dall'uso della ridondanza e da una buona copertura diagnostica, permette ad un componente di soddisfare

il livello di SIL richiesto, come indicato in tabella:

La stima del PFH, quindi, deriva dai tassi di guasto pericolosi λ_D. In molti casi, i costruttori dichiarano il PFH del componente di sicurezza nella scheda tecnica. Altrimenti è possibile fare delle analisi come FMEDA, FTA, ecc. per stimarlo.
A differenza del PFD, in cui l'intevallo del test di prova è fondamentale nel calcolo perché azzera (o quasi) la funzione, nel PFH si preferisce aumentare la Copertura Diagnostica. La diagnostica continua riduce direttamente la componente λ_{DU}. Vengono effettuati anche dei test manuali offline oltre i test di diagnostica, ma è utile che non siano troppo invasivi, e non richiedano il fermo delle operazioni.

2.3 Differenze tra 2010 e 2026

Nella nuova edizione della IEC 61508 sono state introdotte delle modifiche nelle formule per la determinazione del $PFDavg$ in modalità a bassa richiesta, così come nel PFH per modalità di alta richiesta.
Dal 2010 ad oggi il panorama tecnologico e relative applicazioni per la sicurezza nell'industria sono molto differenti. Vengono adottati largamente dispositivi come smart sensors per cui le formule descritte nella versione attuale della norma IEC 61508 sono risultate poco rappresentative della realtà. Le modifiche principali non sono stravolgimenti della teoria di base, ma dei raffinamenti per rendere il calcolo meno approssimativo. In particolare, segue un'analisi per ogni tipologia di architettura del sistema di sicurezza.
Nella IEC 61508-6 troviamo una serie di *assumptions* tali per cui, ogni formula presentata da qui in avanti, rappresenta un'approssimazione della realtà.

2.3.1 Modalità a Bassa Richiesta

Nelle seguenti formule, l'uso dell'MTTR implica che l'intervallo di test diagnostico sia molto piccolo rispetto al tempo di riparazione del componente. In caso contrario, il tempo di diagnostica T verrà trattato come l'intervallo di Proof Test (in tal caso al posto di $MTTR$ verrà inserito $T/2 + MRT$).
Una formula generale del PFD_{avg}, da cui poi derivano tutte le altre formule approssimate, è:

$$PFD_{avg} = \frac{MDT(T)}{T}$$

dove il $MDT(T)$ è il tempo medio di down durante il periodo [0, T] del componente di sicurezza E/E/PE.
In modalità a bassa richiesta, il PFD_{avg} coincide con l'indisponibilità media del canale o del sistema. Per un sistema riparabile, l'indisponibilità media a regime è:

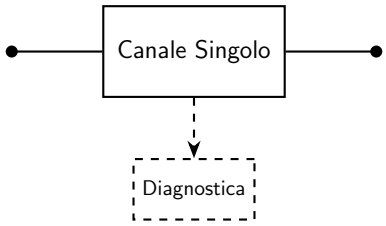
$$PFD_{avg} = \frac{MDT}{MUT + MDT}$$

dove MUT è il Mean Up Time e il MDT indica invece il Mean Down Time. Se il tasso di guasto pericoloso λ_D è costante, allora $MUT = 1/\lambda_D$. Identificando il MDT come il t_{CE} che viene usato comunemente nella norma, otteniamo:

$$PFD_{avg} = \frac{t_{CE}}{\frac{1}{\lambda_D} + t_{CE}} = \frac{\lambda_D t_{CE}}{1 + \lambda_D t_{CE}}$$

Si ipotizza un $\lambda_D \cdot t_{CE}$ molto piccolo, tipico per una bassa richiesta.In questo caso si può approssimare usando uno sviluppo del primo ordine e ottenere $PFD_{avg} \approx \lambda_D t_{CE}$.

1oo1



L'architettura 1oo1 comprende un solo canale, senza ridondanza, in cui è presenta la diagnostica. Nal caso in cui il singolo canale dovesse fallire, anche la funzione di sicurezza verrebbe meno. La formula di PFD è la seguente:

$$\text{PFD} = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} \quad \text{dato} \quad \lambda_D t_{CE} \ll 1$$

Il t_{CE} rappresenta il tempo medio in cui il canale è indisponibile. quest'ultimo viene espresso come:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR} \tag{2.6}$$

dove T_1 indica l'Intervallo del Test di Prova.
Nella formula notiamo i tempi di down per due componenti in serie. Uno con un tasso di guasto pericoloso λ_{DU} dato da i guasti non rilevati, e l'atro con un tasso di guasto pericoloso λ_{DD} dai guasti rilevati. Questi tempi sono pesati in base al loro contributo alla probabilità di guasto totale del canale.
Per semplificare i calcoli, viene ipotizzato il secondo termine molto inferiore rispetto al primo, in quanto $MTTR$ (tipicamente di 8 - 10 h) molto più piccolo di $\frac{T_1}{2} + MRT$.
Anche nel primo termine si suppone MRT molto inferiore a $\frac{T_1}{2}$. Quindi otteniamo:

$$PFD_{avg} \approx \lambda_D t_{CE} \approx \lambda_{DU} \cdot \frac{T_1}{2} \tag{2.7}$$

Questa parte della norma non è stata modificata dal 2010 nella Nuova Edizione. Vengono solo spiegati meglio i parametri che compaiono nelle formule.

1oo2

L'architettura di tipo 1oo2 è costituita da due canali connessi in parallelo, ossia presenta una ridondanza tale per cui il sistema continua a funzionare anche se un canale è guasto. Per calcolare la probabilità che entrambi i canali siano guasti in modo pericoloso contemporaneamente, e quindi non adempiere la funzione di sicurezza, vengono considerati gli stessi fattori visti nel primo caso: guasti pericolosi rilevati e non. Pertanto, la formulazione del t_{CE} è ancora una volta la stessa.
Viene considerato il test della diagnostica non influente sull'output votante. Questo si limita a riportare i guasti riscontrati.
In modalità a bassa richiesta, nella Nuova Edizione della norma vengono apportate alcune modifiche matematiche nel calcolo del t_{GE}, ossia il tempo medio in cui il gruppo 1oo2 è indisponibile. Nella versione del 2010 [3] veniva usato l'$MTTR$ intero, mentre nella nuova si usa $MTTR/2$. Nelle formule vengono evidenziate in rosso le parti presenti nella Prossima Edizione e aggiunte o modificate rispetto all'attuale:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + \mathrm{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\frac{\mathrm{MTTR}}{2} \tag{2.8}$$

Questo è stato introdotto perché in un sistema ridondante, la probabilità che il secondo canale si guasti mentre sto riparando il primo è distribuita probabilisticamente, per cui considero la media di esposizione al guasto durante la finestra di riparazione del primo. Questo è espresso nelle *Hypotesis* della IEC 61508-6, B.3.2.1. In questo modo il PFD risulta leggermente ridotto.
Nell'espressione di PFD viene modificata la notazione di β, ossia il fattore che rappresenta i Guasti di Causa Comune (CCF).
Nella norma del 2010 si usava β per i guasti non rilevati e β_D per i guasti rilevati. Nella nuova versione viene esplicitata la β_{DU} per i guasti pericolosi non rilevati e β_{DD} per i pericolosi rilevati. Questa nuova formulazione rimuove le possibili ambiguità:

$$\begin{aligned}\mathrm{PFD}_G = 2\left[(1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\right]^2 t_{CE}\, t_{GE} + \beta_{DD}\lambda_{DD}\,\mathrm{MTTR} \\ + \beta_{DU}\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right)\end{aligned} \tag{2.9}$$

2oo2

L'architettura 2oo2 comprende due canali disposti in parallelo, ed entrambi possono soddisfare la funzione di sicurezza. Si assume di nuovo che il test diagnostico non può modificare lo stato del sistema.
L'attuale edizione, così come la futura, hanno le stesse formulazioni del tempo equivalente di indisponibilità del canale singolo t_{CE}, la cui formula è stata vista in precedenza. Anche il PFD_G rimane invariato, ed è espresso come:

$$PFD_G = 2\lambda_D t_{CE} \tag{2.10}$$

1oo2D

L'architettura 1*oo*2*D* è composta da due canali attivi connessi in parallelo, con aggiunta la funzione diagnostica che rileva i guasti pericolosi e sicuri su entrambi i canali in maniera indipendente. Viene rilevata una discordanza tra i due canali nel caso di guasto. Quando ciò avviene, il sistema di diagnostica fa in modo che il sistema si adatti di conseguenza, in particolare la funzione di sicurezza viene soddisfatta dal canale non guasto.
Il sistema di adattamento al guasto non è sempre efficiente al massimo, per cui il sistema potrebbe rimanere in 2oo2 come output. Il parametro K rappresenta la frazione funzionamento corretto atteso nel confronto tra i due canali effettuato dalla funziona diagnostica, specifica quanto il sistema gestisca bene la ridondanza interna. Può anche essere visto come l'efficienza (o la copertura) del canale diagnostico.
Già nella versione del 2010 appariva questo fattore, ma solo nel calcolo del PFD_G, mentre nella nuova versione notiamo le formule del t'_{CE} e del PFD_G notevolmente cambiate dall'aggiunta di K e di un fattore moltiplicativo 2. Nello specifico (in rosso le modifiche apportate nella Nuova Edizione):

$$t'_{CE} = \frac{K\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + 2(K\lambda_{DD} + \lambda_{SD})MTTR}{K\lambda_{DU} + 2(K\lambda_{DD} + \lambda_{SD})} \tag{2.11}$$

dove

$$\lambda_{SD} = \lambda_S \cdot DC \tag{2.12}$$

Viene aggiunto un fattore moltiplicativo 2 perché ci sono due canali che possono guastarsi in modo indipendente. Per cui la frequenza totale con cui il sistema entra nello stato di riparazione è il doppio del singolo canale.
Il calcolo del t'_{GE} rimane uguale:

$$t'_{GE} = \frac{T_1}{3} + MRT \tag{2.13}$$

La formula della PFD_G nella Nuova Edizione diventa:

$$\begin{aligned} \mathrm{PFD}_G = {} & 2(1-\beta_{DU})K\lambda_{DU}((1-\beta_{DU})K\lambda_{DU} + 2(1-\beta_{DD})K\lambda_{DD} + 2\lambda_{SD})\times \\ & \times t'_{CE}\, t'_{GE} + 2(1-K)\lambda_{DD}\,\mathrm{MTTR} + 2(1-\beta_{DU})(1-K)\lambda_{DU}\times \\ & \times \left(\frac{T_1}{2} + \mathrm{MRT}\right) + \beta_{DU}\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right) \end{aligned} \tag{2.14}$$

Nella versione attuale, troviamo il valore di t'_{CE} invece del $MTTR$, per questo motivo viene riportato in rosso. Nella futura versione, viene, inoltre, inserito un intero termine, evidenziato in rosso nella formula, che indica la parte di guasti che rimane non rilevata. In questo caso, quindi, non viene avviato il trip di sicurezza, per cui il sistema continua a operare fino al rilevamento durante il Test di Prova.

2oo3

L'architettura 2oo3 contiene tre canali connessi in parallelo, e la diagnostica rileva i discostamenti fra i tre canali, ma non va ad agire sull'output del sistema. Due canali su tre devono essere attivi in modo da performare la funzione di sicurezza. Il t_{CE} è lo stesso visto nell'architettura 1oo1, e il t_{GE} come visto in 1oo2.
Nella formula del PFD_G, rispetto alla versione attuale, cambiano solo i pedici di β, i quali, nella Nuova Edizione, vengono esplicitati tra β_{DD} e β_{DU}, mentre prima venivano inglobati in β e β_D.

$$\begin{aligned}\mathrm{PFD}_G = 6\left[(1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\right]^2 t_{CE}\, t_{GE} + \beta_{DD}\lambda_{DD}\,\mathrm{MTTR} \\ + \beta_{DU}\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right)\end{aligned} \tag{2.15}$$

1oo3

Nell'architettura 1oo3 troviamo tre canali in parallelo con un meccanismo votante per i segnali di output, in cui basta un canale non guasto affinché la funzione di sicurezza venga rispettata. La funzione diagnostica, invece, rileva solo le discrepanze fra canali ma non si attiva per modificare lo stato del sistema. Il t_{CE} e il t_{GE} non cambiano rispetto a quanto già analizzato. La Probabilità Media di Guasto su Richiesta per questo scenario è:

$$\begin{aligned}\mathrm{PFD}_G = 6\left[(1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\right]^2 t_{CE}\, t_{GE}\, t_{G2E} + \beta_{DD}\lambda_{DD}\,\mathrm{MTTR} \\ + \beta_{DU}\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right)\end{aligned} \tag{2.16}$$

Nella formula compare un nuovo parametro, t_{G2E}, che è il tempo medio equivalente del secondo gruppo, ovvero il terzo canale fallisce mentre gli altri due sono già guasti. La finestra temporale si riduce ulteriormente diventando $T_1/4$. Rispetto alla versione del 2010, nel calcolo del t_{G2E} viene aggiunto un fattore riduttivo di 1/3 all'$MTTR$, come charito dalle ipotesi iniziali nella norma IEC 61508-6:2026 B.3.2.1. In un sistema a tre canali votanti 1oo3, con riparazione su linea, dopo che il primo guasto si verifica, i due guasti sugli altri due canali avverranno, in media, ad un terzo e due terzi durante l'$MTTR$ del primo guasto avvenuto.

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + \mathrm{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\frac{\mathrm{MTTR}}{3} \tag{2.17}$$

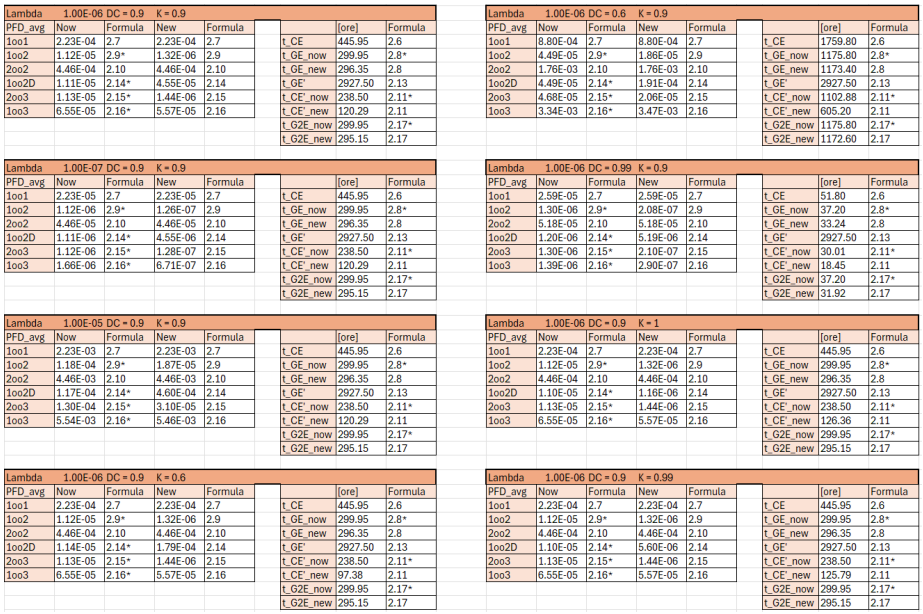
2.3.2 Simulazione di Analisi Comparativa PFD

Di seguito viene fornito un esempio di analisi di confronto tra la versione attuale della norma IEC 61508 e quella futura per tutte le architetture di sicurezza

citate in bassa richiesta di funzionamento. Viene calcolato il valore di PFD_{avg} (Probabilità di Guasto su Richiesta) al variare di alcuni parametri fondamentali, ovvero λ, DC e K. Per ogni architettura viene calcolato il tempo di indisponibilità del canale o del gruppo utili nel calcolo della probabilità di fallimento della funzione di sicurezza. Vengono usati i seguenti dati per la prima tabella, quella ipotizzata come base, con cui poi confrontare le variazioni:

- Frazione di Ripartizione dei Guasti Pericolosi e Sicuri: 0.5
- Tasso Totale di Guasto λ: 1.00×10^{-6} / h
- Copertura Diagnostica DC: 0.9
- Fattore di Causa Comune β: 0.05
- Efficienza della Diagnostica K: 0.9
- Tempo Medio di Ripristino $MTTR = 8$ ore; Tempo Medio di Riparazione MRT: 7.5 ore
- Intervalli di Test: T_1 (Proof Test) = 8760 ore; T_2 (Intervallo Diagnostico) = 1 ora.

Le tabelle riportano il valore del PFD_{avg} con affianco il numero della formula che è stata usata. All'interno di ciascuna tabella vengono riportati come titolo in alto i parametri utilizzati per la specifica tabella.
Di lato, sono stati calcolati i tempi di indisponibilità utili nelle formule del PFD, che variano anch'essi in funzione dei parametri, e anche tra versione attuale della norma e versione aggiornata.
Le formule riportate con l'* indicano la formula specifica non considerando le parti in rosso, che sono le aggiunte fatte nella nuova edizione della norma. Quindi la formula senza l'* indica la versione completa, comprese le parti segnate in rosso, e indica che si sta considerando la nuova edizione della IEC 61508.
Di seguito vengono riportate le tabelle fatte sulla la piattaforma Excel con i risultati ottenuti:



Lambda	1.00E-06	DC = 0.9	K = 0.9				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-04	2.7	2.23E-04	2.7	t_CE	445.95	2.6
1oo2	1.12E-05	2.9*	1.32E-06	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-04	2.10	4.46E-04	2.10	t_GE_new	296.35	2.8
1oo2D	1.11E-05	2.14*	4.55E-05	2.14	t_GE'	2927.50	2.13
2oo3	1.13E-05	2.15*	1.44E-06	2.15	t_CE'_now	238.50	2.11*
1oo3	6.55E-05	2.16*	5.57E-05	2.16	t_CE'_new	120.29	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Lambda	1.00E-06	DC = 0.6	K = 0.9				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	8.80E-04	2.7	8.80E-04	2.7	t_CE	1759.80	2.6
1oo2	4.49E-05	2.9*	1.86E-05	2.9	t_GE_now	1175.80	2.8*
2oo2	1.76E-03	2.10	1.76E-03	2.10	t_GE_new	1173.40	2.8
1oo2D	4.49E-05	2.14*	1.91E-04	2.14	t_GE'	2927.50	2.13
2oo3	4.68E-05	2.15*	2.06E-05	2.15	t_CE'_now	1102.88	2.11*
1oo3	3.34E-03	2.16*	3.47E-03	2.16	t_CE'_new	605.20	2.11
					t_G2E_now	1175.80	2.17*
					t_G2E_new	1172.60	2.17

Lambda	1.00E-07	DC = 0.9	K = 0.9				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-05	2.7	2.23E-05	2.7	t_CE	445.95	2.6
1oo2	1.12E-06	2.9*	1.26E-07	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-05	2.10	4.46E-05	2.10	t_GE_new	296.35	2.8
1oo2D	1.11E-06	2.14*	4.55E-06	2.14	t_GE'	2927.50	2.13
2oo3	1.12E-06	2.15*	1.28E-07	2.15	t_CE'_now	238.50	2.11*
1oo3	1.66E-06	2.16*	6.71E-07	2.16	t_CE'_new	120.29	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Lambda	1.00E-06	DC = 0.99	K = 0.9				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.59E-05	2.7	2.59E-05	2.7	t_CE	51.80	2.6
1oo2	1.30E-06	2.9*	2.08E-07	2.9	t_GE_now	37.20	2.8*
2oo2	5.18E-05	2.10	5.18E-05	2.10	t_GE_new	33.24	2.8
1oo2D	1.20E-06	2.14*	5.19E-06	2.14	t_GE'	2927.50	2.13
2oo3	1.30E-06	2.15*	2.10E-07	2.15	t_CE'_now	30.01	2.11*
1oo3	1.39E-06	2.16*	2.90E-07	2.16	t_CE'_new	18.45	2.11
					t_G2E_now	37.20	2.17*
					t_G2E_new	31.92	2.17

Lambda	1.00E-05	DC = 0.9	K = 0.9				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-03	2.7	2.23E-03	2.7	t_CE	445.95	2.6
1oo2	1.18E-04	2.9*	1.87E-05	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-03	2.10	4.46E-03	2.10	t_GE_new	296.35	2.8
1oo2D	1.17E-04	2.14*	4.60E-04	2.14	t_GE'	2927.50	2.13
2oo3	1.30E-04	2.15*	3.10E-05	2.15	t_CE'_now	238.50	2.11*
1oo3	5.54E-03	2.16*	5.46E-03	2.16	t_CE'_new	120.29	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Lambda	1.00E-06	DC = 0.9	K = 1				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-04	2.7	2.23E-04	2.7	t_CE	445.95	2.6
1oo2	1.12E-05	2.9*	1.32E-06	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-04	2.10	4.46E-04	2.10	t_GE_new	296.35	2.8
1oo2D	1.10E-05	2.14*	1.16E-06	2.14	t_GE'	2927.50	2.13
2oo3	1.13E-05	2.15*	1.44E-06	2.15	t_CE'_now	238.50	2.11*
1oo3	6.55E-05	2.16*	5.57E-05	2.16	t_CE'_new	126.36	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Lambda	1.00E-06	DC = 0.9	K = 0.6				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-04	2.7	2.23E-04	2.7	t_CE	445.95	2.6
1oo2	1.12E-05	2.9*	1.32E-06	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-04	2.10	4.46E-04	2.10	t_GE_new	296.35	2.8
1oo2D	1.14E-05	2.14*	1.79E-04	2.14	t_GE'	2927.50	2.13
2oo3	1.13E-05	2.15*	1.44E-06	2.15	t_CE'_now	238.50	2.11*
1oo3	6.55E-05	2.16*	5.57E-05	2.16	t_CE'_new	97.38	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Lambda	1.00E-06	DC = 0.9	K = 0.99				
PFD_avg	Now	Formula	New	Formula		[ore]	Formula
1oo1	2.23E-04	2.7	2.23E-04	2.7	t_CE	445.95	2.6
1oo2	1.12E-05	2.9*	1.32E-06	2.9	t_GE_now	299.95	2.8*
2oo2	4.46E-04	2.10	4.46E-04	2.10	t_GE_new	296.35	2.8
1oo2D	1.10E-05	2.14*	5.60E-06	2.14	t_GE'	2927.50	2.13
2oo3	1.13E-05	2.15*	1.44E-06	2.15	t_CE'_now	238.50	2.11*
1oo3	6.55E-05	2.16*	5.57E-05	2.16	t_CE'_new	125.79	2.11
					t_G2E_now	299.95	2.17*
					t_G2E_new	295.15	2.17

Figura 2.2: Confronto del valore di PFD_{avg} al variare di λ, DC e K

Dentro ogni tabella, e per ogni configurazione, si può comparare la versione nuova (New) con quella attuale (Now). Le prime tre tabelle sulla sinistra indicano come variano i risultati al variare di λ, che passa da 10^{-6} come dato di input, a 10^{-7} e 10^{-5}. In generale si può dire che nella versione New i valori di PFD sono simili o più bassi rispetto a quelli ricavati con le formule nella versione attuale. Questo significa che i risultati sono più ottimistici e meno conservativi, essendo più accurati.
Nella seconda fila di tabelle, sulla destra, vediamo l'analisi al variare della Copertura Diagnostica DC, che oltre al caso base, viene proposta pari a 0.6, per indicare il caso peggiore, e 0.99 per indicare un'ampia copertura della funzione diagnostica. Intuitivamente, possiamo notare tra le due tabelle che nel caso di DC più basso i valori di PFD tenderanno a salire rispetto al caso migliore. La differenza si nota in particolare per architetture come 1oo3, in cui, se consideriamo la versione New, ci sono quattro ordini di grandezza che dividono il caso in cui la diagnostica rileva i guasti pericolosi solo al 60% e quello in cui li rileva al 99%.
Nelle tabelle in basso si fa variare il valore del fattore K, che indica l'efficienza della diagnostica, da un valore di 0.6 a 0.99 e poi anche si ipotizza pari a 1. Il fattore K si trova solo nella configurazione con diagnostica che agisce in modo attivo sulla funzione di sicurezza, ovvero 1oo2D. Nel caso in cui K sia molto basso, il valore di PFD nel caso "New" è peggiore rispetto alla modellazione attuale. Al contrario, se K è elevato, va a migliorare di un ordine di grandezza la probabilità di fallimento, ovvero abbassandolo, rispetto alla versione attuale. Si può anche notare come, passando dal caso peggiore a quello ideale in cui K

sia pari a 1, per la formulazione "New" il PFD subisce un miglioramento pari a due ordini di grandezza.

2.3.3 Modalità ad Alta o Continua Richiesta

Il calcolo della Probabilità di Fallimento della fuzione di sicurezza per un componente E/E/PE legato alla sicurezza in Modalità ad Alta Richiesta o Continua viene espresso come Frequenza Media di Guasto Pericoloso del sistema PFH_{SYS}. In generale è pari alla somma delle frequenze di guasto dei suoi sotto-sistemi.
Questa modalità comprende le macchine industriali, quali presse, nastri ecc. I calcoli sono basati sulle *hypotesis* espresse in B.3.2.1 di IEC 61508-6:2026.

1oo1

In questa architettura in modalità ad alta richiesta, viene ipotizzato dalle *assumptions* che il sistema di sicurezza metta l'EUC (Equipment Under Control) in uno stato sicuro appena rilevato un guasto. Il calcolo di PFH_G rimane lo stesso rispetto alla precedente edizione della norma:

$$PFH_G = \lambda_{DU} \tag{2.18}$$

1oo2

La Nuova Edizione ha aggiornato questa parte, rendendola più chiara. Se viene rilevato un guasto pericoloso il sistema genera solo un allarme, allora qualsiasi combinazione di guasti in un path e nell'altro, genera una perdita della funzione di sicurezza. Riprendiamo la formulazione di t_{CE}, che non è cambiata rispetto alla vecchia edizione:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\mathrm{MTTR} \tag{2.19}$$

L'uso di $MTTR$ in questa equazione assume che l'intervallo di test della diagnostica è molto piccolo rispetto al tempo di riparazione. Se non è questo il caso, allora l'intervallo del test di diagnostica T può essere trattato come intervallo di Proof Test, quindi ad esempio $MTTR$ diventerà $T/2 + MRT$. Il PFH_G è stato modificato rispetto all'edizione precedente:

$$\mathrm{PFH}_G = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right](1-\beta)\lambda_{DU}\, t_{CE} + \beta\lambda_{DU} \tag{2.20}$$

Invece, nella Nuova Edizione, troviamo una formulazione diversa:

$$\mathrm{PFH}_G = 2\left[(1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\right]^2 t_{CE} + \beta_{DU}\lambda_{DU} + \beta_{DD}\lambda_{DD} \tag{2.21}$$

Se, a seguito della rilevazione di un guasto pericoloso il sistema di sicurezza genera un allarme e avvia un comando di trip entro il tempo di sicurezza previsto,

allora il termine λ_{DD} può essere trattato allo stesso modo di un guasto spurio. Quindi otteniamo:

$$\mathrm{PFH}_G = \left[(1-\beta_{DU})\lambda_{DU}\right]^2 T_1 + \beta_{DU}\lambda_{DU} \tag{2.22}$$

Viene indicato con T_1 l'Intervallo di Proof Test. Queste formule sono state aggiunte rispetto alla vecchia edizione, per questo vengono riportate in rosso.

2oo2

Se si assume che ciascun canale ridondante viene messo in uno stato sicuro appena viene rilevato un guasto, come nell'architettura 1oo1, allora si ottiene:

$$PFH_G = 2\lambda_{DU} \tag{2.23}$$

Questa rimane invariata rispetto all'attuale edizione.

1oo2D

Per questa tipologia di architettura vengono specificati, nella Nuova Edizione, due casi:

$$\lambda_{SD} = \lambda_S DC \tag{2.24}$$

$$t'_{CE} = \frac{K\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + 2\left(K\lambda_{DD} + \lambda_{SD}\right)\mathrm{MTTR}}{K\lambda_{DU} + 2\left(K\lambda_{DD} + \lambda_{SD}\right)} \tag{2.25}$$

$$\begin{aligned}\mathrm{PFH}_G = {} & (1-\beta_{DU})K\lambda_{DU}\left[(1-\beta_{DU})K\lambda_{DU} + 2K\lambda_{DD} + 2\lambda_{SD}\right]\times \\ & \times\left(t'_{CE} + \frac{T_1}{2} + MRT\right) + 2(1-K)\left(\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\right) + \beta_{DU}\lambda_{DU}\end{aligned} \tag{2.26}$$

Invece nella precedente versione, era solo stato inserito il caso in cui:

$$\lambda_{SD} = \frac{\lambda}{2} DC \tag{2.27}$$

$$t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \left(\lambda_{DD} + \lambda_{SD}\right)\mathrm{MTTR}}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}} \tag{2.28}$$

$$\begin{aligned}\mathrm{PFH}_G = {} & 2(1-\beta_{DU})\lambda_{DU}\left[(1-\beta_{DU})\lambda_{DU} + (1-\beta_{DD})\lambda_{DD} + \lambda_{SD}\right]t'_{CE} \\ & + 2(1-K)\lambda_{DD} + \beta_{DU}\lambda_{DU}\end{aligned} \tag{2.29}$$

Anche in questo caso, le aggiunte in rosso indiano la novità, quindi nella versione attuale troviamo i β senza pedice o solo β_D.

2oo3

Per questa architettura in alta domanda, il valore di t_{CE} è stato già espresso nell'architettura 1oo2.
Nella Nuova Edizione, anche in questo caso, è stato distinto il calcolo di PFH_G quando il sistema di rilevamento si limita a generare un allarme dopo aver individuato un guasto. Si ottiene:

$$\text{PFH}_G = 6\Big((1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\Big)^2 t_{CE} + \beta_{DU}\lambda_{DU} + \beta_{DD}\lambda_{DD} \tag{2.30}$$

Se invece, il sistema avvia un comando di trip, ossia porta il sistema in uno stato sicuro entro il tempo di sicurezza predefinito di processo, il λ_{DD} viene trattato come guasto spurio. Per cui si ricava:

$$\text{PFH}_G = 3\big((1-\beta_{DU})\lambda_{DU}\big)^2 T_1 + \beta_{DU}\lambda_{DU} \tag{2.31}$$

Mentre, nell'attuale edizione, veniva riassunto tutto da un'unica formulazione più generica:

$$\text{PFH}_G = 6\Big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\Big)(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU} \tag{2.32}$$

1oo3

Secondo questa configurazione ad alta richiesta, i valori di t_{CE} e t_{GE} sono da intendersi uguali alle architetture 1oo2 in bassa richiesta, come specificato nell'incipit della norma.
Si suddividono, nella Nuova Edizione, i due casi distinti di sistema di rilevamento che si limita a generare un alalrme, e sistema che porta l'EUC in uno stato sicuro in tempo.

$$\text{PFH}_G = 6\Big((1-\beta_{DD})\lambda_{DD} + (1-\beta_{DU})\lambda_{DU}\Big)^3 t_{CE} t_{GE} + \beta_{DU}\lambda_{DU} + \beta_{DD}\lambda_{DD} \tag{2.33}$$

Nel secondo caso, la formula diventa:

$$\text{PFH}_G = \big((1-\beta_{DU})\lambda_{DU}\big)^3 T_1^2 + \beta_{DU}\lambda_{DU} \tag{2.34}$$

Anche questa volta, si riporta la formula della scorsa edizione per completezza:

$$\text{PFH}_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2(1-\beta)\lambda_{DU} t_{CE} t_{GE} + \beta\lambda_{DU} \tag{2.35}$$

2.4 Confronto High Demand con IEC 62061

La IEC 62061 è lo standard specifico per il settore macchine. L'approccio suggerito nella norma IEC 62061 viene applicato solo nel caso in cui la funzione di sicurezza venga richiesta su base giornaliera o settimanale, il che è coerente con

il settore.
La norma IEC 62061 deriva dalla IEC 61508, ma l'approccio che adottano è diverso. Nella IEC 61508 vengono calcolati separatamente λ_{DD} e λ_{DU} e solo dopo si calcola il DC. Nella IEC 62061 notiamo che il calcolo dei due tassi di guasto avviene mediante il tasso totale di guasti pericolosi λ_D e il DC:

$$\lambda_{DU} = \lambda_D \times (1 - DC)$$

$$\lambda_{DD} = \lambda_D \times DC$$

La norma IEC 62061 utilizza principalmente diagrammi a blocchi RBD per il calcolo dell'affidabilità, e si ipotizza che tutti i sottosistemi di sicurezza siano riparabili.

Architettura di un Sotto-sistema di Base A: 1oo1

Questa architettura corrisponde a un singolo canale senza diagnostica, per cui qualsiasi guasto pericoloso di un elemento provoca il fallimento della funzione di sicurezza.
Nel caso di modalità ad alta richiesta, questo tipo di architettura non può usare un intervallo di test di prova che sia più frequente della vita utile del sistema (Mission Time).

$$PFH_D = \sum_{i=1}^{n} \lambda_{D_{e_i}} = \lambda_{D_{e_1}} + \lambda_{D_{e_2}} + \cdots + \lambda_{D_{e_n}} \tag{2.36}$$

Questa è la formula del PFH_D, ossia la somma dei tassi di guasto pericolosi di tutti gli elementi.
In questa tipologia di architettura, ossia con $HFT = 0$, nel caso di componenti elettromeccanici, il livello massimo di SIL raggiungibile è pari a 1.

Architettura di un Sottosistema di Base B: 1oo2

L'architettura Base di un sotto-sistema di tipo B nella IEC 62061 corrisponde a due canali in parallelo, senza alcuna funziona diagnostica. Un singolo guasto in uno dei canali non causa, quindi, la perdita della funzione di sicurezza. avendo un $HFT = 1$.
La formula del PFH_D viene così espressa:

$$PFH_D = (1 - \beta)^2 \, \lambda_{De_1} \, \lambda_{De_2} \, T_1 + \beta \, \frac{\lambda_{De_1} + \lambda_{De_2}}{2} \tag{2.37}$$

dove:

- T_1 è l'intervallo di Proof Test oppure la vita utile del componente, scegliendo il valore minore.
- β è il fattore di sensitività ai guasti dati da una causa comune.

Nel caso di due elementi uguali la formula diventa:

$$PFH_D = (1-\beta)^2 \cdot \lambda_D^2 \cdot T_1 + \beta \cdot \lambda_D \tag{2.38}$$

La formula tiene conto dei due tipi di guasto. Nel primo termine abbiamo la componente dei guasti indipendenti $(1-\beta)$, che cresce con il T_1, ovvero con il tempo in cui il sistema non viene testato.
Nel secondo termine troviamo i guasti da causa comune, quindi che avvengono contemporaneamente, e la media dei tassi di guasto pericoloso dei due elementi. Anche in questo caso, viene distinto il discorso tra componenti elettronici ed elettromeccanici. Per questi ultimi, avendo una $DC = 0$, può essere raggiunto, anche in questo caso, al massimo un SIL 1.
Per i componenti elettronici invece, si segue la tabella sotto:

Safe Failure Fraction	**Hardware Fault Tolerance of an element**		
	HFT = 0	**HFT = 1**	**HFT= 2**
< 0.6	SIL 1*	SIL 1	SIL 2
0.6 - 0.9	SIL 1	SIL 2	SIL 3
0.9 - 0.99	SIL 2	SIL 3	SIL 3
> 0.99	SIL 3	SIL 3	SIL 3

Tabella 2.3: Vincoli di Architettura per un sotto-sistema B: massimo SIL raggiungibile

* Solo se sono usati componenti well-tried

Architettura di un Sottosistema di Base C: 1oo1D

Questa architettura nella IEC 61508 non è presente. Si tratta di un singolo canale con diagnostica. Qualsiasi guasto pericoloso non rilevato provoca il fallimento in modo pericoloso della funzione di sicurezza, mentre nel caso in cui fosse un guasto rilevato, la funzione diagnostica avvia una reazione al guasto.
Il PFH_D viene considerato rappresentativo nel caso in cui la frequenza della diagnostica r_t è almeno 100 volte maggiore della frequenza della funzione di sicurezza r_d e il tempo di reazione della diagnostica è sufficientemente breve da trovarsi in stato sicuro. Oppure nel caso in cui la gestione del guasto viene effettuata continuamente o periodicamente (purché il tempo di intervallo di test, di rilevazione e di reazione siano inferiori al tempo di sicurezza del processo). Se la funzione diagnostica non può portare il sistema in uno stato sicuro, allora bisogna cambiare la configurazione in un 1oo1 e devono essere usati componenti well-tried. In questo caso, il SIL massimo ottenibile sarà di livello 1.

Architettura di un Sottosistema di Base D: 1oo2D

Come visto in precedenza, questa architettura presenta un doppio canale con diagnostica, tale per cui un singolo guasto di un elemento non provoca la perdita

	Stato Sicuro	**No Stato Sicuro**
$r_t/r_d < 100$	1oo1D SIL 2	1oo1 SIL 1
$r_t/r_d \geq 100$	1oo1D SIL 2	1oo1 SIL 1

Tabella 2.4: Sintesi dei possibili casi di 1oo1D

della funzione di sicurezza. Nel caso di guasto, la funzione diagnostica avvia una funzione di reazione al guasto.

$$PFH_D = (1-\beta)^2 \cdot \left[\lambda_{De_1}\lambda_{De_2}(DC_1 + DC_2)\frac{T_2}{2} + \lambda_{De_1}\lambda_{De_2}(2 - DC_1 - DC_2)\frac{T_1}{2}\right] + \beta\frac{\lambda_{De_1}\lambda_{De_2}}{2}$$

In questa formula si considerano due elementi diversi, con ciascuno il proprio λ_{De}, ossia il tasso di guasto pericoloso, e la propria copertura diagnostica DC. Il termine T_1 rappresenta l'intervallo di Proof Test o la vita utile dell'elemento (viene scelto il più piccolo tra i due), e il termine T_2 che, invece, è l'intervallo del test di diagnostica.
Nel caso in cui i due elementi siano uguali, la formula del PFH_D diventa:

$$PFH_D = (1-\beta)^2[DC \cdot T_2 + (1-DC) \cdot T_1] \cdot \lambda_{De}^2 + \beta \cdot \lambda_{De} \tag{2.39}$$

Per la determinazione del SIL massimo, nel caso di componenti elettronici, viene ancora presa in considerazione la Table 2.3.

2.4.1 Simulazione di Analisi Comparativa PFH

In questa sezione viene proposto un esempio di analisi quantitativa eseguita per valutare l'affidabilità di alcune architetture di sicurezza in alta richiesta. Vengono implementate le formule viste finora della PFH (Probabilità di Guasto all'Ora) sulla piattaforma Excel. In particolare sono state confrontate le configurazioni di tipo 1oo1, 1oo2 e 1oo2D, seguendo i due standard IEC 61508 e IEC 62061.
Come nell'analisi di PFD_{avg}, per l'analisi di PFH sono stati usati i seguenti dati di input:

- Frazione di Ripartizione dei Guasti Pericolosi e Sicuri: 0.5
- Tasso Totale di Guasto λ: 1.00×10^{-6} / h
- Copertura Diagnostica DC: 0.9
- Fattore di Causa Comune β: 0.05
- Efficienza della Diagnostica K: 0.9

- Tempo Medio di Ripristino $MTTR = 8$ ore; Tempo Medio di Riparazione MRT: 7.5 ore
- Intervalli di Test: T_1 (Proof Test) = 8760 ore; T_2 (Intervallo Diagnostico) = 1 ora.

Le tabelle indicano il valore di PFH utilizzando le formule viste finora.
Per ciascuna tabella vengono riportati in alto i valori dei parametri che vengono utilizzati in ciascuna formula che poi per ogni tabella vengono fatti variare. Le tabelle riportano, quindi, un'analisi di sensitività, in quanto sono stati fatti variare alcuni parametri fondamentali del sistema. Tra questi il tasso di guasto totale λ che è sato considerato prima pari a 1000 FIT (10^{-6} / h), poi a 10000 FIT e infine a 100 FIT.
Gli altri due parametri che hanno subito una variazione sono la DC, oscillando tra da 0.6 a 0.99, e allo stesso modo è stato fatto per il fattore K, fino a ipotizzarlo pari a 1.
La prima riga di ogni tabella indica la normula del PFH che si trova nella versione attuale della norma IEC 61508. Affianco ad ogni valore di PFH viene riportato il numero di riferimento della formula che viene utilizzata, che corrispondono alle formule nella sezione precedente.
La seconda e terza riga vengono utilizzate per indicare le formule modificate che verranno implementate nella Nuova Edizione della IEC 61508. Per la configurazione 1oo1 non vengono inserite perché rimane invariata la formula del PFH rispetto alla versione attuale. Nella configurazione 1oo2 la seconda riga, "IEC61508 new" indica la versione della formula completa, considerando i guasti rilevati dalla diagnostica all'interno del calcolo, ovvero in cui la diagnostica abbia solo il ruolo di rilevare i guasti. Mentre la terza riga delle tabelle per la configurazione 1oo2, indicata con "IEC 61508 new"', fa riferimento all'introduzione nella Nuova Edizione delle formule di PFH nel caso in cui la diagnostica avvii un trip di sicurezza, ovvero in cui il λ_{DD} non viene incluso perché considerato come sicuro.
Per la configurazione 1oo2D, la prima riga indica il caso attuale, in cui viene incluso il valore di $t_C E'$ derivante dalla Formula 2.28, il quale rimane invariato anche per il calcolo di PFH nella seconda riga (IEC 61508 new). Sulla prima riga in 1oo2D, per il calcolo di PFH, si fa riferimento alla formula 2.29 non per intero, ma solo alle parti in nero, come si trova nella versione attuale, senza includere le aggiunte in rosso. Nella seconda riga, infatti, cambia la formula di PFH perché viene usata la Formula 2.29 completa, anche incluse le parti in rosso, relative ai pedici di β.
Nella terza riga della configurazione 1oo2D, sia la formula del t'_{CE}, etichettato come "new" nella tabella sotto, sia il PFH aumentano la loro dipendenza dal fattore K, che appare frequentemente in entrambe le espressioni.
Nella quarta riga vengono usate le formule del calcolo di PFH espresse nella norma IEC 62061, che fanno riferimento alla sezione precedente.
I valori di λ_{SD} sarebbero diversi tra di loro, ma in questo caso è stato usato un valore di 0.5 della frazione dei tassi sicuri, quindi coincidono.
La prima tabella indica il caso base, in cui troviamo i dati di input definiti nel-

l'elenco sopra.
In Figura 2.2 vengono comparati i valori di PFH e dei tempi medi di indisponibilità calcolati con le diverse formule suggerite dagli approcci visti.

lambda	1.00E-06	DC 0.9	K 0.9			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-08	2.18	2.52E-09	2.20	9.25E-08	2.29 *
IEC61508_new			2.09E-08	2.21	9.03E-08	2.29
IEC61508_new'			2.72E-10	2.22	1.01E-07	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.52E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-07	2.24
t_CE'	238.5	2.28	120.72	2.25

lambda	1.00E-07	DC 0.9	K 0.9			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-09	2.18	2.50E-10	2.20	9.25E-09	2.29 *
IEC61508_new			2.05E-09	2.21	9.03E-09	2.29
IEC61508_new'			2.52E-11	2.22	1.00E-08	2.26
IEC62061	5.00E-08	2.36	2.52E-09	2.38	2.50E-09	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-08	2.24
t_CE'	238.5	2.28	120.29	2.25

lambda	1.00E-05	DC 0.9	K 0.9			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-07	2.18	2.70E-08	2.20	9.27E-07	2.29 *
IEC61508_new			2.42E-07	2.21	9.05E-07	2.29
IEC61508_new'			4.67E-09	2.22	1.04E-06	2.26
IEC62061	5.00E-06	2.36	4.48E-07	2.38	2.70E-07	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-06	2.24
t_CE'	238.5	2.28	120.29	2.25

lambda	1.00E-06	DC 0.6	K 0.9			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	2.00E-07	2.18	1.03E-08	2.20	7.03E-08	2.29 *
IEC61508_new			1.41E-08	2.21	6.43E-08	2.29
IEC61508_new'			4.34E-09	2.22	1.04E-07	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.58E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	1759.8	2.19		
SD	4.50E-07	2.27	3.00E-07	2.24
t_CE'	1102.88	2.28	605.20	2.25

lambda	1.00E-06	DC 0.99	K 0.9			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-09	2.18	2.50E-10	2.20	9.93E-08	2.29 *
IEC61508_new			2.46E-08	2.21	9.90E-08	2.29
IEC61508_new'			2.72E-12	2.22	1.00E-07	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.50E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	51.795	2.19		
SD	4.50E-07	2.27	4.95E-07	2.24
t_CE'	30.0075377	2.28	18.45	2.25

lambda	1.00E-06	DC 0.9	K 1			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-08	2.18	2.52E-09	2.20	2.52E-09	2.29 *
IEC61508_new			2.09E-08	2.21	2.72E-10	2.29
IEC61508_new'			2.72E-10	2.22	6.65E-10	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.52E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-07	2.24
t_CE'	238.5	2.28	126.36	2.25

lambda	1.00E-06	DC 0.9	K 0.6			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-08	2.18	2.52E-09	2.20	3.63E-07	2.29 *
IEC61508_new			2.09E-08	2.21	3.60E-07	2.29
IEC61508_new'			2.72E-10	2.22	4.00E-07	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.52E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-07	2.24
t_CE'	238.50	2.28	97.38	2.25

lambda	1.00E-06	DC 0.9	K 0.99			
	1oo1	Formula	1oo2	Formula	1oo2D	Formula
IEC61508_now	5.00E-08	2.18	2.52E-09	2.20	1.15E-08	2.29 *
IEC61508_new			2.09E-08	2.21	9.27E-09	2.29
IEC61508_new'			2.72E-10	2.22	1.07E-08	2.26
IEC62061	5.00E-07	2.36	2.70E-08	2.38	2.52E-08	2.39

IEC61508	now	Formula	new	Formula
t_CE	445.95	2.19		
SD	4.50E-07	2.27	4.50E-07	2.24
t_CE'	238.5	2.28	125.79	2.25

Figura 2.3: Confronto del valore di PFH al variare di λ, DC e K

Dall'analisi dei risultati in Figura 2.2, emerge che per un sistema con la nuova formula 1oo2 presente nella nuova edizione della IEC 61508-6 con l'avviamento di trip di sicurezza mediante diagnostica (terza riga), il valore di PFH risulta sensibilmente inferiore, ovvero più ottimistico, rispetto allo stesso in un sistema 1oo2 considerando i $\lambda_D D$ ovvero la formula completa contenuta nella nuova edizione della IEC 61508, riportato nella seconda riga delle tabelle.
Un'altra considerazione viene fatta, invece, per la configurazione 1oo2D. Si può notare come nella versione attuale e quella completa, ovvero prima e seconda riga, i valori del tempo di indisponibilità risultano molto simili tra di loro. Questo non accade nella terza riga, in cui i PFH risultano tutti peggiorati, ovvero aumentati, rispetto agli altri casi.

In merito al confronto con la norma IEC 62061, i risultati variano in base ai parametri di input considerati.
Al variare di λ, nelle prime tre tabelle, i PFH della IEC 62061 (quarta riga), quello calcolato con la formula completa del PFH nella IEC 61508 (seconda

riga) e anche con la versione attuale (prima riga) risultano molto simili nella configurazione 1oo2. Nella configurazione 1oo2D, gli stessi sono confrontabili e appartenenti allo stesso ordine di grandezza. Nella 1oo1, questi differiscono di un ordine di grandezza. Questo perché nella IEC 61508 il PFH è pari al tasso dei guasti pericolosi non rilevati, mentre nella IEC 62061 vengono presi tutti i guasti pericolosi.

Mantenendo λ e gli altri dati fissi e facendo variare la Copertura Diagnostica DC (quarta e quinta tabella) i valori di PFH variano. Nel caso in cui DC sia molto bassa, pari a 0.6, le configurazioni 1oo1, 1oo2 e 1oo2D risultano molto simili tra di loro. Al contrario, per DC molto alti, i valori di PFH, soprattutto per la configurazione 1oo2 variano tra loro.
Si noti, inoltre, che per la configurazione 1oo2, dal caso di DC pari a 0.6 a 0.99 il PFH diminuisce di due ordini di grandezza.
Al variare del valore di K, nelle ultime tre tabelle, i valori di PFH della IEC 62061 e delle configurazioni 1oo1 e 1oo2 della IEC 61508 non vengono alterati, dal momento che non contengono K al loro interno.
In configurazione 1oo2D, vediamo tutti i valori per la IEC 61508 variare con K. Nel caso in cui K sia molto elevato, nell'esempio pari a 0.99 o a 1, il PFH in configurazione 1oo2D ad abbassare di due ordini di grandezza il PFH rispetto al caso peggiore.
Si noti, infine, che nella tabella in cui si considera K pari a 1, lasciando tutto il resto come nel caso base, la configurazione 1oo2 con avviamento del trip da parte della diagnostica (terza riga) ha un valore di PFH pari alla configurazione 1oo2D (seconda riga), coerentemente con la definizione e le formulazioni viste finora.

3

Sistemi Misti: Alta e Bassa Richiesta

3.1 Cosa sono i Sistemi Misti

I sistemi in modalità mista sono dei Safety Instrumented System SIS che riescono a gestire diverse funzioni di sicurezza, alcune operative in Bassa Richiesta, altre in Alta o Continua Richiesta. Nel settore delle macchine, spesso accade che la funzione di sicurezza in modalità a bassa richiesta abbia un sottosistema di uscitaa condiviso tra funzioni di sicurezza a bassa che alta richiesta.
Viene riportato l'esempio preso dal libro Functional Safety of Machinery (2023) [2], anche riportato in *Figura* 3.1, di come il motore di una pompa può essere utilizzato per più funzioni. Un interruttore di alta pressione va ad arrestare la pompa nel caso in cui la pressione dovesse aumentare troppo, usando una funzione di sicurezza in bassa richiesta. Il motore della pompa è anche collegato a una porta con interblocco che, invece, opera in alta richiesta.

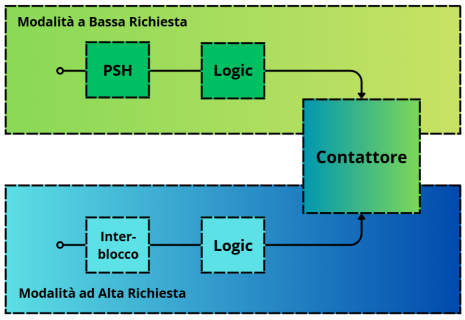


Figura 3.1: Esempio di Sistema Misto: Contattore per Alta e Bassa Richiesta

3.2 Introduzione dei Sistemi Misti nella IEC 61508

La norma IEC 61508:2010 scinde chiaramente le modalità operative di bassa e alta richiesta secondo una soglia temporale fissa: bassa domanda se la funzione viene richiesta meno di una volta all'anno; alta domanda se la frequenza è maggiore di una volta all'anno. Eppure, nei contesti industriali è molto frequente avere un unico sistema che includa diverse logiche. Pertanto, è fondamentale includere nella IEC 61508 un riferimento ufficiale per tali apparecchiature.
Nella norma IEC61508-6:2026 negli Annex B è stata introdotta una sezione a questo proposito, la B.3.3.3.4. Viene riportato direttamente un esempio applicativo. Prendiamo in considerazione per la funzione in alta richiesta un encoder il quale, non appena rileva la posizione specifica richiesta, manda un segnale al PLC di controllo. Questo, a sua volta, comanda un drive il quale toglie l'alimentazione responsabile del movimento e viene azionato il freno. Questa funzione di sicurezza viene avviata frequentemente. Nel frattempo, al rilevamento di una posizione errata da parte di un finecorsa, viene fatto scattare dal PLC di sicurezza il freno, tramite il suo contattore dedicato. Entrambe le situazioni hanno come elemento finale il freno, che agisce per conto di alta e bassa richiesta di funzionamento.
Vengono formulate le seguenti ipotesi:

- I test periodici di prova sono perfetti (100% del rilevamento dei guasti nascosti alla diagnostica); essi vengono eseguiti contemporaneamente per i componenti.
- L'impianto viene fermato durante i test periodici, così da non correre nessun rischio durante il collaudo.
- I guasti pericolosi rilevati e non rilevati sono indipendenti tra di loro.
- I tassi di guasto sono costanti.
- Gli elementi sono come nuovi dopo la riparazione.

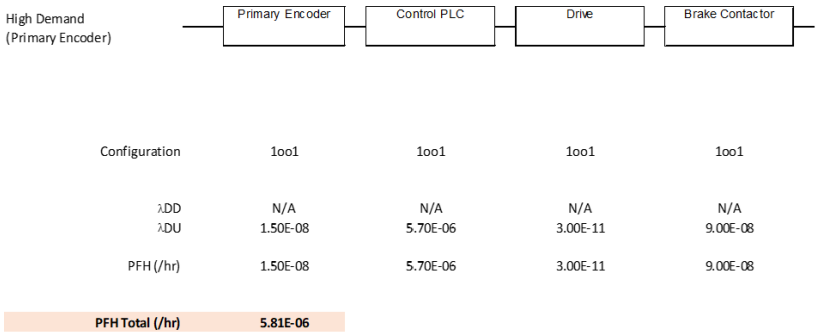
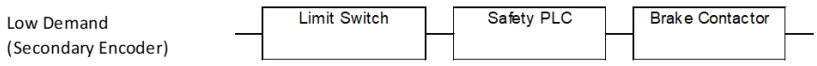


Figura 3.2: SIF Combinata per Modalità in Alta Richiesta, IEC 61508-6:2026 Annex B

La Figura 3.2 analizza la funzione di sicurezza in Alta Richiesta, per cui viene calcolata la frequenza dei guasti pericolosi per ora, la PFH.
La disposizione dei componenti segue un'architettura 1oo1 in cui troviamo un encoder primario che è il sensore di misurazione della posizione, il Control PLC che riceve e rielabora i segnali, il Drive che agisce sul motore elettrico e infine il Contattore del freno che è un componente elettrico che toglie l'alimentazione al freno. Per ciascun elemento viene fornito il tasso dei guasti pericolosi non rilevati λ_{DU_i}. La PFH_i di ciascun componente sarà pari a quest'ultimo.
Per ottenere la PFH_{tot} si sommano i contributi di tutti gli elementi in serie.

$$PFH_{tot} = 1.5 \times 10^{-8} + 5.7 \times 10^{-6} + 3 \times 10^{-11} + 9 \times 10^{-8} = 5.81 \times 10^{-6} \,/\,\mathrm{h}$$

Il valore di PFH del PLC di controllo ha l'affidabilità minore (può raggiungere al massimo SIL 1) e domina l'esito di tutta la catena.
Di seguito viene calcolata la PFD_{avg} per la funzione in bassa richiesta di funzionamento, che prende in considerazione ancora un'architettura 1oo1. In serie troviamo tre elementi: il Limit Switch, o finecorsa, il quale rileva un limite di sicurezza raggiunto o superato e manda dei segnali; il Safety PLC riceve e rielabora i segnali e, in base a questi, interviene; il Contattore del Freno, in tal caso, rimuove l'alimentazione al freno, il quale blocca meccanicamente l'asse e interrompe il movimento.
in Figura 3.3 sono mostrati i dati utili al calcolo della probabilità di guasto quando richiesta la funzione di sicurezza PFD.



	Limit Switch	Safety PLC	Brake Contactor
Configuration	1oo1	1oo1	1oo1
λDD	0.00E+00	6.00E-07	0.00E+00
λDU	3.60E-06	0.00E+00	9.00E-08
MRT/MTTR (hrs)	48	48	48
T1 (hrs)	8760	8760	8760
t_{CE}		3774.1	
PFD	1.36E-02	2.26E-03	3.40E-04
	1.58E-02	2.88E-05	3.94E-04
PFD Total	**1.62E-02**		

Figura 3.3: SIF Combinata per Modalità in Bassa Richiesta, IEC 61508-6:2026 Annex B

La formula applicata per la modalità in bassa richiesta è la seguente:

$$PFD = \lambda_D \cdot t_{CE}$$

dove

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{2} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

I fattori λ_D nella formula del PFD possono essere semplificati, ottenendo uno snellimento nelle formule.
In particolare, per il Limit Switch (Finecorsa) la diagnostica è assente ($\lambda_{DD} = 0$), il calcolo di PFD sarà pari a:

$$PFD = \lambda_{DU} \cdot \left(\frac{T_1}{2} + MRT\right) = 3.60 \cdot 10^{-6} \cdot (\frac{8760}{2} + 48) = 1.58 \cdot 10^{-2}$$

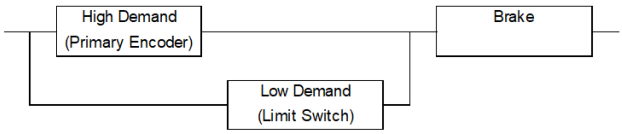
Stesso ragionamento per il Safety PLC, in cui $\lambda_{DU} = 0$, quindi tutto il rischio ricade sul secondo termine, relativo al tempo di riparazione:

$$PFD = \lambda_{DD} \cdot MTTR = 6 \cdot 10^{-7} \cdot 48 = 2.88 \cdot 10^{-5}$$

Per ultimo, il Contattore del Freno ha un tasso dei guasti rilevati dalla diagnostica $\lambda_{DD} = 0$. Ne segue che:

$$PFD = \lambda_{DU} \cdot \left(\frac{T_1}{2} + MRT\right) = 9 \cdot 10^{-8} \cdot (\frac{8760}{2} + 48) = 3.94 \cdot 10^{-4}$$

La somma dei singoli valori di PFD diventa $PFD_{tot} = 1.62 \cdot 10^{-2}$, che corrisponde ad un SIL 1.



Configuration	1oo1	1oo1	1oo1
λDD			N/A
λDU			3.00E-08
MRT/MTTR (hrs)			48
T1 (hrs)			8670
t_{CE}			
PFD/ PFH	5.81E-06	1.62E-02	3.00E-08
PFH (/hr)	9.40E-08		
PFH Total (/hr)	**1.24E-07**		

Figura 3.4: SIF Combinata per Modalità in Alta e Bassa Richiesta, IEC 61508-6:2026 Annex B

La Figura 3.4 rappresenta il sistema completo, secondo uno schema a blocchi in cui le due funzioni in alta e bassa richiesta hanno in comune (in serie) l'elemento finale: il Freno.
Quest'ultimo è un elemento meccanico e ha il suo tasso di guasto non rilevato λ_{DU}, così come la sua totale probabilità di guasto.
Per il sistema combinato, la probabilità che le SIF falliscano contemporaneamente è:

$$PFH_{combined} = PFH_{high} \cdot PFD_{low} = (5.81 \cdot 10^{-6}) \cdot (1.62 \cdot 10^{-2}) = 9.40 \cdot 10^{-8} \,/\, \mathrm{h}$$

Essendo il Freno in serie, per avere la PFH_{totale} del sistema complessivo, bisogna sommare i contributi:

$$PFH_{tot} = 9.40 \cdot 10^{-8} + 3.00 \cdot 10^{-8} = 1.24 \cdot 10^{-7} \,/\, \mathrm{h}$$

Il metodo appena utilizzato è l'espressione matematica della Fault Tree Analysis.
Nella norma viene anche citato un approccio diverso descritto nello specifica tecnica IEC TS 63394:2023 nell'Annex J con ulteriori esempi. Questa metodologia è basata sul rapporto delle probabilità di fallimento (Ratio Approach), che vedremo nel dettaglio nella Sezione 3.3.2.

3.3 Altri Approcci per Sistemi Combinati

I sottosistemi legati alla sicurezza utilizzati sia in modalità ad alta che a bassa richiesta sono stati trattati nella norma IEC 61511:2016, lo standard internazionale per la progettazione di SIS in impianti di processo. Per valutare i sistemi misti, la norma suggerisce due tipologie di procedimento.

3.3.1 Metodo del confronto tra i tassi di guasto

Il metodo prevede inizialmente la stima del tasso di guasto del sottosistema condiviso. Il calcolo avviene in base ai dati forniti sull'utilizzo del componente: il λ_D per il sistema in alta richiesta e per il suo utilizzo in bassa richiesta.
Una volta ottenuti i due valori dei tassi di guasto, viene scelto quello peggiorativo, ovvero il più elevato, e viene inserito nel calcolo delle probabilità.
Ipotizzando che il componente usato in alta richiesta venga azionato in maniera frequente, supponiamo molte volte all'ora, il tasso di guasto in questa situazione sarà più elevato rispetto al suo uso in bassa richiesta. Può succedere anche la situazione opposta in cui la funzione in l'alta richiesta viene attivata poche volte, come una al mese, e il tasso di guasto determinante potrebbe risultare quello relativo alla sua funzione in bassa richiesta.
In generale, le funzioni di sicurezza implementate in modalità ad alta richiesta possono essere anche usate in bassa richiesta.
Esiste un metodo semplificato e conservativo per stimare il valore di PFD_{avg} a partire dal PFH_D. Per la sua applicazione sono necessarie determinate condizioni:

- La funzione di sicurezza utilizzata in bassa richiesta deve essere la stessa di quella specificata per il funzionamento in alta richiesta; inoltre, gli stati considerati sicuri in un caso devono essere gli stessi per l'altro.
- La funzione di sicurezza deve essere attivata per i test secondo quanto specificato dal costruttore.

In questo caso si può scrivere:

$$PFD_{avg} = \frac{PFH_D \cdot T_1}{2}$$

dove T_1 è il tempo di missione del sistema oppure l'intervallo del Test di Prova, nel caso in cui quest'ultimo fosse più breve.
Questo calcolo è rapido e prudenziale, valido solo per le condizioni sopracitate.

3.3.2 Metodo secondo IEC TS 63394

Il seguente metodo può essere applicato solo se entrambi i sistemi, in alta e in bassa richiesta, devono raggiungere lo stesso obiettivo di integrità SIL.
Nella IEC TS 63394 Annex J.3.3.2 [4], in primo luogo, i sottosistemi in ingresso, logica ed uscita si pone un obiettivo di SIL. vengono valutati in modalità ad Alta Richiesta.
Se tale valutazione porta al raggiungimento del SIL richiesto, ad esempio si trovano sotto il PFH_{max} per ciascun SIL (vedi Figura 3.5), ovvero la condizione del SIL massimo è rispettata, il sottosistema di sicurezza in modalità a bassa richiesta viene valutato solo come sottosistema in ingresso. Questo perché la logica e l'uscita rispettano già la verifica del SIL dell'alta richiesta.

SIL	PFD_avg_max	PFH_D_max
1	10^-1	10^-5
2	10^-2	10^-6
3	10^-3	10^-7

Figura 3.5: Valori massimi di PFD_{avg} e PFH_D per i rispettivi SIL target

Per ogni SIL esiste un rischio massimo ammesso e l'idea è, per ciascun sottosistema, di verificare che consumino solo una parte del rischio totale disponibile relativo al SIL. Il rischio dei sottosistemi viene normalizzato rispetto a quello totale massimo mediante il parametro RPF (Ratio of Probability of Failure). La somma delle RPF totale del sistema deve essere inferiore al 100%.

$$RPF_{SUB} = \frac{PFD_{avg_{SUB}}}{PFD_{avg_{MAX(SIL)}}}$$

Questo per quanto riguarda i sottosistemi in input, come i sensori. Per i sottosistemi di Logica e Attuatore avremo, seguendo lo stesso principio:

$$RPF_{SUB} = \frac{PFH_{D_{SUB}}}{PFH_{D_{MAX(SIL)}}}$$

La somma poi degli RPF di tutti i componenti deve essere inferiore al rischio massimo, quindi al 100%, affinché venga rispettato il vincolo di budget massimo. Se avessimo adottato il metodo appena visto nell'esempio della Sezione 3.2, relativo alla IEC 61508, avremmo ottenuto:

$RPF_{input} = \frac{1.62 \cdot 10^{-2}}{10^{-1}} = 1.61 \cdot 10^{-1}$

$RPF_{PLC_{high}} = \frac{5.70 \cdot 10^{-6}}{10^{-5}} = 5.7 \cdot 10^{-1}$

$RPF_{drive} = \frac{3 \cdot 10^{-11}}{10^{-5}} = 3 \cdot 10^{-6}$

$RPF_{contactor} = \frac{9 \cdot 10^{-8}}{10^{-5}} = 9 \cdot 10^{-3}$

Infine si sommano i contributi e otteniamo un valore di 0.741, il quale, essendo inferiore a 1, conferma che il sistema rientra nel Livello di Integrità SIL 1.

4

Affidabilità della Funzione Diagnostica

4.1 Introduzione alla Funzione Dagnostica

Secondo la definizione descritta nella IEC 61508-4, la funzione diagnostica è quella tale per cui un suo guasto non può causare direttamente il fallimento della funzione di sicurezza.
Viene accennata la definizione di Copertura Diagnostica *DC* nella Sezione 2.2 sui Parametri di Affidabilità. La *DC* viene principalmente usata nella modalità ad Alta Richiesta e abbiamo visto nella Parte 2.4, dedicata al confronto con la norma IEC 62061, il calcolo dei tassi di guasto pericolosi rilevati e non tramite la *DC*. La separazione dei due regimi di funzionamento è fondamentale.
In Modalità a Bassa Richiesta della Funzione di Sicurezza, la diagnostica serve a riscontrare guasti che altrimenti rimarrebbero latenti. In questo caso, il test di diagnostica viene effettuato circa una volta al mese.
In Alta Richiesta, la diagnostica deve essere molto rapida. Il tempo tra la rilevazione del guasto e l'attivazione di una risposta deve essere inferiore al tempo di sicurezza, ossia l'intervallo oltre cui il sistema passa in uno stato pericoloso.
Per i componenti che si occupano di Alta Richiesta, spesso si tratta di dispositivi intelligenti i quali hanno al proprio interno una funzione di auto-diagnostica incorporata, il test diagnostico avviene circa ogni minuto.

4.1.1 Ruolo della Diagnostica

Come definito nella IEC 61508, la sicurezza funzionale non si incentra solo sulla robustezza dei componenti, ma anche sulla capacità del sistema di fare auto-analisi e di rispondere tempestivamente ad un possibile guasto, portanto il sistema in uno stato sicuro. La presenza della diagnostica, dunque, è fondamentale ed aumenta l'affidabilità del sistema.

Lo scopo della diagnostica è la rilevazione sia di guasti sicuri λ_{SD}, che di guasti pericolosi λ_{DD}. Quindi, migliore è la diagnostica, più si aumenta l'SFF, che poi andrà a impattare sul SIL massimo potenziale, insieme all'HFT.

4.2 Novità nella Nuova Edizione

Nella Nuova Edizione della serie IEC 61508 vengono aggiunti o chiariti alcuni aspetti riguardanti la funzione diagnostica.
Nello specifico, nella Parte 2, viene inserita per intero la clausola 7.4.12, nella quale troviamo in dettaglio come trattare le funzioni di diagnostica.

4.2.1 Tipi di Funzioni Diagnostiche

Distinguiamo due tipi di funzioni diagnostiche: quelle che monitorano esclusivamente altre funzioni diagnostiche e quelle che fanno parte direttamente della funzione di sicurezza.
Queste ultime, indicate come Tipo A, partecipano alla funzione di sicurezza, pertanto non sono considerate delle "funzioni diagnostiche", secondo la definizione che troviamo nella IEC61508-4, citata prima. Queste avranno gli stessi requisiti di integrità di sicurezza e di capacità sistematica della funzione di sicurezza. Un watchdog timer semplice, ossia un sistema di controllo continuo del funzionamento corretto di server o hardware, può essere classificato di Tipo A.
Invece, nel caso di funzioni diagnostiche ridondanti, che coprono gli stessi modi di guasti, o nel caso di funzioni diagnostiche della diagnostica stessa, non vengono applicati requisiti aggiuntivi, dal momento che non aumenta la sicurezza reale della funzione.
Le funzioni diagnostiche più complesse vengono indicate come Tipo B. La norma spiega che per architetture con un SIL di livello n, la SC della diagnostica può essere ridotta a $n-1$, ma deve comunque essere almeno pari a SC 1. Questo aiuta nella progettazione, perché evita costi elevati per SIL elevati, dove non si viene direttamente a impattare sulla funzione di sicurezza.
Per la quantificazione dei guasti delle funzioni diagnostiche viene aggiunto l'Allegato F della IEC61508-6:2026.

4.2.2 Tassi di Guasto della Diagnostica e $DSFF$

Nella nuova edizione, si approfondisce il tema della diagnostica, nello specifico si intuisce che anche la diagnostica deve essere controllata. Questa analisi viene fatta con un nuovo parametro: la Frazione di Guasti Sicuri della Diagnostica $DSFF$.
Nella Parte 4, clausola 3.6.30.5, viene definita la $DSFF$ come una proprietà della funzione diagnostica, e si tratta del rapporto tra la somma dei tassi medi di guasti sicuri della diagnostica λ_{DIAG_S} e quelli rilevati λ_{DIAG_D}, con la somma dei tassi medi di guasti sicuri, quelli rilevati e non rilevati della diagnostica

λ_{DIAG_U}.

$$DSFF = \frac{\sum \lambda_{\text{DIAG\_S}} + \sum \lambda_{\text{DIAG\_D}}}{\sum \lambda_{\text{DIAG\_S}} + \sum \lambda_{\text{DIAG\_D}} + \sum \lambda_{\text{DIAG\_U}}}$$

Questa frazione indica quanto bene riesco a rilevare i guasti della diagnostica stessa, e include la somma di tutte le funzioni diagnostiche. Non è riferito a una singola, ma all'intera catena diagnostica. Non esiste, infatti, alcun requisito obbligatorio di $DSFF$ per un singolo componente.

4.2.3 Requisiti Aggiuntivi per Sistemi Non Ridondanti

La Nuova Edizione si focalizza sui casi in cui l'architettura non ha nessuna tolleranza al guasto hardware $HFT = 0$. Questi sono casi critici perché un singolo guasto potrebbe causare la perdita della funzione di sicurezza. In questi casi, vengono inseriti dei livelli minimi di $DSFF$ da rispettare.
Per architetture SIL 2 con $HFT = 0$, il guasto delle funzioni diagnostiche di Tipo B deve essere rilevato con un valore di $DSFF \geq 60\%$.
Per architetture SIL 3, con $HFT = 0$, invece, deve essere rilevato con un valore di $DSFF \geq 90\%$.
Viene anche specificata un'indicazione di intervallo di test appropriato per la rilevazione dei guasti della funzione diagnostica. Possono essere scelti per la Modalità a Bassa Richiesta: uguale all'intervallo di Proof Test della funzione di sicurezza per funzioni SIL 2, oppure ogni anno circa; per funzioni SIL 3 il test che sia dieci volte più frequente rispetto al Proof Test, oppure circa ogni mese. Sono anche ammessi test non automatici, che siano periodici.

4.3 L'Importanza dell'Annex F

Nella IEC 61508-6 Nuova Edizione viene aggiunta un'intera sezione, l'Annex F, di tipo informativo, dedicata alla funzione diagnostica e a come i guasti di essa debbano essere inclusi nel calcolo di PFH o PFD_{avg}. Vengono forniti alcuni esempi di metodi di calcolo nei paragrafi successivi.

Approccio A

Per conoscere i parametri correlati alla funzioni di diagnostica, la norma indica che è necessaria un'analisi FMEDA o altri metodi equivalenti. In questo modo verranno determinati i tassi di guasto λ_{DIAG} da integrare per correggere i parametri di tassi di guasto del sistema e le conseguenti formule di Probabilità di Fallimento della Funzione di Sicurezza PFD_{avg} o PFH.
I possibili guasti della funzione di sicurezza calcolati dall'analisi FMEDA sono: i guasti pericolosi che la diagnostica rileva λ_{DD}, quelli pericolosi che non rileva λ_{DU} e i guasti sicuri λ_S. Si vuole, inoltre, tenere conto dei guasti della funzione diagnostica stessa λ_{DIAG}.
Per ciascun elemento preso in considerazione, e per ciascuna Element Safety Function (ESF), vengono indicati i seguenti guasti della funzione di sicurezza:

- $\lambda_{DU(ESF)}$ tasso di guasto pericoloso non rilevato della funzione di sicurezza dell'elemento, assumendo l'assenza di guasti della funzione diagnostica.
- $\lambda_{DU(ESF_{ADJ})}$ nuovo tasso di guasto pericoloso non rilevato, corretto in modo tale da tenere conto anche dei guasti della funzione diagnostica.
- $\lambda_{DD(ESF)}$ tasso di guasto pericoloso rilevato della ESF, senza tenere conto i guasti della funzione diagnostica.
- $\lambda_{DD(ESF_{ADJ})}$ tasso di guasto pericoloso rilevato, corretto che include i guasti della funzione diagnostica.
- $\lambda_{S(ESF)}$ tasso di guasto sicuro della ESF, assumendo l'assenza di guasti della funzione diagnostica.
- $\lambda_{S(ESF_{ADJ})}$ nuovo tasso di guasto sicuro, corretto includendo i guasti della funzione diagnostica.
- T_{EL} Expected Life, vita utile attesa dell'elemento prima che avvenga una sostituzione o revisione completa.

Il calcolo dei nuovi parametri di sicurezza funzionale, tenendo conto della diagnostica rispetto ai guasti casuali dell'hardware viene così formulato:

- Il tasso di guasto pericoloso non rilevato corretto con i guasti della diagnostica sarà:

$$\lambda_{DU_{(ESF_{ADJ})}} = \lambda_{DU_{(ESF)}} + \left[\left(\lambda_{\text{DIAG\_U}} \times \frac{T_{EL}}{2}\right) \times \lambda_{DD_{ESF}})\right]$$

- Il tasso di guasto pericoloso rilevato della funzione di sicurezza dell'elemento, includendo i gusti della diagnostica sarà:

$$\lambda_{DD_{(ESF_{ADJ})}} = \lambda_{DD_{(ESF)}} - \left[\left(\lambda_{\text{DIAG\_U}} \times \frac{T_{EL}}{2}\right) \times \lambda_{DD_{ESF}})\right]$$

- Il tasso di guasti sicuri della funzione di sicurezza, inclusi i guasti della funzione diagnostica, è:

$$\lambda_{S_{(ESF_{ADJ})}} = \lambda_{S_{(ESF)}} + \lambda_{DIAG_S}$$

Usando questo approccio otterremo dei tassi di guasto del sistema che comprendono sia i tassi di guasto del sistema iniziali con l'aggiunta dei tassi di guasto della diagnostica.
Concettualmente, quello che le formule indicano è che una parte di guasti pericolosi rilevati DD dell'elemento, si trasferisce nei guasti pericolosi non rilevati DU quando la diagnostica è in stato di guasto non rilevato.
Se la diagnostica fallisce silenziosamente, le future anomalie del componente non verranno più rilevate dalla diagnostica.

Il T_{EL} è equiparabile all'idea di intervallo di Proof Test, in quanto indica il tempo medio in cui la diagnostica rimane in stato guasto senza che questo venga rilevato. Viene ipotizzato il danno a metà della vita utile attesa dell'elemento. Per i guasti DD, la stessa quota viene sottratta perché quei guasti prima inclusi, non verranno più rilevati.
Consideriamo, ad esempio, un solo componente di sicurezza, con relativa funzione diagnostica e guasti della diagnostica.
Ipotizziamo i seguenti parametri: λ_{DD_ESF} pari a 3×10^{-7} / h; λ_{DU_ESF} uguale a 1×10^{-7} / h; λ_{DIAG_U} di 5×10^{-8} / h; T_{EL} si ipotizza pari a 20 anni.
Per il calcolo dei tassi di guasto pericolosi "adjusted" avremo:

$$\lambda_{DU_{(ESF_{ADJ})}} = 1 \times 10^{-7} + [(5 \times 10^{-8} \times \frac{20 \times 8760}{2}) \times 3 \times 10^{-7}] = 1.013 \times 10^{-7} \text{ / h}$$

$$\lambda_{DD_{(ESF_{ADJ})}} = 3 \times 10^{-7} - [(5 \times 10^{-8} \times \frac{20 \times 8760}{2}) \times 3 \times 10^{-7}] = 2.987 \times 10^{-7} \text{ / h}$$

Quindi, per la funzione in bassa richiesta otteniamo un valore di PFD_{avg} pari a:

$$PFD_{avg} = \frac{\lambda_{DU_{(ESF_{ADJ})}} \cdot T_1}{2} = \frac{1.013 \times 10^{-7} \cdot 8760}{2} = 4.437 \times 10^{-4}$$

Mentre, nel caso di alta richiesta:

$$PFH = \lambda_{DU_{(ESF_{ADJ})}} = 1.013 \times 10^{-7} \text{ / h}$$

Approccio B

L'approccio B riguarda la modallazione dell'affidabilità tramite il metodo di Markov Multifase.
Questo approccio è uno dei raccomandati nella IEC 61508-6 per la valutazione dell'affidabilità di una SIF. La guida per l'applicazione dell'approccio markoviano per i CTMC (Continuous-Time Markov Chain) è ripresa nello standard IEC 61165. Di seguito viene riportato il metodo appreso dal testo Reliability of Safety-Critical Systems (2014) [5], in cui viene espresso che il modello di Markov è usato per analizzare come lo stato di un sistema può variare col tempo. Questo richiede che il sistema sia identificato in un numero finito di stati discreti, rappresentati dalla variabile X, detto vettore degli stati. Se $X(t)$ denota lo stato del sistema al tempo t ed è una variabile casuale, $Pr(X(t) = i) = P_i(t)$ è la probabilità di trovarsi nello stato i al tempo t. Questo processo viene chiamato processo stocastico o a tempo continuo.
I modelli di Markov sono tecniche che utilizzano diagrammi di stato. In questi diagrammi troviamo solo due simboli: i cerchi che rappresentano uno stato del sistema, sia guasto che funzionante, e gli archi direzionati che rappresentano il movimento tra gli stati causati da un guasto o da una riparazione.
I modelli di Markov esprimono in modo chiaro e figurativo le sequenze di guasti che possono verificarsi e vengono usati per modellare le probabilità di trovarsi in ciascuno stato in funzione del tempo.

Per ogni processo stocastico, sussistono le prorietà di Markov. Una di queste afferma che in un sistema che si trova allo stato i al tempo s, la probabilità che il sistema sia in stato j al tempo $s + t$ è indipendente da quanto è successo al sistema prima di s. Questo vuol dire che il passato non ha influenza su ciò che accade nel futuro, e viene definito il processo come "memoryless".
Inoltre, se assumiano che se il sistema si trova nello stato i al tempo s, la probabilità che questo si trovi allo stato j in un tempo t unità più avanti, è indipendente dal tempo s.

$$P_{ij}(t) = Pr(X(s + t) = j|X(s) = i) \qquad \text{(per ogni } s\text{)}$$

Sopra ogni arco viene inserito il tasso di guasto o il tasso di riparazione relativo.
Un modello di Markov può essere rappresentato da una matrice quadrata Q che mostra le probabilità di transizione tra ciascuno stato, detta matrice delle probabilità di transizione.
Questa matrice Q viene moltiplicata per un vettore che rappresenta lo stato iniziale, lo stato in cui tutto funziona. Ne risulta un vettore che fornisce le probabilità degli stati dipendenti dal tempo per ciascuno stato, quindi l'evoluzione temporale delle probabilità.
Le ipotesi principali di questo metodo, come specificato nella norma, sono:

- I guasti sicuri non vengono considerati
- Per i guasti non rilevati, si ipotizza un tempo di rilevamento di una volta all'anno (8760 ore)
- La durata di riparazione dei guasti non rilevati non viene considerata
- I modi di guasto sono disgiunti, ossia può verificarsi un giasto rilevato o uno non rilevato, non entrambi.
- Sistema e diagnostica sono indipendenti.
- Viene considerata una causa comune (CC), ad esempio eventi esterni, che potrebbe provocare un guasto pericoloso rilevato del sistema e insieme un guasto pericoloso non rilevato della diagnostica.

Vediamo un esempio numerico del modello. Consideriamo un sistema 1oo1 e ipotizziamo i seguenti parametri:

- λ_{DD} (3×10^{-7} / h): Guasti pericolosi rilevati dalla diagnostica interna.
- λ_{DU} (1×10^{-7} / h): Guasti pericolosi non rilevati.
- λ_{DIAG_DU} (5×10^{-8} / h): Guasti pericolosi non rilevati della diagnostica stessa.
- λ_{CC} (2.5×10^{-9} / h): Guasti di causa comune che colpisce sia il sistema che la diagnostica.

- μ (0.1/ h): Tasso di riparazione del guasto rilevato.
- T (8760 ore): Intervallo di Proof Test.

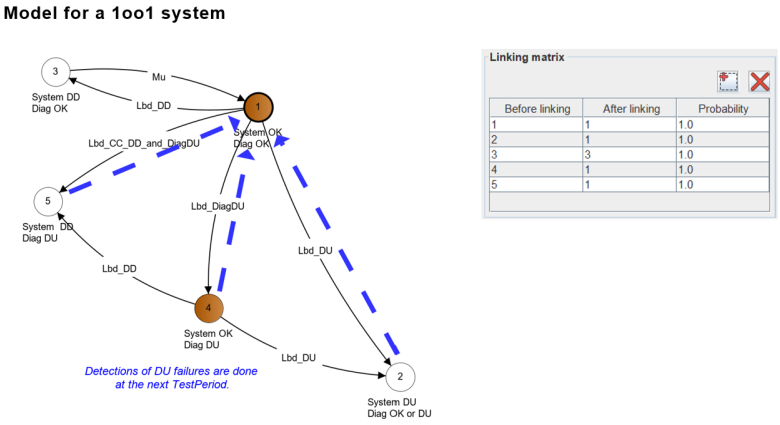


Figura 4.1: Esempio IEC 61508-6:2026 Annex F.2

Nella figura i cerchi di colore marrone indicano gli stati in cui il sistema è sotto controllo, quelli bianchi, invece, uno stato di guasto. In particolare:

- Stato 1: Il sistema funziona e la diagnostica è attiva.
- Stato 2: Il sistema ha un guasto pericoloso non rilevato. Questo può essere perché il guasto era non rilevabile, o perché la diagnostica è guasta.
- Stato 3: Il sistema ha un guasto pericoloso, ma la diagnostica lo ha rilevato. Quindi vediamo che il sistema ritorna allo stato 1 tramite la riparazione.
- Stato 4: Il sistema funziona ma la diagnostica ha un guasto che non viene rilevato.
- Stato 5: Un guasto al sistema che normalmente sarebbe stato rilevato diventa nascosto perché la diagnostica è guasta, oppure a causa di un evento comune.

Le frecce tratteggiate in blu rappresentano il Proof Test che, indipendentemente dallo stato del sistema, lo riporta allo Stato 1, ovvero come nuovo, ogni 8760 ore.
La catena di Markov multistrato a tempo continuo si risolve partendo dalla costruzione della matrice dei tassi Q, una matrice 5×5. Per $i \neq j$ con i stato di partenza e j stato di arrivo, allora $q_{ij} = \lambda_{ij}$, ovvero il tasso di transizione da

i a j.
Sulla diagonale $q_{ii} = -\sum_{j \neq i} \lambda_{ij}$, tale per cui ogni riga sommata risulta 0.

$$Q = \begin{pmatrix} -(\lambda_{DU} + \lambda_{DD} + \lambda_{DIAG\_DU} + \lambda_{CC}) & \lambda_{DU} & \lambda_{DD} & \lambda_{DiagDU} & \lambda_{CC} \\ 0 & 0 & 0 & 0 & 0 \\ \mu & 0 & -\mu & 0 & 0 \\ 0 & \lambda_{DU} & 0 & -(\lambda_{DU} + \lambda_{DD}) & \lambda_{DD} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Ogni riga rappresenta lo stato di partenza mentre la colonna quello di arrivo.
Viene impostato il sistema ipotizzando che ogni anno la curva dell'indisponibilità andrà a 0, dopo il Proof Test che porta il sistema ad una condizione ex novo.
Invece, per il calcolo dell'andamento in crescita, dobbiamo far riferimento agli stati in cui avremo l'indisponibilità consapevole e inconsapevole della funzione di sicurezza. Il $PFD(t)$ sarà dato, quindi, dalla somma delle probabilità del sistema di trovarsi negli stati di indispoibilità, quindi 2, 3 e 5.
Il seguente codice Matlab risolve l'esercizio e calcola la PFD_{avg} del sistema di sicurezza.
Nel codice definiamo prima i parametri, poi viene costruita la matrice Q dei tassi di transizione. Ad esempio, negli stati 2 e 5 viene inserita una riga di 0 perché il sistema, una volta che si trova in quello stato, rimane guasto finché non interviene il Proof Test manuale. Ciascuna riga della matrice Q indica, in Figura 4.1, gli archi in uscita dallo stato a cui la riga corrisponde.
Il vettore p0 nel codice rappresenta lo Stato 1 attivo, in cui sia il sistema che la diagnostica sono perfettamente funzionanti.
La funzione "ode" di Matlab è un solver di equazioni differenziali. In particolare, "ode45" ad ogni passo calcola due approssimazioni (di ordini 4 e 5), stima la differenza tra le due soluzioni come errore e poi si adatta per il passo successivo.
Con la funzione "odeset" si impostano dei valori di RelTol e AbsTol per cui ogni passo deve avere un errore che rientra negli intervalli di tolleranza relativi e assoluti definiti. Infine, MaxStep pari a 1 forza il solver a non superare 1 ora per passo, per avere un'accuratezza approfondita.
Se $p(t) = [p_1(t), ...p_5(t)]^\top$ è il vettore colonna delle probabilità di stato, ovvero di trovarsi in ciascuno stato al tempo t.
t_1 sarà un vettore di griglia temporale non uniforme creato dall'algoritmo sull'intervallo [0 T]. Il sistema differenziale lineare da risolvere sarà:

$$\frac{d}{dt} p(t) = Q^\top p(t)$$

Queste equazioni sono chiamate "Equazioni di Kolmogorov".

Dopo aver simulato un anno, viene avviato un ciclo for per replicare lo stesso andamento per 10 anni. Questa è un'approssimazione modellistica, per cui viene ipotizzato che il profilo annuale si ripeta identico e che dopo il Proof Test il sistema ritorni alle sue condizioni di partenza ottimali.
Viene stimato il $PFD(t)$, ovvero l'indisponibilità del sistema appena arriva una

domanda. L'andamento sarà pari alla somma delle probabilità per cui il sistema debba passare dallo Stato di magiore disponibilità 1 agli Stati di indisponibilità 2, 3 e 5. Lo stato 4 vede il sistema funzionante e la sua funzione di sicurezza ancora disponibile, pertanto non viene incluso nel calcolo.

$$PFD(t) = p_2(t) + p_3(t) + p_5(t)$$

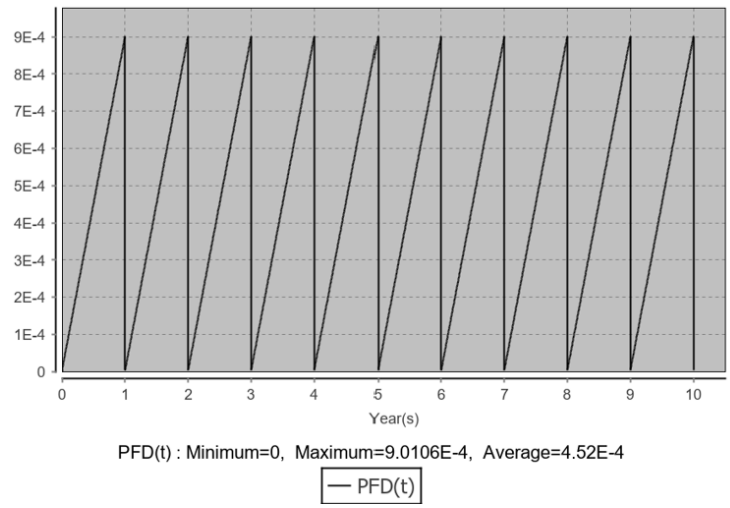
La media su un ciclo di test T è pari a:

$$PFD_{avg} = \frac{1}{T} \int_0^T [p_2(t) + p_3(t) + p_5(t)]\, dt$$

Viene usata la funzione "trapz" per fornire l'integrale numerico sulla griglia temporale restituita da "ode45". Dividendo per la durata totale si ottiene la media temporale di $PFD(t)$.
Il PFD_{avg} è il valore scalare medio su [0 T] che poi verrà usato nella determinazione del SIL.

```
clc;
clear;

% Parametri
lambda_DD = 3e-7;
lambda_DU = 1e-7;
lambda_DIAG_DU = 5e-8;
lambda_CC = 2.5e-9;
mu = 0.1;

T = 8760;   % [h]
anni = 10;

% Matrice Q
Q = [ -(lambda_DD+lambda_DU+lambda_DIAG_DU+lambda_CC), lambda_DU,
    lambda_DD, lambda_DIAG_DU, lambda_CC;
 0, 0, 0, 0, 0;
 mu, 0, -mu, 0, 0;
 0, lambda_DU, 0, -(lambda_DU+lambda_DD), lambda_DD;
 0, 0, 0, 0, 0 ];


% Stato iniziale
p0 = [1; 0; 0; 0; 0];

% ODE45 con tolleranze strette e passo massimo <= 1 h
opts = odeset('RelTol', 1e-11, 'AbsTol', 1e-14, 'MaxStep', 1);

% Simulo un anno
[t1, p1] = ode45(@(t,p) Q' * p, [0 T], p0, opts);
PFD1 = p1(:,2) + p1(:,5) + p1(:,3);  % Stati pericolosi: 2, 3 e 5
PFD_avg_1y = trapz(t1, PFD1)/T;

% Ripeto per 10 anni
t_tot = [];
PFD_tot = [];

for k = 1:anni
    t_tot = [t_tot; t1 + (k-1)*T];
    PFD_tot = [PFD_tot; PFD1];

end

% Conversione ore in anni
t_anni = t_tot / 8760;

% PFD medio
PFD_avg = trapz(t_tot, PFD_tot)/(anni * T);


% Grafico
figure;
plot(t_anni, PFD_tot, 'LineWidth', 2);
xlabel('Tempo [anni]');
ylabel('PFD(t)');
grid on;
title(sprintf('PFD con proof test annuali - Media: %.5e', PFD_avg));
```

Otteniamo:



Il grafico di $PFD(t)$ ha un andamento a "dente di sega" perché la probabilità di avere un guasto non rilevato cresce con il tempo, ma poi viene riportata a 0 dal Proof Test. La massima del grafico Dalla simulazione vale $PFD_{avg} = 4.52 \cdot 10^{-4}$, coerente con il risultato ottenuto usando l'Approccio A visto nella sezione precedente.
Si possono fare alcune considerazioni in relazione alla diagnostica. Vediamo che l'impatto maggiore alla pendenza della curva è dato dal tasso λ_{DU} e dal λ_{CC}, che già da soli arrivano quasi al contributo totale dell'indisponibilità (sommandoli e moltiplicando per T otteniamo 8.979×10^{-4}, quasi il valore massimo della curva).
Notiamo, quindi, che il λ_{DIAG_DU} di per sé non è pericoloso, o meglio non produce indisponibilità, bensì rende il canale vulnerabile. Infatti vediamo che dallo Stato 1 arriviamo allo Stato 4, anch'esso considerato non pericoloso, e poi come secondo step possiamo raggiungere gli Stati 2 o 5.

Per l'analisi dello stesso esempio in Alta Richiesta, i calcoli e le considerazioni da fare riguardano la frequenza di guasto istantanea $w(t)$, ovvero la frequenza di accadimento di qualsiasi guasto. Questa è definita come la probabilità che un sistema si trovi in uno stato di funzionamento al tempo t (Stati 1 e 4) moltiplicata per il tasso di transizione verso uno stato di guasto qualsiasi, anche rilevato.

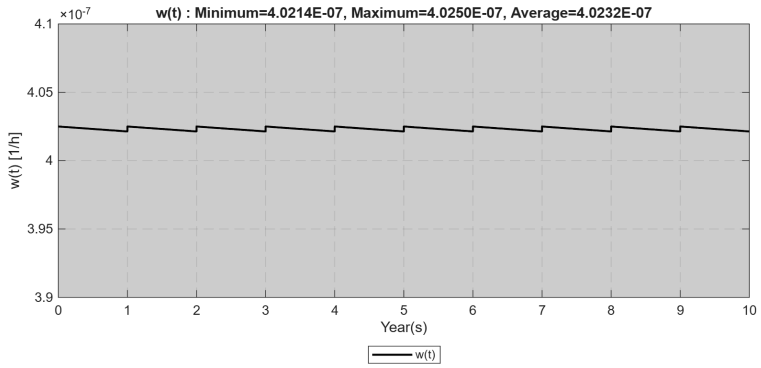
$$w(t) = p_1(t) \cdot (\lambda_{DD} + \lambda_{DU} + \lambda_{CC}) + p_4(t) \cdot (\lambda_{DD} + \lambda_{DU})$$

Quindi, per ogni stato i, si somma la probabilità di trovarsi in quello stato i per il tasso di uscita verso gli stati che generano un evento pericoloso.
Come visto per il PFD, abbiamo definito la matrice Q dei tassi di transizione da uno stato ad un altro.

Il codice Matlab in questo caso sarà, considerando gli stessi parametri di input del caso in bassa richiesta:

```
% Definizione Matrice di Transizione
Q = [
 -(lambda_DD+lambda_DU+lambda_DIAG_DU+lambda_CC), lambda_DU, lambda_DD,
 lambda_DIAG_DU, lambda_CC;
 0, 0, 0, 0, 0;
 mu, 0, -mu, 0, 0;
 0, lambda_DU, 0, -(lambda_DU+lambda_DD), lambda_DD;
 0, 0, 0, 0, 0 ];

% Simulazione con reset annuale
p0 = [1; 0; 0; 0; 0]; % Stato iniziale: tutto funzionante

% ODE45 su un anno
opts = odeset('RelTol', 1e-11, 'AbsTol', 1e-14, 'MaxStep', 1);

[t1, p1] = ode45(@(t,p) Q.' * p, [0 T], p0, opts);

w1 = p1(:,1).*(lambda_DD + lambda_DU + lambda_CC) +
+ p1(:,4).*(lambda_DD + lambda_DU);


% replica su N anni
t_tot = [];
w_tot = [];
for k = 1:anni
    t_tot = [t_tot; t1 + (k-1)*T];
    w_tot = [w_tot; w1];
end

% Calcolo Statistiche
w_avg = trapz(t_tot, w_tot) / (anni * T);
w_min = min(w_tot);
w_max = max(w_tot);

% Conversione ore in anni
t_anni = t_tot / T;

% Grafico
figure('Color', [1 1 1]);
plot(t_tot, w_tot, 'k', 'LineWidth', 1.5);
hold on;
grid on;
set(gca, 'Color', [0.8 0.8 0.8]); % sfondo grigio
set(gca, 'GridLineStyle', '--');

xlabel('Year(s)');
ylabel('w(t) [1/h]');
title(sprintf('w(t) : Minimum=%.4E, Maximum=%.4E, Average=%.4E', ...
    w_min, w_max, w_avg))
xlim([0 anni]);
xticks(0:T:anni);
xticklabels(string(0:anni));
ylim([3.9e-7 4.1e-7]);

legend('w(t)', 'Location', 'southoutside');
```

Dall'implementazione del codice si ottiene il seguente grafico:



Il grafico per l'alta richiesta rappresenta la funzione w(t), ossia la frequenza con cui il sistema entra in uno stato di guasto pericoloso, che notiamo essere quasi costante.
Ogni anno il sistema ritorna come nuovo, allo Stato 1, quando avviene l'ispezione che individua e ripara i guasti latenti.
Come visto in precedenza, è stata usata la funzione di risoluzione "ode45" e poi con la funzione "trapz" è stata generata la media, inserita in alto nel grafico.

$$PFH = \frac{1}{T} \int_0^T w(t)\, dt$$

Il valore di PFH, come si vede nel grafico, è pari a $4.0232 \cdot 10^{-7}$ / h.
Questa formulazione del PFH include i guasti DD, i guasti dati da cause comuni CC, che non venivano inclusi nell'Approccio A. Questo spiega un valore di PFH molto più elevato rispetto al primo caso.

Approccio C

L'ultimo modello visto nella norma per il calcolo dell'affidabilità è l'albero dei guasti (Fault Tree) indicata come FTA. La teoria che riguarda questo metodo è stata presa dal libro Safety Instrumented Systems Verification: Practical Probabilistic Calculations (2005) [6]. La FTA è una tecnica molto comune per mostrare le combinazioni di probabilità che portano alla frequenza di accadimento di un evento indesiderato, ad esempio un guasto del sistema di sicurezza. Con questo metodo, si nota chiaramente il contributo dei guasti pericolosi non rilevati della funzione diagnostica λ_{DIAG_U} rispetto al tasso di guasti pericolosi non rilevati totale.
Le probabilità di guasto del sistema sono calcolate utilizzando il valore del tasso di guasto pericoloso includendo gli errori DU della diagnostica, λ_{DU_ADJ}, che troviamo come evento indesiderato.
Il modello del Fault Tree parte da una rappresentazione grafica con alcuni simboli specifici. Tra quelli comuni troviamo i simboli delle porte (Or o And) e poi un rettangolo con all'interno gli eventi intermedi o il Top Event, e nei cerchi un Evento Base, il quale non viene indagato ulteriormente. Il metodo utilizza una

logica booleana e la porta OR viene utilizzata come un'unione in insiemistica, quindi ogni input devono essere presenti per generare l'output, e la porta AND come un'intersezione, quindi tutti gli eventi in input devono verificarsi affinché si verifichi l'output.
Il metodo dell'Albero dei Guasti può essere risolto quantitativamente come metodo di combinazione probabilistica.
Nella norma troviamo specificate le ipotesi per questo modello:

- I guasti sicuri non vengono considerati
- Il rilevamento dei guasti Undetected avviene una volta all'anno, coincidente con il Proof Test.
- La durata della riparazione dei guasti non rilevati non è considerata.
- I modi di guasto sono indipendenti, possono verificarsi guasti sia DD che DU senza che i due eventi siano disgiunti.
- Sistema e diagnostica sono indipendenti.
- Viene ipotizzata una causa comune per il guasto DD del sistema e il guasto DU della diagnostica.
- L'ordine di occorrenza dei guasti tra un guasto DD del sistema e uno DU della diagnostica, non viene considerato.

Il metodo del Fault Tree, infatti, non modella sequenze temporali in modo esplicito, ma è utile per mostrare come i guasti della diagnostica contribuiscono al totale dei guasti Undetected del sistema.
Per fare un esempio, nella norma si riportano i dati di input con gli stessi valori dell'esempio visto nell'approccio B. Si tratta ancora di un'architettura 1oo1 e l'albero dei Guasti viene riportato in Figura 4.2:

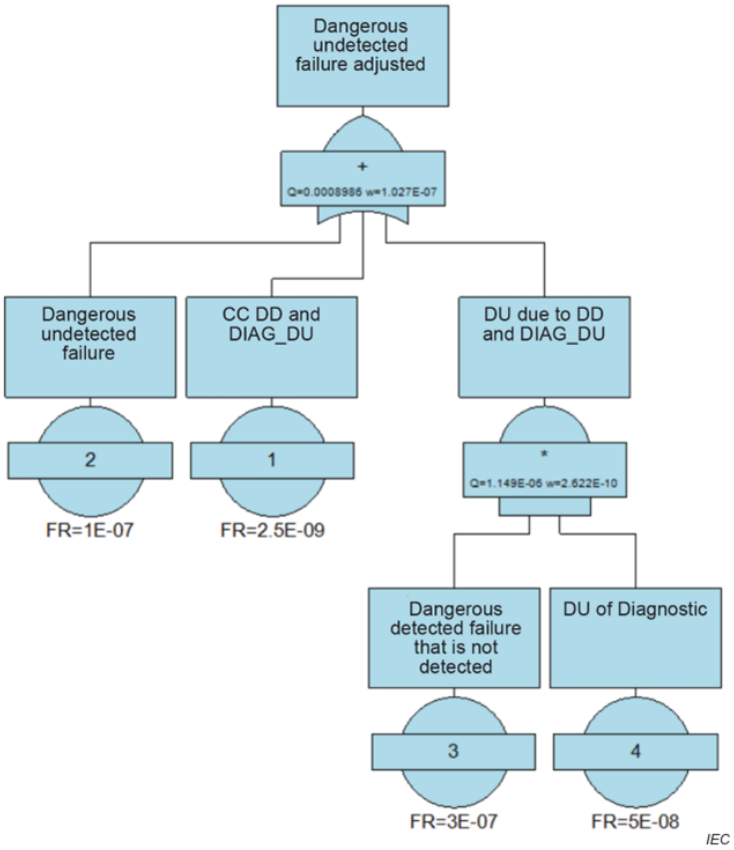


Figura 4.2: Albero dei Guasti IEC 61508-6:2026 Annex F.3

L'evento finale da calcolare (Top Event) è un Dangerous Undetected Failure Adjusted, ossia il tasso di guasto del sistema in stato pericoloso non rilevato, corretto con al proprio interno i guasti della diagnostica.
Questo è ottenuto dalla combinazione di tre contributi mediante la porta logica OR (che indica la somma):

- Guasti Pericolosi non Rilevati
- Guasti Pericolosi Rilevabili uniti a Guasti della Diagnostica non Rilevati, dovuti a Fattori di Cause Comuni.
- Guasti Pericolosi Rilevati, ma la diagnostica non li segnala perché ha un Guasto non Rilevato.

Nell'albero dei guasti vediamo che compaiono due grandezze. Q indica la probabilità che l'evento si verifichi almeno una volta nell'intervallo di prova T. Per un singolo modo di guasto con tasso di guasto costante λ ed eventi rari abbiamo

un'aprossimazione lineare:

$$Q \approx \lambda \cdot T$$

L'altro fattore è w ovvero la frequenza di guasto equivalente all'Alta Richiesta. Per un singolo modo di guasto con tasso costante λ:

$$w = \lambda$$

Nel primo ramo, in un sistema 1oo1, il contributo in Modalità di Bassa Richiesta e Alta Richiesta deriva solamente dai λ_{DU} del sistema, per cui:

$$Q_1 = \lambda_{DU} \cdot T = 10^{-7} \cdot 8760 = 8.76 \cdot 10^{-4}$$

Nella teoria del calcolo di PFD_{avg} si dovrebbe dividere per 2, in modo da considerare il guasto a metà dell'intervallo di Proof Test. In questi calcoli, invece, troviamo tutto moltiplicato per 2, affinché il modello sia conservativo, che quindi va ad elidere il termine.
Per l'Alta Richiesta si avrà: $w_1 = \lambda_{DU} = 10^{-7}/\text{h}$.
Il ramo centrale riguarda i guasti di causa comune, ovvero:

$$Q_2 = \lambda_{CC} \cdot T = 2.5 \cdot 10^{-9} \cdot 8760 = 2.19 \cdot 10^{-5}$$

mentre $w_2 = \lambda_{CC} = 2.5 \times 10^{-9}\,/\,\text{h}$.
Il terzo ramo riguarda la funzione diagnostica che fallisce nel segnalare un guasto. Affinché ciò avvenga, devono esistere contemporaneamente due stati (Porta Logica AND):

- Guasto Pericoloso Rilevato del sistema
- Guasto Pericoloso Non Rilevato della Diagnostica

Nel caso di bassa richiesta la probabilità che in T si verifichi almeno un evento DD e almeno 1 evento DU della diagnostica sarà:

$$Q_{and} \approx (\lambda_{DD}T) \cdot (\lambda_{DIAG\_DU}T) = \lambda_{DD} \cdot \lambda_{DIAG\_DU} \cdot T^2 = (3 \cdot 10^{-7}) \cdot (5 \cdot 10^{-8}) \cdot 8760^2 = 1.148 \cdot 10^{-6}$$

Nel caso di alta richiesta viene usata la formula:

$$w_{and} \approx \lambda_{DD} \cdot \lambda_{DIAG\_DU} \cdot (T_{DD} + T_{DIAG\_DU}) = (3 \cdot 10^{-7}) \cdot (5 \cdot 10^{-8}) \cdot (8760 \cdot 2) = 2.622 \cdot 10^{-10}\,/\,\text{h}$$

Per la diagnostica non rilevata in automatico, il tempo di rilevamento di un guasto è pari all'intervallo di Proof Test $T = T_{DIAG\_DU}$. Nel caso di un guasto DD del sistema, la norma invece di usare $T_{DD} = 1/\mu$ assume conservativamente un tempo di rilevazione pari a T.
Nel caso di bassa richiesta la Probabilità che il Top Event si verifichi sarà:

$$Q_{TOP} = Q_1 + Q_2 + Q_{and} = 8.99 \cdot 10^{-4}$$

Notiamo che il contributo è circa il doppio rispetto allo stesso esempio calcolato nell'Approccio A. Con questo metodo stiamo sovrastimando la probabilità media di trovarci in uno stato di guasto, in quanto l'intervallo di Proof Test viene considerato per intero e non metà intervallo come visto nel primo approccio.
Per l'alta richiesta, sommiamo i tre contributi di w e otteniamo:

$$w_{TOP} = w_1 + w_2 + w_{and} = 10^{-7} + 2.5 \cdot 10^{-9} + 2.622 \cdot 10^{-10} = 1.027 \cdot 10^{-7} \,/\,\mathrm{h}$$

Questo risultato è coerente con quanto è emerso in alta richiesta nell'Approccio A.

Analisi di Confronto dei Metodi di Calcolo

Nella norma IEC 61508-6:2026 sono forniti due esempi di calcolo della probabilità di fallimento in alta e bassa richiesta di funzionamento. Per l'approccio B e l'approccio C vengono usati gli stessi dati in input, ma viene implementato ciascun modello seguendo delle scelte diverse. Per l'approccio A, invece, non vengono forniti esempi applicativi direttamente nella norma.
L'approccio A prevede una semplificazione utilizzando una correzione parametrica: una parte dei guasti DD dell'ESF diventa DU quando la diagnostica è guasta. Questo avviene, in media, al tempo $T_{EL}/2$. In questo caso PFD_{avg} dipende quasi esclusivamente dall'intervallo di Proof Test $T/2$.
Per il PFH si assume che la frequenza sia pari solamente a $\lambda_{DU_{ADJ}}$.
Il metodo di Markov ha lo scopo di modellare l'evoluzione degli stati operativi nel tempo, includendo il Proof Test periodico. Questo è il modello più accurato, in quanto include anche il tempo di riparazione per i DD in bassa richiesta, e include ogni passaggio dagli stati attivi a quelli pericolosi in alta richiesta, valutandone la frequenza istantanea.
Nel FTA si evidenziano contributi di ogni singolo ramo e combinazioni fino al Top Event.
Andando a confrontare i tre metodi, notiamo alcune discrepanze.

	PFDavg	PFH [1/h]
A - Semplificato	4.44E-04	1.01E-07
B - Markov (CTMC)	4.52E-04	4.02E-07
C - FTA	8.99E-04	1.03E-07

In bassa richiesta, gli approcci A e B danno un risultato simile, mentre per l'approccio C è circa il doppio. Questo accade perché volutamente il modello non divide per 2 l'intervallo di Proof Test, adottando una stima conservativa.
In alta richiesta, notiamo che usando l'approccio B viene un valore di PFH molto più alto rispetto agli approcci A e C. Il motivo è da attribuire al fatto che nel modello di Markov includiamo i contributi DD nella frequenza di passaggio agli stati pericolosi, mentre gli approcci A e C, così formulati, non includono i guasti DD "puri". Nel Fault Tree vengono inclusi i guasti DD solo se uniti a

guasti della dagnostica non rilevati, dovuto a un guasto specifico della diagnostica (terzo ramo) o dovuti a fattori di cause comuni CC (secondo ramo).

Metodo di Calcolo Semplificato

Nella norma viene, infine, riportato un modo semplificato per inserire i guasti della diagnostica all'interno dei guasti pericolosi non rilevati.

$$\lambda_{DU} = \lambda_{DU\_FMEDA} + 0.05 \cdot \lambda_{DIAG\_U}$$

In questa formulazione si assume che il componente e il circuito di diagnostica siano posizionati vicini tra di loro, sulla stessa scheda a circuito stampato (PCB). Questo rappresenta il fattore di causa comune nel caso peggiore.

$$\lambda_{DU} = \lambda_{DU\_FMEDA} + 0.02 \cdot \lambda_{DIAG\_U}$$

Nella formula sopra, viene modificato l'apporto da dare alla diagnostica. In particolare, questo è il caso in cui il componente e il circuito di diagnostica siano collocati su PCB differenti ma nello stesso rack o quadro.

$$\lambda_{DU} = \lambda_{DU\_FMEDA} + 0.01 \cdot \lambda_{DIAG\_U}$$

Si assume, in questo caso, ch il componente e la diagnostica siano collocati su PCB differenti e in rack differenti.

Al fine di semplificare il trattamento dei guasti pericolosi non rilevati della funzione di diagnostica, la IEC 61508 consente di includere una frazione conservativa di tali guasti direttamente nel tasso di guasto pericoloso non rilevato della funzione di sicurezza, con un fattore percentuale dipendente dal grado di separazione fisica tra il componente diagnosticato e il circuito di diagnostica.

4.4 Limiti della Funzione Diagnostica

Nell'attuale edizione della norma emerge una quesito importante, ossia la funzione diagnostica come può commutare un canale nel caso di guasti pericolosi non rilevabili? Non si può fare, ed è per questo motivo che è stata introdotta nella Nuova Edizione la diagnostica della diagnostica. L'uso di questi sistemi porta a nuovi questiti, aumentando la complessità dell'analisi. Da un lato, riduce la probabilità di guasti nascosti nei circuiti di test, dall'altro la funzione diagnostica diviene un elemento attivo che può fallire in modi nuovi e dinamici. Un esempio è il fallimento nella commutazione verso il canale sano, o la commutazione errata verso un canale guasto, o il guasto comune tra il sistema e il canale di switching.
Un limite che riguarda l'HFT sorge perché esso viene visto come un valore statico (il numero di guasti che un'archtettura può tollerare). In realtà, questo termine ha una logica sequenziale, ovvero che l'HFT è un valore dinamico,

varia in funzione della sequenza temporale degli eventi. La IEC 61508 gestisce queste interazioni tramite il beta factor β, che modella i guasti di causa comune. Tuttavia, anche questo parametro risulta statico e non descrive bene i guasti sequenziali. Ad esempio, il sistema non tiene conto che la funzione di diagnostica stessa è un elemento che può essere colpito dallo stesso guasto di causa comune che ha colpito i canali.
Il rapporto tecnico IEC TR 63039 tenta di risolvere questi problemi, cerca di fornire un'analisi di sistemi complessi in cui la sicurezza deriva dalla sequenza dei guasti e dalle decisioni logiche prese in tempo reale. L'approccio prevede lo studio di come il guasto si propaga nel tempo. Infine, viene valutato se la diagnostica sia sufficientemente indipendente da non essere soggetta alle stesse cause di fallimento dei canali.
Per migliorare l'accuratezza dei calcoli probabilistici, è necessario distinguere le funzioni di diagnostica in base al loro comportamento dopo il rilevamento di un guasto:

- Diagnostica passiva che rileva il guasto e lo segnala o porta il sistema in uno stato sicuro
- Diagnostica attiva che "decide" di isolare il guasto e mantiene la funzione operativa su un altro canale sano.

Nel secondo caso, il tempo di commutazione e l'affidabilità del commutatore diventano variabili importanti da considerare.

5

Conclusioni

Lo scopo del lavoro è stato quello di confrontare la Nuova Edizione della serie di norme IEC 61508, che verrà pubblicata prima dell'autunno del 2026, con la versione attuale pubblicata nel 2010.
Il tempo trascorso tra le due edizioni fa capire la necessità di un suo aggiornamento, considerando che la normativa tecnica ha un'evoluzione periodica naturale di circa 10 anni.
Le novità sono diverse, tra cui l'aggiunta di nuove parti, come la IEC 61508-6-1, la quale dettaglia come trattare l'Hardware e Software sviluppato secondo la serie di norme ISO 26262, norma di riferimento per la sicurezza dell'automotive.
Il mio Lavoro si è concentrato su alcune novità come:

- Modifiche alle formule per il calcolo del PFD e PFH
- L'analisi di sistemi di sicurezza che includono sia componenti funzionanti in Alta Richiesta che in Bassa Richiesta, chiamati Sistemi Misti.
- Nuove considerazioni rispetto alla Funzione di Diagnostica

Dall'analisi condotta sulla nuova edizione della norma IEC 61508 emergono nuovi approcci di progettazione per le architetture di sicurezza industriali.
Il calcolo di affidabilità rivolto alle configurazioni solitamente implementate cerca di interpretare sempre meglio il comportamento reale delle apparecchiature.
Nei modelli di indisponibilità sono state affinate le formule e le ipotesi riguardo le funzioni di sicurezza in bassa e alta richiesta di esercizio.
Uno degli obiettivi è stato quello di comprendere ed evidenziare i nuovi criteri di calcolo delle grandezze fondamentali PFD_{avg} e PFH e di confrontarle con lo standard settoriale IEC 62061 per la modalità operativa ad alta richiesta.
Un intero capitolo della tesi tratta l'aggiornamento delle formule di PFD e PFH. Emergono alcuni schemi per l'aggiornamento delle formule. Ad esempio, vengono sostituiti rispettivamente i parametri β e β_D con β_{DU} e β_{DD}. Vengono così esplicitate le quote di causa comune per guasti rilevati e per quelli non rilevati. In questo modo otteniamo i valori di PFD e PFH più sensibili rispetto alla diagnostica e alla separazione tra DD e DU.

Nell'architettura 1oo2 in bassa richiesta, il calcolo del t_{GE} è leggermente diverso, e viene proposto $MTTR/2$ invece di $MTTR$. Questo perché si ipotizza di avere un guasto rilevabile sul secondo canale a metà della finestra di riparazione del primo. Simile ragionamento viene fatto nella configurazione 1oo3 in cui nel calcolo di t_{G2E} viene implementato il fattore riduttivo $MTTR/3$.
Un'importante innovazione è stata fatta in alta richiesta in cui vengono distinti i ruoli della diagnostica: questa può avere un ruolo passivo, ovvero in cui si limita a rilevare i guasti DD, e uno attivo in cui, oltre a rilevare i guasti, sposta la funzione di sicurezza sul canale funzionante. Quindi si distingue il caso in cui il tasso di guasto pericoloso rilevabile DD sia incluso nel calcolo, dal momento che il guasto viene solo rilevato ma deve essere gestito, oppure quello in cui non vengano inclusi perché considerati come sicuri, in seguito all'avvio di un trip di sicurezza automatico della funzione diagnostica.
Questa distinzione avviene solo in alta richiesta dal momento che in bassa richiesta l'utilizzo della funzione di sicurezza è un evento raro, e quando accade un guasto deve essere subito rilevato e gestito.
Per entrambi i casi, in alta e bassa richiesta, viene fornito un esempio di confronto tra l'edizione attuale della IEC 61508 (nelle tabelle definita come "Now") e la prossima edizione ("New"). Vengono valutati i valori di PFD_{avg} e PFH con un'analisi di sensitività su parametri chiave quali il tasso totale di guasto λ, la Copertura Diagnostica DC e l'efficienza della diagnostica K.
I risultati sono coerenti con le formule e i dati utilizzati.
Per DC più basse, ad esempio, aumentano le probabilità di guasto sia in bassa che in alta richiesta.
Per K che varia, il PFH si sposta di due ordini di grandezza nella configurazione 1oo2D, che è quella in cui il K ha più rilevanza.
La nuova versione della norma IEC 61508 risulta complessivamente più accurata e meno conservativa su PFD_{avg} e PFH.
Per quanto riguarda l'allineamento con la norma IEC 62061 i risultati sono coerenti nel caso di configurazione 1oo2 e 1oo2D. Nel caso di architetture 1oo1 si nota uno scostamento di un ordine di grandezza sul valore di PFH, perché la IEC 61508 utilizza i λ_{DU}, mentre la IEC 62061 usa tutti i guasti pericolosi.

Un ulteriore aspetto di rilievo riguarda i sistemi combinati tra alta e bassa richiesta di funzionamento, che rappresentano una realtà classica e sempre più diffusa in ambito industriale. L'analisi proposta evidenzia come questa estensione renda possibile una progettazione più integrata e flessibile nei dispositivi condivisi.
Nell'Annex B.3.3.3.4 della IEC 61508-6:2026 viene introdotto un riferimento ufficiale alla gestione dei sistemi combinati e viene proposto un esempio applicativo. Nell'esempio viene fornito un sistema misto che ha in alta richiesta un encoder, in bassa richiesta un finecorsa (Limit Switch). L'elemento in condivisione che agisce sia in alta che in bassa richiesta è un freno, posto in serie come elemento finale. Nell'esempio suggerito dalla norma, è stato calcolato il PFD per la bassa richiesta, il PFH per l'alta richiesta e poi moltiplicati i due valori ottenendo un PFH combinato. Poi viene sommato il PFH del freno e si

ottiene un valore di PFH_{tot} comprensivo del freno. Questo metodo rappresenta l'espressione analitica della Fault Tree Analysis.
Vengono successivamente proposti due metodi aggiuntivi, il primo ripreso nel libro "Functional Safety of Machinery"(2023)[2], che riporta una stima conservativa di PFD_{avg} a partire dal PFH_D. L'altro metodo analizzato è quello riportato nella IEC TS 63394:2023, riguardante l'uso delle Ratio od Probability of Failure (Ratio Approach), che invece è un approccio più pratico per la verifica del SIL massimo raggiungibile.

Un ulteriore elemento dell'evoluzione della norma è l'integrazione delle funzioni di diagnostica con le considerazioni sulle sue possibili modalità di guasto. La modifica avviene attraverso l'introduzione di specifici fattori relativi alla diagnostica, oltre il parametro di efficienza K, il quale era già presente nell'attuale edizione.
Il riconoscimento della funzione diagnostica come soggetta anch'essa a guasti sistematici e casuali ha portato all'imposizione di soglie minime di $DSFF$, coerenti con le architetture, volte a delimitare un livello di integrità SIL che includa anche i guasti della diagnostica.
I modelli utilizzati per stimare la probabilità di guasto latente con la correzione del tasso di guasto della funzione diagnostica sono stati l'analisi Fault Tree e i modelli multifase di Markov.
I risultati ottenuti differiscono tra di loro, ma questo avviene per la formulazione e le ipotesi di ciascun metodo utilizzato.
Per l'approccio A viene ipotizzato un tempo medio di vita attesa del componente della diagnostica T_{EL} pari a 20 anni. L'idea è quella di ottenere una formula per il calcolo di $\lambda_{DU_{ADJ}}$, ovvero il tasso di guasto che tenga conto anche dei guasti della funzione diagnostica nel tempo T_{EL}, ipotizzando un guasto di quest'ultima a metà dell'intervallo, così come avveniva per il Proof Test in bassa richiesta. Il calcolo è rapido e mediamente conservativo per il PFD_{avg}, in quanto tiene conto soltanto dei λ_{DU}, in questo caso "adjusted".
Per il calcolo di PFH si assume che la frequenza dei guasti pericolosi sia pari a $\lambda_{DU_{ADJ}}$. Questo potrebbe generare una potenziale sottostima di PFH nel caso in cui i guasti pericolosi rilevati DD o i guasti dati da fattori di causa comune CC fossero rilevanti nel calcolo.
L'approccio B usato nella norma tratta il Metodo Multifase di Markov, il quale è stato poi implementato su Matlab per riportare il grafico dell'andamento della funzione precisa nel tempo.
Per il PFD_{avg} viene incluso il tempo dopo un guasto pericoloso rilevato DD passato in stato di riparazione, quindi risulta leggermente superiore rispetto al Caso A.
Il PFH viene valutato considerando i tassi di guasto relativi al trasferimento da uno stato di funzionamento del sistema ad uno anomalo. Vengono sommati i tassi di guasto pesati per ciascuna probabilità del sistema di trovarsi in quello stato. Il PFH risulta decisamente superiore in questo caso, quattro volte superiore rispetto ai metodi A e C. Questo quindi è dato dalla definizione di PFH che conteggia anche le situazioni di guasto rilevato DD e di guasto dato

da fattori di causa comune CC per il sistema e la diagnostica.
Infine, l'approccio C riguarda l'implementazione di un'analisi di un albero dei guasti (FTA). In bassa richiesta operativa, viene usato un metodo di calcolo conservativo, che porta il risultato ad essere grande il doppio rispetto ai casi A e B. Per ogni ramo viene calcolata la sua probabilità di indisponibilità Q, che poi viene sommata per ottenere la probabilità totale di un guasto pericoloso non rilevato che include i tassi di guasto della funzione diagnostica.
Per il calcolo del PFH in alta richiesta, allo stesso modo, viene sommata la frequenza di guasto dei tre rami che componevano il sistema di guasti. Il terzo ramo riguarda i guasti che dovrebbero essere rilevati, ma che non vengono segnalati perché la diagnostica ha un guasto non rilevato DU. I risultati si dimostrano coerenti con l'approccio A, e appaiono differenti dal metodo di Markov perché non vengono considerati i guasti DD che vadano a impattare direttamente sul tasso di guasto DU "adjusted".

Bibliografia

[1] 65A-61508-6-Ed3-IS-FDIS-HL03 - IEC 61508

[2] Tacchini Marco, *Functional Safety of Machinery: How to apply ISO 13849-1 and IEC 62061*, Wiley, 2023.

[3] IEC 61508-2010.

[4] IEC TS 63394 ED 1, 2022

[5] Marvin Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*, Wiley, 2014.

[6] William Globe, Harry Cheddie, *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*, ISA, 2005.