POLITECNICO DI MILANO

Scuola di Ingegneria Industriale e dell'Informazione

Corso di Laurea Magistrale

Ingegneria della Prevenzione e della Sicurezza nell'Industria di Processo

POLITECNICO
MILANO 1863

La sicurezza funzionale ad alta richiesta: analisi e sviluppo delle normative ISO 13849-1 ed IEC 62061.

Relatore: Prof. **Loredana Cristaldi**

Correlatore: Ing. **Marco Tacchini**

Tesi di Laurea di:

Matteo Crippa

Matricola 918287

Anno Accademico 2019 / 2020

Indice

Sommario **6**

1. Ingegneria dell'affidabilità: introduzione ed approfondimenti **8**

1.1 Conformità ed affidabilità 8

1.2 Guasti e tasso di guasto 9

1.3 Affidabilità e distribuzioni di probabilità 12

1.4 Metodo empirico 17

1.5 Diagramma a blocchi di affidabilità (RBD) 23

1.6 Modello di Markov 37

1.7 Disponibilità e dispositivi riparabili 41

1.8 Altri metodi di analisi dei sistemi 54

2. La sicurezza funzionale **63**

2.1 Introduzione alla sicurezza funzionale 63

2.2 Tolleranza al guasto hardware e copertura diagnostica 70

2.3 Cause comuni di guasto 73

2.4 Dispositivi soggetti a wearout 77

2.5 IEC 62061 79

2.6 ISO 13849-1 84

3. Analisi dei sistemi di sicurezza con il modello di Markov **92**

3.1 Motivazioni dello sviluppo delle equazioni per il calcolo del PFHD 92

3.2 Assunzioni utilizzate nella modellazione 93

4. Architetture a canale singolo **95**

4.1 Modello 1oo1D, introduzione 95

4.2 Modello 1oo1D, semplificazione 100

4.3 Utilizzo del modello di Markov a due stati 108

4.4 Modello 1oo1D, calcolo PFH_D con test non tempo ottimale 110

4.5 Modello 1oo1D, calcolo PFHD con test tempo ottimale 115

4.6 Modello 1oo1 117

5. Architetture a due canali **119**

5.1 Modello 1oo2D, introduzione 119

5.2 Modello 1oo2D, semplificazione 123

5.3 Utilizzo del modello di Markov a tre stati 134

5.4 Modello 1oo2D, calcolo PFH_D con test a tempo discreto 137

5.5 Modello 1oo2D, calcolo PFH_D con test continuo 138

5.6 Modello 1oo2D, soluzione semplificata per test a tempo discreto e continuo 138

5.7 Modello 1oo2 146

6. Applicazione ... 148
6.1 Caso di studio ... 148
6.2 Analisi di rischio ... 150
6.2.1 Analisi di rischio con normativa IEC 62061 ... 150
6.2.2 Analisi di rischio con normativa ISO 13849-1 ... 152
6.3 Analisi del sistema di sicurezza ... 152
6.3.1 Sottosistema di input ... 153
6.3.2 Sottosistema di logica ... 153
6.3.3 Sottosistema di output ... 154
6.3.4 Sottosistema di output 1oo2 ... 156
6.3.5 Sottosistema di output 1oo1D ... 156
6.3.6 Sottosistema di output 1oo2(1D) ... 157
6.3.7 Sottosistema di output 1oo2D ... 158
6.4 Procedura con applicazione della normativa IEC 62061 ... 159
6.4.1 IEC 62061: 1oo1 ... 159
6.4.2 IEC 62061: 1oo2 ... 160
6.4.3 IEC 62061: 1oo1D ... 160
6.4.4 IEC 62061: 1oo2(1D) ... 161
6.4.5 IEC 62061: 1oo2D ... 162
6.4.6 Vincoli di architettura ... 163
6.4.7 Risultati con IEC 62061 ... 163
6.5 Procedura con applicazione della normativa ISO 13849-1 ... 164
6.5.1 Risultati con ISO 13849-1 ... 166
6.6 Procedura con applicazione del set di equazioni ottenuto nei capitoli 4 e 5 ... 167
6.6.1 Set di equazioni: 1oo1 ... 167
6.6.2 Set di equazioni: 1oo1D ... 167
6.6.3 Set di equazioni: 1oo2D ... 168
6.6.4 Set di equazioni: 1oo2 ... 169
6.6.5 Set di equazioni: 1oo2(1D) ... 169
6.6.6 Risultati ottenuti con set di equazioni ... 170
6.7 Soluzione con confronto dei risultati ottenuti ... 170
7. Considerazioni sulle normative ... 174
7.1 Considerazioni sulla normativa ISO 13849-1 ... 174
7.2 Considerazioni sulla normativa IEC 62061 ... 175
8. Conclusioni ... 178
Bibliografia ... 180

Sommario

La sicurezza funzionale tratta la riduzione dei rischi associati al funzionamento di un qualsiasi sistema, attraverso l'utilizzo di un sistema di sicurezza. Il sistema di sicurezza interviene per evitare eventi che possono causare danno a persone, cose o all'ambiente. La sicurezza funzionale ad alta richiesta (in inglese High Demand) è relativa a sistemi di sicurezza ai quali è richiesto di intervenire più di una volta all'anno.

Le due normative, che, allo stato attuale della tecnica, forniscono indicazioni sulla sicurezza funzionale ad alta richiesta e, in particolare, sulla sicurezza dei macchinari, sono la ISO 13849-1, sviluppata dall'Organizzazione Internazionale per la Normazione (2015), e la IEC 62061, sviluppata dalla Commissione Elettrotecnica Internazionale (2020).

Per l'analisi di entrambe le normative è necessaria la comprensione di alcuni argomenti trattati nel campo dell'ingegneria dell'affidabilità, quali i concetti di conformità, di affidabilità, di disponibilità e dispositivi riparabili, di guasto, di tasso di guasto e di diagramma a blocchi di affidabilità, con particolare interesse sulle configurazioni di dispositivi in serie ed in parallelo, configurazione che tratta l'importante concetto di ridondanza.

Ogni normativa presenta differenti soluzioni per la valutazione e progettazione di un sistema di sicurezza, partendo dalla definizione della riduzione del rischio richiesta fino al metodo risolutivo per il calcolo di un valore comune ad entrambe le normative: il PFH_D, definito dalla ISO 13849-1 come una probabilità di guasto pericoloso per ora e dalla IEC 62061, più correttamente, come una frequenza di guasto pericoloso per ora.

La normativa IEC 62061 valuta la riduzione del rischio in livelli di sicurezza integrata (SIL, Safety Integrity Level) tramite delle equazioni da applicare per ogni Architettura (A, B, C o D), mentre la normativa ISO 13849-1 valuta la riduzione del rischio in livelli di performance (PL, Performance Level) tramite una soluzione tabellare da applicare per ogni Categoria (B, 1, 2, 3 o 4). Esiste una corrispondenza tra SIL e PL dovuta alla definizione degli stessi con analoghi intervalli di PFH_D. Tra le due normative sono presenti, inoltre, alcune corrispondenze tra le Architetture della IEC 62061 e le Categorie della ISO 13849-1.

Il presente lavoro, oltre ad analizzare le due normative sopra citate, ha anche analizzato il documento "*Markov model-based calculation of the PFHD of safety functions for machines: derivation of a set of PFHD equations for typical machine control subsystem architectures*" (2017), scritto da Michael Dorra. Il documento è stato scritto per sottolineare la natura comune di entrambe le normative, che sono appunto i modelli di Markov, utilizzati nell'ingegneria dell'affidabilità. Il documento fornisce un set di equazioni per il calcolo del PFH_D.

Le due normative presentano tra loro analogie e differenze e comportano alcune limitazioni, in particolar modo la ISO 13849-1. Il documento di Michael Dorra fornisce uno strumento più flessibile, più preciso e soggetto a meno limitazioni. Una semplice applicazione delle due normative e del documento di Michael Dorra, relativa ad un caso pratico, è stata in grado di evidenziare la maggior precisione di quest'ultimo strumento, anche nell'analisi di un nuovo modello, non presente nelle Architetture della IEC 62061 e nelle Categorie della ISO 13849-1.

1. Ingegneria dell'affidabilità: introduzione ed approfondimenti

1.1 Conformità ed affidabilità

Dando una prima definizione, l'affidabilità, nel campo dell'ingegneria che tratta il suo studio, è la capacità di un elemento, di un componente o di un sistema anche complesso di rispettare, nel tempo, le specifiche tecniche di funzionamento.

Nel seguito della trattazione si farà riferimento al termine dispositivo, ovvero una qualsiasi unità funzionale o strutturale di complessità arbitraria, la quale può essere considerata come un'entità per effettuare indagini; può essere un sistema, un sottosistema, un componente, un elemento o un'attrezzatura e può essere completamente hardware, completamente software oppure comprendente sia parte hardware che parte software.

Per introdurre meglio il concetto di affidabilità è necessario introdurre prima quello di conformità di un dispositivo. La conformità indica la risposta, positiva o meno, a dei parametri funzionali del dispositivo oggetto di indagine o a delle specifiche tecniche, ovvero a dei valori prestabiliti di conformità. La conformità è misurabile (ad esempio valori nominali, tolleranza o percentuale di dispositivi difettosi). Un dispositivo conforme ha la capacità tecnica di svolgere in modo appropriato la funzione che gli viene richiesta e per la quale è stato progettato.

L'affidabilità è la caratteristica di un dispositivo che consente di valutarne la conformità durante lo scorrere del tempo; è definita come la probabilità che lo stesso riesca a svolgere la propria funzione durante un intervallo di tempo ben definito, sotto determinate condizioni operative. Lo studio di essa consente di comparare differenti design di progettazione e di valutare diverse soluzioni per ottenere come risultato le stesse caratteristiche funzionali. È inoltre di aiuto nell'identificazione di azioni correttive da effettuare su dispositivi che potrebbero causare o subire guasti e malfunzionamenti.

Nella normativa IEC[1], nello standard IEC 60050[2], vengono fornite due definizioni di affidabilità:

- Definizione qualitativa: abilità di un elemento di rimanere funzionale.
- Definizione quantitativa: probabilità che nessuna interruzione operativa accada durante un intervallo di tempo definito.

Per ricavare il valore di affidabilità di un dispositivo si può procedere attraverso modelli matematici e leggi dell'affidabilità, procedendo al suo calcolo dall'analisi della struttura del dispositivo in oggetto ed utilizzando i dati di affidabilità degli elementi primari che compongono tale struttura. In questo caso si parla di predizione dell'affidabilità.

[1] L'IEC è l'International Electrotechnical Commission, una commissione internazionale di normazione, che si occupa di stilare e pubblicare norme per tutte le tecnologie elettriche ed elettroniche.
[2] Lo standard IEC 60050 contiene il vocabolario elettrotecnico internazionale (IEV – International Electrotechnical Vocabulary), che promuove l'unificazione della terminologia nel campo dell'elettrotecnica, dell'elettronica e delle telecomunicazioni.

Un'altra via per ricavare l'affidabilità di un dispositivo è ricorrere a dei test di affidabilità, sotto opportune condizioni operative, per ricavare dati con il supporto di misurazioni e parametri statistici. In questo caso si parla di stima dell'affidabilità.

L'affidabilità, in genere, viene indicata con la lettera R (dall'inglese Reliability), ed essendo funzione del tempo si è soliti indicarla con $R(t)$. Un dato di affidabilità, che per definizione è una probabilità e quindi è adimensionale, per essere completo necessita, oltre ovviamente del valore numerico di probabilità, anche delle definizioni di: funzione richiesta (può esserne richiesta anche più di una), condizioni operative e profilo di missione.

La funzione richiesta specifica il compito del dispositivo. Le condizioni operative indicano le condizioni che devono essere controllate oppure alle quali è soggetto il dispositivo durante il suo periodo di funzionamento. Sia la funzione richiesta che le condizioni operative possono essere dipendenti dal tempo, in questo caso occorre definire un profilo di missione, che racchiude tutte le informazioni appena citate come funzioni del tempo in aggiunta alla durata dell'analisi, ovvero al tempo di missione.

L'affidabilità di un dispositivo deve sempre essere messa in relazione ai dati appena introdotti.

1.2 Guasti e tasso di guasto

Se un dispositivo risulta conforme allora è in grado di svolgere correttamente la sua funzione richiesta e le sue performance risultano adeguate. Nel corso del tempo, tuttavia, le sue performance potrebbero, in un certo istante, non rispettare più le specifiche e far sì che la funzione richiesta non sia più eseguita adeguatamente: in questo caso è avvenuto un guasto. C'è una stretta correlazione tra la probabilità che si verifichi un guasto ad un dispositivo e la sua affidabilità, come verrà illustrato meglio in seguito, dopo un'introduzione sui guasti.

Un guasto è definito come l'evento che avviene quando un dispositivo abbandona il suo stato operativo, ovvero uno stato nel quale funziona correttamente, ed entra in uno stato definito di guasto, ovvero uno stato non operativo dove il dispositivo non è in grado di svolgere la sua funzione. In altre parole, l'evento di guasto sancisce la fine dello svolgimento della funzione richiesta da parte del dispositivo e lo stato di guasto è caratterizzato dall'inabilità del dispositivo oggetto di studio di svolgere la sua funzione.

I guasti posso essere classificati in base alla loro causa nel seguente modo:

- Guasti da uso improprio: sono dovuti all'applicazione, durante l'utilizzo, di stress che eccedono le capacità specifiche del dispositivo.
- Guasti primari: i guasti vengono definiti primari quando la causa di guasto, diretta o indiretta, non è dovuta a guasti di altri dispositivi.
- Guasti secondari o guasti indotti: al contrario dei guasti primari sono causati dal guasto di un altro dispositivo.
- Guasti precoci: sono attribuibili a debolezze intrinseche nella costruzione del dispositivo e le cui cause sono normalmente identificabili durante il processo di produzione. In genere si manifestano durante il periodo iniziale di utilizzo.

- Guasti casuali: così definiti quando dovuti a fattori incontrollabili che interagiscono con il dispositivo durante il suo periodo di utilizzo. La loro probabilità è indipendente nel tempo.
- Guasti detti di wearout: ci si riferisce così a guasti dovuti, appunto, a wearout, ovvero ad usura, logoramento, consumo e degradazione del dispositivo. In genere sono generati da fenomeni chimico-fisici e la loro probabilità di accadimento è crescente nel tempo.

A livello di conseguenze sul sistema e sull'ambiente i guasti possono essere classificati in:

- Guasti critici (o pericolosi): sono guasti in grado di causare un danno inaccettabile a persone, cose, ambiente o parti del sistema nel quale si trova il dispositivo con un'alta probabilità, con un rischio elevato.
- Guasto totale: guasto che causa variazioni nelle caratteristiche dell'elemento gravi a tal punto da compromettere completamente la sua o le sue funzioni.
- Guasti di primaria importanza: guasti che possono ridurre la funzionalità di un sistema.
- Guasto parziale: il guasto è causa di variazione di una o più caratteristiche dell'elemento, che non impediscono completamente il suo funzionamento.
- Guasti di secondaria importanza: guasti che non riducono mai la funzionalità di un sistema.
- Guasto intermittente: guasto caratterizzato da una successione, generalmente casuale, di periodi di normale funzionamento e di periodi di guasto e quindi di interruzione del funzionamento, che diventa, appunto, intermittente.

Ad un guasto può essere associata anche una sua modalità, ovvero l'effetto locale che permette di osservare l'evento di guasto. È importante, inoltre, conoscere il meccanismo di guasto, che è il processo chimico, fisico o di qualsiasi altro tipo che determina l'evento di guasto.

Sulle cause di guasto, già trattate, è necessaria una distinzione in due tipologie: cause di guasto intrinseche (dovute a indebolimenti del dispositivo, wearout) e cause di guasto estrinseche (dovute ad utilizzi sbagliati o ad errori in fase di design, produzione o installazione del dispositivo). Le cause estrinseche possono portare a guasti sistematici ed in questo caso vanno considerati non come guasti ma come difetti.

Il tempo al guasto rappresenta la durata totale del tempo di operatività di un dispositivo, ovvero il tempo compreso dall'istante in cui un dispositivo conforme inizia a svolgere la sua funzione fino al verificarsi di un guasto. Il tempo al guasto è una variabile casuale per l'elevata aleatorietà delle variabili in gioco, come la costituzione del materiale usato, che non è mai completamente uniforme, così come i risultati dei fattori di stress o le condizioni operative di funzionamento.

È importante definire due concetti distinti: lo stato di guasto, ovvero lo stato di un sistema che non è in grado di eseguire la funzione richiesta ed il guasto inteso come l'evento che porta un sistema allo stato di guasto.

La frequenza con cui un dispositivo si guasta è valutata, nell'ingegneria dell'affidabilità, tramite il tasso di guasto. Il tasso di guasto è espresso in termini di guasti per unità di tempo ed essendo una frequenza la sua unità di misura è generalmente espressa come $[1/h]$ oppure come FIT (dall'inglese Failures In Time, ovvero il numero di guasti attesi per un miliardo (10^9) di ore di funzionamento).

In genere è espresso con la lettera greca lambda (λ). Può essere considerato, in base ad opportune ipotesi relative alla natura del dispositivo oggetto di studio, costante nel tempo oppure variabile. Se il tasso di guasto è funzione del tempo viene espresso con $\lambda(t)$.

In base alle nozioni introdotte in precedenza sulle cause di guasto, il tasso di guasto di una popolazione numerosa di dispositivi statisticamente identici ed indipendenti può essere rappresentato nel tempo attraverso una curva definita "a vasca da bagno", che viene di seguito rappresentata in Figura 1.1 e poi descritta:

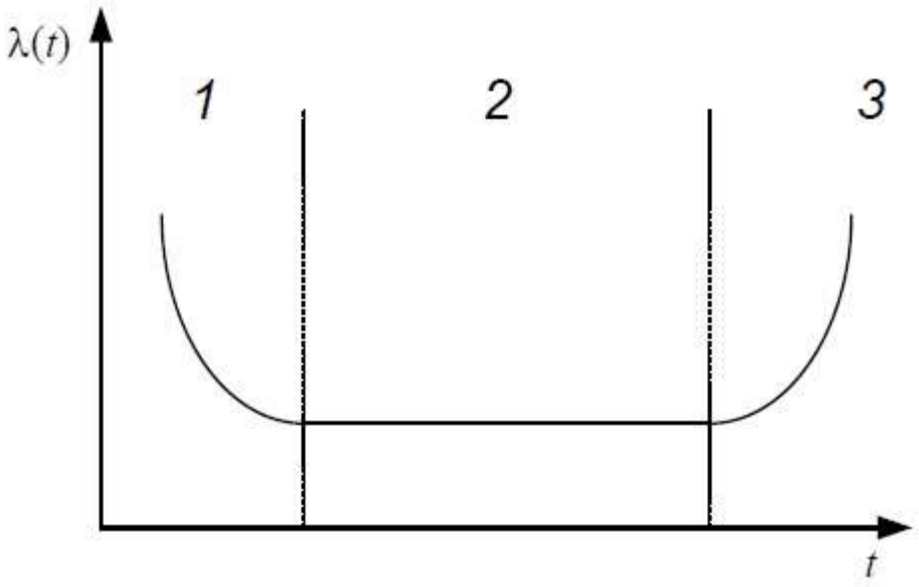


Figura 1.1: modello del tasso di guasto: "curva a vasca da bagno".

I guasti possono essere distinti in tre categorie, numerate anche in Figura 1.1. Ogni categoria di guasto avviene in periodi di funzionamento differenti:

1. Guasti iniziali: guasti prematuri, che avvengono nel primo periodo di utilizzo e pertanto chiamati anche guasti per mortalità infantile. Sono guasti dovuti a debolezze nei materiali, nei componenti o nel processo produttivo e sono distribuiti casualmente tra i vari dispositivi prodotti e nel tempo. Il tasso di guasto $\lambda(t)$ decresce rapidamente nel tempo.
2. Guasti con tasso di guasto $\lambda(t)$ costante (o quasi costante): avvengono dopo il primo periodo operativo del dispositivo, caratterizzato dalla presenza dei guasti iniziali. Sono caratterizzati dalla distribuzione di Poisson[3].
3. Guasti da wearout: come già detto dovuti ad usura, logoramento, fatica. Il tasso di guasto $\lambda(t)$ incrementa nel tempo.

La vita utile di ogni dispositivo appartenente alla popolazione dai quali deriva la curva è l'intervallo di tempo che inizia dalla messa in funzione dello stesso e che termina quando il tasso di guasto diventa troppo elevato ed inaccettabile a causa dei guasti da wearout. La vita utile comprende quindi gli intervalli di tempo 1 e 2, rappresentati in Figura 1.1, e termina all'inizio dell'intervallo 3. Il wearout provoca un forte incremento del tasso di guasto e di conseguenza una diminuzione

[3] La distribuzione di Poisson, in teoria della probabilità, è una distribuzione di probabilità discreta che esprime la probabilità per il numero di eventi in un intervallo di tempo, sapendo che mediamente se ne verifica un certo numero.

vertiginosa dell'affidabilità del dispositivo, rendendo conveniente cessare il suo utilizzo prima del periodo 3.

1.3 Affidabilità e distribuzioni di probabilità

Riguardo all'affidabilità, che, come già descritto, è la probabilità che un dispositivo esegua correttamente la sua funzione richiesta nel tempo, si possono fare delle osservazioni qualitative.

Un dispositivo conforme messo in operazione avrà una probabilità del 100% di funzionare correttamente nell'istante iniziale, quindi l'affidabilità sarà, in principio, ovvero nell'istante in cui il dispositivo inizia a funzionare (in genere si considera $t = 0$), pari ad 1 ($R(0) = 1$).

Durante il tempo di missione, con il dispositivo in operazione, è possibile in ogni istante che avvenga un guasto, con una probabilità che dipende dal tasso di guasto $\lambda(t)$: è intuitivo pensare che, con lo scorrere del tempo, c'è sempre un aumento della probabilità che sia avvenuto un guasto, considerando l'istante in questione e tutto il periodo di funzionamento precedente, pertanto la probabilità che il dispositivo rimanga funzionante, e quindi l'affidabilità, sarà decrescente nel corso del tempo. Quest'ultima considerazione è lecita qualsiasi sia la variazione del tasso di guasto nel corso del tempo.

Infine, considerando che prima o poi, presto o tardi, avverrà un guasto, si può stabilire che per un tempo infinito la probabilità che il dispositivo sia ancora funzionante tenda a zero ($R(\infty) \to 0$).

I passaggi seguenti, con il supporto di nozioni sulle distribuzioni di probabilità, forniscono un'idea più chiara del significato di affidabilità e portano ad un'espressione della stessa in termini matematici, che contribuiranno a confermare le osservazioni qualitative appena descritte.

Come già riportato, la funzione di affidabilità è definita come $R(t)$, con il tempo variabile aleatoria. Nel profilo di missione si considera per semplicità l'inizio della valutazione dell'affidabilità a tempo zero. Le condizioni del dispositivo ad inizio tempo di missione ($t = 0$) influenzano il risultato finale, ad esempio nel caso in cui il dispositivo abbia già operato precedentemente.

$R(t)$ è la probabilità che il dispositivo oggetto di studio non si guasti in un intervallo di tempo $[0, t]$. Si ritiene che il primo guasto del dispositivo in oggetto avvenga ad un tempo $\hat{t}$. La condizione $\hat{t} > t$ indica che ad un istante generico non è avvenuto (ancora) nessun guasto, indica che il tempo al guasto è maggiore dell'istante di tempo considerato. L'affidabilità non è nient'altro che la probabilità che questa condizione sia rispettata. Secondo queste considerazioni può essere assegnata all'affidabilità la seguente espressione:

$$R(t) = \Pr(dispositivo\ funziona\ nel\ periodo\ [0, t]) = \Pr(\hat{t} > t) \qquad (1.1)$$

A volte è d'interesse l'affidabilità riferita ad un intervallo di tempo $[t_1, t_2]$, sotto la condizione che il dispositivo abbia già operato senza guasti da un istante iniziale t_0 fino al tempo t_1 (ovviamente con la condizione $t_0 < t_1 < t_2$). In questo caso è utile introdurre la probabilità condizionata (l'affidabilità desiderata è la probabilità che il dispositivo lavori correttamente da t_1 a t_2, con la condizione imposta sulla variabile t).

L'affidabilità, in questo caso, è la probabilità che il dispositivo funzioni correttamente fino al tempo t_2, sapendo che ha funzionato correttamente fino al tempo t_1.

La seguente equazione 1.2 riporta l'espressione della probabilità condizionata relativa a due generici eventi, denominati A e B, in particolare è la probabilità che si verifichi l'evento A sapendo che si è verificato l'evento B:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{1.2}$$

L'affidabilità condizionata è espressa nella seguente equazione 1.3, in accordo con l'equazione 1.2 e con quanto descritto per l'affidabilità riferita ad un intervallo di tempo $[t_1, t_2]$:

$$R(t_1, t_2) = \Pr\{\hat{t} > t_2 | \hat{t} > t_1\} = \frac{R(t_2)}{R(t_1)} \tag{1.3}$$

La probabilità che una variabile aleatoria generica X assuma un definito valore x è descritta con l'ausilio di una distribuzione di probabilità.

Quando viene considerata una variabile aleatoria discreta la distribuzione può essere vista come una tabella che associa i possibili valori che può assumere la variabile aleatoria, gli x_i, alla loro probabilità $p(x_i)$.

È rappresentato, nella seguente Figura 1.2, un esempio di distribuzione di probabilità per una variabile aleatoria discreta:

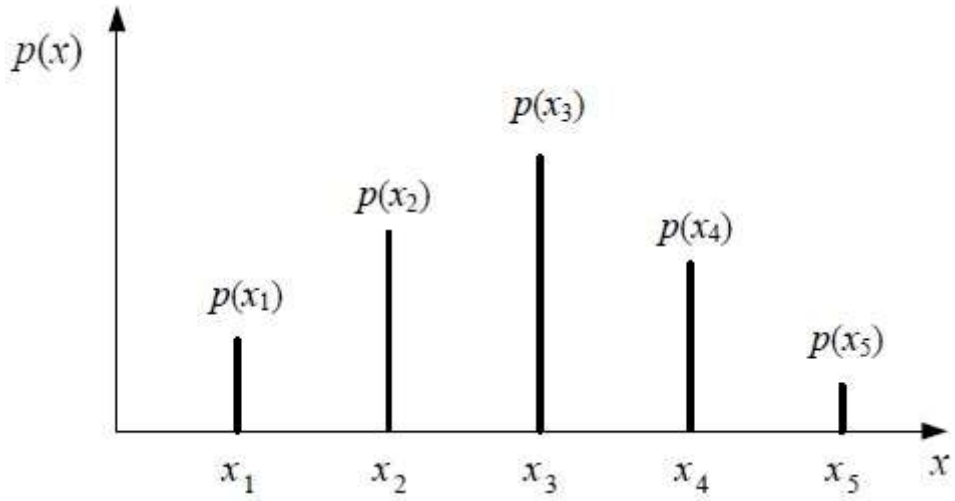


Figura 1.2: distribuzione di probabilità per variabili aleatorie discrete.

La sommatoria delle probabilità di ogni x_i è pari ad 1:

$$\sum_i p(x_i) = 1 \tag{1.4}$$

Se la variabile aleatoria è continua la probabilità viene descritta mediante una funzione continua di densità di probabilità, denominata $f(x)$.

La seguente Figura 1.3 rappresenta un esempio:

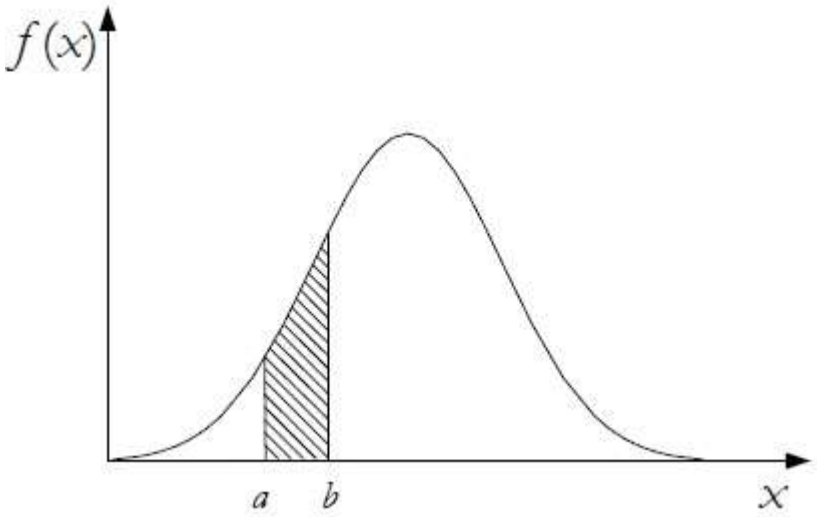


Figura 1.3: funzione di densità di probabilità per variabili aleatorie continue.

In modo analogo a quanto visto per le funzioni discrete, la sommatoria delle probabilità di tutti i valori che può assumere la variabile aleatoria è pari a 1. Essendo la variabile aleatoria continua è necessario l'utilizzo dell'operatore integrale:

$$\int_{-\infty}^{+\infty} f(x)dx = 1 \tag{1.5}$$

La funzione di densità di probabilità è sempre maggiore o uguale a zero per ogni possibile valore che può assumere la variabile aleatoria:

$$f(x) \geq 0 \tag{1.6}$$

La probabilità che la variabile aleatoria assuma un valore compreso tra due valori generici, definiti come a e b, è pari all'integrale della funzione di densità di probabilità, avente come estremi di integrazione gli stessi valori. È rappresentato un esempio in Figura 1.3, dove la probabilità è l'area sottesa dalla curva. L'espressione è la seguente:

$$P\{a \leq X \leq b\} = \int_{a}^{b} f(x)dx \tag{1.7}$$

La distribuzione di una variabile aleatoria continua può essere descritta tramite la funzione di distribuzione cumulativa, indicata con $F(x)$ e definita dalla seguente equazione 1.8:

$$F(x) = P(X \leq x) = \int_{-\infty}^{x} f(x)dx \quad con \ -\infty < x < +\infty \tag{1.8}$$

Vengono indicati in seguito i valori della distribuzione cumulativa per i suoi estremi ($x = \pm\infty$):

$$F(-\infty) = 0 \tag{1.9}$$

$$F(+\infty) = 1 \tag{1.10}$$

$F(x)$, la funzione di distribuzione cumulativa, è una funzione non decrescente ed assegna la probabilità che la variabile aleatoria assuma un valore uguale o minore di x. È rappresentata graficamente nella seguente Figura 1.4, dove viene anche confrontata con la funzione di densità di probabilità:

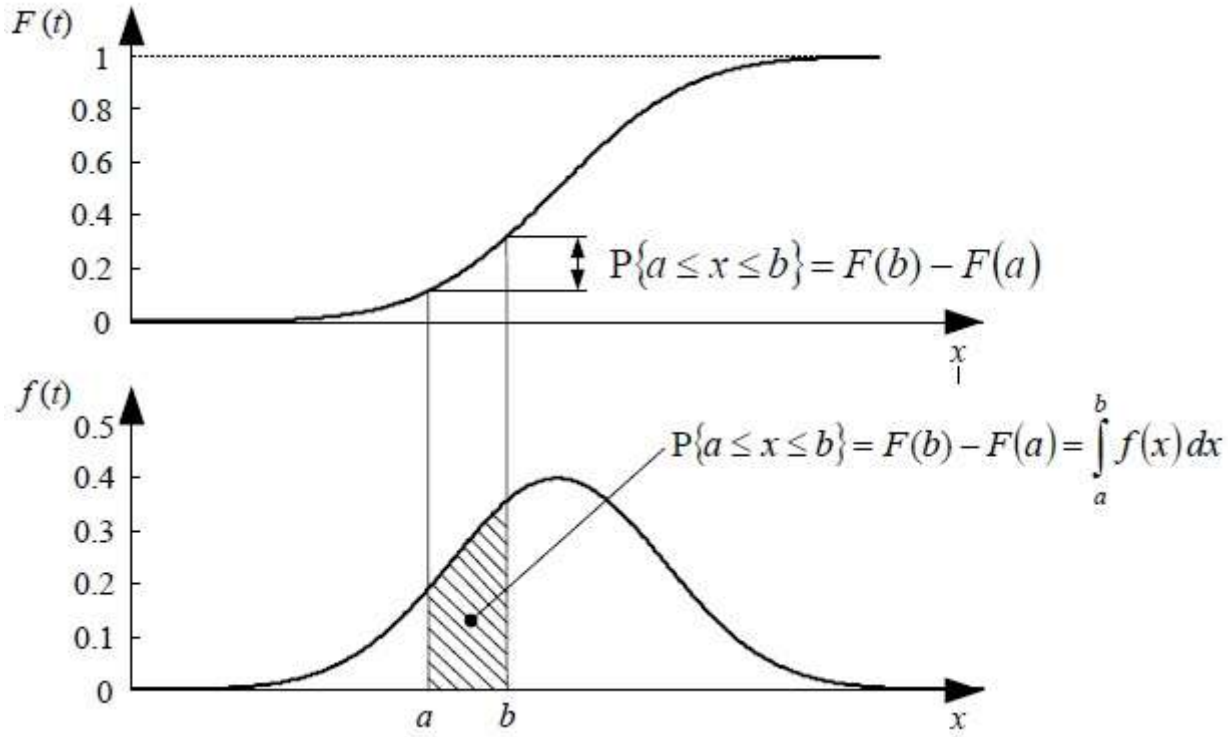


Figura 1.4: funzione di distribuzione cumulativa e funzione di densità di probabilità a confronto.

Possiamo osservare che la funzione di densità di probabilità della variabile aleatoria X è la derivata della funzione di distribuzione cumulativa:

$$f(x) = \frac{dF(x)}{dx} \tag{1.11}$$

La probabilità che il valore assunto dalla variabile aleatoria sia compreso tra due estremi, a e b, è descritta nella seguente equazione, che utilizza entrambe le distribuzioni, $F(x)$ ed $f(x)$:

$$P\{a \le x \le b\} = F(b) - F(a) = \int_a^b f(x)dx \tag{1.12}$$

L'evento $\{x > a\}$ è complementare all'evento $\{x \le a\}$:

$$Pr\{x > a\} = 1 - F(a) \tag{1.13}$$

L'evento $\{x_1 < x \le x_2\}$ può essere espresso dal complementare dell'evento $\{x \le x_1\} \cup \{x > x_2\}$, quindi si può ricavare la seguente equazione, con l'ausilio della precedente equazione 1.13:

$$Pr(x_1 < x \leq x_2) = 1 - (F(x_1) + 1 - F(x_2)) = F(x_2) - F(x_1) \quad (1.14)$$

Si può osservare che la funzione di distribuzione cumulata $F(x)$, relativa ad una variabile aleatoria continua x, è anch'essa continua. Il coefficiente differenziale di $F(x)$, pertanto, deve esistere, ad eccezione di alcuni punti, relativamente pochi:

$$\lim_{x \to X_2} F(x) = F(x)_{x=X_2} \quad (1.15)$$

Sapendo che:

$$\lim_{X_1 \to X_2} Pr[X_1 < x < X_2] = 0 \quad (1.16)$$

$$Pr[x = X_2] \leq Pr[X_1 < x < X_2] \quad (1.17)$$

Si ricava:

$$Pr[x = X_2] = 0 \quad (1.18)$$

Per quando riportato nell'equazione 1.18, in ciascun gruppo di eventi in seguito riportato, la probabilità di ogni evento è la stessa:

- $\{x_1 < x < x_2\},\ \{x_1 \leq x < x_2\}, \{x_1 < x \leq x_2\}, \{x_1 \leq x \leq x_2\}$;
- $\{x < x_1\}, \{x \leq x_1\}$;
- $\{x > x_1\}, \{x \geq x_1\}$.

Vale pertanto la seguente equazione, con $A = \{x_1 \leq x \leq x_2\}$ e $B = \{x_1 < x < x_2\}$:

$$Pr(A) = Pr(x = x_1) + Pr(B) + Pr(x = x_2) = Pr(B) \quad (1.19)$$

Con il limite per un valore $\delta \to 0$:

$$f(a) = \lim_{\delta \to 0} \frac{Pr(a \leq x \leq a + \delta)}{\delta} \neq 0 \quad (1.20)$$

L'inaffidabilità, definita $F(t)$, è la probabilità che un dispositivo si guasti nell'intervallo di tempo $[0, t]$, è l'evento complementare all'affidabilità. Viene definita dalla seguente espressione, ricordando che con $\hat{t}$ si indica il tempo al guasto:

$$F(t) = \Pr\{\hat{t} \leq t\} \quad (1.21)$$

Tra le sue proprietà, si ricordano le seguenti:

$$0 \leq F(t) \leq F(t') \quad per \quad 0 \leq t \leq t' \quad (1.22)$$

$$F(t) \to 1 \quad per \quad t \to \infty \quad (1.23)$$

Si può ricavare l'affidabilità, essendo l'evento complementare all'inaffidabilità:

$$R(t) = \Pr\{\hat{t} > t\} = 1 - \Pr\{\hat{t} \leq t\} = 1 - F(t) \tag{1.24}$$

Derivando i termini dell'equazione 1.24 si ottiene la seguente correlazione tra le derivate dell'affidabilità e dell'inaffidabilità:

$$dR(t) = -dF(t) \tag{1.25}$$

Essendo l'inaffidabilità funzione di distribuzione cumulativa della funzione di distribuzione di densità di probabilità, con relazione espressa nell'equazione 1.11, e con quanto riportato nell'equazione 1.25, si può ricavare la seguente equazione:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{1.26}$$

Integrando la precedente equazione 1.26 (utilizzando la derivata dell'affidabilità nel tempo) e ricordando che $R(0) = 1$ si ricava la seguente espressione dell'affidabilità:

$$R(t) = 1 - \int_0^t f(t)dt \tag{1.27}$$

La probabilità di guasto nel periodo di tempo $[t, t + dt]$ sarà pari a $f(t)dt$. Integrando la probabilità di guasto per un tempo infinito si ricava la conferma di quando detto qualitativamente: presto o tardi il sistema subirà un guasto e l'inaffidabilità tende a 1 per un tempo infinito:

$$F(\infty) = \int_0^\infty f(t)dt = 1 \tag{1.28}$$

1.4 Metodo empirico

Il metodo empirico, attraverso dei risultati ottenuti da delle prove eseguite su un campione omogeneo di dispositivi appartenenti allo stesso lotto, può essere utilizzato per ricavare dei modelli validi per l'affidabilità, per il tasso di guasto e per il tempo medio al guasto, indicato più comunemente come MTTF (dall'inglese Mean Time To Failure).

Nelle prove sopra citate si considera un numero n di dispositivi, statisticamente identici e statisticamente indipendenti tra di loro. Essi vengono messi in operazione contemporaneamente ad un tempo $t = 0$, con le stesse condizioni operative, e ne viene testato il funzionamento.

La variabile $v(t)$ indica il sottoinsieme dei dispositivi che non ha ancora subito un guasto, ad un generico istante di tempo t (sono i dispositivi, che hanno svolto correttamente la loro funzione nell'intervallo di tempo $[0, t]$).

Vengono definiti $t_1, t_2, \ldots t_n$ come i periodi di tempo osservati senza guasti, quindi ad ognuno di questi istanti di tempo avviene il guasto di uno degli n dispositivi. Si considerano tali tempi come

valori indipendenti della variabile aleatoria $\hat{t}$ (non sono punti arbitrari sull'asse del tempo). Viene in seguito riportato in Figura 1.5 l'andamento del sottoinsieme $v(t)$, che decresce di un dispositivo ad ogni guasto e quindi ad ogni istante t_i.

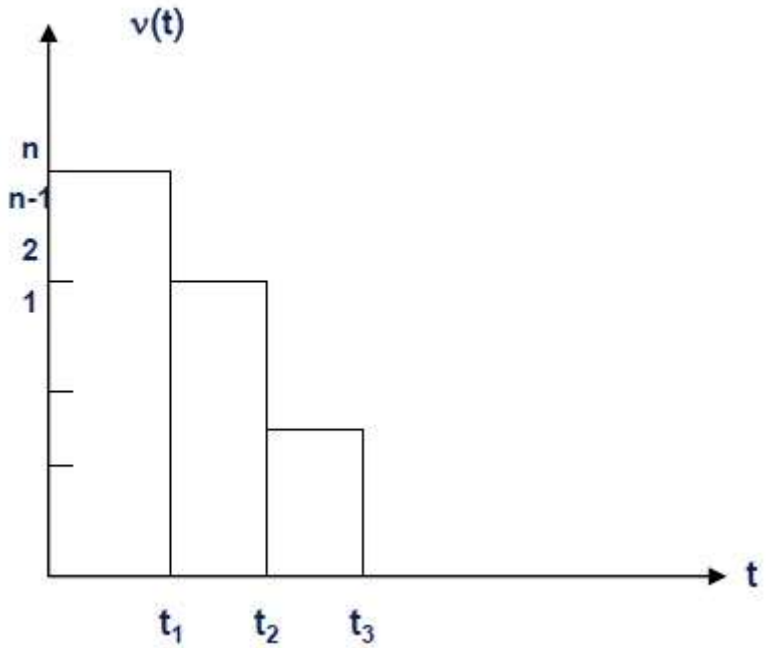


Figura 1.5: andamento nel tempo del numero di dispositivi funzionanti.

La seguente espressione rappresenta il valore empirico aspettato di $\hat{t}$, costruito tramite la media empirica. Il suo valore è stimato statisticamente e rappresenta il tempo medio empirico al guasto, indicato con $\hat{E}$ e descritto dalla seguente equazione:

$$\hat{E} = \frac{t_1 + t_2 + \cdots + t_n}{n} \tag{1.29}$$

La media empirica del tempo al guasto, per un valore di $n \to \infty$, converge alla media reale e quindi al vero tempo medio al guasto, al MTTF:

$$\hat{E} = MTTF \qquad per \;\; n \to \infty \tag{1.30}$$

Se la prova viene interrotta prima che ogni dispositivo si sia guastato, quindi considerando un numero di guasti pari a r, con $r < n$, si può stimare un MTTF conservativo, considerando che i restanti $(n - r)$ dispositivi si siano guastati nel momento di interruzione del test e quindi considerando nel calcolo un numero $(n - r)$ di tempi di guasto pari al tempo di fine test, definito t_r.

In generale, si può esprimere la probabilità partendo dal concetto di frequenza relativa, come evidenziato dalle seguenti equazioni, con il parametro h che rappresenta la larghezza di ogni classe:

$$\hat{f}(x) \cdot h = \frac{n(x)}{n} \tag{1.31}$$

$$\hat{f}(x) = \frac{1}{h} \cdot \frac{n(x)}{n} \tag{1.32}$$

Nell'esempio trattato, h rappresenta l'intervallo tra un guasto ed il successivo. Si ricava la seguente equazione introducendo la variabile $n_f(t)$, che rappresenta il numero di dispositivi guasti al tempo t:

$$\hat{f}(t) = \frac{1}{h} \cdot \frac{n_f(t+h) - n_f(t)}{n} \tag{1.33}$$

Quindi viene indicata l'espressione dell'inaffidabilità empirica come il rapporto tra i dispositivi guasti ed i dispositivi totali e la correlazione tra la stessa e la probabilità di guasto empirica:

$$\hat{F}(t) = \frac{n - \hat{v}(t)}{n} = \frac{n_f(t)}{n} \tag{1.34}$$

$$\hat{f}(t) = \frac{\hat{F}(t+h) - \hat{F}(t)}{h} \tag{1.35}$$

Viene definito "tasso di guasto istantaneo" il rapporto tra gli elementi che si sono guastati nell'intervallo $(t,\ t+h]$ ed il numero degli elementi funzionanti al tempo t, ovvero $v(t)$. Da ciò si può ricavare un'equazione, la 1.39, che lega il tasso istantaneo di guasto con la funzione di probabilità e l'affidabilità:

$$\hat{\lambda}(t) = \frac{1}{h} \cdot \frac{\hat{v}(t) - \hat{v}(t+h)}{\hat{v}(t)} \tag{1.36}$$

$$\hat{R}(t) = \frac{\hat{v}(t)}{n} \tag{1.37}$$

$$\hat{\lambda}(t) = \frac{1}{h} \cdot \frac{\hat{F}(t+h) - \hat{F}(t)}{\hat{R}(t)} = \frac{1}{h} \cdot \frac{\hat{R}(t) - \hat{R}(t+h)}{\hat{R}(t)} \tag{1.38}$$

$$\hat{\lambda}(t) = \frac{\hat{f}(t)}{\hat{R}(t)} \tag{1.39}$$

Per definire un tasso di guasto istantaneo, quando viene trattata una variabile aleatoria continua, si considera l'evento di guasto di un dispositivo nell'intervallo $[t,\ t+dt]$. L'evento di guasto in dato intervallo è condizionato dal fatto che il dispositivo non abbia subito un guasto prima dell'istante di tempo t.

Grazie alla teoria della probabilità, si ricorda, come già visto nel capitolo precedente, l'espressione generica di una probabilità condizionata. Viene riportata pertanto l'equazione 1.2:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{1.2}$$

La probabilità condizionata dell'evento di guasto di un dispositivo nell'intervallo $[t,\ t+dt]$ può essere espressa pertanto come segue, sempre considerando $\hat{t}$ come il tempo al guasto considerando l'equazione 1.2:

$$Pr\{t < \hat{t} < t + dt \mid \hat{t} > t\} = \frac{Pr\{t < \hat{t} < t + dt\}}{Pr\{\hat{t} > t\}} = \frac{f(t)dt}{R(t)} \tag{1.40}$$

Il tasso di guasto $\lambda(t)$ di un dispositivo può essere definito come il seguente limite:

$$\lambda(t) = \lim_{dt \to 0} \frac{1}{dt} \cdot \Pr\{t < \hat{t} \leq t + h \mid \hat{t} > t\} \tag{1.41}$$

Quindi, dalle equazioni 1.40 e 1.41 si ottiene la seguente espressione del tasso di guasto:

$$\lambda(t) = \lim_{dt \to 0} \frac{1}{dt} \cdot \frac{Pr(t < \hat{t} < t + dt)}{Pr(\hat{t} > t)} = \frac{f(t)}{R(t)} \tag{1.42}$$

Sapendo che $Pr(\hat{t} \leq t) = F(t)$, si ricava:

$$Pr(\hat{t} > t) = 1 - F(t) \tag{1.43}$$

E, se la funzione di distribuzione cumulativa, $F(t)$, è derivabile:

$$\lambda(t) = \lim_{dt \to 0} \frac{1}{dt} \cdot \frac{F(t + h) - F(t)}{R(t)} \tag{1.44}$$

Si ricava che:

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{1.45}$$

Si può esprimere la precedente equazione ricordando la relazione tra le funzioni di densità e di affidabilità espressa nell'equazione 1.26:

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} = -\frac{d}{dt} \log\big(R(t)\big) \tag{1.46}$$

Quindi, integrando la precedente 1.46:

$$R(t) = e^{-\int_0^t \lambda(t)dt} \tag{1.47}$$

Per $t = 0$:

$$R(0) = 1 \tag{1.48}$$

Si ottiene un'espressione della probabilità di guasto dalle equazioni 1.45 e 1.47:

$$f(t) = \lambda(t) \cdot e^{-\int_0^t \lambda(t)dt} \tag{1.49}$$

L'affidabilità in $(t, t+h)$ è espressa dalla seguente equazione:

$$R_m(t, t+h) = \frac{R(t+h)}{R(t)} = \frac{\exp\left(-\int_0^{t+h} \lambda(t)dt\right)}{\exp\left(-\int_0^t \lambda(t)dt\right)} \cong e^{-\lambda(t)h} \tag{1.50}$$

Utilizzando la definizione di media si ottiene l'espressione del tempo medio al guasto, MTTF, espressa dalla seguente equazione 1.51: e 1.52 nell'equazione 1.53:

$$MTTF = \int_0^\infty t \cdot f(t)dt = -\int_0^\infty t \cdot \frac{dR(t)}{dt}dt = -[t \cdot R(t)]_0^\infty + \int_0^\infty R(t)dt \tag{1.51}$$

Si può notare, considerando il primo termine del risultato nell'equazione 1.51, che:

$$-[t \cdot R(t)]_0^\infty = 0 \tag{1.52}$$

Dalle equazioni 1.51 e 1.52 si ricava la seguente espressione del MTTF:

$$MTTF = \int_0^\infty R(t)dt \tag{1.53}$$

Considerando un tasso di guasto costante si ottengono le seguenti espressioni di affidabilità, di probabilità di guasto e di MTTF. I grafici delle funzioni (1.54) e (1.55) sono riportati in Figura 1.6:

$$R(t) = e^{-\lambda t} \tag{1.54}$$

$$f(t) = \lambda(t) \cdot R(t) = \lambda \cdot R(t) = \lambda e^{-\lambda t} \tag{1.55}$$

$$MTTF = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda} \tag{1.56}$$

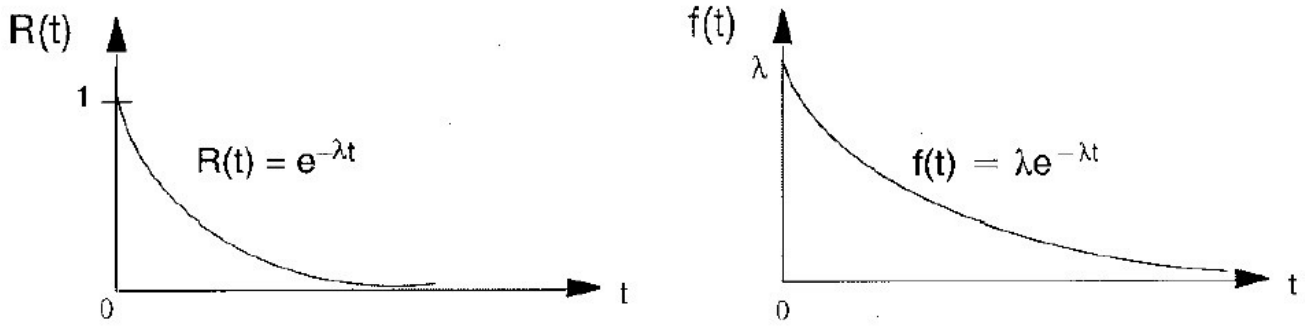


Figura 1.6: R(t) ed f(t) per dispositivo con tasso di guasto costante.

Le equazioni 1.54, 1.55 e 1.56 sono valide solamente in caso di tasso di guasto costante.

Se non è possibile modellare le caratteristiche del dispositivo con questa condizione si può utilizzare una modellazione dell'affidabilità chiamata **distribuzione di Weibull**[4], che è caratterizzata da tre parametri:

- γ: questo parametro è chiamato vita minima, è considerato come un periodo dove il dispositivo non può subire guasti, spesso si considera $\gamma = 0$,
- η: parametro di scala, chiamato anche vita caratteristica,
- β: parametro di forma.

La funzione di affidabilità è data da un sistema di equazioni, contenenti i tre parametri appena descritti. L'affidabilità, per istanti di tempo minori della vita minima del dispositivo, è pari a 1. Quando il dispositivo conclude il periodo dove opera senza la possibilità di subire guasti, la vita minima appunto, la sua affidabilità assume una forma simile alla esponenziale, con la vita caratteristica che si può vedere come l'inverso del tasso di guasto ed il parametro di forma che eleva alla sua potenza l'esponente della funzione esponenziale:

$$R(t) = \begin{cases} e^{-(\frac{t-\gamma}{\eta})^{\beta}} & t \geq \gamma \\ 1 & t \leq \gamma \end{cases} \tag{1.57}$$

Se si trascura la vita minima, quindi $\gamma = 0$, e se si inserisce un nuovo parametro che trasforma la vita caratteristica in una frequenza, $\lambda = 1/\eta$, la funzione di affidabilità per la distribuzione di Weibull è data dalla seguente equazione, ricavata dal sistema 1.57 e dalle precedenti supposizioni:

$$R(t) = e^{-(\lambda t)^{\beta}} \tag{1.58}$$

La funzione di densità ed il tasso di guasto, indicato con $\lambda^*(t)$, saranno dati dalle seguenti equazioni:

$$f(t) = \beta \cdot \lambda \cdot (\lambda \cdot t)^{\beta-1} \cdot e^{-(\lambda t)^{\beta}} \tag{1.59}$$

$$\lambda^*(t) = \beta \cdot \lambda \cdot (\lambda \cdot t)^{\beta-1} \tag{1.60}$$

Il tasso di guasto, nella distribuzione di Weibull, è funzione del tempo ed ha diverse caratteristiche nel tempo in base al parametro di forma β:

- Decresce per $\beta < 1$,
- Cresce per $\beta > 1$,
- Rimane costante per $\beta = 1$.

Viene riportato, come esempio e nella seguente Figura 1.7, l'andamento del tasso di guasto in caso di distribuzione di Weibull con $\beta = 2$. Essendo $\beta > 1$ la funzione sarà crescente:

[4] La distribuzione prende il nome dal matematico svedese Waloddi Weibull, che la descrisse nel 1951.

Figura 1.7: Grafico del tasso di guasto di una distribuzione di Weibull con β=2

1.5 Diagramma a blocchi di affidabilità (RBD)

Un diagramma a blocchi di affidabilità, chiamato più semplicemente RBD (dall'inglese Reliability Block Diagram), è una rappresentazione grafica a blocchi che mostra le interconnessioni logiche tra le funzioni dei dispositivi facenti parte dello stesso sistema e legati dalla missione richiesta al dispositivo. Per sistema si intende pertanto un set di dispositivi connessi logicamente al fine di garantire una o più performance funzionali. Un dispositivo facente parte di un sistema viene generalmente chiamato elemento o componente del sistema. L'affidabilità del sistema dipende dall'affidabilità dei suoi elementi e dal modo in cui essi sono interconnessi, rappresentato graficamente appunto da un RBD. È un diagramma degli eventi, determina quali elementi sono necessari per la funzione richiesta e quali invece possono guastarsi senza effetti sul funzionamento. Ogni funzione richiesta eseguita da un dispositivo può essere rappresentata mediante il suo diagramma a blocchi di affidabilità (RBD), partendo dalla configurazione più semplice relativa ad un sistema composto da un solo elemento fino a configurazioni molto più complesse.

Caratteristiche del metodo RBD:

- Esistono solo due stati in cui può trovarsi il sistema e nei quali può trovarsi ogni singolo elemento di esso: lo stato operativo (OK) e lo stato di guasto (FAULT). Un sistema, o un elemento, si trova nello stato operativo quando è in grado di svolgere la propria funzione correttamente e si trova nello stato di guasto quando non è in grado di eseguirla. Avendo solo due possibili stati, sia il sistema che ogni suo singolo elemento rispondono ad una logica binaria.
- Ogni elemento è rappresentato da un blocco ed è indipendente dagli altri.
- Gli elementi necessari per il funzionamento sono disposti in serie.
- Gli elementi che possono guastarsi senza effetti sul sistema sono disposti in parallelo.
- Le funzioni che non hanno rilevanza nella missione analizzata sono rimosse dal diagramma a blocchi.

Configurazione **in serie**: gli elementi vengono connessi in serie quando è necessario, per il funzionamento del sistema, che ogni elemento svolga la sua funzione richiesta. Il sistema, se composto da soli elementi connessi in serie, è operativo solo se tutti i suoi elementi lo sono. L'ordine degli elementi in serie nel diagramma a blocchi è arbitrario. La configurazione in serie rappresenta il più semplice e comune modello di affidabilità.

Nella Figura 1.8 è rappresentato un RBD relativo ad un generico sistema composto da elementi in serie. In particolare, è raffigurato un sistema *S* composto da un numero n di elementi chiamati E_i, con $i = 1, 2, \ldots n$. Il sistema è considerato operativo se e solo se tutti gli elementi E_i funzionano correttamente contemporaneamente. Nel sistema non è presente alcuna ridondanza.

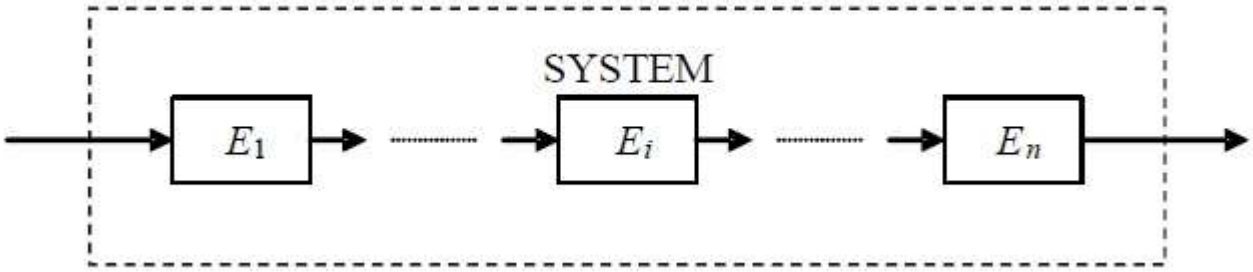


Figura 1.8: RBD, configurazione di n elementi in serie.

Viene assunto che lo stato di ogni elemento del sistema, operativo o di guasto, è indipendente dagli altri elementi e dai loro stati. Nella configurazione in serie il primo guasto di un elemento coincide con il guasto del sistema: il primo elemento che si guasta causa il guasto del sistema.

Viene definito l'evento elementare $\{E_i\}$ come il funzionamento dell'elemento i-esimo nel periodo di tempo $(0, t]$. La probabilità di tale evento è l'affidabilità dell'elemento, espressa ricordando che deve essere definito il tempo di guasto dell'elemento i-esimo, in questo caso come τ_i:

$$\{E_i\} = \{l'elemento\ E_i\ funziona\ senza\ guasti\ nel\ periodo\ (0, t] \mid \text{è}\ nuovo\ a\ t = 0\} \tag{1.61}$$

$$Pr\{E_i\} = Pr\{\tau_i > t\} = R_i(t) \quad con\ R_i(0) = 1 \tag{1.62}$$

Viene definito l'evento $\{W\}$ come il funzionamento del sistema *S* nel periodo di tempo $(0, t]$. Dato che ogni elemento deve essere operativo per garantire il funzionamento del sistema, l'evento $\{W\}$ è formato dall'intersezione tra tutti gli eventi $\{E_i\}$:

$$\{W\} = \{E_1\} \cap \{E_2\} \cap \ldots\ldots \{E_n\} \tag{1.63}$$

$$\begin{aligned} Pr\{W\} &= Pr\{E_1 \cap E_2 \cap \ldots E_n\} \\ &= Pr\{E_1\} * Pr\{E_2|E_1\} * Pr\{E_3|(E_1 \cap E_2)\} * \ldots Pr\{E_n|(E_1 \cap E_2 \ldots E_{n-1})\} \end{aligned} \tag{1.64}$$

Ricordando che ogni elemento si guasta indipendentemente dagli altri si può semplificare l'equazione 1.64, che può essere ridotta semplicemente al prodotto delle probabilità degli eventi. Nella seguente equazione 1.65 viene mostrato anche che le probabilità degli eventi $\{E_i\}$ non sono nient'altro che le affidabilità dei singoli elementi:

$$Pr\{W\} = R_s(t) = Pr\{E_1\} * Pr\{E_2\} * \dots Pr\{E_n\} = R_1(t) * R_2(t) * \dots R_n(t) = \prod_{i=1}^{n} R_i(t) \quad (1.65)$$

Nella seguente equazione viene riportato in forma compatta quanto espresso dalla 1.64:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) \quad (1.66)$$

In caso di tassi di guasto costanti, ovvero se $\lambda(t) = \lambda$ si può ricavare un'espressione dell'affidabilità del sistema in serie con la funzione esponenziale. Si nota inoltre, come riportato nell'equazione 1.68, che il tasso di guasto complessivo del sistema è la sommatoria dei tassi di guasto dei singoli elementi:

$$R_s(t) = e^{-(\lambda_1+\lambda_2+\dots\ \lambda_n)*t} \quad (1.67)$$

$$\lambda_s = \sum_{i=1}^{n} \lambda_i \quad (1.68)$$

L'espressione del tempo medio al guasto del sistema in serie è la seguente:

$$MTTF_s = \frac{1}{\lambda_s} \quad (1.69)$$

Considerando che l'affidabilità di ogni elemento è un numero compreso tra 0 e 1 si può notare che l'affidabilità del sistema (fissato un certo istante di tempo) sarà sempre più piccola del minor valore di affidabilità relativo ad un singolo elemento. Un sistema di elementi in serie, in termini di affidabilità, avrà sempre delle performance peggiori rispetto al peggior elemento componente lo stesso (elemento con affidabilità minore e tasso di guasto maggiore, in caso di tassi di guasto costanti). L'affidabilità di un sistema decresce rispetto al numero di elementi considerati necessari per la funzione richiesta: ogni elemento aggiunto ad una configurazione in serie causa un peggioramento delle performance. Viene riportato nell'equazione 1.70 il concetto appena espresso:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) \ \rightarrow \ R_s(t) \leq min\{R_i(t)\} \quad (1.70)$$

Si considera in Figura 1.9 un esempio di un sistema in serie composto da tre elementi con i tassi di guasto che seguono la relazione $\lambda_1 < \lambda_2 < \lambda_3$: si può notare quanto detto precedentemente. L'equazione 1.71 descrive il tasso di guasto del sistema, espresso nel grafico in Figura 1.9 in modo esplicito:

$$\lambda_s = \lambda_1 + \lambda_2 + \lambda_3 \quad (1.71)$$

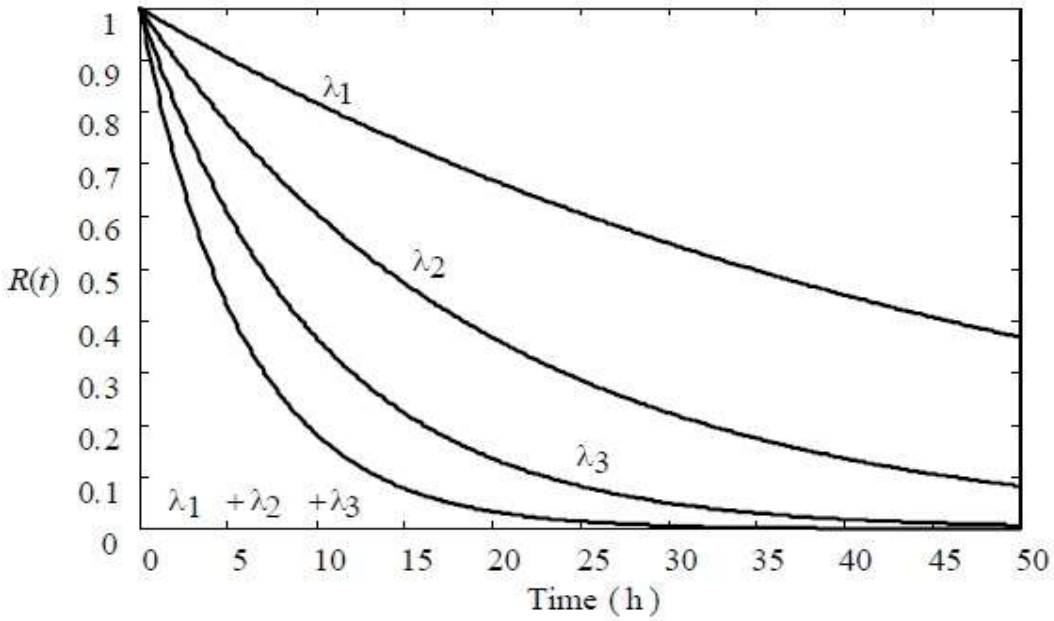


Figura 1.9: confronto affidabilità tra singoli elementi e sistema di elementi in serie.

Per introdurre un'altra principale configurazione, quella in parallelo, è necessario il concetto di ridondanza, che come già detto non è presente nei sistemi configurati in serie. La ridondanza è l'esistenza di più di un modo per rendere il sistema in grado di eseguire la sua funzione. In particolare, esistono più elementi di un sistema in grado di renderlo funzionante, indipendentemente dagli altri elementi. La ridondanza non implica necessariamente la duplicazione dell'hardware. Per carico si intende una grandezza relativa al funzionamento di un elemento, che lo quantifica (ad esempio corrente, voltaggio, forza, momento, velocità o frequenza di operazione). Sono presenti diverse tipologie di ridondanza:

- Attiva: gli elementi ridondanti sono sottoposti dall'inizio allo stesso carico durante la loro operazione. In caso di elementi indipendenti non è possibile condividere il carico.
- Warm: gli elementi sono soggetti ad un certo carico quando sono in operazione e, nell'istante in cui uno degli elementi subisce un guasto, il suo carico viene ridistribuito tra gli elementi ancora operativi, che quindi avranno un aumento di carico rispetto a quello iniziale, quando tutti gli elementi erano operativi. È presente quindi una condivisione del carico. In genere all'aumentare del carico aumenta anche il tasso di guasto.
- Standby: uno o più elementi non sono soggetti ad alcun carico (sono appunto in standby) e diventano operativi quando è necessario a seguito di un guasto di un altro elemento che era operativo. In questo caso si considera il tasso di guasto degli elementi in standby pari a zero.

Nelle ridondanze di tipo warm e standby è presente un dispositivo facente parte del sistema, chiamato switch, la cui funzione è la distribuzione del carico tra gli elementi.

Configurazione **in parallelo**: in caso di ridondanza attiva gli elementi sono connessi tra loro in parallelo. In questa configurazione sono presenti elementi che sono rilevanti, che rendono il sistema operativo con il loro funzionamento. Tali elementi non sono però necessari, non sono indispensabili, perché in caso di guasto non portano automaticamente il sistema a fallire nell'esecuzione della sua funzione: possono fallire senza effetti sul sistema. In un sistema con soli elementi connessi in parallelo viene eseguita la funzione richiesta nel caso in cui almeno uno degli elementi sia operativo

e, parimenti, la funzione richiesta non viene eseguita solo nel caso in cui tutti gli elementi non siano operativi.

Nella seguente Figura 1.10 è rappresentato un RBD relativo ad un sistema generico formato da soli elementi in parallelo:

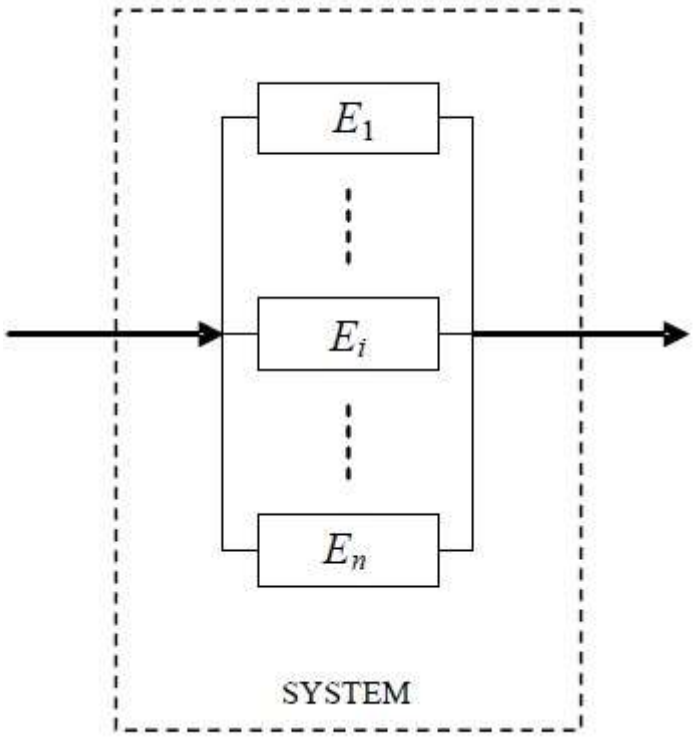


Figura 1.10: RBD, configurazione di n elementi in parallelo.

Il sistema *S*, come detto, è operativo se almeno uno dei suoi elementi E_i è funzionante. Si può risolvere il problema nel calcolo della probabilità attraverso il teorema di addizione, che viene riportato nelle seguenti equazioni per due elementi, A e B, nell'equazione 1.72 e per tre elementi, A, B e C, nell'equazione 1.73. Ovviamente il numero di eventi è pari al numero di elementi:

$$Pr\{A \cup B\} = Pr\{A\} + Pr\{B\} - Pr\{A \cap B\} \tag{1.72}$$

$$\begin{aligned} Pr\{A \cup B \cup C\} \\ &= Pr\{A\} + Pr\{B\} + Pr\{C\} - Pr\{A \cap B\} - Pr\{A \cap C\} - Pr\{B \cap C\} \\ &+ Pr\{A \cap B \cap C\} \end{aligned} \tag{1.73}$$

Ricordando che il sistema non è operativo se e solo se tutti i suoi elementi non lo sono, si può esprimere l'inaffidabilità del sistema come il prodotto delle inaffidabilità dei suoi singoli elementi:

$$F_s(t) = \prod_{i=1}^{n} F_i(t) \tag{1.74}$$

L'affidabilità del sistema viene ricavata partendo dalla sua complementarità con l'inaffidabilità e dall'espressione di quest'ultima in equazione 1.74:

$$R_s(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{n} F_i(t) \tag{1.75}$$

Nel passaggio successivo si sostituisce l'inaffidabilità dei singoli elementi, contenuta nell'equazione 1.75, esprimendola come funzione dell'affidabilità. Viene ricordato inoltre che l'affidabilità di ogni elemento, a tempo zero, è pari a 1 ($R_i(0) = 1$):

$$R_s(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)) \tag{1.76}$$

Il tempo medio al guasto (*MTTF*$_S$) ed il tasso di guasto del sistema $\lambda_s(t)$ sono dati dalle seguenti equazioni, ricavate in precedenza ed in questo caso riferite ad un sistema:

$$MTTF_s = \int_0^{+\infty} R_s(t)dt \tag{1.77}$$

$$\lambda_s(t) = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{1.78}$$

L'affidabilità del sistema (fissato un certo istante di tempo) sarà sempre più grande rispetto al maggior valore di affidabilità riferito al singolo elemento. Un sistema di elementi in parallelo, in termini di affidabilità, avrà sempre delle performance migliori rispetto al miglior elemento del sistema (elemento con affidabilità maggiore e tasso di guasto minore, in caso di tassi di guasto costanti). La probabilità che un sistema in parallelo funzioni è una funzione che cresce con l'incremento del numero di elementi che costituiscono il parallelo: ogni elemento aggiunto ad una configurazione in parallelo causa un miglioramento delle performance. Viene riportato nell'equazione 1.79 il concetto appena espresso:

$$R_s(t) \geq max\{R_i(t)\} \tag{1.79}$$

Si considera ora una configurazione in parallelo composta da due elementi con tasso di guasto uguale e costante nel tempo, definito λ. Le funzioni di affidabilità dei due elementi, definiti 1 e 2, sono riportate nell'equazione 1.80:

$$R_1(t) = R_2(t) = e^{-\lambda t} \tag{1.80}$$

Si ricava l'espressione dell'affidabilità del sistema tramite l'equazione 1.76 ed il MTTF del sistema tramite l'equazione 1.77:

$$R_s(t) = 2 \cdot e^{-\lambda t} - e^{-2 \cdot \lambda t} \tag{1.81}$$

$$MTTF_s = \frac{3}{2 \cdot \lambda} \tag{1.82}$$

Viene ora ricavato il tasso di guasto del sistema dall'equazione 1.78:

$$\lambda_s(t) = \frac{1}{2 \cdot e^{-\lambda t} - e^{-2\lambda t}} \cdot 2\lambda\{e^{-\lambda t} - e^{-2\lambda t}\} = 2\lambda \frac{e^{-\lambda t} - e^{-2\lambda t}}{2 \cdot e^{-\lambda t} - e^{-2\lambda t}} = 2\lambda \frac{e^{-\lambda t}(1 - e^{-\lambda t})}{e^{-\lambda t}(2 - e^{-\lambda t})} = 2\lambda \frac{(1 - e^{-\lambda t})}{(2 - e^{-\lambda t})} \tag{1.83}$$

Si può notare che, in presenza di ridondanza attiva, il tasso di guasto del sistema è funzione del tempo anche se i tassi di guasto di tutti gli elementi sono costanti. Il tasso di guasto è una funzione crescente. I limiti del tasso di guasto per il tempo che tende a zero ed a infinito sono i seguenti: $\lambda_s(0) = 0$ e $\lambda_s(\infty) = \lambda$.

Nella seguente Figura 1.11 è presente una comparazione dell'affidabilità nel tempo in tre diverse configurazioni. Per semplicità si considerano tutti gli elementi aventi tasso di guasto identico e pari a λ. Le configurazioni rappresentate sono le seguenti, con riportate le funzioni di affidabilità ed il MTTF:

- (**a**): sistema composto da due elementi in parallelo ($R_s(t) = 2e^{-\lambda t} - e^{-2\lambda t}$; $MTTF_s = \frac{3}{2\lambda}$),
- (**b**): sistema composto da un singolo elemento ($R_s(t) = e^{-\lambda t}$; $MTTF_s = \frac{1}{\lambda}$),
- (**c**): sistema composto da due elementi in serie ($R_s(t) = e^{-2\lambda t}$; $MTTF_s = \frac{1}{2\lambda}$).

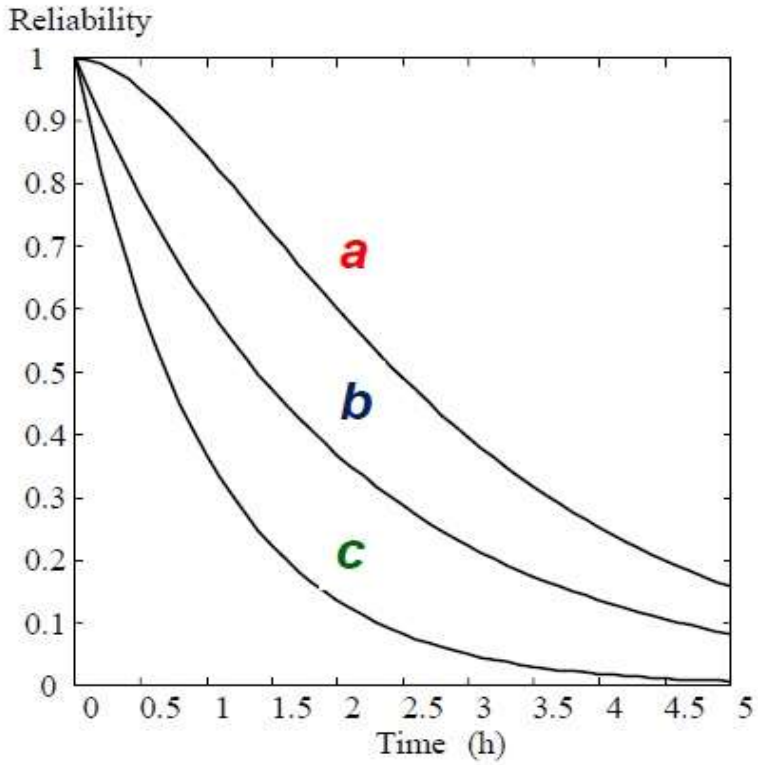


Figura 1.11: confronto affidabilità tra configurazione in serie, in parallelo ed elemento singolo.

Nella Figura 1.11 si può notare quanto descritto precedentemente: le performance di affidabilità di un sistema di elementi in serie sono peggiori rispetto a quelle dell'elemento singolo, mentre le performance migliori sono ottenute con la configurazione in parallelo.

Configurazione **k-out-of-n**: è una configurazione che rappresenta sistemi formati da n elementi in ridondanza attiva, come nella configurazione in parallelo. Questi sistemi, tuttavia, sono in grado di svolgere la loro funzione richiesta se sono funzionanti almeno k elementi appartenenti alla configurazione (da qui il significato di k-out-of-n, tradotto più chiaramente come "sono necessari k elementi funzionanti su n elementi totali").

La configurazione in parallelo è un caso particolare della configurazione k-out-of-n con la condizione di avere il numero minimo di elementi funzionanti richiesto pari ad 1 ($k = 1$). Anche la configurazione in serie è un caso particolare della configurazione k-out-of-n con la condizione di avere un numero di elementi funzionanti richiesto pari ad n ($k = n$), ovvero è richiesto il funzionamento di tutti gli elementi. La rappresentazione grafica resta uguale a quella della configurazione in parallelo ed è riportata nella seguente Figura 1.12:

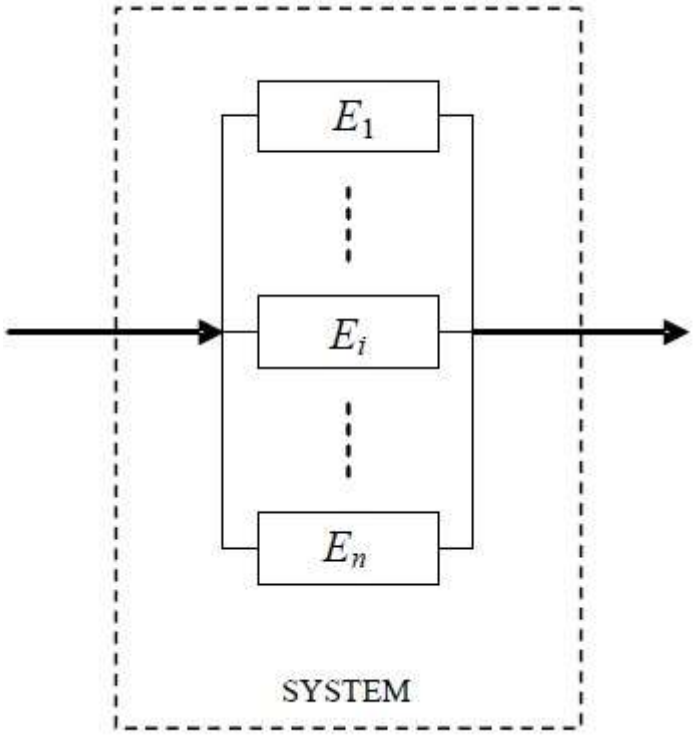


Figura 1.12: RBD, configurazione k-out-of-n.

Per analizzare i sistemi con questa configurazione RBD è necessario assumere le seguenti ipotesi:

- Gli elementi hanno lo stesso tasso di guasto λ.
- $1 \leq k \leq n$
- Utilizzo della distribuzione binomiale per il calcolo dell'affidabilità.
- Il generico elemento del sistema può assumere solamente due condizioni: funzionamento corretto oppure condizione di guasto.

L'affidabilità del sistema è data dalla seguente equazione, che addiziona tramite una sommatoria le probabilità di avere un numero di dispositivi funzionanti compreso tra k ed n:

$$R_S(t) = \sum_{i=k}^{n} \binom{n}{i} \big(R(t)\big)^i \big(1 - R(t)\big)^{n-i} \tag{1.84}$$

Viene esplicitato in seguito il significato del termine comprendente le combinazioni semplici senza ripetizioni, presente nella precedente equazione 1.84:

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!} \tag{1.85}$$

Considerando il modello esponenziale al tasso di guasto λ costante l'equazione 1.84 diventa:

$$R_S(t) = \sum_{i=k}^{n} \binom{n}{i} (e^{-\lambda t})^i (1 - e^{-\lambda t})^{n-i} \tag{1.86}$$

Come già detto, l'espressione dell'affidabilità nell'equazione 1.86 è utilizzabile per ricavare l'affidabilità per le configurazioni in serie ed in parallelo, semplicemente inserendo le opportune condizioni nei parametri della k-out-of-n: rispettivamente ($k = n$) e ($k = 1$) per serie e parallelo.

Come esempio nell'utilizzo dell'equazione 1.86 viene riportata la configurazione 2 out of 3 ed anche il suo MTTF:

$$R_S(t) = \sum_{i=2}^{3} \binom{3}{i} (e^{-\lambda t})^i (1 - e^{-\lambda t})^{n-i} = \binom{3}{2} e^{-2\lambda t}(1 - e^{-\lambda t}) + \binom{3}{3} e^{-3\lambda t} = 3e^{-2\lambda t} - 2e^{-3\lambda t} \tag{1.87}$$

$$MTTF = \int_{-\infty}^{\infty} (3e^{-2\lambda t} - 2e^{-3\lambda t})dt \tag{1.88}$$

Nella seguente Figura 1.13 è presente una comparazione dell'affidabilità nel tempo in quattro diverse configurazioni. Per semplicità si considerano tutti gli elementi aventi tasso di guasto identico e pari a λ. Le configurazioni rappresentate sono le seguenti, con riportate le funzioni di affidabilità ed il MTTF:

- (**a**): sistema composto da un singolo elemento ($R_s(t) = e^{-\lambda t}$; $MTTF_s = \frac{1}{\lambda}$),
- (**b**): sistema costituito da una configurazione 1-out-of-2, che corrisponde ad un sistema composto da due elementi disposti in parallelo ($R_s(t) = 2e^{-\lambda t} - e^{-2\lambda t}$; $MTTF_s = \frac{3}{2\lambda}$),
- (**c**): sistema costituito da una configurazione 1-out-of-3, che corrisponde ad un sistema di tre elementi disposti in parallelo ($R_s(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$; $MTTF_s = \frac{11}{6\lambda}$),
- (**d**): sistema costituito da una configurazione 2-out-of-3 ($R_s(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$; $MTTF_s = \frac{5}{6\lambda}$).

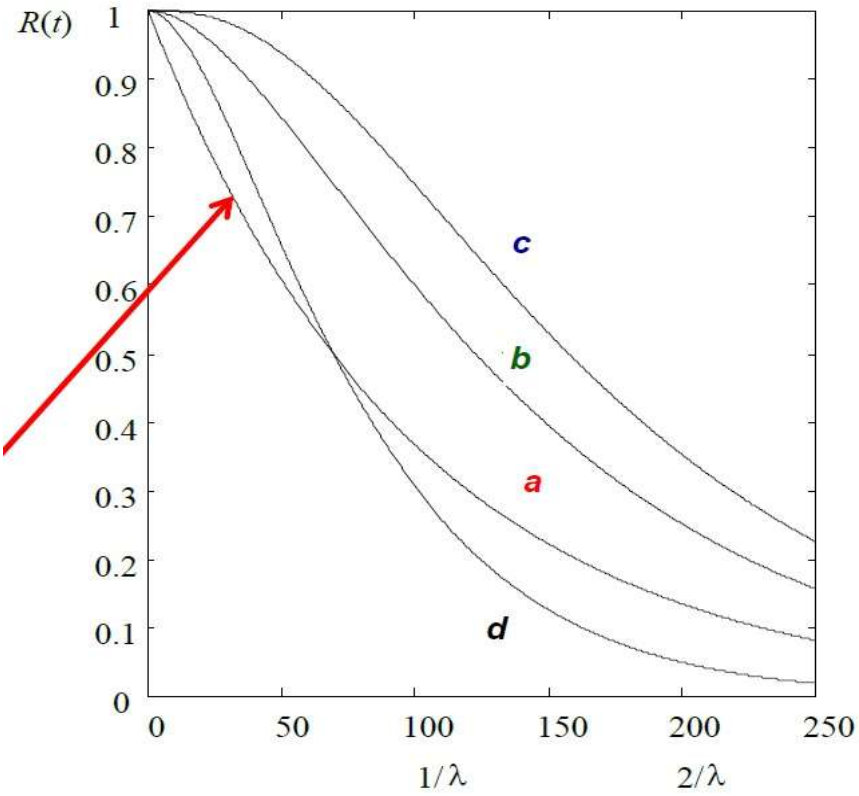


Figura 1.13: confronto tra diverse configurazioni k-out-of-n.

Si può notare dal grafico in Figura 1.13 che le configurazioni in parallelo hanno le migliori performance di affidabilità (ovviamente con tre elementi in parallelo i risultati sono migliori rispetto che con due). La configurazione 2-out-of-3 inizialmente ha un'affidabilità migliore rispetto all'elemento singolo, come mostrato dalla freccia rossa in figura, mentre nel lungo periodo ed a stazionario ha una performance inferiore rispetto al singolo elemento, anche in termini di MTTF.

Esempio di configurazione **mista**: nel seguente esempio viene riportata una configurazione più complessa, formata sempre da interconnessioni in serie ed in parallelo tra gli elementi del sistema. I tassi di guasto degli elementi del sistema sono considerati tutti costanti. Ogni elemento E_i del sistema ha un proprio tasso di guasto λ_i. La Figura 1.14 fornisce un esempio di configurazione complessa che può essere risolta mediante la suddivisione del sistema in sottosistemi formati da elementi o altri sottosistemi interconnessi in serie o in parallelo, che produce un RBD semplificato:

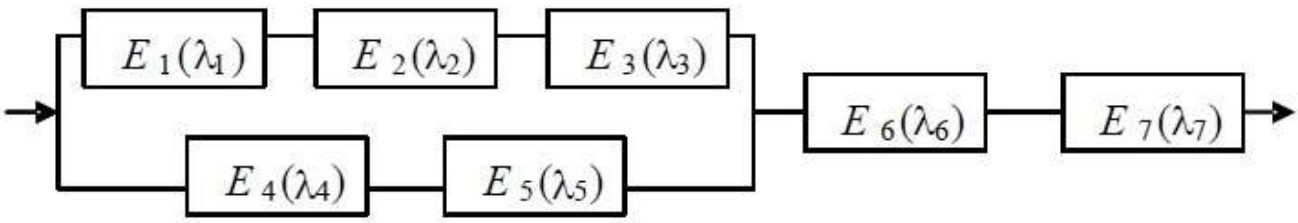


Figura 1.14: RBD, esempio di configurazione mista.

Nella procedura risolutiva si considerano inizialmente i tre seguenti sottosistemi:

- Sottosistema S_1: composto dagli elementi E_1, E_2 ed E_3 in serie.
- Sottosistema S_2: composto dagli elementi E_4ed E_5 in serie.
- Sottosistema S_3: composto dagli elementi E_6 ed E_7 in serie.

Il diagramma a blocchi risultante da questa semplificazione è il seguente, rappresentato dalla Figura 1.15 :

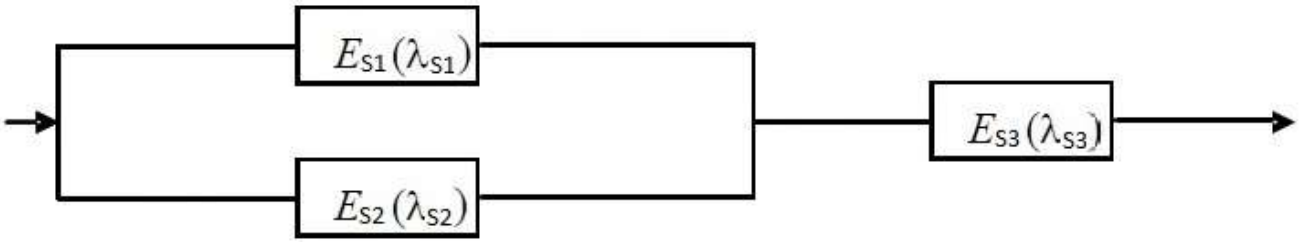


Figura 1.15: RBD, configurazione mista, prima semplificazione.

Si procede all'analisi dell'affidabilità di questi tre sottosistemi. Ogni sottosistema è composto esclusivamente da elementi in serie:

$$R_{S_1}(t) = e^{-(\lambda_1+\lambda_2+\lambda_3)t} \tag{1.89}$$

$$R_{S_2}(t) = e^{-(\lambda_4+\lambda_5)t} \tag{1.90}$$

$$R_{S_3}(t) = e^{-(\lambda_6+\lambda_7)t} \tag{1.91}$$

Si considera in seguito un altro sottosistema:

- Sottosistema S_4: composto dai sottosistemi S_1 ed S_2 in parallelo.

Il diagramma a blocchi risultante da questa semplificazione è il seguente, rappresentato dalla seguente Figura 1.16:

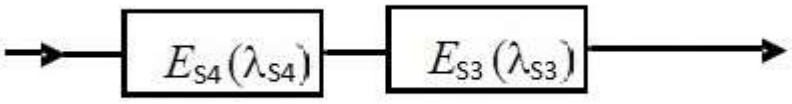


Figura 1.16: RBD, configurazione mista, seconda semplificazione.

Si procede all'analisi dell'affidabilità di quest'altro sottosistema, utilizzando la configurazione in parallelo e le funzioni di affidabilità dei due sottosistemi in questione, ricavate nelle equazioni 1.89 e 1.90:

$$R_{S_4}(t) = e^{-(\lambda_1+\lambda_2+\lambda_3)t} + e^{-(\lambda_4+\lambda_5)t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5)t} \tag{1.92}$$

L'RBD è stato semplificato in una configurazione in serie, che viene risolta considerando le funzioni di affidabilità dei due sottosistemi in questione, ricavate nelle equazioni 1.91 e 1.92:

$$R(t) = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7)t} + e^{-(\lambda_4+\lambda_5+\lambda_6+\lambda_7)t} - e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7)t} \quad (1.93)$$

Il MTTF è calcolato come segue, con l'ausilio dell'equazione 1.77:

$$MTTF = \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7} + \frac{1}{\lambda_4+\lambda_5+\lambda_6+\lambda_7} - \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7} \quad (1.94)$$

Configurazione con ridondanza **standby:** gli elementi ridondanti del sistema non sono soggetti ad alcun carico fino a che un elemento in operazione subisce un guasto. Il tasso di guasto dell'elemento ridondante, quando non è in operazione, è assunto essere pari a zero. Viene introdotto un nuovo elemento, lo switch S, che serve a rilevare il guasto dell'elemento operante e mettere in funzione l'elemento di riserva. In questo caso lo switch è considerato ideale e la sua affidabilità è ritenuta costante e pari ad 1 in ogni istante.

Nella Figura 1.17 è rappresentato un RBD comprendente due sistemi in ridondanza di tipo standby: l'elemento B è di riserva, entra in funzione a seguito del guasto dell'elemento A tramite l'azione dello switch:

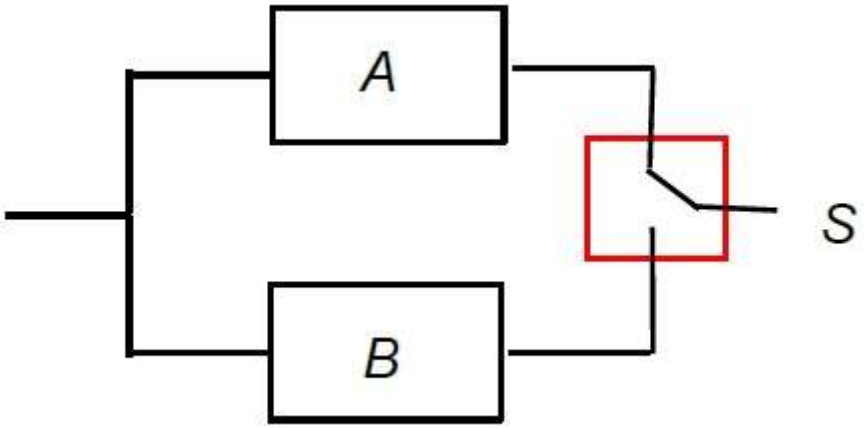


Figura 1.17: RBD, sistema con ridondanza di tipo standby ed elemento di switch S.

Il sistema, considerando un generico tempo t, può essere operativo fino a quell'istante in due casi indipendenti, ognuno dei quali darà pertanto un contributo nel computo dell'affidabilità. I due casi sono i seguenti:

- Caso α: l'elemento A funziona nel periodo di tempo $[0, t]$, in questo caso l'elemento inizialmente operativo non subisce guasti durante tutto il tempo di missione.
- Caso β: l'elemento A subisce un guasto ad un tempo $r < t$ ed a seguito di questo evento entra in operazione l'elemento di riserva B, che funziona nel periodo di tempo $[r, t]$.

I due casi sono rappresentati, per una migliore comprensione, nella Figura 1.18:

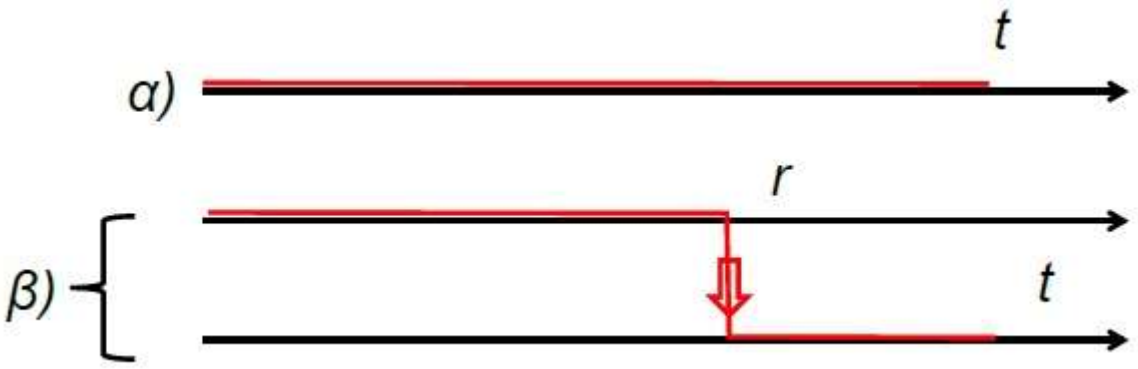


Figura 1.18: rappresentazioni dei casi di affidabilità per sistema con ridondanza di tipo standby.

La probabilità dell'evento α è data semplicemente dall'affidabilità dell'elemento A:

$$Pr(\alpha) = R(t) = R_A(t) \tag{1.95}$$

La probabilità dell'evento β è data dalla integrazione della probabilità di guasto dell'elemento A moltiplicata per l'affidabilità dell'elemento B nel periodo del tempo di missione in cui deve funzionare:

$$Pr(\beta) = \int_0^t f_A(r) \cdot R_B(t-r)dr \tag{1.96}$$

L'affidabilità del sistema, essendo gli eventi α e β disgiunti ed indipendenti, è data semplicemente dalla somma delle due probabilità ricavate nelle equazioni 1.95 e 1.96:

$$R(t) = R_A(t) + \int_0^t f_A(r) \cdot R_B(t-r)dr \tag{1.97}$$

Sviluppando ed integrando l'equazione 1.97 si ottiene la seguente espressione dell'affidabilità, come funzione esclusivamente dei tassi di guasto dei due elementi e del tempo:

$$R(t) = \frac{\lambda_B}{\lambda_B - \lambda_A} e^{-\lambda_A t} + \frac{\lambda_A}{\lambda_A - \lambda_B} e^{-\lambda_B t} \tag{1.98}$$

Il calcolo del MTTF avviene come illustrato in seguito:

$$MTTF = \int_0^{+\infty} \frac{\lambda_B}{\lambda_B - \lambda_A} e^{-\lambda_A t} + \frac{\lambda_A}{\lambda_A - \lambda_B} e^{-\lambda_B t}\, dt \tag{1.99}$$

$$MTTF = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} = MTTF_A + MTTF_B \tag{1.100}$$

Configurazione con ridondanza **warm**: gli elementi ridondanti del sistema sono soggetti ad un carico minore fino a che un elemento in operazione subisce un guasto. Il tasso di guasto dell'elemento ridondante, quando opera con un carico inferiore assieme all'altro elemento, è assunto essere

minore rispetto al tasso di guasto dello stesso elemento quando è in operazione da solo, con l'altro elemento quindi guasto. È sempre presente lo switch S, che serve a rilevare il guasto dell'elemento operante e ridistribuire il carico all'elemento rimasto funzionante. Lo switch è considerato ideale e la sua affidabilità è ritenuta costante e pari ad 1 in ogni istante.

L'RBD relativo alla ridondanza di tipo warm, riferita ad un sistema con due elementi, è identica a quella utilizzata per la ridondanza di tipo standby, rappresentata in Figura 1.17.

Il sistema, considerando un generico tempo t, può essere operativo fino a quell'istante in due casi indipendenti, ognuno dei quali darà pertanto un contributo nel computo dell'affidabilità. I due casi sono i seguenti:

- Caso α: l'elemento A funziona nel periodo di tempo $[0, t]$, in questo caso è presente un elemento che non subisce guasti durante tutto il tempo di missione e, pertanto, lo switch non ridistribuisce il carico.
- Caso β: l'elemento A subisce un guasto ad un tempo $r < t$ ed a seguito di questo evento entra in operazione a pieno carico l'elemento B, che ha funzionato con un carico ridotto nel periodo di tempo $[0, r]$ e che dovrà operare a pieno carico fino al termine del tempo di missione, ovvero nell'intervallo $[r, t]$.

I due casi sono rappresentati, per una migliore comprensione, nella Figura 1.19:

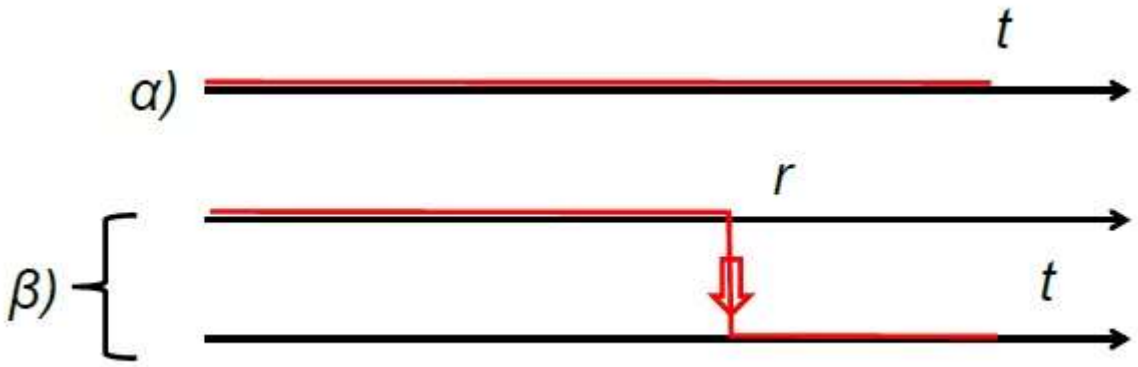


Figura 1.19: rappresentazioni dei casi di affidabilità per sistema con ridondanza di tipo warm.

La probabilità dell'evento α è data semplicemente dall'affidabilità dell'elemento A:

$$Pr(\alpha) = R(t) = R_A(t) = e^{-\lambda_A t} \tag{1.101}$$

La probabilità dell'evento β è data dalla integrazione della probabilità di guasto dell'elemento A moltiplicata per l'affidabilità dell'elemento B nei due periodi di tempo. L'affidabilità dell'elemento B cambia in quanto cambia la sua missione al verificarsi dell'evento di guasto A: ciò comporta un diverso tasso di guasto nelle due finestre temporali individuate. Nel primo periodo di funzionamento dell'elemento B il tasso di guasto viene definito λ'_B, mentre a seguito del guasto dell'elemento A il suo tasso di guasto viene definito λ_B.

Alla luce di quanto descritto in precedenza il tasso di guasto a pieno carico sarà maggiore del tasso di guasto in condizioni di ridondanza warm: $\lambda'_B < \lambda_B$. La probabilità dell'evento β è espressa dalla seguente equazione:

$$Pr(\beta) = \int_0^t f_A(r) \cdot R_B(r) \cdot R_B(t|r)dr = \lambda_A \int_0^t e^{-\lambda_A t} \cdot e^{-\lambda'_B t} \cdot e^{-\lambda_B (t-r)} dr \quad (1.102)$$

L'affidabilità del sistema, essendo gli eventi α e β disgiunti ed indipendenti, è data semplicemente dalla somma delle due probabilità ricavate nelle equazioni 1.101 e 1.102:

$$R(t) = e^{-\lambda_A t} + \lambda_A \int_0^t e^{-\lambda_A t} \cdot e^{-\lambda'_B t} \cdot e^{-\lambda_B (t-r)} dr \quad (1.103)$$

Sviluppando ed integrando quanto riportato nell'equazione 1.103 si ottiene la seguente espressione dell'affidabilità:

$$R(t) = e^{-\lambda_A t} + \frac{\lambda_A}{(\lambda_A + \lambda'_B) - \lambda_B} \cdot [e^{-\lambda_B t} - e^{-(\lambda_A + \lambda'_B)t}] \quad (1.104)$$

Calcolo del MTTF:

$$MTTF = \frac{1}{\lambda_A} + \frac{\lambda_A}{(\lambda_A + \lambda'_B)} \cdot \frac{1}{\lambda_B} \quad (1.105)$$

Si può notare che, se si considera una configurazione con ridondanza standby come una configurazione con ridondanza warm avente il tasso di guasto del dispositivo pari a zero in condizioni di funzionamento a carico ridotto, si possono ricavare le equazioni della ridondanza standby partendo da quelle relative alla ridondanza warm, applicando la condizione $\lambda'_B = 0$.

1.6 Modello di Markov

Il modello di Markov[5] è un modello stocastico utilizzato per modellare sistemi che cambiano stato, è basato su una rappresentazione grafica delle caratteristiche del sistema oggetto di analisi quali l'affidabilità ed anche altre, che verranno trattate in seguito, quali manutenibilità, disponibilità e incolumità (safety). Il modello consente di osservare gli effetti, sull'intero sistema, dell'inaffidabilità dei componenti elementari.

Con la stessa ipotesi utilizzata per lo studio di sistemi tramite gli RBD, un dispositivo, sia esso un elemento di un sistema oppure il sistema stesso, può assumere solamente due condizioni mutualmente esclusive: funzionamento corretto oppure guasto.

Il modello definisce gli stati del sistema come combinazione degli stati di funzionamento e di guasto dei suoi singoli elementi. Vista la logica binaria utilizzata, con un numero N di elementi, gli stati del sistema saranno un numero pari a 2^N. Il modello definisce come stati del sistema le 2^N combinazioni degli stati dei singoli elementi, che permettono al sistema di funzionare oppure no.

[5] Il modello prende il nome da Andrej Andreevič Markov, matematico e statistico russo.

I cambiamenti nello stato del sistema, dovuti a cambiamenti di stato del singolo elemento, sono chiamati transizioni e la loro cronologia descrive l'evoluzione temporale del sistema. La procedura del modello richiede il calcolo della probabilità di trovare il sistema in ogni suo possibile stato.

Ipotesi del modello:

- Il processo deve essere stazionario: la probabilità di transizione tra due stati deve rimanere la stessa durante l'intervallo di tempo considerato.
- I tassi di transizione tra due stati devono rimanere costanti durante il tempo di osservazione, di conseguenza la distribuzione di probabilità deve essere esponenziale.
- Il processo deve essere senza memoria: il comportamento futuro del sistema, che è casuale, dipende solamente dal suo stato attuale e non dagli stati nel quale il sistema è stato precedentemente.

Caratteristiche degli stati:

- Gruppo ergodico: un gruppo di stati con la seguente proprietà: una volta che il sistema è entrato in uno degli stati facenti parte del gruppo, non ne è più capace di uscirne, ovvero di trovarsi in futuro in uno stato non facente parte del gruppo ergodico.
- Gruppo di transizione: un gruppo di stati con la seguente proprietà: una volta che il sistema si trova in uno stato facente parte del gruppo ed ha una transizione verso uno stato che non si trova nel gruppo di transizione, il sistema non potrà più ritrovarsi nuovamente in uno stato del gruppo di transizione.
- Stato assorbente: è uno stato con la seguente proprietà: una volta che il sistema ha raggiunto questo stato non potrà più effettuare una transizione verso un altro stato.

Il processo di Markov, nel tempo continuo, rappresenta un sistema con un numero finito di stati. Il sistema, nell'istante generico di tempo t, può fare una transizione, nell'intervallo $[t, t+\delta t]$,da un generico stato i ad uno stato finale j. La transizione è caratterizzata da una probabilità $\pi_{ij}(t)$, che dipende da un generico valore $\lambda_{ij}(t)$, definito funzione di rischio transizione. La probabilità di transizione dipende dal tempo, come riportato nella seguente equazione:

$$\pi_{ij}(t) = \lambda_{ij}(t)\,\delta t \tag{1.106}$$

Tutte le probabilità di transizione $\pi_{ij}(t)$ possono essere raggruppate in una matrice P, con le seguenti caratteristiche:

- L'indice di riga (i) rappresenta lo stato iniziale della transizione e l'indice di colonna (j) rappresenta lo stato finale della transizione.
- La matrice P è una matrice quadrata.
- Le righe sono stocastiche: la somma degli elementi di ogni riga rappresenta la probabilità di rimanere in un certo stato o di uscirne entrando in un altro stato. La somma delle probabilità di ogni riga è uguale ad 1.

Se viene indicata con $P_i(t)$ la probabilità di osservare il sistema nello stato i ad un tempo t, la probabilità di osservare lo stesso stato ad un tempo $(t+\delta t)$ è data dalla somma delle probabilità che competono per due eventi mutualmente esclusivi:

- Il sistema era nello stato j all'istante t ed è passato allo stato i durante δt, tramite una transizione.
- Il sistema era nello stato i all'istante t e non è passato in nessun altro stato durante δt.

La probabilità di trovare il sistema nello stato i nell'istante di tempo $(t + \delta t)$, alla luce di quanto descritto, è data dalla seguente equazione:

$$P_i(t + \delta t) = \sum_{i \neq j} \pi_{ij}(t)\delta t \, P_j(t) + [1 - \sum_{i \neq j} \pi_{ij}(t)\delta t]P_i(t)] \tag{1.107}$$

Viene ora trattato il caso di sistema costituito semplicemente da un **dispositivo non riparabile**, con tasso di guasto costante. Il numero di stati che può assumere il sistema è pari a $2^1 = 2$. I due stati del sistema differiscono per lo stato del dispositivo, che può essere operativo o di guasto.

Il dispositivo può assumere solamente due stati:

- Stato operativo, indicato come S_0.
- Stato di guasto, indicato come S_1.

Possono essere definite le seguenti quantità:

- $P_0(t)$, probabilità che il dispositivo si trovi nello stato S_0 al tempo t,
- $P_1(t)$, probabilità che il dispositivo si trovi nello stato S_1 al tempo t,
- Tasso di guasto costante, $\lambda(t) = \lambda$,
- $\lambda\delta t$, probabilità di transizione dallo stato S_0 allo stato S_1.

Viene riportato nella seguente Figura 1.20 il diagramma di transizione degli stati relativo:

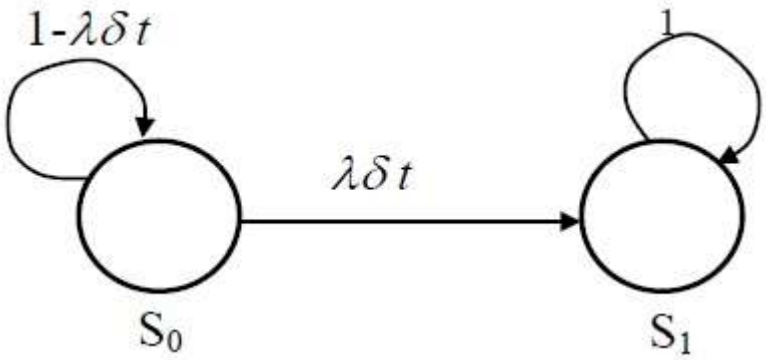


Figura 1.20: diagramma di transizione degli stati di un dispositivo non riparabile.

La probabilità che il sistema si trovi nello stato S_0 all'istante $(t + \delta t)$ è data dalla somma di due contributi. Il primo contributo è dato dalla probabilità che il sistema si trovi nello stato S_0 al tempo t moltiplicata per la probabilità che non ci siano transizioni di stato nel periodo δt verso l'altro stato, quindi per $(1 - \lambda\delta t)$. Il secondo contributo è dato dalla probabilità che il sistema si trovi nello stato S_1 al tempo t moltiplicata per la probabilità che ci sia una transizione di stato nel periodo δt verso lo stato S_0. Il secondo contributo è pari a zero perché è zero anche la probabilità di transizione descritta: lo stato S_1 è uno stato assorbente.

La probabilità che il sistema si trovi nello stato S_1 all'istante $(t + \delta t)$ è data dalla somma di due contributi. Il primo contributo è dato dalla probabilità che il sistema si trovi nello stato S_0 al tempo t moltiplicata per la probabilità che ci sia una transizione di stato nel periodo δt verso S_1, quindi per $(\lambda \delta t)$. Il secondo contributo è dato dalla probabilità che il sistema si trovi nello stato S_1 al tempo t moltiplicata per la probabilità che il sistema resti nello stesso stato dopo il periodo δt, ovvero, dato che S_1 è uno stato assorbente, per 1.

Il diagramma di transizione degli stati descrive correttamente il comportamento di un dispositivo non riparabile: dopo un guasto non può tornare allo stato operativo.

Il seguente sistema di equazioni riporta quanto appena descritto:

$$\begin{cases} P_0(t + \delta t) = P_0(t)(1 - \lambda \delta t) + P_1(t) \cdot 0 \\ P_1(t + \delta t) = P_0(t)\lambda \delta t + P_1(t) \cdot 1 \end{cases} \quad (1.108)$$

Semplificando il sistema 1.108 e dividendo ogni membro delle equazioni per δt si ottiene:

$$\begin{cases} \dfrac{P_0(t + \delta t) - P_0(t)}{\delta t} = -\lambda P_0(t) \\ \dfrac{P_1(t + \delta t) - P_1(t)}{\delta t} = \lambda P_0(t) \end{cases} \quad (1.109)$$

Considerando il limite per $\delta t \to 0$ delle equazioni nel sistema 1.109 si ottiene il seguente sistema di equazioni differenziali:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda P_0(t) \\ \dfrac{dP_1(t)}{dt} = \lambda P_0(t) \end{cases} \quad (1.110)$$

Le condizioni iniziali assegnate sono le seguenti: il dispositivo si trova inizialmente nello stato operativo, S_0:

$$\begin{cases} P_0(0) = 1 \\ P_1(0) = 0 \end{cases} \quad (1.111)$$

Integrando la prima equazione riportata nel sistema 1.110 si ottiene:

$$\int \frac{dP_0(t)}{P_0(t)} = -\int \lambda \, dt \quad (1.112)$$

$$\log P_0(t) = -\lambda \cdot t + C \quad (1.113)$$

Con la condizione iniziale $P_0(0) = 1$, riportata nel sistema 1.111, si semplifica l'equazione 1.113 con l'eliminazione della costante C (C =0). Il risultato ottenuto è l'affidabilità del sistema, essendo lo stato S_0 l'unico stato operativo del dispositivo:

$$P_0(t) = R(t) = e^{-\lambda \cdot t} \tag{1.114}$$

In ogni istante di tempo la somma delle probabilità di ogni stato è pari ad 1:

$$P_0(t) + P_1(t) = 1 \tag{1.115}$$

Dalle equazioni 1.114 e 1.115 si può ricavare l'espressione di $P_1(t)$. Il risultato ottenuto è l'inaffidabilità del sistema, essendo lo stato S_1 l'unico stato di guasto del dispositivo:

$$P_1(t) = 1 - P_0(t) = 1 - R(t) = F(t) = 1 - e^{-\lambda \cdot t} \tag{1.116}$$

1.7 Disponibilità e dispositivi riparabili

Il già menzionato vocabolario internazionale dell'elettrotecnica (IEV), nel documento IEC 60050, definisce la disponibilità come l'abilità di un dispositivo di essere in uno stato nel quale è in grado di eseguire la funzione richiesta sotto determinate condizioni, in un dato istante di tempo oppure durante un dato intervallo di tempo, assumendo che siano fornite le risorse esterne.

Una definizione operativa di disponibilità potrebbe essere la seguente: è la percentuale di tempo, rispetto al tempo totale, dove è richiesto al dispositivo di essere operativo, ovvero la frazione di tempo nel quale al dispositivo è richiesto di funzionare, di essere disponibile.

La disponibilità è un concetto tipico dei dispositivi riparabili, dispositivi che vengono descritti dalla definizione fornita dalla normativa IEC 60050. Vengono riportate inoltre le definizioni di disponibilità istantanea e di dispositivo non riparabile, sempre fornite dalla normativa IEC 60050:

- Disponibilità istantanea: probabilità, per un dispositivo, di essere in uno stato operativo, ovvero la probabilità che il dispositivo sia in grado di eseguire la sua funzione richiesta, in un dato istante di tempo. È rappresentata generalmente con $A(t)$ *(*dall'inglese Availability). È funzione del tempo.
- Dispositivo riparabile: dispositivo che può, sotto date condizioni ed a seguito di un guasto, ritornare in uno stato nel quale possa eseguire la sua funzione richiesta.
- Dispositivo non riparabile: dispositivo che non può, sotto date condizioni ed a seguito di un guasto, ritornare in uno stato nel quale possa eseguire la sua funzione richiesta.

La normativa specifica che, per definire un dispositivo riparabile o meno, le date condizioni possono includere considerazioni tecniche, economiche o di altro tipo. Specifica inoltre che un dispositivo riparabile sotto date condizioni può non essere riparabile sotto altre condizioni, e viceversa.

Riassumendo quando detto precedentemente, un dispositivo riparabile è operativo ad eccezione dei periodi di riparazione che hanno lo scopo di riportarlo al suo stato di funzionamento originale e che avvengono a seguito di un guasto. Il ciclo di vita operativo di un dispositivo riparabile è descritto quindi da una sequenza alternata di intervalli di tempo di funzionamento e di intervalli di tempo di guasto. La seguente Figura 1.21 rappresenta un esempio di ciclo operativo di un dispositivo riparabile:

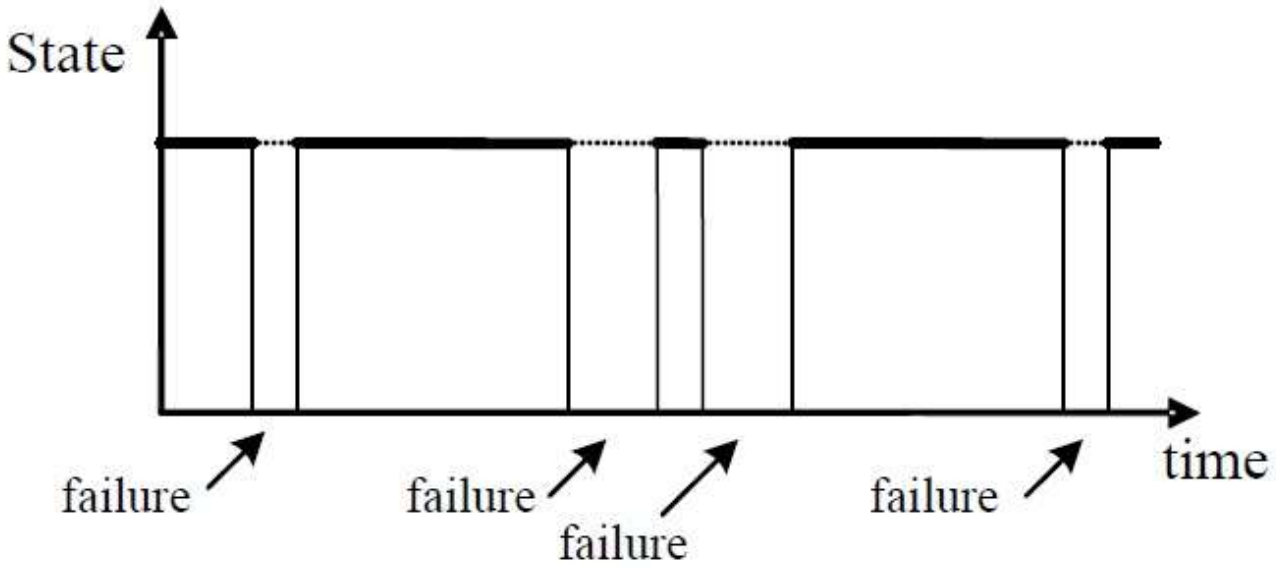


Figura 1.21: andamento nel tempo dello stato di un dispositivo riparabile.

L'evento di riparazione è descritto meglio grazie all'introduzione del concetto di manutenibilità. La manutenibilità è una proprietà dei dispositivi riparabili ed è definita come la facilità con la quale il dispositivo può essere riparato una volta che si è manifestato un guasto. Operativamente, la manutenibilità (in inglese Maintainability), indicata come $M(t)$, è la probabilità che un dispositivo non funzionante venga ripristinato al suo corretto funzionamento entro il tempo t.

Per iniziare a comprendere il concetto di manutenibilità ed il rapporto che ha con la disponibilità si può analizzare un valore limite: $M(0) = 1$. In questo caso il dispositivo in questione ha una probabilità pari a 1 di essere riparato in un tempo di zero secondi/ore: la riparazione non richiede tempo, è istantanea (riparazione ideale). Se la riparazione è istantanea il dispositivo in questione non trascorrerà intervalli di tempo nello stato di guasto, avrà un tempo alla riparazione nullo e si troverà sempre nello stato operativo e pertanto la probabilità del dispositivo di essere funzionante in un generico istante (e quindi la sua disponibilità) sarà sempre pari a 1.

Il parametro che permette di valutare il tempo medio richiesto ad un dispositivo in stato di guasto per ritornare al suo stato di funzionamento originale è il MTTR (dall'inglese Mean Time To Repair), ovvero il tempo medio alla riparazione, che nell'esempio precedente di riparazione ideale era stato considerato nullo.

Nella seguente Figura 1.22 è rappresentato, similmente alla Figura 1.21, lo stato di un dispositivo riparabile nel tempo: sono sempre presenti intervalli di tempo alternati di funzionamento e di riparazione e vengono introdotti in aggiunta alla figura precedente i generici tempi di funzionamento t_{fi} ed i generici tempi di riparazione t_{ri}:

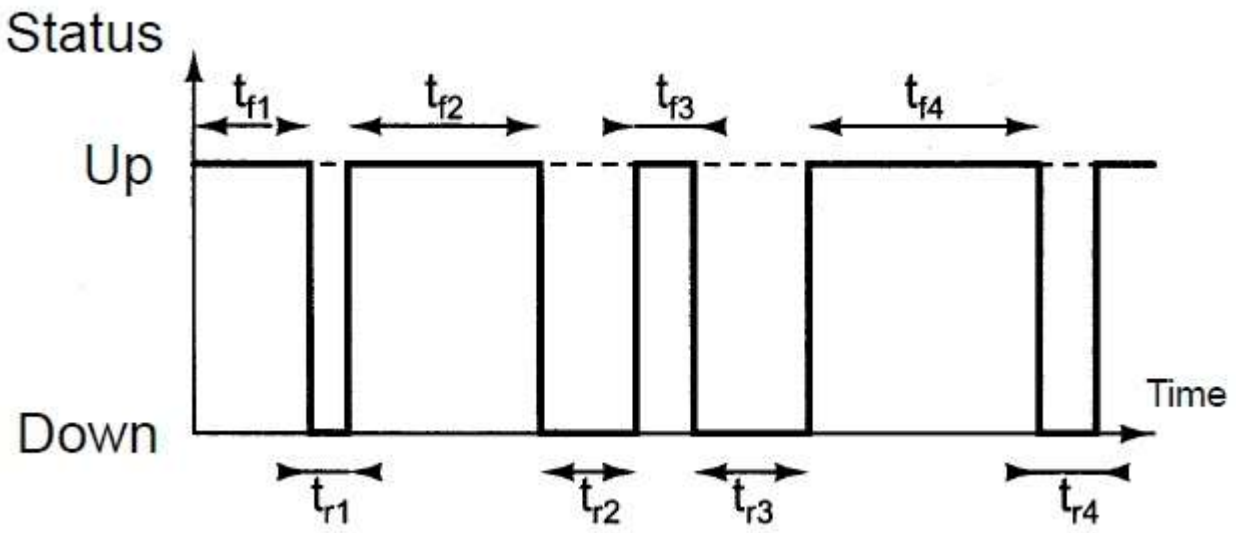


Figura 1.22: tempi di funzionamento e di riparazione di un dispositivo riparabile.

Vengono in seguito indicate le equazioni rappresentanti tre parametri importanti nella valutazione della disponibilità: il MTTF, il MTTR ed il tempo medio tra guasti, denominato MTBF (dall'inglese Mean Time Between Failure).

Il MTTF è la media di n tempi di funzionamento, con $n \to \infty$:

$$MTTF = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} t_{fi} \tag{1.117}$$

Il MTTR è la media di n tempi di riparazione, con $n \to \infty$:

$$MTTR = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} t_{ri} \tag{1.118}$$

Il MTBF è il tempo medio tra guasti: si può notare che tra un guasto ed il successivo è presente un periodo di riparazione seguito da un periodo di funzionamento, pertanto il MTBF sarà la media di n tempi di riparazione sommati al successivo tempo di funzionamento, con $n \to \infty$. Agendo sulla sommatoria si può ottenere il seguente rapporto, utilizzando le equazioni 1.117 e 1.118:

$$MTBF = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} (t_{fi} + t_{ri}) = MTTF + MTTR \tag{1.119}$$

Il MTTR può essere trattato come la somma di altri due periodi di tempo medi: il tempo medio di riparazione MRT (dall'inglese Mean Repair Time), ed il ritardo logistico medio MLD (dall'inglese Mean Logistic Delay), che vengono descritti in seguito:

- MRT: tempo medio di riparazione, indica la somma degli intervalli di tempo richiesti per la localizzazione, la correzione ed il test del dispositivo. È riferito al caso di manutenzione correttiva per dispositivi riparabili. È il valore medio del tempo di riparazione.

- MLD: ritardo logistico medio, è utilizzato per indicare il tempo che trascorre tra il guasto e l'inizio della riparazione per ragioni logistiche. È il valore medio del ritardo logistico.
- MTTR: tempo medio alla riparazione, come detto si può definire come $MRT + MLD$.

La disponibilità è definita intrinseca quando non sono presenti errori umani durante la riparazione e non è presente nessun ritardo dovuto alla logistica. Il tempo medio alla riparazione sarà uguale al tempo medio di riparazione ($MTTF = MRT$, con $MLD = 0$).

Per completezza viene riportata la definizione di disponibilità intrinseca fornita dal documento IEC 60050: è la disponibilità definita in fase di design, sotto condizioni ideali di operazione e manutenzione. Sono esclusi i ritardi associati alla manutenzione, come ritardi logistici ed amministrativi.

È possibile trovare delle analogie tra le funzioni di manutenibilità e di affidabilità. Sono indicate nella seguente Tabella 1.1:

Funzioni di manutenibilità	Analoghe funzioni di affidabilità
$g(t)$: Densità di probabilità di riparazione normale	$f(t)$: Distribuzione della probabilità di guasto
$M(t)$: Probabilità di riparazione (manutenibilità)	$F(t)$: Inaffidabilità
$N(t)$: Probabilità di non riparazione	$R(t)$: Affidabilità
$\mu(t)$: Tasso di riparazione (istantaneo)	$\lambda(t)$: Tasso di guasto (istantaneo)

Tabella 1.1: comparazione tra manutenibilità ed affidabilità.

La definizione di tempo medio di riparazione è data da:

$$MTTR = \sum_i t_i \cdot g(t_i) \cdot \Delta t_i \tag{1.120}$$

Con le seguenti ipotesi ed osservazioni:

- La probabilità che la riparazione termini entro l'intervallo $[t,\ t + \Delta t]$ è data da: $g(t) \cdot \Delta t$.
- $t = 0$ (il guasto avviene a tempo $t = 0$).
- La probabilità che la riparazione termini entro l'intervallo $[0,\ t]$ è data da: $M(t)$.
- La probabilità che la riparazione termini nell'intervallo$[t,\ t + \Delta t]$ non essendo stata completata al tempo $t = 0$ è data da: $\mu(t) \cdot \Delta t$.

Se il tasso di riparazione è costante, quindi se $\mu(t) = \mu$, il rapporto tra MTTR e tasso di riparazione è analogo a quello esistente tra MTTF e tasso di guasto, riportato in precedenza nell'equazione 1.56, che viene in seguito riportata nuovamente:

$$MTTF = \int_0^\infty e^{-\lambda t} dt = \frac{1}{\lambda} \tag{1.56}$$

Ne consegue la seguente equazione 1.129:

$$MTTR = \frac{1}{\mu} \tag{1.121}$$

Per ottenere un'espressione matematica della disponibilità di un dispositivo riparabile con tassi di guasto e di riparazione costanti si può ricorrere, come già fatto per il caso dell'affidabilità per un dispositivo non riparabile, al modello di Markov.

Il sistema è quindi costituito da un **dispositivo riparabile**, con tasso di guasto e tasso di riparazione entrambi costanti. Il numero di stati che può assumere il sistema è sempre pari a $2^1 = 2$, lo stesso numero di stati che può assumere il dispositivo riparabile: stato operativo o di guasto.

Il modello di Markov utilizzato differisce dal modello relativo ad un dispositivo non riparabile, rappresentato in Figura 1.20, dalla transizione dovuta alla riparazione, che riporta il sistema dallo stato di guasto S_1 allo stato operativo S_0.

Viene riportato nella Figura 1.23 il diagramma di transizione degli stati relativo ad un dispositivo riparabile:

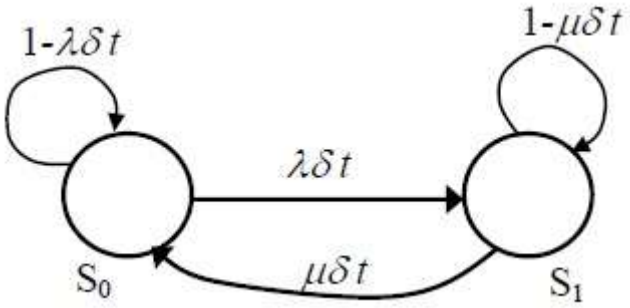


Figura 1.23: diagramma di transizione degli stati di un dispositivo riparabile.

Le condizioni iniziali assegnate sono uguali a quelle relative al dispositivo non riparabile: il dispositivo si trova inizialmente nello stato operativo, S_0. Viene riportata l'equazione 1.111:

$$\begin{cases} P_0(0) = 1 \\ P_1(0) = 0 \end{cases} \tag{1.111}$$

Il modello differisce da quello relativo al dispositivo non riparabile per le probabilità di transizione presenti quando il sistema si trova nello stato S_1: la probabilità di transizione verso lo stato S_0 era pari a zero nel modello non riparabile mentre ora, che è presente la riparazione nel modello, è pari a $\mu\delta t$; parallelamente la probabilità di transizione verso lo stesso stato, S_1, era pari ad 1 nel modello non riparabile mentre ora il sistema può abbandonare lo stato di guasto, che cessa pertanto di essere uno stato assorbente, con una probabilità di transizione pari a $(1 - \mu\delta t)$.

Il seguente sistema di equazioni riporta quanto appena descritto:

$$\begin{cases} P_0(t+\delta t) = P_0(t) \cdot (1 - \lambda\delta t) + P_1(t)\mu\delta t \\ P_1(t+\delta t) = P_0(t)\lambda\delta t + P_1(t) \cdot (1 - \mu\delta t) \end{cases} \tag{1.122}$$

Semplificando il sistema 1.122 e dividendo ogni membro delle equazioni per δt si ottiene:

$$\begin{cases} \dfrac{P_0(t+\delta t) - P_0(t)}{\delta t} = -\lambda P_0(t) + \mu P_1(t) \\ \dfrac{P_1(t+\delta t) - P_1(t)}{\delta t} = \lambda P_0(t) - \mu P_1(t) \end{cases} \tag{1.123}$$

Considerando il limite per $\delta t \to 0$ delle equazioni nel sistema 1.123 si ottiene il seguente sistema di equazioni differenziali:

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu P_1(t) \\ \dfrac{dP_1(t)}{dt} = \lambda P_0(t) - \mu P_1(t) \end{cases} \tag{1.124}$$

Le equazioni differenziali vengono risolte in questo caso utilizzando la trasformata di Laplace[6], trasformando le equazioni dalla variabile tempo alla variabile di Laplace (s).

Si ricorda che la trasformata di una derivata è pari alla funzione in termini di Laplace, moltiplicata per la variabile di Laplace (s), e con sottratto il valore della funzione nel tempo in $t = 0$.

Il sistema 1.124 viene trasformato e riportato nel seguente sistema 1.125:

$$\begin{cases} s \cdot P_0(s) - P_0(0) = -\lambda P_0(s) + \mu P_1(s) \\ s \cdot P_1(s) - P_1(0) = +\lambda P_0(s) - \mu P_1(s) \end{cases} \tag{1.125}$$

Sostituendo alle equazioni nel sistema 1.125 le condizioni iniziali riportate nel sistema 1.119 e sistemando gli altri termini si ottiene il seguente sistema:

$$\begin{cases} s \cdot P_0(s) + \lambda P_0(s) = 1 + \mu P_1(s) \\ s \cdot P_1(s) + \mu P_1(s) = \lambda P_0(s) \end{cases} \tag{1.126}$$

In ogni istante di tempo la somma delle probabilità di tutti gli stati del sistema (in questo caso $P_0(t)$ e $P_1(t)$) è pari ad 1. Viene aggiunta un'altra equazione che esprime quanto appena descritto:

$$P_0(t) + P_1(t) = 1 \tag{1.127}$$

Viene anch'essa trasformata con Laplace, utilizzando una delle trasformate fondamentali per il valore 1 a destra dell'uguale nell'equazione 1.127. L'equazione ottenuta è la seguente:

$$P_0(s) + P_1(s) = \frac{1}{s} \tag{1.128}$$

Dalla quale si ricava:

$$P_0(s) = \frac{1}{s} - P_1(s) \tag{1.129}$$

[6] La trasformata di Laplace è un operatore lineare che associa ad una funzione di variabile reale una funzione di variabile complessa. Il nome è dovuto a Pierre Simon Laplace, matematico, fisico e nobile francese.

Sostituendo l'espressione di $P_0(s)$ ottenuta nella 1.129 nella seconda equazione contenuta nel sistema 1.134 si ottiene un'espressione di $P_1(s)$ che non contiene $P_0(s)$:

$$s \cdot P_1(s) + \mu P_1(s) = \frac{\lambda}{s} - \lambda P_1(s) \tag{1.130}$$

Raccogliendo $P_1(s)$ nell'equazione 1.130 si ottiene:

$$[s + (\mu + \lambda)]P_1(s) = \frac{\lambda}{s} \tag{1.131}$$

Isolando $P_1(s)$ nella 1.131 si ottiene:

$$P_1(s) = \frac{\lambda}{s \cdot [s + (\mu + \lambda)]} \tag{1.132}$$

A questo punto è presente un'espressione di $P_1(s)$ che può essere antitrasformata con l'ausilio delle espansioni di Heaviside[7], al fine di ottenere $P_1(t)$: espressione della probabilità del sistema di trovarsi nello stato di guasto in funzione del tempo e quindi della sua inaffidabilità.

Per procedere con le espansioni di Heaviside è necessario individuare i poli di $P_1(s)$, ovvero quei termini della variabile di Laplace che rendono nullo il denominatore. I poli, indicati con P_i sono facilmente individuabili: $P_1 = 0$ e $P_2 = -(\mu + \lambda)$.

Si riscrive l'espressione di $P_1(s)$ introducendo le costanti C_i ed utilizzando i poli appena ricavati:

$$P_1(s) = \frac{C_1}{s - P_1} + \frac{C_2}{s - P_2} = \frac{C_1}{s} + \frac{C_2}{s + (\mu + \lambda)} \tag{1.133}$$

Confrontando le diverse espressioni di $P_1(s)$ contenute rispettivamente nelle equazioni 1.140 e 1.141 si ricava la seguente equazione 1.142:

$$\frac{\lambda}{s \cdot [s + (\mu + \lambda)]} = \frac{C_1}{s} + \frac{C_2}{s + (\mu + \lambda)} \tag{1.134}$$

Per ricavare la costante C_1 il primo passo è isolarla. Per fare ciò si moltiplicano tutti i membri dell'equazione 1.134 per il denominatore di C_1, in questo caso per s, e lo si semplifica:

$$\frac{\lambda}{s \cdot [s + (\mu + \lambda)]} \cdot s = \frac{C_1}{s} \cdot s + \frac{C_2}{s + (\mu + \lambda)} \cdot s \tag{1.135}$$

$$\frac{\lambda}{[s + (\mu + \lambda)]} = C_1 + \frac{C_2}{s + (\mu + \lambda)} \cdot s \tag{1.136}$$

[7] Le espansioni di Heaviside sono una tecnica per l'applicazione della trasformata di Laplace alla risoluzione di equazioni differenziali lineari. La tecnica è stata descritta da Oliver Heaviside, matematico, fisico e ingegnere britannico.

In seguito, si elimina il termine che contiene l'altra costante, C_2, ponendo la variabile di Laplace pari ad un valore che renda nullo il termine da eliminare. In questo caso si pone $s = 0$ e si ricava l'espressione di C_1:

$$C_1 = \frac{\lambda}{(\mu + \lambda)} \tag{1.137}$$

Si può ricavare C_2 in modo analogo, essendo i due poli distinti non c'è bisogno di derivare l'equazione, come richiesto nelle espansioni di Heaviside in caso di poli coincidenti.

Si moltiplica in questo caso ogni membro dell'equazione 1.134 per il denominatore di C_2, quindi per $[s + (\mu + \lambda)]$. In questo modo si isola la costante C_2 come mostrato dalle seguenti equazioni:

$$\frac{\lambda}{s \cdot [s + (\mu + \lambda)]} \cdot [s + (\mu + \lambda)] = \frac{C_1}{s} \cdot [s + (\mu + \lambda)] + \frac{C_2}{s + (\mu + \lambda)} \cdot [s + (\mu + \lambda)] \tag{1.138}$$

$$\frac{\lambda}{s} = \frac{C_1}{s} \cdot [s + (\mu + \lambda)] + C_2 \tag{1.139}$$

In seguito, si elimina il termine che contiene l'altra costante, C_1, ponendo la variabile di Laplace pari ad un valore che renda nullo il termine da eliminare. In questo caso si pone $[s = -(\mu + \lambda)]$ e si ricava l'espressione di C_2:

$$C_2 = -\frac{\lambda}{(\mu + \lambda)} \tag{1.140}$$

Inserendo le costanti ricavate nelle equazioni 1.137 e 1.140 nell'equazione 1.141 si ricava la seguente equazione 1.141:

$$P_1(s) = \frac{\lambda}{(\mu + \lambda) \cdot s} - \frac{\lambda}{(\mu + \lambda) \cdot [s + (\mu + \lambda)]} \tag{1.141}$$

Il passo successivo consiste nell'antitrasformare l'equazione 1.141, ovvero nel trovare la sua equivalente equazione espressa in funzione del tempo.

Per procedere si utilizza la trasformata inversa fondamentale, riportata in seguito in una forma generica:

$$\frac{a}{(s + b)^{n+1}} = \frac{a}{n!} \cdot t^n \cdot e^{-bt} \tag{1.142}$$

L'antitrasformata fondamentale riportata nell'equazione 1.142 viene applicata a ciascuno dei due termini dell'equazione 1.141. Il parametro n della 1.142 è pari a zero in entrambi i termini della 1.141: ne consegue un'importante semplificazione nel calcolo, come riportato nelle seguenti equazioni, che portano a ricavare $P_1(t)$:

$$P_1(t) = \frac{\lambda}{(\mu+\lambda)\cdot 0!}\cdot t^0 \cdot e^{-0\cdot t} - \frac{\lambda}{(\mu+\lambda)\cdot 0!}\cdot t^0 \cdot e^{-(\mu+\lambda)\cdot t} \tag{1.143}$$

$$P_1(t) = \frac{\lambda}{(\mu+\lambda)} - \frac{\lambda}{(\mu+\lambda)}\cdot e^{-(\mu+\lambda)\cdot t} \tag{1.144}$$

Viene ricavata dalla 1.127 una relazione tra le probabilità dei due stati, riportata nella seguente equazione 1.145:

$$P_0(t) = 1 - P_1(t) \tag{1.145}$$

Sostituendo nell'equazione 1.145 l'espressione di $P_1(t)$ riportata nell'equazione 1.144, raccogliendo a fattor comune l'espressione e semplificando, si può ottenere l'espressione di $P_0(t)$:

$$P_0(t) = \frac{\mu+\lambda-\lambda}{(\mu+\lambda)} + \frac{\lambda}{(\mu+\lambda)}\cdot e^{-(\mu+\lambda)\cdot t} = \frac{\mu}{(\mu+\lambda)} + \frac{\lambda}{(\mu+\lambda)}\cdot e^{-(\mu+\lambda)\cdot t} \tag{1.146}$$

La disponibilità è data dalla sommatoria delle probabilità di tutti gli stati operativi del sistema, in questo caso dalla probabilità del solo stato S_0, unico stato operativo del sistema. Si ricava da quanto detto e dall'equazione 1.146 la disponibilità del sistema:

$$A(t) = \frac{\mu}{(\mu+\lambda)} + \frac{\lambda}{(\mu+\lambda)}\cdot e^{-(\mu+\lambda)\cdot t} \tag{1.147}$$

Dall'equazione 1.147 si può ricavare l'affidabilità di un dispositivo non riparabile semplicemente escludendo nel computo della disponibilità le riparazioni. Matematicamente ciò si ottiene ponendo il tasso di riparazione pari a zero, $\mu = 0$:

$$R(t) = \frac{0}{(0+\lambda)} + \frac{\lambda}{(0+\lambda)}\cdot e^{-(0+\lambda)\cdot t} = e^{-\lambda t} \tag{1.148}$$

L'affidabilità permette di valutare l'accadimento del primo guasto del dispositivo mentre la disponibilità valuta la probabilità di trovare il dispositivo in uno stato di funzionamento al generico istante di tempo t.

In caso di dispositivi non riparabili la disponibilità coincide con l'affidabilità, perché dopo il primo guasto non è possibile la riparazione:

$$R(t) = A(t) \tag{1.149}$$

In caso di dispositivi riparabili l'affidabilità sarà sempre minore o uguale della disponibilità, perché dopo un guasto, il dispositivo viene riparato:

$$R(t) \leq A(t) \tag{1.150}$$

Portando a stazionario le equazioni 1.144 e 1.146, ovvero per $(t \to \infty)$, vengono semplificati in entrambe le equazioni i termini esponenziali negativi, che tenderanno a zero. Le equazioni ottenute sono riportate in seguito:

$$P_0(\infty) = \frac{\mu}{(\mu + \lambda)} \tag{1.151}$$

$$P_1(\infty) = \frac{\lambda}{(\mu + \lambda)} \tag{1.152}$$

Le probabilità dei due stati rappresentano quindi sempre la disponibilità (stato S_0) e l'indisponibilità (stato S_1) del sistema. Le equazioni valide in regime stazionario, la 1.151 e la 1.152, possono essere riscritte sostituendo rispettivamente al tasso di guasto il MTTF ed al tasso di riparazione il MTTR, come mostrato nelle seguenti equazioni 1.153 e 1.154:

$$P_0(\infty) = \frac{\mu}{(\mu + \lambda)} = \frac{\frac{1}{MTTR}}{\frac{1}{MTTR} + \frac{1}{MTTF}} = \frac{\frac{1}{MTTR}}{\frac{MTTF + MTTR}{MTTR \cdot MTTF}} = \frac{MTTF}{MTTF + MTTR} \tag{1.153}$$

$$P_1(\infty) = \frac{\lambda}{(\mu + \lambda)} = \frac{\frac{1}{MTTF}}{\frac{1}{MTTR} + \frac{1}{MTTF}} = \frac{\frac{1}{MTTF}}{\frac{MTTF + MTTR}{MTTR \cdot MTTF}} = \frac{MTTR}{MTTF + MTTR} \tag{1.154}$$

Le probabilità degli stati si avvicinano ad un set di probabilità note come probabilità di stato limite, che sono le probabilità in regime stazionario. Questi valori di probabilità sono indipendenti dal transitorio e quindi anche dallo stato nel quale il processo di Markov inizia (dalle condizioni iniziali). La probabilità di stato limite può essere ottenuta grazie alla matrice differenziale, che si ricava dal sistema di equazioni differenziali ottenuto in precedenza.

Viene riportato pertanto il sistema 1.132:

$$\begin{cases} \frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu P_1(t) \\ \frac{dP_1(t)}{dt} = \lambda P_0(t) - \mu P_1(t) \end{cases} \tag{1.132}$$

Il sistema 1.132 viene riportato sotto forma di matrici:

$$\begin{bmatrix} \frac{dP_0(t)}{dt} \\ \frac{dP_1(t)}{dt} \end{bmatrix} = [P_0(t) \quad P_1(t)] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \tag{1.155}$$

La condizione di stazionarietà è espressa dal valore nullo delle derivate delle probabilità degli stati, come espresso in seguito:

$$\lim_{t\to\infty}\frac{dP_0(t)}{dt}=\lim_{t\to\infty}\frac{dP_1(t)}{dt}=0 \tag{1.156}$$

Con la condizione di stazionarietà espressa nella 1.156 vengono riscritte le matrici contenute nell'equazione 1.155:

$$\begin{bmatrix}0\\0\end{bmatrix}=[P_0(t)\quad P_1(t)]\begin{bmatrix}-\lambda & \lambda\\ \mu & -\mu\end{bmatrix} \tag{1.157}$$

Dalla 1.157 si ottiene nuovamente un sistema di equazioni facilmente risolvibile perché contenente equazioni algebriche. I risultati ottenuti coincidono con quelli ricavati dalle equazioni differenziali e posti a stazionario. Viene aggiunta al sistema anche la già citata equazione 1.127:

$$\begin{cases}-\lambda P_0(t)+\mu P_1(t)=0\\ \lambda P_0(t)-\mu P_1(t)=0\\ P_0(t)+P_1(t)=1\end{cases} \tag{1.158}$$

Viene riportato come esempio la disponibilità, ottenuta ricavando un'espressione di $P_1(t)$ dalla terza equazione del sistema 1.158:

$$P_1(t)=1-\ P_0(t) \tag{1.159}$$

L'equazione 1.159 viene inserita nella prima equazione del sistema 1.166 e si ricava l'espressione della disponibilità:

$$-\lambda P_0(t)+\mu(1-\ P_0(t))=0 \tag{1.160}$$

$$P_0(t)=\frac{\mu}{\mu+\lambda} \tag{1.161}$$

Riassumendo, la disponibilità del sistema è data dalla somma delle probabilità relative agli stati che garantiscono il corretto funzionamento del sistema ed è ricavabile tramite il modello di Markov esclusivamente in caso di tassi di guasto e di riparazione costanti. Viene riportata nuovamente l'espressione matematica della disponibilità ricavata con l'ausilio del modello di Markov:

$$A(t)=\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} \tag{1.147}$$

La disponibilità a stato stazionario, già ricavata con il modello di Markov è rappresentata da A ed è definita anche dalla normativa IEC 60050 con la seguente definizione: è il limite, se esiste, della disponibilità istantanea quando il tempo tende ad infinito. In questa nuova equazione viene inserito il MTBF, tramite la relazione presente nell'equazione 1.119:

$$\lim_{t\to\infty}A(t)=A=\frac{\mu}{\lambda+\mu}=\frac{MTTF}{MTTF+MTTR}=\frac{MTTF}{MTBF} \tag{1.162}$$

Come stabilito dalla normativa IEC 61703[8], la disponibilità a stato stazionario può essere espressa dal rapporto tra il tempo medio di funzionamento e la somma dello stesso con il tempo medio di guasto (non essendo presenti altri stati oltre a quelli di funzionamento e di guasto l'ultimo termine coincide con il tempo totale):

$$A = \frac{MTTF}{MTBF} = \frac{TempoFunzionamento}{TempoTotale} = \frac{TempoFunzionamento}{TempoFunzionamento\ + TempoGuasto} \tag{1.163}$$

Viene introdotta anche l'indisponibilità a stato stazionario, rappresentata da U e definita anch'essa dalla normativa IEC 60050 con la seguente definizione: è il limite, se esiste, dell'indisponibilità istantanea quando il tempo tende ad infinito:

$$U = 1 - A = 1 - \frac{MTTF}{MTTF + MTTR} = \frac{MTTR}{MTTF + MTTR} = \frac{MTTR}{MTBF} \tag{1.164}$$

Analogamente a quando stabilito per la disponibilità, la normativa IEC 61703 stabilisce che l'indisponibilità a stato stazionario può essere espressa può essere espressa dal rapporto tra il tempo medio di guasto e la somma dello stesso con il tempo medio di funzionamento:

$$U = \frac{MTTR}{MTBF} = \frac{TempoGuasto}{TempoTotale} = \frac{TempoGuasto}{TempoFunzionamento\ + TempoGuasto} \tag{1.165}$$

Si può ricavare un'altra espressione di disponibilità, dalla 1.162, semplicemente dividendo numeratore e denominatore del termine a destra per il MTTF:

$$A = \frac{MTTF}{MTBF} = \frac{MTTF}{MTTF + MTTR} = \frac{1}{1 + \frac{MTTR}{MTTF}} \tag{1.166}$$

Qualora il tempo di riparazione sia trascurabile rispetto al tempo di funzionamento, si può ricavare un'espressione approssimata per l'inaffidabilità, dalla 1.172, non considerando il contributo del termine MTTR al denominatore:

$$U = \frac{MTTR}{MTTF + MTTR} \cong \frac{MTTR}{MTTF} = \frac{\lambda}{\mu} \tag{1.167}$$

Nella seguente Figura 1.24 è rappresentato tramite grafico l'andamento nel tempo (in questo caso pesato alla somma dei tassi) della disponibilità A e dell'indisponibilità U. La disponibilità inizialmente è pari a 1, come l'affidabilità, ma dopo il transitorio iniziale converge al valore di disponibilità a stato stazionario:

[8] La normativa IEC 61703, denominata "Mathematical expressions for reliability, availability, maintainability and maintenance support terms" tratta le espressioni matematiche di affidabilità, disponibilità e manutenibilità.

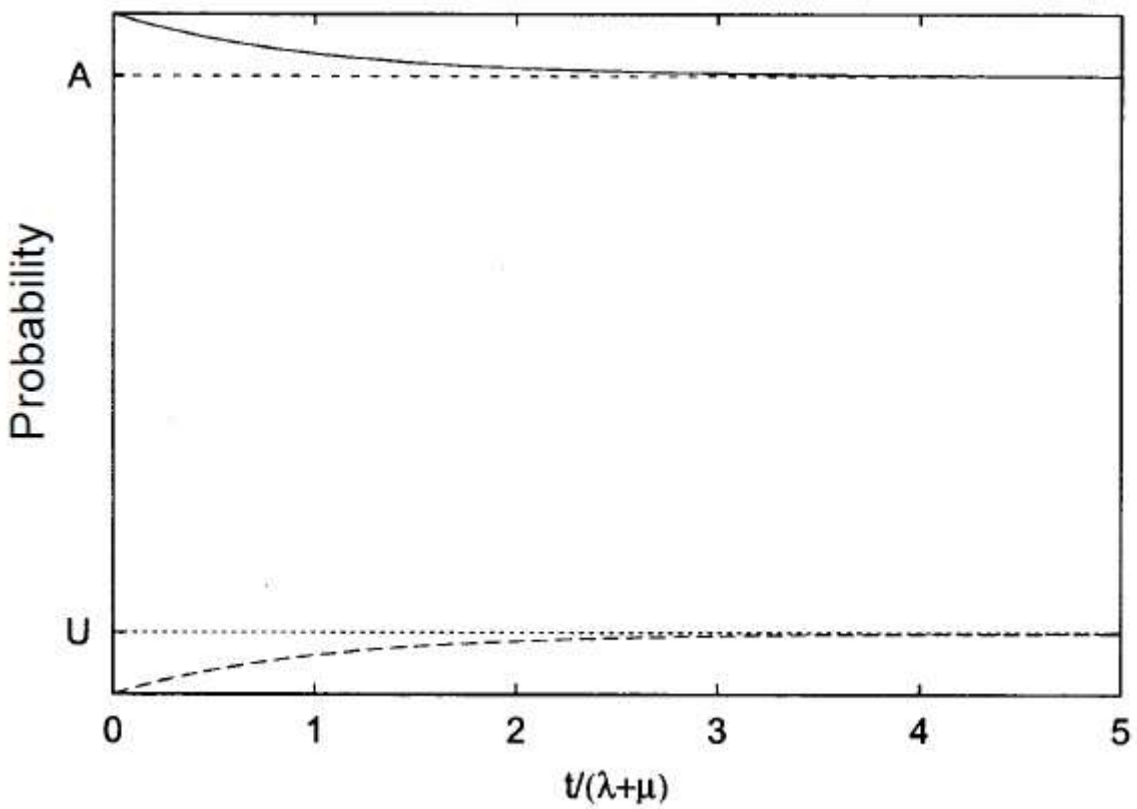


Figura 1.24: grafico della disponibilità nel tempo

Per valutare la disponibilità (e l'affidabilità) bisogna avere le seguenti informazioni:

- Funzioni di distribuzione del tempo al guasto e del tempo alla riparazione.
- Diagramma a blocchi del dispositivo (relazioni tra gli elementi facenti parte dello stesso sistema),
- Tipologia di ridondanza,
- Strategia di manutenzione (numero di riparazioni e priorità di intervento),
- Strategia adottata per il supporto logistico.

Per valutare la disponibilità (e l'affidabilità) nella modalità proposta si devono fare le seguenti assunzioni:

- I tassi di guasto ed i tassi di riparazione sono costanti,
- Le riparazioni sono indipendenti tra tutti i dispositivi presenti, non ci sono problematiche di allocazione delle risorse di riparazione. La riparazione di un dispositivo non è influenzata da altre possibili riparazioni contemporanee di altri dispositivi,
- Dopo una riparazione il dispositivo riparato è assunto avere un funzionamento ed una affidabilità pari a quando era appena stato messo in operazione, a quando era nuovo. La riparazione è completa. Le caratteristiche del dispositivo non sono dipendenti dal numero di guasti (e quindi di riparazioni) che esso ha subito (non ci sono fenomeni di wearout o di invecchiamento).

Per le configurazioni standard di elementi in serie ed elementi in parallelo, utilizzate nei diagrammi a blocchi di affidabilità RBD è possibile valutare la disponibilità del sistema conoscendo le disponibilità dei suoi singoli elementi.

Nella configurazione **in serie** la disponibilità del sistema è pari alla produttoria delle disponibilità dei singoli elementi, poiché il sistema, per essere disponibile, ha bisogno della disponibilità di tutti i suoi elementi. Viene riportato in seguito, nella Figura 1.25, un RBD relativo alla configurazione in serie per ricordarne la struttura e nell'equazione 1.168 viene espresso quanto detto riguardo alla disponibilità del sistema:

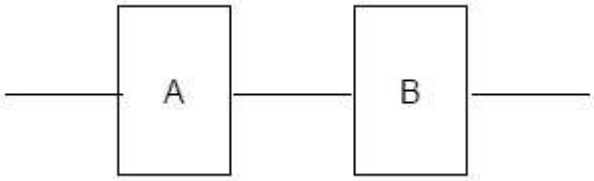


Figura 1.25: RBD, sistema composto da due elementi in serie.

$$A_{serie} = \prod_i A_i \tag{1.168}$$

Nella configurazione **in parallelo** si procede invece analizzando l'indisponibilità del sistema: essa è pari alla produttoria delle indisponibilità dei singoli elementi, poiché il sistema è indisponibile solamente se tutti i suoi elementi lo sono. Una volta ricavata l'indisponibilità del sistema si può ricavare la disponibilità essendo eventi mutualmente esclusivi. Viene riportato in seguito, nella Figura 1.26, un RBD relativo alla configurazione in parallelo per ricordarne la struttura e nelle equazioni 1.169 e 1.170 viene espresso quanto detto riguardo alla disponibilità del sistema:

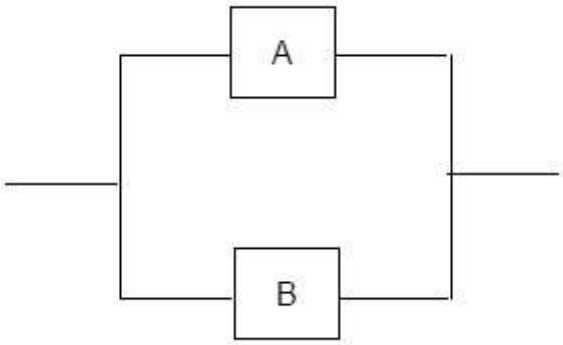


Figura 1.26: RBD, sistema composto da due elementi in parallelo.

$$U_{parallelo} = \prod_i U_i \tag{1.169}$$

$$A_{parallelo} = 1 - U_{parallelo} \tag{1.170}$$

1.8 Altri metodi di analisi dei sistemi

Nell'ingegneria dell'affidabilità, per l'analisi di una qualsiasi tipologia di sistema ed in particolare per sistemi con una configurazione non riconducibile a quelle trattate precedentemente, è possibile utilizzare delle **tabelle di verità booleane** (note generalmente con il termine inglese Boolean Truth Table). Questo metodo è particolarmente utile quando il diagramma a blocchi di affidabilità del sistema oggetto di analisi non è semplificabile mediante semplificazioni di tipo serie e parallelo. È

possibile ricavare, tramite il suo utilizzo ed in genere con l'ausilio di un software, delle caratteristiche di un sistema quali disponibilità e affidabilità.

Il metodo consiste nell'analisi, tramite appunto una tabella di verità, di ogni possibile stato del sistema. Gli stati del sistema sono combinazioni binarie degli stati di ogni elemento di esso, quindi, come già descritto, per un sistema composto da n elementi, gli stati dello stesso saranno pari a 2^n.

Gli stati del sistema sono indipendenti tra loro e sono caratterizzati da una probabilità pari al prodotto di quelle che ogni elemento del sistema ha di trovarsi nello stato di funzionamento o di guasto, in base alla caratteristica di quello stato del sistema.

Essendo gli stati indipendenti è sufficiente, per ottenere l'affidabilità o la disponibilità del sistema, sommare le probabilità che ha il sistema di trovarsi in ogni stato di funzionamento.

Per la trattazione di questo metodo è utilizzato un esempio di RBD non semplificabile e non riconducibile ad alcuna delle configurazioni già analizzate, rappresentato nella seguente Figura 1.27:

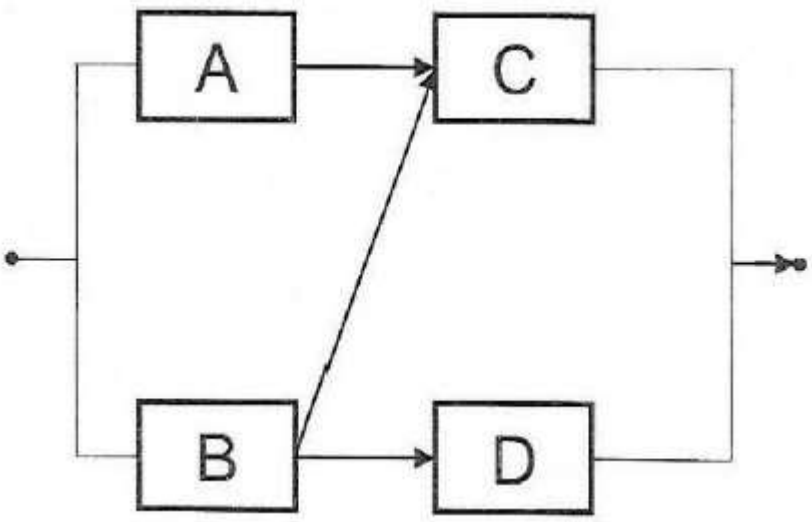


Figura 1.27: RBD, configurazione semplificabile con serie o parallelo.

Il metodo, ricapitolando, consiste nell'analizzare ogni stato del sistema, sempre considerando una logica booleana del sistema stesso e dei suoi elementi, ovvero con soli due stati possibili, di funzionamento corretto o di guasto. Per verificare il funzionamento o meno del sistema è sufficiente, tramite RBD, verificare se esiste almeno un sentiero di funzionamento, ovvero un insieme di uno o più elementi che, se funzionanti, consentono al sistema di funzionare.

Viene in seguito riportata la tabella di verità booleana relativa all'esempio mostrato in Figura 1.27, con già presente la probabilità di ogni stato (indicata in questo caso come prodotto delle affidabilità o inaffidabilità dei singoli elementi):

A	B	C	D	Sistema	Probabilità dello stato
0	0	0	0	0	$(1-R_A(t))\cdot(1-R_B(t))\cdot(1-R_C(t))\cdot(1-R_D(t))$
0	0	0	1	0	$(1-R_A(t))\cdot(1-R_B(t))\cdot(1-R_C(t))\cdot R_D(t)$
0	0	1	0	0	$(1-R_A(t))\cdot(1-R_B(t))\cdot R_C(t)\cdot(1-R_D(t))$
0	0	1	1	0	$(1-R_A(t))\cdot(1-R_B(t))\cdot R_C(t)\cdot R_D(t)$
0	1	0	0	0	$(1-R_A(t))\cdot R_B(t)\cdot(1-R_C(t))\cdot(1-R_D(t))$
0	1	0	1	1	$(1-R_A(t))\cdot R_B(t)\cdot(1-R_C(t))\cdot R_D(t)$
0	1	1	0	1	$(1-R_A(t))\cdot R_B(t)\cdot R_C(t)\cdot(1-R_D(t))$
0	1	1	1	1	$(1-R_A(t))\cdot R_B(t)\cdot R_C(t)\cdot R_D(t)$
1	0	0	0	0	$R_A(t)\cdot(1-R_B(t))\cdot(1-R_C(t))\cdot(1-R_D(t))$
1	0	0	1	0	$R_A(t)\cdot(1-R_B(t))\cdot(1-R_C(t))\cdot R_D(t)$
1	0	1	0	1	$R_A(t)\cdot(1-R_B(t))\cdot R_C(t)\cdot(1-R_D(t))$
1	0	1	1	1	$R_A(t)\cdot(1-R_B(t))\cdot R_C(t)\cdot R_D(t)$
1	1	0	0	0	$R_A(t)\cdot R_B(t)\cdot(1-R_C(t))\cdot(1-R_D(t))$
1	1	0	1	1	$R_A(t)\cdot R_B(t)\cdot(1-R_C(t))\cdot R_D(t)$
1	1	1	0	1	$R_A(t)\cdot R_B(t)\cdot R_C(t)\cdot(1-R_D(t))$
1	1	1	1	1	$R_A(t)\cdot R_B(t)\cdot R_C(t)\cdot R_D(t)$

Tabella 1. 2: Esempio di tabella di verità booleana.

Nella tabella di verità ogni riga rappresenta uno stato di un sistema. Gli stati sono pari a $2^4 = 16$ e per ricavare ogni possibile stato del sistema è sufficiente utilizzare la numerazione binaria. Ogni cella rappresenta, tramite uno 0 oppure un 1, il funzionamento o meno degli elementi e del sistema. Lo 0 indica lo stato di guasto, mentre l'1 indica il funzionamento.

Gli stati di funzionamento del sistema sono evidenziati in verde. La probabilità di ogni stato è data da una combinazione tra le affidabilità e le inaffidabilità dei singoli elementi del sistema. La somma delle probabilità di ogni stato è pari ad 1.

Per calcolare l'affidabilità del sistema è sufficiente sommare le probabilità di ogni stato di funzionamento dello stesso, in questo caso sono presenti otto stati di funzionamento, le cui espressioni di probabilità sono già riportate nella Tabella 1. 2:

$$R_{sistema}(t) = \sum_{i=0}^{n} Pr_{stato\ OK}(t) \tag{1.171}$$

Quanto descritto per l'affidabilità e l'inaffidabilità può essere utilizzato per il calcolo della disponibilità del sistema, utilizzando i dati di disponibilità e indisponibilità dei singoli elementi.

In caso di sistemi con un numero elevato di elementi, che richiederebbero una tabella di verità molto grande visto l'incremento esponenziale del numero degli stati e quindi notevoli calcoli di probabilità, è possibile utilizzare il metodo Monte Carlo[9], con l'ausilio di un software.

Per l'analisi di affidabilità e disponibilità di un sistema è possibile ricorrere al metodo dei percorsi minimi di funzionamento, definito in genere metodo dei **Minimal Path Set**. Il metodo consiste nell'analizzare i sentieri minimi di funzionamento di un sistema, ovvero la combinazione minima di uno o più elementi di esso che consentono al sistema di funzionare.

Nell'esempio riportato in Figura 1.27 nessun elemento è in grado di far funzionare il sistema da solo ma sono presenti alcuni percorsi di funzionamento composti da due elementi, che sono elencati in seguito:

- Percorso formato dagli elementi A e C.
- Percorso formato dagli elementi B e C.
- Percorso formato dagli elementi B e D.

Il sistema, per funzionare, necessita che almeno uno di questi sentieri sia operante, pertanto viene riprodotto un RBD con i percorsi di funzionamento disposti in parallelo tra loro. Il singolo percorso è funzionante se e solo se tutti i suoi elementi lo sono, quindi gli elementi facenti parte dello stesso percorso sono disposti in serie.

In base a quanto descritto è rappresentato in seguito un RBD che prevede che siano presenti più blocchi relativi allo stesso elemento:

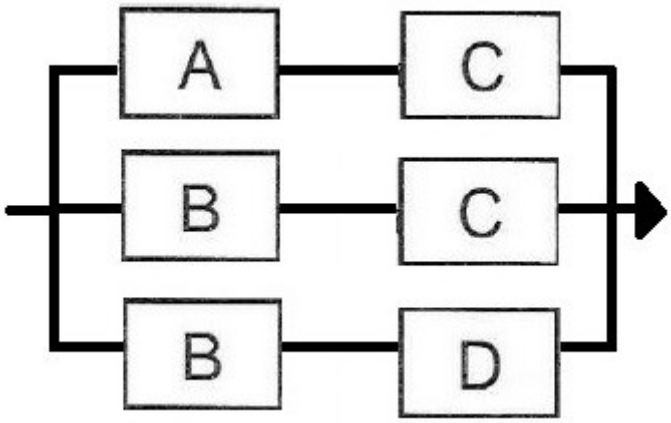


Figura 1.28: RBD, percorsi minimi di funzionamento.

Il risultato, di affidabilità o di disponibilità, è facilmente ricavabile con quanto descritto per gli RBD con configurazioni in serie e parallelo ma causa, rispetto all'utilizzo delle tabelle di verità booleane, una sovrastima dovuta alla configurazione in parallelo di più blocchi rappresentanti lo stesso elemento.

[9] Il metodo Monte Carlo è numerico e consente di trovare soluzioni di problemi matematici con molte variabili e che non possono essere risolti facilmente. Prende il nome dall'omonimo casinò.

Per l'analisi di affidabilità e disponibilità di un sistema è possibile ricorrere in modo diametralmente opposto a quanto descritto in precedenza con il metodo dei Minimal Path Set, ovvero ricorrendo al metodo dei **Minimal Cut Set**. Il metodo consiste nell'analizzare i sentieri minimi di guasto di un sistema, ovvero la combinazione minima di uno o più elementi di esso che, se non dovessero funzionare, porterebbero inevitabilmente il sistema ad un guasto.

Nell'esempio riportato in Figura 1.27 nessun elemento è in grado di causare un guasto del sistema da solo ma sono presenti alcune combinazioni di due elementi che possono provocare il mancato funzionamento del sistema, che sono elencati in seguito:

- Percorso formato dagli elementi A e B.
- Percorso formato dagli elementi B e C.
- Percorso formato dagli elementi B e D.

Il sistema, per funzionare, necessita che ognuno di questi sentieri sia operante, dato che ne basterebbe uno non funzionante per causare un guasto, pertanto viene riprodotto un RBD con i percorsi di funzionamento disposti in serie tra loro. Il singolo percorso causa un guasto se e solo se tutti i suoi elementi sono guasti, quindi gli elementi facenti parte dello stesso percorso sono disposti in parallelo.

In base a quanto descritto è rappresentato in seguito un RBD che prevede che siano presenti più blocchi relativi allo stesso elemento:

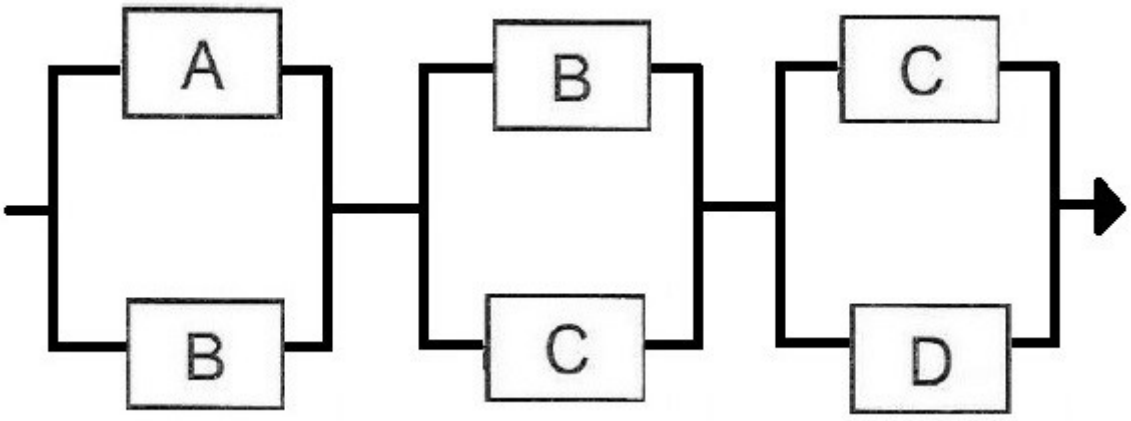


Figura 1.29: RBD, percorsi minimi di guasto (MCS).

Il risultato, di affidabilità o di disponibilità, è facilmente ricavabile con quanto descritto per gli RBD con configurazioni in serie e parallelo ma causa, rispetto all'utilizzo delle tabelle di verità booleane, una sottostima dovuta alla configurazione in serie di più blocchi rappresentanti lo stesso elemento.

Un'altra tecnica utilizzabile è l'analisi dell'albero dei guasti, tecnica chiamata più comunemente **FTA** (dall'inglese Fault Tree Analysis). Questa tecnica è volta a determinare da un lato i modi credibili di accadimento di un qualsiasi evento causato da un concatenarsi complesso di altri eventi, ad esempio guasti (analisi qualitativa) e dall'altro a stimare la frequenza di accadimento dell'evento oggetto di studio sulla base delle frequenze di accadimento degli eventi che lo causano (analisi quantitativa).

Si tratta di una metodologia deduttiva, che utilizza una logica top-down e che è adatta all'analisi di sistemi complessi la cui evoluzione può essere facilmente decomposta in una successione di eventi più semplici.

L'evento oggetto di studi è in genere un evento indesiderato (solitamente indicato con il termine inglese Top Event). Una volta definito il Top Event si rappresentano in modo grafico tutte le combinazioni di eventi che possono portare al suo verificarsi. In estrema sintesi, un albero dei guasti non è altro che un insieme di porte che consentono oppure no il passaggio della logica di guasto attraverso l'albero.

L'assunzione di base per le porte è la logica binaria, nel caso di un elemento esso può funzionare perfettamente oppure non funzionare del tutto. Le porte logiche principali sono le seguenti:

- Porta OR: perché l'output della porta avvenga è sufficiente che avvenga uno degli input della porta stessa.
- Porta AND: perché l'output della porta avvenga è necessario che avvengano tutti gli input della porta stessa.

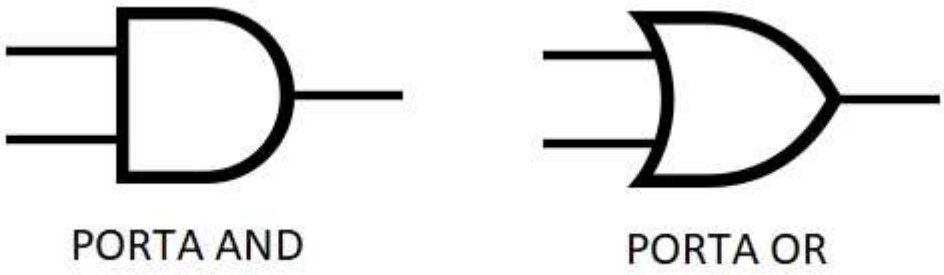


Figura 1.30: Porte logiche AND e OR.

Il numero di input nelle porte logiche è necessariamente maggiore di uno.

Le porte logiche interconnettono tra di loro degli eventi, che possono essere di diverso tipo:

- Top Event: rappresentato da un rettangolo, si trova in cima all'albero dei guasti e da esso si procede con un'analisi deduttiva connettendo ad esso gli altri eventi che lo possono provocare.
- Eventi intermedi: rappresentati da rettangoli, sono eventi che avvengono prima o dopo un altro evento e rappresentano la causa dell'evento successivo. Sono connessi agli eventi precedenti e successivi tramite porte logiche.
- Eventi primari: rappresentati da cerchi, si tratta di eventi che, per diverse ragioni, non vengono ulteriormente indagati. Per analizzarli quantitativamente sono necessari dei dati di affidabilità.

Un esempio di costruzione di albero dei guasti può essere illustrato considerando un generico impianto di illuminazione schematizzato nella seguente Figura 1.31 e costituito da due lampadine (L1 ed L2), un generatore di energia (P) ed un interruttore (I):

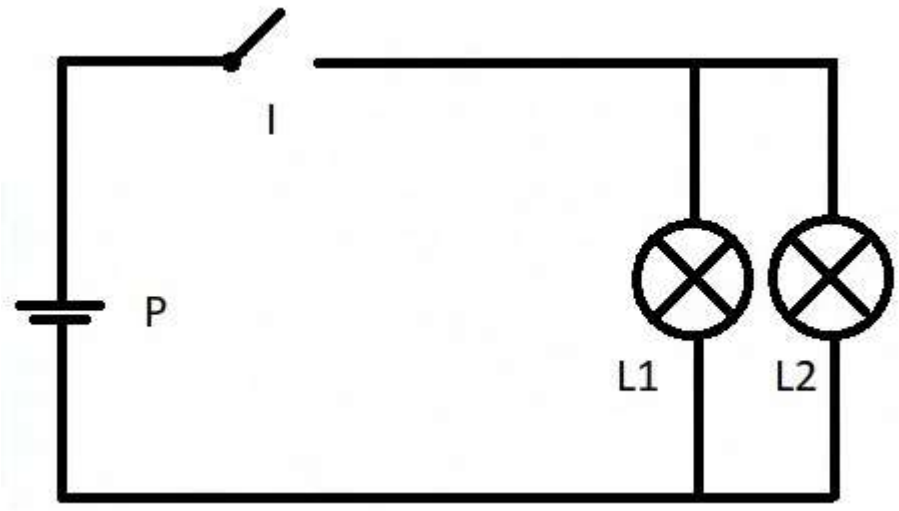


Figura 1.31: Schema di un generico impianto di illuminazione

L'evento indesiderato considerato è la mancanza di luce; le cause immediate, necessarie e sufficienti che possono essere ipotizzate perché il avvenga sono le seguenti:

- Interruttore I rotto,
- Generatore P non funzionante,
- Entrambe le lampadine L1 ed L2 rotte

I primi due eventi possono essere considerati primari mentre il mancato funzionamento di entrambe le lampadine può essere considerato un evento intermedio, le cui cause immediate, necessarie e sufficienti sono che entrambe le lampadine, L1 ed L2, siano simultaneamente rotte.

L'albero dei guasti relativo è rappresentato nella seguente Figura 1.32:

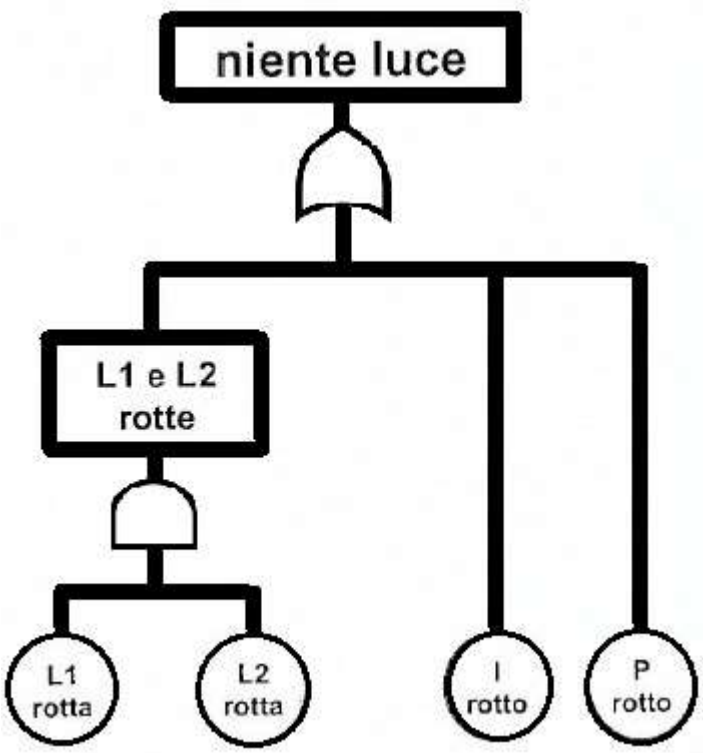


Figura 1.32: Albero dei guasti per l'evento "mancanza di luce".

Una volta terminata questa prima parte di analisi qualitativa si procede con la quantificazione della probabilità di accadimento dell'evento indesiderato, che può essere eseguita tramite i MCS (Minimal Cut Set), ovvero le minime combinazioni di eventi primari necessari e sufficienti affinché si verifichi l'evento indesiderato. In altri termini, perché si produca l'evento indesiderato, tutti gli eventi contenuti nel MCS devono avvenire simultaneamente.

Il numero di eventi coinvolti in un MCS è chiamato "ordine del MCS" ed in genere, per un sistema, i MCS vengono elencati con l'ordine crescente, in quanto i MCS con un numero ridotto di eventi primari necessari (a volte anche un solo evento) sono in genere i più rilevanti.

L'analisi delle modalità e degli effetti dei guasti, chiamata più semplicemente **FMEA** (dall'inglese Failure Modes and Effect Analysis) è una procedura sistematica per l'analisi dei sistemi e serve per identificare le modalità di guasto, le loro cause e gli effetti sul sistema.

L'analisi generalmente si svolge in via preventiva, nel ciclo di sviluppo di un sistema, per rimuovere più problematiche possibili riguardanti i guasti.

La FMEA è un processo iterativo preceduto da una scomposizione gerarchica del sistema in elementi di esso da analizzare, in genere rappresentati con un diagramma a blocchi. L'analisi inizia dagli elementi di livello gerarchico più basso, è un'analisi induttiva e segue una tecnica bottom-up (al contrario della FTA che è deduttiva ed utilizza una logica top-down). Un guasto ad un elemento del sistema potrebbe, come effetto, essere causa di guasto per un altro elemento. L'analisi procede fino a che vengono identificati tutti i possibili effetti dei guasti del sistema.

Dopo aver suddiviso in più elementi il sistema si procede alla numerazione degli stessi ed alla creazione dei fogli di lavoro. Sarà presente un foglio di lavoro per ogni elemento del sistema, che in genere è indicato come dispositivo.

Nella FMEA vengono introdotti alcuni indici relativi alle modalità di guasto:

- Severità: indicata come S (dall'inglese Severity), è un valore numerico che corrisponde alla gravità degli effetti del guasto. In genere il range utilizzato per assegnare il valore va da 1 (nessun effetto) a 10 (effetto catastrofico). Tiene conto delle performance degradate del sistema, dei mancati funzionamenti che può causare il guasto e della magnitudo degli eventi che possono verificarsi a seguito del guasto.
- Probabilità di accadimento: indicata come O (dall'inglese Occurrence), è un valore numerico che corrisponde alla probabilità che si verifichi il guasto. Anche per la probabilità il range utilizzato per assegnare il valore va da 1 (probabilità remota) a 10 (probabilità molto alta). Tiene conto di tutte le cause potenziali di guasto, inclusi errori umani, wearout o condizioni di utilizzo improprie.
- Rilevabilità: indicata come D (dall'inglese Detection), è un valore numerico che corrisponde alla capacità di rilevamento del guasto. Il range utilizzato va sempre da 1 (rilevamento certo) a 10 (rilevamento non possibile). Tiene conto di tutte le modalità di rilevamento, sia tramite operatore che tramite strumenti di rilevamento.

Il valore dei tre indici appena descritti è in genere determinato tramite delle tabelle di valutazione, utilizzate per attribuire il valore numero ad ogni indice in base a caratteristiche e/o parametri. Possono variare in base alla tipologia di sistema oggetto di studio.

L'indice di priorità di rischio, definito come RPN (dall'inglese Risk Priority Number) è descritto dal prodotto degli indici di severità, probabilità e rilevabilità ed è un numero che consente di valutare facilmente quali sono le modalità di guasto più rilevanti. Se i tre indici che lo compongono hanno valori compresi da 1 a 10, l'indice di priorità di rischio sarà un numero compreso tra 1 e 1000.

L'espressione dell'indice di priorità di rischio è riportata nella seguente equazione:

$$RPN = S \cdot P \cdot D \tag{1.172}$$

Ogni elemento del sistema verrà analizzato e conterrà, nel foglio di lavoro, i seguenti dati:

- Nome dispositivo/funzione,
- Descrizione del dispositivo/funzione,
- Elenco delle possibili modalità di guasto,
- Per ogni modalità di guasto:
    - Cause di guasto,
    - Effetti di guasto (distinti in locali e globali),
    - Metodi di rilevazione/controllo del guasto,
    - Valutazione severità (S), probabilità (P) e rilevabilità (D) del guasto,
    - Calcolo dell'indice di priorità di rischio,
    - Azioni raccomandate.

2. La sicurezza funzionale

2.1 Introduzione alla sicurezza funzionale

Per introdurre la sicurezza funzionale è necessario trattare il concetto di pericolo ed il concetto di rischio. Si definisce, nel contesto della sicurezza industriale, pericolo (o in modo equivalente fattore o sorgente di rischio) una proprietà intrinseca di un materiale, macchinario, impianto o situazione in grado di arrecare danno alle cose, all'ambiente o alle persone. Trattandosi di una proprietà intrinseca, un pericolo segue una logica binaria: o è presente o è assente. In altri termini un pericolo può essere eliminato ma non può essere ridotto. È evidente che in qualsiasi attività umana sono presenti intrinsecamente dei pericoli per le cose, per l'ambiente o per le persone. È quindi particolarmente importante, nella progettazione e gestioni di impianti, dispositivi, processi o macchinari, considerare, oltre agli aspetti produttivi, anche quelli della sicurezza. La presenza di un pericolo può avere conseguenze pratiche molto diverse in funzione di due variabili: il fatto che il pericolo si concretizzi in un evento indesiderato o meno e l'entità del danno causato dall'evento indesiderato stesso.

Il concetto di rischio sintetizza in un solo parametro la probabilità che il pericolo si concretizzi in un effetto dannoso (la probabilità di accadimento dell'evento indesiderato, indicata in seguito con P), e l'entità del danno, cioè la sua magnitudo, indicata con M. La magnitudo di un evento a sua volta dipende dall'intensità, I, dell'effetto causato dall'incidente e dalla vulnerabilità, V, delle persone, delle cose o dell'ambiente esposto.

In termini matematici si può dire che il rischio, R, è una funzione delle probabilità di accadimento di un evento indesiderato e della sua magnitudo, parametro a sua volta funzione dell'intensità degli effetti a esso associati e della vulnerabilità delle persone o dell'ambiente colpiti da tali effetti:

$$R = f(P, M) = f(P, I, V) \tag{2.1}$$

Per stimare quantitativamente il rischio, si possono utilizzare diverse soluzioni, ad esempio considerare un semplice operatore moltiplicativo tra probabilità di accadimento e magnitudo oppure utilizzare delle correlazioni tabellari, in genere assegnando dei valori numerici ai parametri di rischio tramite una scala ben definita.

La sicurezza funzionale è definita nello standard IEC 61508[10] come parte della sicurezza complessiva di un sistema o di un dispositivo che dipende dal corretto funzionamento dei sistemi di sicurezza e delle misure di riduzione del rischio. L'obiettivo della sicurezza funzionale è la riduzione del rischio ad un livello accettabile, in un impianto, processo o macchinario, tramite un sistema di sicurezza.

In un processo, il sistema di controllo (ad esempio un controllore PID, proporzionale integrale derivativo) si assicura che tutte le variabili siano stabilizzate al loro set-point, mentre il sistema di sicurezza si assicura che, in caso di perdita di controllo, il processo venga inibito o comunque venga portato ad uno stato sicuro, nel quale non è possibile il verificarsi di eventi pericolosi.

[10] Lo standard IEC 61508 è intitolato "Sicurezza funzionale dei sistemi elettrici / elettronici / elettronici programmabili relativi alla sicurezza", l'ultimo aggiornamento è del 2020.

Il controllo automatizzato consente ai macchinari di operare e si occupa della produttività mentre la sicurezza è "trasparente" fino a quando non sorge una situazione pericolosa che ne richiede l'intervento.

Viene introdotto come esempio, in Figura 2.1, un semplice processo con un sistema di controllo ed uno di sicurezza, in particolare è rappresentata una caldaia. Il sistema di controllo implementato si occupa, tramite una valvola di regolazione, della portata uscente dalla stessa caldaia mentre il sistema di sicurezza si occupa di interrompere l'afflusso di gas combustibile e quindi di calore che la alimenta, in caso di emergenza e tramite una valvola on/off.

Nella seguente Figura 2.1 viene introdotto l'acronimo EUC, derivato dall'inglese "Equipment Under Control", letteralmente attrezzatura sotto controllo. Per EUC si può intendere un'intera installazione, una parte di essa oppure parte di un dispositivo, attrezzatura, macchinario o impianto:

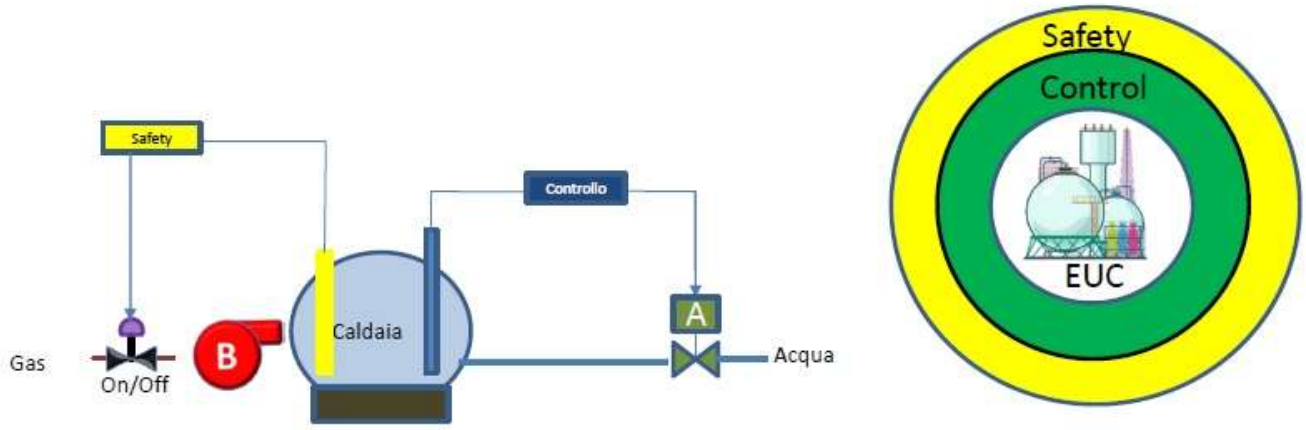


Figura 2.1: Esempio di sistemi di controllo e di sicurezza in un processo.

La sicurezza funzionale è un importante mezzo in grado di diminuire il numero di morti ed infortuni sul posto di lavoro. Il rapido sviluppo tecnologico nel settore dei sistemi di controllo ha portato i normatori a cercare di regolare con criteri quantitativi il livello di affidabilità dei sistemi di controllo che assolvono funzioni di sicurezza.

Maggiore è la magnitudo di un evento pericoloso introdotto da un processo e maggiore dovrebbe essere teoricamente la sua affidabilità, in altre parole dovrebbe essere tanto più limitata la sua probabilità di guasto quanto più sono severe le conseguenze degli eventi indesiderati. È possibile valutare il rischio e quantificare la riduzione dello stesso dovuta all'introduzione di un sistema di sicurezza, definito anche anello di sicurezza.

Quando è necessario implementare un sistema di sicurezza sono richiesti i dati di affidabilità relativi ad ogni componente dello stesso. Alcuni esempi di dispositivi utilizzati negli anelli di sicurezza sono: trasmettitori di pressione, valvole, teleruttori, interblocchi ed unità logiche di sicurezza e sono rappresentati nella seguente Figura 2.2:

Figura 2.2: Esempi di dispositivi utilizzati negli anelli di sicurezza.

La normativa IEC 61511[11] introduce i seguenti due concetti relativi ai sistemi di sicurezza:

- Sistema strumentale di sicurezza, definito S.I.S. (dall'inglese Safety Instrumented System): è l'aspetto fisico e materiale del sistema di sicurezza, formato ad esempio da sensori, unità logiche ed elementi finali di controllo.
- Funzione strumentale di sicurezza, definita S.I.F. (dall'inglese Safety Instrumented Function): è l'aspetto matematico del sistema di sicurezza.

Un esempio di S.I.S. e di S.I.F. è rappresentato nella seguente Figura 2.3:

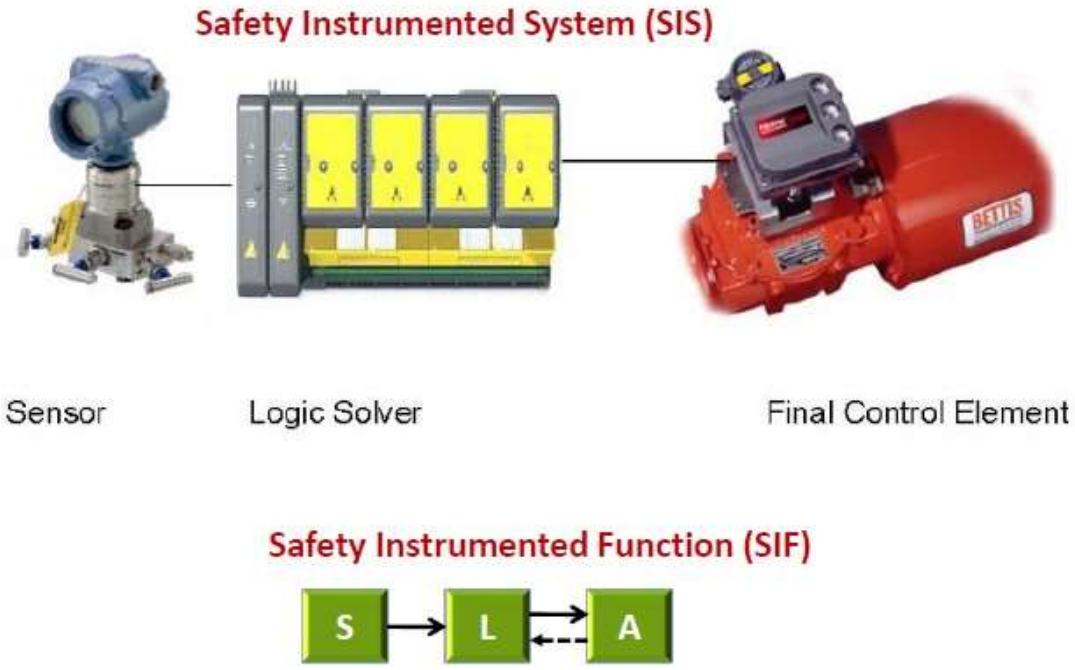


Figura 2.3: Esempio di sistema strumentale di sicurezza e funzione strumentale di sicurezza.

[11] La normativa IEC 61511 è intitolata "Sicurezza funzionale, sistemi strumentali di sicurezza per il settore dell'industria di processo", l'ultimo aggiornamento è del 2010.

L'esempio in Figura 2.3 rappresenta un classico esempio di sistema strumentale di sicurezza: un sensore misura una variabile del processo (temperatura, portata o pressione ad esempio), trasmette il valore misurato come input ad un controllore logico (in genere tramite un segnale elettrico di tensione o di corrente oppure tramite un segnale pneumatico che verrà convertito in elettrico) e quest'ultimo trasmette il comando all'elemento finale di controllo, all'attuatore, che si occupa fisicamente di portare il processo in uno stato sicuro.

La funzione strumentale di sicurezza rappresenta tramite un diagramma a blocchi i vari dispositivi componenti il sistema strumentale di sicurezza: il blocco "S" rappresenta il sensore mentre il blocco "L" il controllore logico ed il blocco "A" l'attuatore.

Un canale funzionale rappresenta parte di un sistema di sicurezza ed ha lo scopo di eseguire la funzione di sicurezza, quando richiesto o in modo continuo. È rappresentato generalmente da un blocco a funzione discreta e può essere formato da più elementi connessi in serie. Il sistema di sicurezza sarà rappresentato pertanto da un diagramma a blocchi.

Per un canale funzionale perdere l'abilità di eseguire la funzione di sicurezza è descritto come un guasto pericoloso.

Le due norme che più nel dettaglio stabiliscono criteri e requisiti di sicurezza funzionale per i sistemi di controllo sono la già citata IEC 62061 e la ISO[12] 13849-1[13].

In entrambe le norme un sistema di sicurezza è modellizzato tramite tre sottosistemi: il sottosistema di input (I), il sottosistema di logica (L) ed il sottosistema di output (O), come mostrato nell'esempio in Figura 2.3, dove i blocchi prendono il nome dal dispositivo utilizzato. In particolare, nell'esempio, il sensore è il sottosistema di input, il controllore logico programmabile il sottosistema di logica e l'attuatore il sottosistema di output.

In entrambe le norme sono descritte procedure per la progettazione e la realizzazione di sistemi di controllo di sicurezza, in modo che questi tendano ad avere valori di affidabilità accettabili. Il livello di rischio accettabile viene valutato, relativamente al sistema o all'apparecchiatura oggetto di studio, con un approccio probabilistico, pertanto come funzione della frequenza o probabilità di accadimento del guasto e della gravità delle conseguenze del guasto stesso. Il rischio introdotto da un processo o da un macchinario è normalmente più elevato di quello accettabile e deve essere ridotto del necessario tramite una o più funzioni di sicurezza.

In altri termini, partendo dal presupposto che non è possibile il rischio zero, lo scopo della IEC 61508 è di fornire una metodologia per realizzare sistemi di sicurezza di affidabilità ben definita, attraverso una quantificazione del rischio intrinseco in un certo evento e la sua riduzione fino ad un livello detto socialmente accettabile.

Nella normativa ISO 13849-1, che tratta l'affidabilità dei sistemi di sicurezza delle machine, introduce il concetto di SRP/CS (dall'inglese Safety Related Parts of Control System), ovvero parte del sistema di controllo che risponde a segnali di ingresso legati alla sicurezza e genera segnali di

[12] L'ISO è l'organizzazione internazionale per la normazione (dall'inglese International Organization for Standardization), è la più importante organizzazione, a livello mondiale, che si occupa della definizione di norme tecniche.

[13] Lo standard ISO 13849-1 è intitolato "Sicurezza dei macchinari – parti di sistemi di controllo legate alla sicurezza", l'ultimo aggiornamento è del 2015.

uscita anch'essi legati alla sicurezza.

I sistemi di sicurezza possono essere attivati spesso o raramente: se vengono attivati spesso (ad esempio nelle protezioni mobili o nei comandi per direttive nell'automazione), entrano nell'ambito della modalità di operazione ad alta richiesta (in inglese definita High Demand Mode) mentre se vengono attivati raramente (come nel caso degli impianti di processo che, ad esempio, attivano un anello di sicurezza in caso di innalzamento della temperatura di un reattore chimico), appartengono all'ambito della modalità di operazione a bassa richiesta (in inglese definita Low Demand Mode).

Questi due "mondi" fanno parte della stessa materia di studio, l'ingegneria dell'affidabilità, ma seguono modalità differenti nel calcolo dell'affidabilità di un anello di sicurezza.

Riguardo alla modalità di operazione a **bassa richiesta**, come da normativa IEC 61511, ci sono due tipologie di dati di affidabilità per un sistema di sicurezza:

- λ: è il tasso di guasto, già trattato nel capitolo precedente,
- PFD_{avg}: è la probabilità di guasto media su richiesta (in inglese questo dato di affidabilità viene definito come Average Probability of Failure on Demand). La richiesta è intesa come richiesta della funzione di sicurezza. È utilizzato tipicamente per i dispositivi complessi ed essendo una probabilità è un valore adimensionale.

Nella normativa IEC 61511 l'affidabilità di un sistema di sicurezza è misurata in livelli di sicurezza integrata, definiti anche SIL (dall'inglese Safety Integrity Levels). Per determinare il SIL di un sistema di sicurezza bisogna correlarlo con dei range di valori del PFD_{avg}. Esistono quattro livelli di sicurezza integrata che, elencati in ordine crescente di affidabilità, sono i seguenti: SIL 1, SIL 2, SIL 3 e SIL 4.

La relazione tra SIL e PFD_{avg} è riportata nella seguente Tabella 2.1:

Livello di sicurezza integrata (SIL)	Probabilità media di un guasto pericoloso in domanda ($\mathbf{PFD_{avg}}$)
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$

Tabella 2.1: Livelli di sicurezza integrata (IEC 61511).

Il PFD_{avg} può essere calcolato tramite la seguente equazione:

$$PFD_{avg} = \frac{1}{TI} \cdot \int_0^{TI} \lambda_{DU} \cdot t \cdot dt = \frac{\lambda_{DU} \cdot t}{TI} \tag{2.2}$$

Nell'equazione è presente un parametro di tempo: TI, che rappresenta l'intervallo di test (dall'inglese Test Interval) ed è il tempo che trascorre tra un test di un canale funzionale ed il successivo.

Per quanto concerne la modalità di operazione ad **alta richiesta**, secondo le normative ISO 13849-1 e IEC 62061, esistono tre tipologie di dati di affidabilità per un sistema di sicurezza. In ognuna di esse il pedice "D" indica che gli indici sono relativi a guasti pericolosi (dall'inglese Dangerous):

- B_{10D}: è il numero di cicli operativi nel quale, se viene posto in operazione, nello stesso istante, un numero elevato di dispositivi, il 10% di questi ultimi ha subito un guasto pericoloso. In altri termini è il numero di cicli nel quale un dispositivo ha subito un guasto pericoloso con una probabilità del 10%. È utilizzato, come verrà illustrato in seguito, per dispositivi soggetti a wearout,
- $MTTF_D$: è il tempo medio al guasto pericoloso, tipico per componenti non soggetti a wearout (è utilizzato anche λ_D, il tasso di guasto pericoloso),
- PFH_D: è la probabilità di guasto pericoloso per ora (in inglese Probability of Dangerous Failure per Hour). La sua unità di misura è $[1/h]$. È utilizzato tipicamente per dispositivi complessi.

La misura dell'affidabilità di un sistema di sicurezza, in entrambe le normative, è correlata al PFH_D.

Nella normativa ISO 13849-1 l'affidabilità di un sistema di sicurezza è misurata in livelli di performance, definiti anche PL (dall'inglese Performance Level). I livelli di performance utilizzati sono, in ordine crescente di affidabilità, i seguenti: PL=a, PL=b, PL=c, PL=d e PL=e.

Nella normativa IEC 62061 l'affidabilità di un sistema di sicurezza è misurata, come per la modalità di operazione a bassa richiesta, in livelli di sicurezza integrata, SIL. Anche in questo caso i livelli di sicurezza integrata utilizzati sono i seguenti, elencati in ordine crescente di affidabilità: SIL 1, SIL 2 e SIL 3.

Le relazioni tra range di PFH_D, PL (ISO 13849-1) e SIL (IEC 62061) sono rappresentate nella seguente tabella:

Livello di performance (PL)	Probabilità di guasto pericoloso per ora ($\mathbf{PFH_D}$) [1/h]	Livello di sicurezza integrata (SIL)
a	$10^{-5} \leq PFH_D < 10^{-4}$	-
b	$3 \cdot 10^{-6} \leq PFH_D < 10^{-5}$	1
c	$10^{-6} \leq PFH_D < 3 \cdot 10^{-6}$	1
d	$10^{-7} \leq PFH_D < 10^{-6}$	2
e	$10^{-8} \leq PFH_D < 10^{-7}$	3

Tabella 2.2: Livelli di sicurezza integrata (IEC 62061) e livelli di performance (ISO 13849-1).

Nel caso più semplice, relativo ad un sottosistema composto da un singolo canale funzionale senza diagnostica, che verrà definita meglio in seguito, la probabilità di guasto pericoloso per ora, essendo una frequenza, è pari al tasso pericoloso di guasto, come riportato nella seguente equazione:

$$PFH_D = \lambda_D \tag{2.3}$$

Un sistema di sicurezza, che come già descritto è formato da tre sottosistemi (di input, di logica e di

output), avrà un PFH_D che sarà funzione dei PFH_D relativi ai suoi sottosistemi. Essendo il funzionamento di questi ultimi indispensabile per eseguire la funzione di sicurezza, i tre sottosistemi saranno disposti in serie e quindi il PFH_D del sistema sarà pari alla somma dei PFH_D dei tre sottosistemi.

Viene riportato in seguito un esempio di sottosistemi a singolo canale funzionale senza diagnostica, come appena descritto, il PFH_D del sistema sarà pari alla somma dei tassi di guasto pericolosi dei tre sottosistemi:

$$PFH_D = PFH_{D,input} + PFH_{D,logica} + PFH_{D,output} = \lambda_{D,input} + \lambda_{D,logica} + \lambda_{D,output} \quad (2.4)$$

Un canale relativo ad un sottosistema, spesso, è formato da un numero n di elementi connessi tra loro in serie. Nella seguente Figura 2.4 è rappresentato un generico canale, definito come CH e composto da n elementi, definiti come E_i. Ogni elemento componente il canale ha il suo tasso di guasto pericoloso costante, indicato in Figura 2.4 come λ_{EiD}:

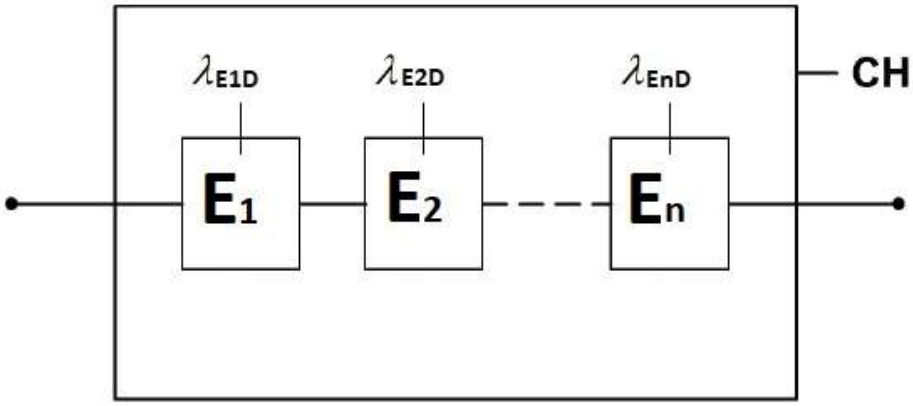


Figura 2.4: Canale formato da n elementi in serie.

Il canale, essendo formato da elementi in serie, ha un guasto pericoloso quando almeno un elemento tra quelli che ne fanno parte lo ha. Il tasso di guasto pericoloso del canale, λ_{CHD}, è definito dalla seguente equazione:

$$\lambda_{CHD} = \lambda_{E1D} + \lambda_{E2D} + \cdots + \lambda_{EnD} \quad (2.5)$$

Per progettare un sistema di sicurezza, procedimento effettuato spesso all'interno di un'analisi di rischio relativa ad un intero impianto, processo, reparto o azienda, si può utilizzare la seguente procedura, contenuta nella normativa ISO 13849-1:

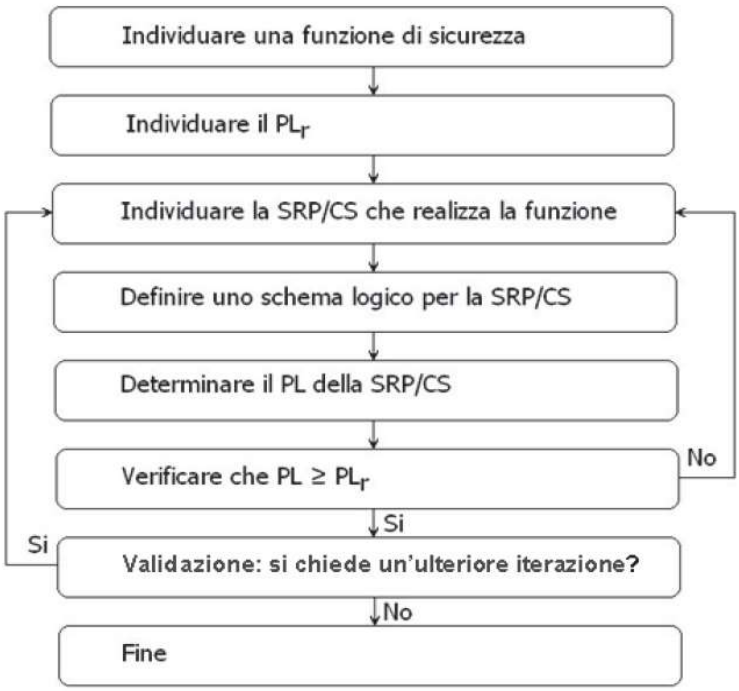


Figura 2.5: Procedura descritta nella normativa ISO 13849-1 per la progettazione di un sistema di sicurezza.

Nella procedura si individua in principio la funzione di sicurezza oggetto di analisi ed in seguito il PL richiesto con delle procedure che verranno illustrate dettagliatamente in seguito (sempre considerando come già detto che ad un maggiore rischio corrisponderà un maggiore PL).

Si sceglie un sistema di sicurezza e, per verificarne l'idoneità, lo si modellizza con lo schema logico già illustrato e composto dai sottosistemi di input, di logica e di output. Infine, si determina il PL del sistema di sicurezza e lo si confronta con quello richiesto, valutando nuove modifiche allo stesso, che si rendono indispensabili in caso esso non raggiunga il PL richiesto.

La stessa procedura può essere applicata considerando la normativa IEC 62061 e quindi il SIL anziché il PL.

2.2 Tolleranza al guasto hardware e copertura diagnostica

La normativa IEC 61508 introduce il concetto di tolleranza al guasto hardware, definita in genere come HFT (dall'inglese Hardware Fault Tolerance): è l'abilità di un sistema di essere in grado di svolgere la sua funzione strumentale di sicurezza in presenza di uno o più guasti nell'hardware.

Per aumentare le performance di affidabilità e disponibilità di un sistema di sicurezza può essere presente della ridondanza nell'hardware, introducendo più di un canale funzionale in grado di svolgere la funzione di sicurezza. Nella seguente tabella vengono elencate delle architetture presenti nella normativa IEC 61511, accompagnate dalla corrispettiva configurazione in RBD e dalla HFT appena introdotta:

Architettura	HFT	RBD
1oo1	$HFT = 0$	Canale singolo
1oo2	$HFT = 1$	Due canali in parallelo
1oo3	$HFT = 2$	Tre canali in parallelo
2oo3	$HFT = 1$	Tre canali in configurazione 2-out-of-3
2oo4	$HFT = 2$	Quattro canali in configurazione 2-out-of-4

Tabella 2.3: Tolleranza al guasto hardware per diverse architetture.

In un sistema di sicurezza è possibile implementare la diagnostica, ovvero la verifica del canale funzionale, ad intervalli di tempo definiti od in modo continuo, tramite dei test. La diagnostica può essere implementata tramite un apposito canale, definito canale di monitor, oppure, nel caso di sistemi di sicurezza aventi ridondanza, può essere eseguita tramite gli stessi canali funzionali, che eseguono la diagnostica ad altri canali funzionali.

La perdita diagnostica non provoca di per sé ad un guasto della funzione di sicurezza, tuttavia un suo guasto è descritto come pericoloso perché costituisce la situazione meno favorevole di guasto in termini di sicurezza.

Quando la diagnostica rileva un guasto pericoloso del canale funzionale porta il sistema in uno stato sicuro; non è tuttavia in grado di rilevare tutte le tipologie di guasto che può subire un canale funzionale ma solo una frazione di esse; parametro denominato copertura diagnostica e che verrà introdotto subito dopo un altro parametro, la frazione di guasti sicuri.

Nella normativa IEC 61508 viene introdotta una scomposizione per un generico tasso di guasto λ in diversi suoi contributi. I diversi contributi, espressi sempre come tasso di guasto, sono relativi ad una determinata tipologia di guasti, i pedici utilizzati derivano dalla terminologia inglese:

- Guasti sicuri rilevabili, tasso di guasto λ_{Sd} (Safe, Detected),
- Guasti sicuri non rilevabili, tasso di guasto λ_{Su} (Safe, Undetected),
- Guasti pericolosi rilevabili, tasso di guasto λ_{Dd} (Dangerous, Detected),
- Guasti pericolosi non rilevabili, tasso di guasto λ_{Du} (Dangerous, Undetected).

La scomposizione del tasso di guasto totale, indicato nella seguente equazione come λ_{tot}, è espressa come segue, considerando la precedente scomposizione ed una intermedia semplicemente tra guasti sicuri e pericolosi:

$$\lambda_{tot} = \lambda_S + \lambda_D = \lambda_{Sd} + \lambda_{Su} + \lambda_{Dd} + \lambda_{Du} \tag{2.6}$$

È possibile definire la frazione di guasti sicuri di un dispositivo come il rapporto tra la somma del tasso di guasto sicuro e del tasso di guasto pericoloso rilevabile con il tasso di guasto totale. Questo valore è indicato come SFF (dall'inglese Safe Failure Fraction):

$$SFF = \frac{\lambda_S + \lambda_{Dd}}{\lambda_{tot}} \tag{2.7}$$

Sempre nella normativa IEC 61508 viene definita la copertura diagnostica, in genere indicata con DC (dall'inglese Diagnostic Coverage): la copertura diagnostica è la frazione di guasti pericolosi che può

essere rilevata ed in termini matematici è espressa come il rapporto tra il tasso di guasto pericoloso rilevabile ed il tasso di guasto pericoloso, come mostrato dalla seguente equazione:

$$DC = \frac{\lambda_{Dd}}{\lambda_D} \tag{2.8}$$

Nella seguente Figura 2.6 è rappresentata, con un grafico a torta, la scomposizione del tasso di guasto utilizzata per esprimere la copertura diagnostica e la frazione di guasti sicuri. Non si tiene conto della scomposizione tra guasti sicuri rilevabili e non rilevabili:

Figura 2.6: Suddivisione dei guasti in diverse tipologie (sicuri, pericolosi rilevabili, pericolosi non rilevabili).

Uno dei chiarimenti più importanti presenti nella normativa IEC 62061 è che, nei componenti elettromeccanici, la frazione di guasti sicuri è sempre uguale a zero ($\lambda_S = 0$). Questo fa sì che la frazione di guasti sicuri sia uguale alla copertura diagnostica, come si può notare dalle equazioni 2.7 e 2.8 ed esclusivamente considerando componenti elettromeccanici (come ad esempio un contattore).

In un canale funzionale composto da n elementi disposti in serie, nel quale è implementata la diagnostica, quest'ultima può differire tra i singoli elementi se considerati singolarmente. La copertura diagnostica avrà più peso negli elementi con un alto tasso di guasto pericoloso rispetto agli elementi con un tasso di guasto pericoloso minore. È rappresentato, nella seguente Figura 2.7, un generico canale composto da n elementi disposti in serie che riprende la Figura 2.6, con l'aggiunta delle coperture diagnostiche relative ai singoli elementi, definite come DC_i:

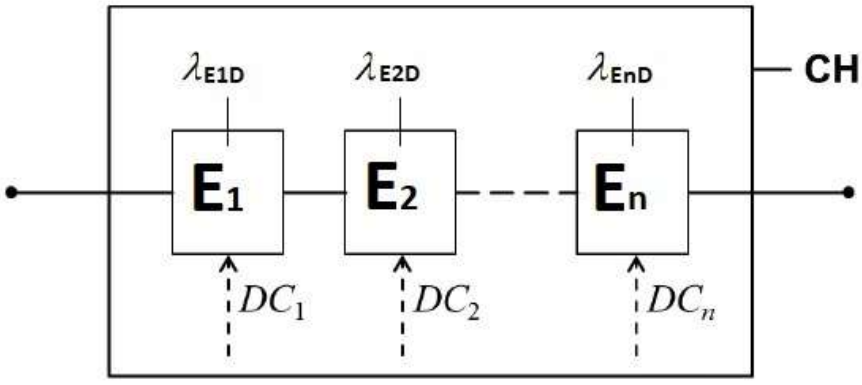


Figura 2.7: Coperture diagnostiche dei singoli elementi di un canale.

La copertura diagnostica relativa al canale, definita DC_{CH} , può essere calcolata tramite una media delle coperture diagnostiche dei singoli elementi, pesata sul rapporto tra il tasso di guasto pericoloso del singolo elemento ed il tasso di guasto pericoloso totale del canale:

$$DC_{CH} = \frac{\lambda_{E1D}}{\lambda_{CHD}} DC_1 + \frac{\lambda_{E2D}}{\lambda_{CHD}} DC_2 + \cdots + \frac{\lambda_{EnD}}{\lambda_{CHD}} DC_n \quad (2.9)$$

Nella normativa ISO 13849-1, per la quantificazione della DC in un esempio pratico, sono presenti delle tabelle che stimano la copertura diagnostica in base alla misura effettuata per lo svolgimento della diagnostica. Sono presenti tre tabelle da utilizzare, una per i dispositivi di input, una per le logiche di controllo ed una per i dispositivi di output.

Viene riportata in seguito, a titolo di esempio, una tabella contenente alcuni esempi di correlazione tra la misura effettuata e la copertura diagnostica, relativamente ai dispositivi di output e, come detto, contenuti nella normativa ISO 13849-1:

Misura	DC
Monitoraggio delle uscite da parte di uno dei canali, senza prova dinamica.	Da 0% a 99% a seconda di quanto spesso l'applicazione produce una variazione di segnale
Monitoraggio incrociato delle uscite senza prova dinamica	Da 0% a 99% a seconda di quanto spesso l'applicazione produce una variazione di segnale
Monitoraggio delle uscite con prova dinamica senza rilevamento dei cortocircuiti (I/O multipli)	90%
Monitoraggio incrociato delle uscite e dei risultati intermedi della logica di controllo (L) e monitoraggio software (temporale e logico) del flusso del programma e rilevamento dei guasti statici e dei cortocircuiti (I/O multipli)	99%
Monitoraggio indiretto (ad esempio il monitoraggio con interruttori di pressione, monitoraggio elettrico del posizionamento degli attuatori)	Da 0% a 99% a seconda dell'applicazione
Monitoraggio diretto (ad esempio il monitoraggio elettrico del posizionamento delle valvole di controllo, monitoraggio dei dispositivi elettromeccanici per mezzo di contatti azionati meccanicamente)	99%

Tabella 2.4: Stime di coperture diagnostiche di dispositivi di output, normativa ISO 13849-1.

2.3 Cause comuni di guasto

I canali appartenenti ad un sottosistema, siano essi canali funzionali o di test, possono subire un guasto contemporaneamente tramite una delle cause comune di guasto, definite anche CCF (dall'inglese Common Cause Failures).

Le cause comuni di guasto riducono i miglioramenti di performance di un sottosistema, in termini di affidabilità, dovuti all'introduzione della ridondanza e/o della diagnostica. L'effetto più consistente è presente nei sistemi a più canali funzionali ma è presente anche nei sistemi a canale singolo dotati

di diagnostica, perché il canale di test è in grado di portare il sistema in uno stato sicuro.

Per poter valutare le cause comuni di guasto è necessario considerare che ogni canale avrà un proprio tasso di guasto pericoloso indipendente dalle cause comuni di guasto, ovvero che comprende nel suo valore anche quei guasti avvenuti per le cause comuni. Le cause comuni di guasto avranno quindi un tasso di guasto pericoloso che sarà pari ad una frazione dei tassi di guasto dei canali in questione, in particolare è necessario escludere dal computo tutti quei guasti di un canale che non causano guasti anche all'altro canale. Per considerare correttamente le cause comuni di guasto all'interno di un sistema è necessaria un'opportuna modellazione delle stesse, che verrà discussa in seguito.

Per avere una stima del tasso di guasto dovuto a cause comuni può essere utilizzato il modello a fattore beta (β). Il modello non possiede una precisione elevata ma può essere utilizzato con il supporto degli standard IEC 61508, IEC 62061 ed ISO 13849.

In questo modello, nel caso di architettura composta da due canali funzionali, definiti come A e B, il tasso di guasto dovuto a cause comuni è stimato essere il prodotto tra il fattore delle cause comuni, β, ed il minimo tra i tassi di guasto pericolosi dei due canali.

Il tasso di guasto pericoloso utilizzato per ogni canale funzionale esclude alcuni guasti, definiti "soft", che sono guasti lievi e non in grado di causare un guasto dovuto a causa comune. Nei pedici dei tassi di guasto è indicato quanto descritto come "soft-free".

Da quanto descritto, per la stima del tasso di guasto dovuto a cause comuni tra due canali funzionali A e B, è utilizzata la seguente equazione:

$$\lambda_{CC} = \beta * min(\lambda_{AD,soft-free}, \lambda_{BD,soft-free}) \quad (2.10)$$

Analogamente si possono applicare le stesse considerazioni per stimare il tasso di guasto dovuto a cause comuni nel caso di sistema composto da un canale funzionale F ed un canale di monitor M:

$$\lambda_{CC} = \beta * min(\lambda_{FD,soft-free}, \lambda_{MD,soft-free}) \quad (2.11)$$

L'utilizzo nelle precedenti equazioni del minor tasso di guasto tra i due canali è spiegato nella seguente Figura 2.8, che prende come esempio una architettura a due canali funzionali, A e B, e con asimmetria nei tassi di guasto tra i due canali:

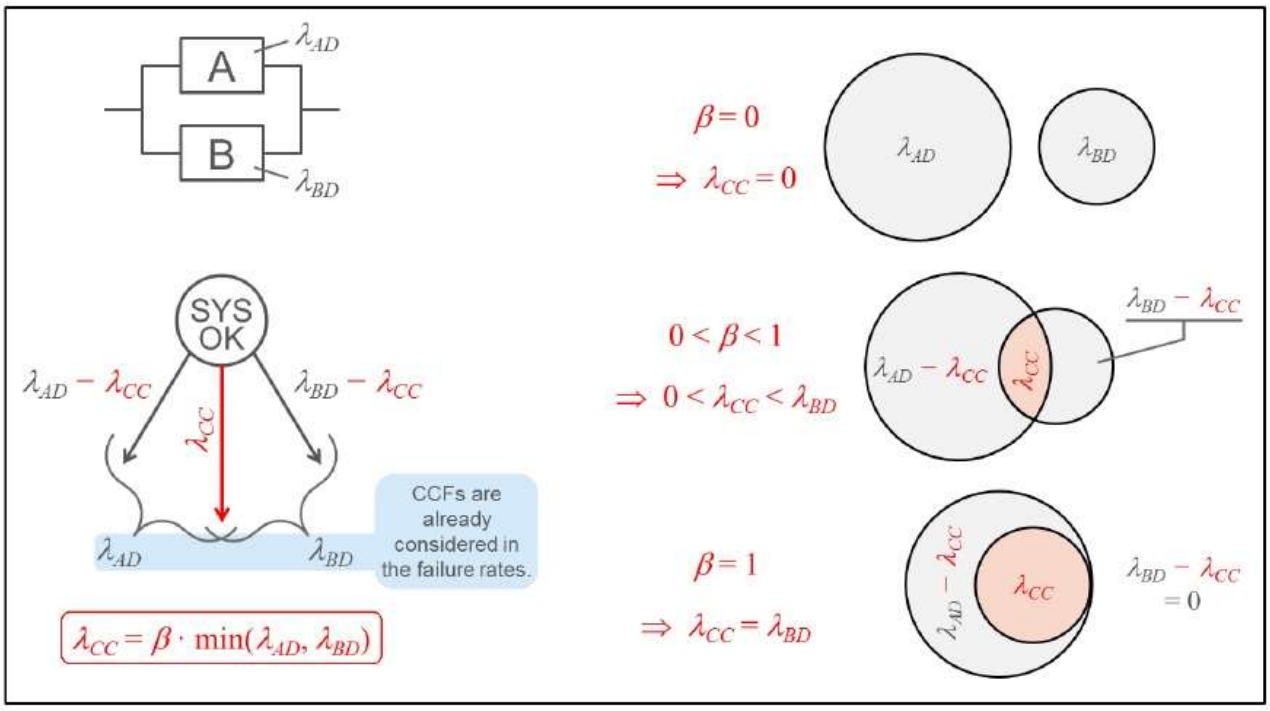


Figura 2.8: Cause comuni di guasto analizzate con modello a fattore β, con asimmetria.

La considerazione di base è l'assunzione che la combinazione fisica dei canali A e B non causi un incremento dei loro tassi di guasto pericoloso individuali, in altre parole non è presente effetto mutuale.

Le cause comuni di guasto sono già considerate nei rispettivi tassi di guasto, λ_{AD} e λ_{BD}. Il concetto è descritto nella parte sinistra della Figura 2.8, dove vengono rappresentate delle transizioni di un generico modello di Markov che evidenziano la scomposizione dei due tassi di guasto originari, λ_{AD} e λ_{BD}, includendo le cause comuni di guasto ed ottenendo tre tassi:

- λ_{CC}: tasso di guasto dovuto a cause comuni,
- $(\lambda_{AD} - \lambda_{CC})$: tasso di guasto indipendente del canale A, che esclude la componente dovuta alle cause comuni di guasto,
- $(\lambda_{BD} - \lambda_{CC})$: tasso di guasto indipendente del canale B, che esclude la componente dovuta alle cause comuni di guasto.

Il fattore β è adimensionale ed è compreso tra zero ed uno ($0 \leq \beta \leq 1$). Nella parte destra della Figura 2.8 sono rappresentati tutti i casi possibili, relativamente al valore assunto da β:

- $\beta = 0$: non sono presenti cause comuni di guasto, il tasso di guasto relativo è pertanto pari a zero ($\lambda_{CC} = 0$),
- $0 < \beta < 1$: è presente una certa incidenza delle cause comuni di guasto, il tasso di guasto relativo sarà maggiore di zero e minore del minor tasso di guasto tra i due canali, in questo caso minore del tasso di guasto del canale B ($0 < \lambda_{CC} < \lambda_{BD}$),
- $\beta = 1$: è presente la massima incidenza possibile delle cause comuni di guasto, il tasso relativo sarà pari al minor tasso di guasto dei due canali, in questo caso sarà pari al tasso di guasto del canale B ($\lambda_{CC} = \lambda_{BD}$).

Ogni caso è rappresentato in Figura 2.8 con l'ausilio di un diagramma di Venn. Generalmente, in essi, è rappresentata la probabilità di un evento e non il tasso: si può ottenere un diagramma di Venn convenzionale semplicemente moltiplicando ogni tasso per lo stesso intervallo di tempo generico Δt.

Si può notare che, anche nel caso estremo dove $\beta = 1$, l'equazione per il tasso di guasto per cause comuni, λ_{CC}, che è mostrata anche nella parte in basso a sinistra della Figura 2.8, assicura sempre la presenza di valori di tassi di guasto indipendenti.

In questo caso i tassi di guasto indipendenti, $(\lambda_{AD} - \lambda_{CC})$ e $(\lambda_{BD} - \lambda_{CC})$, saranno sempre maggiori o uguali a zero e quindi non negativi, che sarebbero assurdi.

Nell'applicazione pratica del modello a fattore beta per le cause comuni di guasto in genere si può considerare il tasso di guasto "soft-free" pari al tasso di guasto pericoloso di ogni canale presente, considerando ciò come una semplificazione cautelativa.

Per la quantificazione di β, nelle normative ISO 13849-1 ed IEC 62061, si può utilizzare una tabella che descrive un metodo euristico, basato su un giudizio ingegneristico, per valutare se nel sistema di sicurezza sono state adottate un numero sufficiente di misure contro i CCF. Se così è, allora si può presumere che il valore della frazione di guasti di causa comune sia minore o uguale al 2%. In genere, per portare a risultati più cautelativi e tendenti dal lato della sicurezza si considera $\beta = 2\%$.

Nella seguente tabella sono elencate una serie di misure contro i CCF e dei valori numerici ad essi associati. Ad ogni misura contenuta nella lista può essere associato solo il valore riportato o il valore zero (se una misura è solo parzialmente adottata il valore ad essa associato è zero).

Se alla fine della verifica di ogni si ottiene un valore complessivo pari o maggiore di 65, su un massimo di 100, allora si possono considerare le misure adottate contro i CCF come sufficienti e si può ritenere che la frazione di CCF sia minore o uguale al 2%, viceversa se il valore complessivo è inferiore a 65 è necessario adottare ulteriori misure.

Utilizzando la ISO 13849-1 non è possibile analizzare un sistema di sicurezza con un fattore beta maggiore del 2%, mentre utilizzando la IEC 62061 è possibile procedere considerando un valore maggiore dello stesso, ottenuto in caso di misure non sufficienti. In ogni caso, anche utilizzando la IEC 62061, si tende a non procedere nell'analisi con un fattore beta maggiore di 2% ed adottare ulteriori misure contro i CCF.

In seguito sono riportate due tabelle, la Tabella 2.5 serve per quantificare le misure contro i CCF adottate e la Tabella 2.6 è utilizzata per la quantificazione del fattore beta, partendo dal dato ricavato con la tabella precedente:

	Misure contro i CCF	Valore
1	**Separazione/segregazione**	
	Separazione fisica tra i percorsi dei segnali, ad esempio: • Separazione nel percorso dei cavi /tubature; • Rilevamento di cortocircuiti o circuiti aperti.	15
2	**Diversità**	
	Utilizzo di differenti tecnologie o processi fisici, ad esempio: • Attivazione della funzione di sicurezza diversa per ogni canale (elettronica, elettronica programmabile o elettromeccanica); • Componenti di costruttori diversi.	20
3	**Progetto/applicazione/esperienza**	
3.1	Protezione contro sovratensioni, sovracorrenti, sovrapressioni, sovratemperature ecc.	15
3.2	Uso di componenti ben provati.	5
4	**Valutazione/analisi**	
	Per ogni funzione di sicurezza è condotta una FMEA per evitare CCF.	5
5	**Competenza/addestramento**	
	Addestramento dei progettisti per comprendere le cause e le conseguenze dei CCF.	5
6	**Misure contro le influenze ambientali**	
6.1	Protezione dalla contaminazione (polveri, liquidi, sporco) e dai disturbi elettromagnetici, per i sistemi elettrici/elettronici.	25
6.2	Requisiti per l'immunità da altre influenze ambientali (temperature, urti, vibrazioni, umidità), secondo quanto riportato nelle norme applicabili.	10
	Totale massimo raggiungibile	**100**

Tabella 2.5: Quantificazione delle misure contro i CCF.

Totale raggiunto	Valutazione delle misure contro i CCF
65 o superiore	Misure sufficienti (la frazione di CCF per il canale di un sistema di sicurezza è minore o uguale al 2%
Inferiore a 65	Misure insufficienti, ne devono essere adottate di ulteriori

Tabella 2.6: Valutazione del fattore beta in base alle misure contro i CCF.

2.4 Dispositivi soggetti a wearout

Quando il guasto di un dispositivo è determinato essenzialmente dal già discusso wearout, il suo tasso di guasto ha un andamento crescente nel tempo. Potrebbe essere utile poter assegnare ad uno di questi dispositivi soggetti a wearout un tasso di guasto costante, ad esempio per poter utilizzare i modelli di Markov che non sono in grado di gestire tassi di guasto che cambiano nel tempo.

Le normative IEC 62061 e ISO 13849-1 hanno un approccio pragmatico per ottenere un tasso di guasto costante che si basa sulla seguente ipotesi: l'utilizzo dell'elemento soggetto a wearout è limitato al periodo precedente alla forte fase di usura alla fine della sua vita utile.

Viene calcolato, per il dispositivo, un tasso di guasto surrogato e costante, come approssimazione del tasso di guasto risultante nella fase di utilizzo limitato. Il calcolo è descritto nella ISO 13849-1 ed è riportato in seguito.

Il valore B_{10} rappresenta il numero di cicli di lavoro dopo i quali il 10% degli elementi ha subito un guasto pericoloso. È specificato che il dispositivo soggetto a wearout non opererà per più di un numero di cicli pari a B_{10D}, pertanto, quando un dispositivo raggiungerà tale numero di cicli di lavoro, sarà sostituito.

La durata di un ciclo corrisponde al reciproco della frequenza di operazione n_{op} ed il tempo T_{10D} sarà il tempo impiegato da un elemento per compiere un numero di cicli pari a B_{10D}. La relazione è la seguente, considerando un generico elemento E:

$$T_{10D,E} = \frac{B_{10D,E}}{n_{op}} \tag{2.12}$$

Il tasso di guasto pericoloso surrogato dell'elemento E, definito come λ_{ED}, è assunto costante nel tempo e deve essere definito nell'istante di tempo $T_{10D,E}$. Come da definizione la probabilità di guasto pericoloso in tale istante di tempo è del 10%, quindi si ricava la seguente espressione di inaffidabilità:

$$1 - e^{-\lambda_{ED} T_{10D,E}} = \frac{1}{10} \tag{2.13}$$

Risolvendo l'equazione precedente ed isolando λ_{ED}, si ottiene:

$$\lambda_{ED} = \frac{1}{T_{10D,E}} ln \frac{10}{9} \approx \frac{1}{10\, T_{10D,E}} \tag{2.14}$$

Dalle precedenti equazioni 2.12 e 2.14 si ricava la seguente espressione di λ_{ED}:

$$\lambda_{ED} = \frac{n_{op}}{10\, B_{10D,E}} \tag{2.15}$$

A causa del λ_{ED}, assunto costante nel tempo, il $MTTF_{D,E}$ surrogato dell'elemento E è il suo reciproco:

$$MTTF_{D,E} = \frac{10\, B_{10,D,E}}{n_{op}} \tag{2.16}$$

2.5 IEC 62061

La IEC 62061, come già detto, è una delle due norme di sicurezza funzionale per i macchinari, l'altra è la ISO 13849-1.

La norma è derivata dalla IEC 61508 ed è destinata ai costruttori di macchine. Essa ha lo scopo di facilitare la specificazione delle prestazioni dei sistemi di controllo elettrico di sicurezza in relazione ai pericoli significativi delle macchine.

La IEC 62061 specifica i requisiti per la progettazione, l'integrazione e la convalida dei sistemi di sicurezza elettrici, elettronici e sistemi di controllo elettrici programmabili; chiamati sistemi di controllo elettrici legati alla sicurezza o SCS (dall'inglese Safety Control System).

In questa norma, l'affidabilità di una funzione di sicurezza è misurata, come già illustrato, in SIL. È presente una procedura per assegnare un SIL richiesto alla funzione di sicurezza, che utilizza una matrice di rischio. La procedura è descritta in seguito:

Si procede con la determinazione della classe di rischio, prodotta dalla somma di tra parametri: durata, probabilità ed evitabilità dell'evento indesiderato. Nelle seguenti tabelle, per ogni parametro appena citato, è presente una correlazione tra un valore quantitativo o qualitativo dello stesso ed un valore numerico, compreso tra 1 e 5, che indica il punteggio da considerare per il calcolo della classe di rischio. Il numero 5 indica le condizioni peggiori mentre il numero 1 quelle migliori.

Frequenza dell'esposizione	Durata esposizione <= 10 min	Durata esposizione > 10 min
$F \geq 1/ora$	5	5
$1/giorno \leq F < 1/ora$	4	5
$2/settimana \leq F < 1/giorno$	3	4
$1/anno \leq F < 2/settimana$	2	3
$F < 1/anno$	1	2

Tabella 2.7: Valutazione della durata (D).

Probabilità di accadimento	(P)
Molto alta	5
Probabile	4
Possibile	3
Scarsa	2
Trascurabile	1

Tabella 2.8: Valutazione della probabilità di accadimento (P).

Evitabilità o limitazione	(E)
Impossibile	5
Possibile	3
Probabile	1

Tabella 2.9: Valutazione dell'evitabilità (E).

La classe di rischio, essendo la somma dei tre parametri D, P ed E, sarà pertanto un valore numerico compreso tra 3 e 15. Ad esso deve essere correlato un ulteriore parametro: la gravità (G), compresa tra 1 e 4 in base alle conseguenze dell'evento indesiderato, classificate qualitativamente:

Conseguenze	Gravità	Classe				
		3-4	5-7	8-10	11-13	14-15
Irreversibile: morte o perdita di un braccio o di un occhio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Irreversibile: rottura di uno o più arti, perdita di dita	3		Altre misure	SIL 1	SIL 2	SIL 3
Reversibile: richiede l'intervento di un medico	2			Altre misure	SIL 1	SIL 2
Reversibile: richiede cure di un pronto soccorso	1				Altre misure	SIL 1

Tabella 2.10: Valutazione del SIL richiesto tramite la matrice del rischio (IEC 62061).

Si può notare che, nella sicurezza dei macchinari, non sono presenti situazioni di alcun tipo che richiedano una riduzione del rischio maggiore di SIL 3. Una riduzione di rischio maggiore può essere richiesta in alcuni processi che introducono delle magnitudo maggiori della morte di una singola persona, che è indicata nella IEC 62061 come conseguenza di gravità massima (4).

La normativa IEC 62061 ha sviluppato un approccio semplificato per la stima della probabilità di guasti pericolosi e fornisce formule che possono essere utilizzate per i sottosistemi realizzati a partire da elementi di sottosistema di bassa complessità o da elementi di sottosistema complessi.

Le formule sono di per sé una semplificazione della teoria dell'analisi dell'affidabilità ed hanno lo scopo di fornire stime che sono orientate verso la direzione più sicura.

La normativa introduce quattro differenti architetture per la descrizione dei sottosistemi di sicurezza, denominate come architettura A, B, C e D.

L'**architettura A** (1oo1) è a canale singolo senza diagnostica, ogni guasto pericoloso di un elemento causa la perdita della funzione di sicurezza. Non è presente copertura diagnostica ($DC = 0$) e la tolleranza di guasto hardware è pari a zero ($HFT = 0$).

L'architettura è rappresentata nella seguente Figura 2.9: il sottosistema di sicurezza è formato da un numero n di elementi in serie tra loro: è sufficiente il guasto di uno di essi per rendere il sottosistema non più in grado di eseguire la funzione di sicurezza.

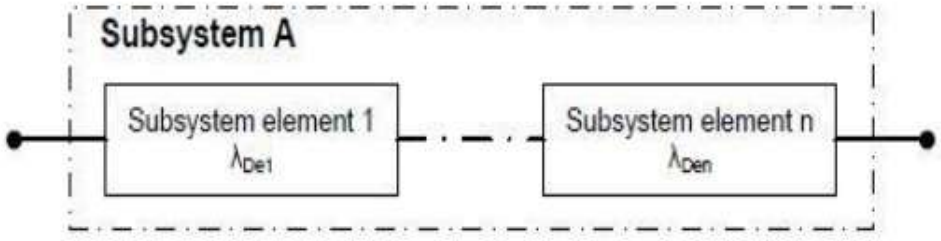


Figura 2.9: Architettura A nella normativa IEC 62061.

Il PFH_D è dato dalla somma dei tassi di guasto pericolosi di tutti gli elementi del sottosistema, essendo essi collegati in serie:

$$PFH_D = \lambda_{De1} + \ldots + \lambda_{Den} \tag{2.17}$$

L'**architettura B** (1oo2) è a due canali senza diagnostica, un singolo guasto pericoloso di uno qualsiasi dei due elementi non causa la perdita della funzione di sicurezza. Non è presente copertura diagnostica ($DC = 0$) e la tolleranza di guasto hardware è pari ad uno ($HFT = 1$).

L'architettura è rappresentata nella seguente Figura 2.10: il sistema di sicurezza è formato da due elementi in parallelo tra loro: la funzione di sicurezza non può essere eseguita dal sistema solo nel caso in cui entrambi gli elementi siano guasti. Per considerare le cause comuni di guasto, che vengono aggiunte a parte e che quindi devono essere sottratte ai tassi di guasto dei singoli elementi, viene rappresentato in serie un ulteriore blocco:

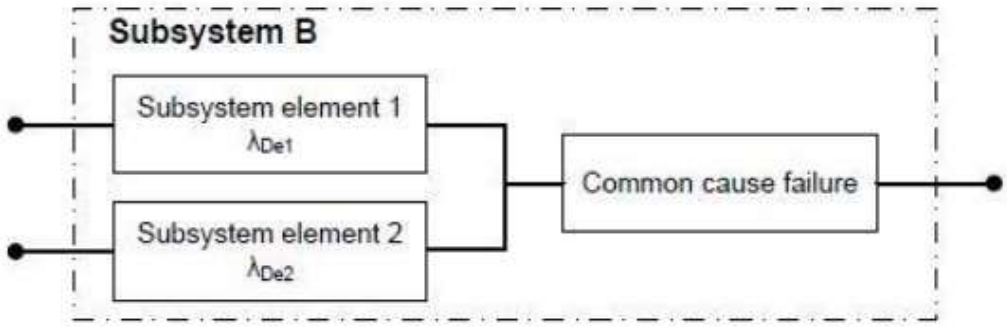


Figura 2.10: Architettura B nella normativa IEC 62061.

La formula per il calcolo del PFH_D è la seguente:

$$PFH_D = [(1-\beta)^2(\lambda_{De1} \cdot \lambda_{De2} \cdot T_1)] + [\beta(\lambda_{De1} + \lambda_{De2})/2] \tag{2.18}$$

Sono descritti in seguito i parametri presenti nell'equazione 2.18:

- T_1 è il tempo più piccolo tra l'intervallo di prova e la vita utile. La vita utile è il tempo minore tra il T_{10D} e 20 anni,
- β è il fattore di suscettibilità ai guasti di causa comune,
- λ_{De1} è il tasso di guasto pericoloso dell'elemento e1,
- λ_{De2} è il tasso di guasto pericoloso dell'elemento e2.

L'**architettura C** (1oo1D) è a canale singolo con diagnostica, qualsiasi guasto pericoloso non rilevato di un elemento causa la perdita della funzione di sicurezza. In questo caso è presente copertura diagnostica ($0 < DC < 1$) e la tolleranza di guasto hardware è pari a zero ($HFT = 0$). Quando viene rilevato un guasto di un elemento la funzione diagnostica avvia una reazione al guasto.

È un'architettura difficile da analizzare, per via del guasto della funzione diagnostica, chiamata funzione di gestione dei guasti, mentre il canale funzionale è ancora in funzione. La funzione di gestione dei guasti comprende sia la funzione di rilevamento dei guasti (chiamata TE, dall'inglese Test Equipment) che la funzione di reazione ai guasti (chiamata OTE, dall'inglese Output of the Test Equipment).

L'architettura è rappresentata nella seguente Figura 2.11: il sistema di sicurezza è formato da n elementi in serie tra loro: è sufficiente il guasto di uno di essi per rendere il sistema non più in grado di eseguire la funzione di sicurezza:

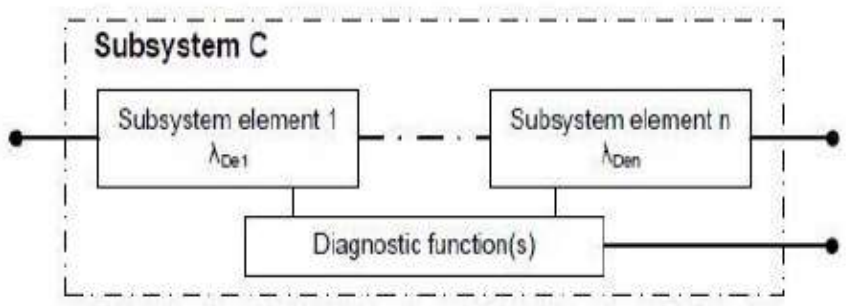


Figura 2.11: Architettura C nella normativa IEC 62061.

Il PFH_D, nel caso in cui la funzione di diagnostica sia fornita da un dispositivo esterno al sistema di sicurezza, è dato dalla somma dei tassi di guasto pericolosi dei singoli elementi, essendo essi collegati in serie. Bisogna considerare esclusivamente i guasti pericolosi che non rientrano nella copertura diagnostica applicando un fattore moltiplicativo pari a $(1 - DC)$:

$$PFH_D = (1 - DC_1)\lambda_{De1} + \ldots + (1 - DC_n)\lambda_{Den} \quad (2.19)$$

Il PFH_D, nel caso in cui il sottosistema necessiti di un dispositivo che si occupi di portare il macchinario in uno stato sicuro, necessita del computo anche dell'affidabilità di questo dispositivo. L'equazione presente è la seguente:

$$PFH_D = \lambda_{De} - DC[\lambda_{De} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})] \cdot [1 - \frac{1}{2} \cdot (\lambda_{D\,FH} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})T_1)] \quad (2.20)$$

Sono descritti in seguito i parametri presenti nell'equazione 2.20:

- T_1 è il tempo più piccolo tra l'intervallo di prova e la vita utile. La vita utile è il tempo minore tra il T_{10D} e 20 anni,
- β è il fattore di suscettibilità ai guasti di causa comune,
- λ_{De} è il tasso di guasto pericoloso dell'elemento e, che esegue la funzione di sicurezza,
- $\lambda_{D\,FH}$ è il tasso di guasto pericoloso dell'elemento che si occupa della reazione alla rilevazione dei guasti,

- DC è la copertura diagnostica dell'elemento e.

L'equazione 2.20 è soggetta a dei vincoli di applicazione. Se sono tutti rispettati o se al massimo uno di essi non è rispettato l'equazione è utilizzabile. I vincoli sono i seguenti:

- $\beta \leq 2\%$,
- $DC \leq 99\%$,
- $1/\lambda_{De} \leq 1\,000\ anni$,
- Il $MTTF_{D\,FH}$, ovvero il reciproco di $\lambda_{D\,FH}$, deve avere un certo valore minimo, dipendente dalla copertura diagnostica. I valori minimi sono indicati nella seguente Tabella 2.11:

DC	Valore minimo di $\frac{1}{\lambda_{D\,FH}}$ [anni]
$60\% \leq DC < 65\%$	44
$65\% \leq DC < 70\%$	59
$70\% \leq DC < 75\%$	100
$75\% \leq DC < 80\%$	170
$80\% \leq DC < 85\%$	300
$85\% \leq DC < 90\%$	550
$90\% \leq DC < 95\%$	1200
$95\% \leq DC \leq 99\%$	5900

Tabella 2.11: Valori minimi di applicabilità dell'equazione 2.20, in termini di $1/\lambda_{F\,DH}$.

L'**architettura D** (1oo2D) è a due canali con diagnostica, un singolo guasto pericoloso di uno qualsiasi dei due elementi non causa la perdita della funzione di sicurezza. In questo caso è presente copertura diagnostica ($0 < DC < 1$) e la tolleranza di guasto hardware è pari ad uno ($HFT = 1$).

Quando viene rilevato un guasto di un elemento la funzione diagnostica, o le funzioni diagnostiche, avviano una funzione di reazione ai guasti.

L'architettura è rappresentata nella seguente Figura 2.12: il sistema di sicurezza è formato da due elementi in parallelo tra loro:

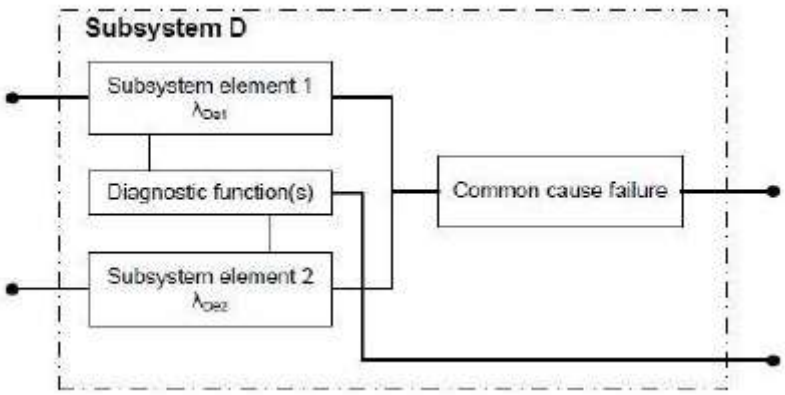


Figura 2.12: Architettura D nella normativa IEC 62061.

La formula per il calcolo del PFH_D è la seguente:

$$PFH_D = (1-\beta)^2[\lambda_{De1}\lambda_{De2}(DC_1 + DC_2)\frac{T_2}{2} + \lambda_{De1}\lambda_{De2}(2 - DC_1 - DC_2)\frac{T_1}{2}] + \beta\frac{\lambda_{De1} + \lambda_{De2}}{2} \quad (2.21)$$

Sono descritti in seguito i parametri presenti nell'equazione 2.21:

- T_1 è il tempo più piccolo tra l'intervallo di prova e la vita utile. La vita utile è il tempo minore tra il T_{10D} e 20 anni,
- T_2 è l'intervallo del test diagnostico,
- β è il fattore di suscettibilità ai guasti di causa comune,
- λ_{De1} è il tasso di guasto pericoloso dell'elemento e1,
- λ_{De2} è il tasso di guasto pericoloso dell'elemento e2,
- DC_1 è la copertura diagnostica dell'elemento e1,
- DC_2 è la copertura diagnostica dell'elemento e2,

Se gli elementi e1 ed e2 sono identici l'equazione può essere semplificata come segue, considerando uguali la copertura diagnostica ed i tassi di guasto pericoloso dei due elementi:

$$PFH_D = (1-\beta)^2[DC \cdot T_2 + (1 - DC) \cdot T_1]{\lambda_{De}}^2 + \beta\lambda_{De} \quad (2.22)$$

Nell'applicazione della IEC 62061 è necessario considerare i **vincoli di architettura**, esplicitati dalla seguente tabella, che fornisce il massimo SIL raggiungibile per un sottosistema di sicurezza, in base alla sua frazione di guasti sicuri ed alla sua tolleranza al guasto hardware:

Frazione di guasti sicuri (SFF)	Tolleranza al guasto hardware (HFT)		
	0	1	2
$SFF < 60\%$	Non permesso (SIL 1 se componenti ben provati)	SIL 1	SIL 2
$60\% \leq SFF < 90\%$	SIL 1	SIL 2	SIL 3
$90\% \leq SFF < 99\%$	SIL 2	SIL 3	SIL 3
$SFF \geq 99\%$	SIL 3	SIL 3	SIL 3

Tabella 2.12: Massimo SIL raggiungibile per vincoli di architettura.

2.6 ISO 13849-1

La norma ISO 13849-1, come già detto, è l'altra normativa che tratta l'affidabilità dei sistemi di sicurezza delle macchine. Il campo di applicazione è legato alle parti dei sistemi di comando legate alla sicurezza, ovvero alle SRP/CS (dall'inglese Safety-Related Partes of Control System), definite dalla norma come parte del sistema di controllo che risponde a segnali di ingresso legati alla

sicurezza e genera segnali in uscita anch'essi legati alla sicurezza.

Lo scopo della norma è di fornire una guida alla progettazione e valutazione dei sistemi di comando con funzioni di sicurezza da integrare in sistemi di protezione volti alla riduzione del rischio. La valutazione di tali SRP/CS si basa sulla loro capacità di eseguire la funzione di sicurezza in condizioni prevedibili, come già stabilito si definiscono i cinque livelli di prestazione (PL).

Il primo passo che il progettista deve compiere consiste nella stima del rischio, la quale si effettua su tre parametri: severità della lesione, frequenza e/o tempo di esposizione al pericolo e possibilità di evitare il pericolo. Una volta effettuata la stima del rischio si stabilisce il livello di performance richiesto che deve raggiungere il sistema di sicurezza al quale si sta ricorrendo per ridurre il rischio stimato. Questo livello di affidabilità richiesto sarà tanto maggiore quanto maggiore è il rischio che il sistema di sicurezza deve ridurre.

La procedura per la determinazione del livello di performance richiesto è euristica e consiste nell'assegnazione di valori qualitativi ai tre parametri considerati:

- S: severità della lesione, può assumere i seguenti valori:
  - S1: lesione leggera e generalmente reversibile,
  - S2: lesione grave e generalmente irreversibile o morte;
- F: frequenza e/o tempo di esposizione al pericolo, può assumere i seguenti valori:
  - F1: esposizione al pericolo da rara a infrequente e/o di breve durata,
  - F2: esposizione al pericolo da frequente a continua e/o di lunga durata;
- P: possibilità di evitare il pericolo o di limitarne il danno, può assumere i seguenti valori:
  - P1: possibile evitare il pericolo o limitarne il danno, in condizioni specifiche,
  - P2: scarsamente possibile evitare il pericolo o limitarne il danno.

L'esperienza mostra che tali parametri possono essere combinati, come mostrato nella seguente Figura 2.13, in modo da fornire una scala di classificazione del rischio. Il dato ottenuto da questa analisi è il PL richiesto:

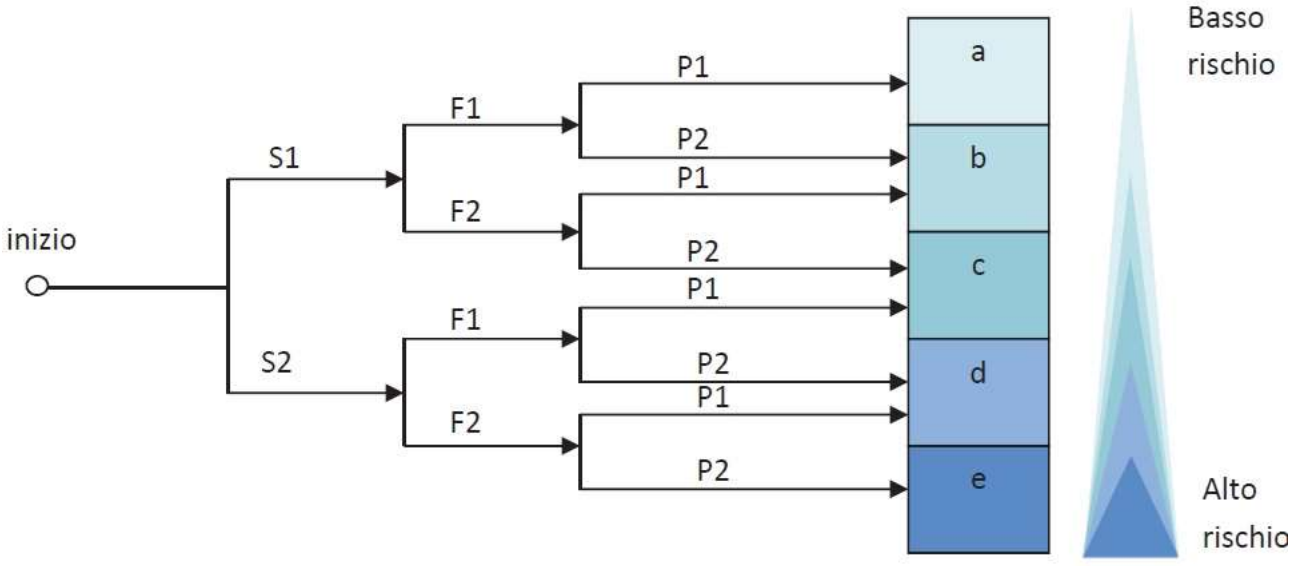


Figura 2.13: Determinazione del PL richiesto nella normativa ISO 13849-1.

La normativa fornisce ulteriori indicazioni sulla determinazione dei tre parametri necessari.

Per stimare la severità della lesione è necessario tenere in conto le conseguenze degli incidenti ed i normali processi di guarigione (ad esempio lividi e lacerazioni senza complicazioni possono essere classificati come S1 mentre la morte o le amputazioni sono classificate come S2).

Il parametro F deve essere scelto valutando la frequenza e la durata dell'accesso al pericolo. F2 dovrebbe essere scelta se una persona è esposta al rischio frequentemente o in maniera continua. È irrilevante se ad essere esposti al rischio sono una persona soltanto o persone diverse in tempi successivi. Se è necessario avvicinarsi regolarmente al macchinario ad ogni ciclo di lavoro per caricare o movimentare il pezzo in lavorazione allora dovrebbe essere scelta la frequenza F2. Se non vi sono altre informazioni e la frequenza è più alta di una volta ogni 15 minuti allora deve essere scelta la frequenza F2. F1 può essere scelta se il tempo di esposizione cumulativo non supera 1/20 del tempo totale di funzionamento e la frequenza non è più alta di una volta ogni 15 minuti.

Il parametro P è utilizzato per discriminare i casi in cui una situazione pericolosa può essere riconosciuta prima di aver causato danno ed essere evitata. Quando si presenta la situazione pericolosa, se c'è una possibilità reale di evitare il rischio o di limitarne gli effetti, allora deve essere scelto P1, altrimenti deve essere scelto P2. L'esposizione ad un certo pericolo può essere identificata direttamente da alcune caratteristiche fisiche, oppure si può ricorrere a strumenti appositi in grado di riconoscere tali caratteristiche fisiche. Tra i fattori da considerare durante la scelta del parametro P vi sono la velocità con cui il pericolo si presenta, la possibilità di evitare il pericolo (ad esempio allontanandosi), l'addestramento e la capacità dell'operatore e la presenza o meno di supervisione durante il lavoro.

La normativa ISO 13849-1 stabilisce, per la suddivisione dei sottosistemi di sicurezza in categorie, una classificazione qualitativa della copertura diagnostica, rappresentata nella seguente Tabella 2.13:

Livello di copertura diagnostica	Range di copertura diagnostica (DC)
Nulla	$DC < 60\%$
Bassa	$60\% \leq DC < 90\%$
Media	$90\% \leq DC < 99\%$
Alta	$99\% \leq DC$

Tabella 2.13: Livello di copertura diagnostica.

Vengono in seguito descritte le cinque categorie descritte dalla normativa ISO 13849-1, che vengono identificate come categoria B, 1, 2, 3 e 4.

La **categoria B** ha le seguenti caratteristiche:

- Copertura diagnostica nulla ($DC < 60\%$),
- Sistema a singolo canale funzionale,
- Utilizzo di principi di sicurezza collaudati,
- Massimo livello di performance raggiungibile: $PL = b$.

La seguente Figura 2.14 rappresenta un sistema di sicurezza appartenente alla categoria B tramite un diagramma, introducendo i seguenti blocchi:

- Elemento di input, definito come I (ad esempio un sensore),
- Elemento di unità logica, definito come L (ad esempio un'unità logica di sicurezza),
- Elemento di output, definito come O (ad esempio un teleruttore),
- Vengono definite inoltre, come i_m, le interconnessioni tra diversi blocchi. Sono rappresentate da frecce.

Figura 2.14: Categoria B nella normativa ISO 13849.

La **categoria 1** ha le seguenti caratteristiche:

- Copertura diagnostica nulla ($DC < 60\%$),
- Sistema a singolo canale funzionale,
- Utilizzo dei principi di sicurezza collaudati, gli stessi utilizzati nella categoria B,
- Utilizzo di componenti collaudati,
- Massimo livello di performance raggiungibile: $PL = c$.

L'utilizzo di componenti collaudati consente alla categoria 1 della ISO 13849-1 di corrispondere all'architettura A descritta dalla IEC 62061 e rappresentata in Figura 2.9. La categoria B, a differenza della categoria 1, non fornisce performance sufficienti per la corrispondenza appena descritta.

La seguente Figura 2.15 rappresenta un sistema di sicurezza appartenente alla categoria 1 tramite un diagramma a blocchi. Il diagramma corrisponde a quello utilizzato per la categoria B.

Figura 2.15: Categoria 1 nella normativa ISO 13849.

La **categoria 2** ha le seguenti caratteristiche:

- Copertura diagnostica bassa o media ($60\% \leq DC < 99\%$),
- Sistema a singolo canale funzionale,
- Utilizzo di principi di sicurezza collaudati, gli stessi utilizzati nella categoria B,

- Massimo livello di performance raggiungibile: $PL = d$.

La categoria 2 della ISO 13849-1 corrisponde all'architettura C descritta dalla IEC 62061 e rappresentata in Figura 2.11.

La seguente Figura 2.16 rappresenta un sistema di sicurezza appartenente alla categoria 2 tramite un diagramma, introducendo i seguenti blocchi, in aggiunta ai diagrammi relativi alle categorie B e 1:

- Elemento di test, definito come TE (rappresenta il canale di monitor),
- Elemento di output del canale di test, definito come OTE,
- Vengono definite inoltre, con la lettera m , le connessioni di monitoraggio, che rappresentano le possibilità di rilevazione di un guasto. Sono rappresentate da frecce tratteggiate ed indicano il monitoraggio di tutti gli elementi: di input, l'unità logica e di output.

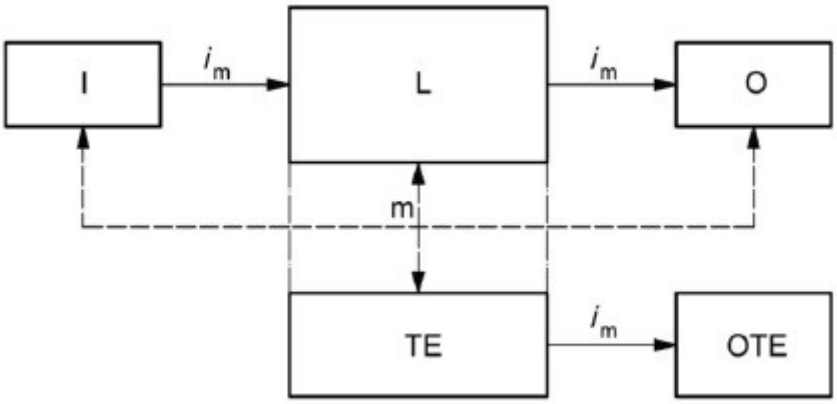


Figura 2.16: Categoria 2 nella normativa ISO 13849.

La **categoria 3** ha le seguenti caratteristiche:

- Copertura diagnostica bassa o media ($DC \geq 60\%$),
- Sistema a due canali funzionali,
- Utilizzo di principi di sicurezza collaudati, gli stessi utilizzati nella categoria B,
- Un guasto non causa la perdita della capacità di eseguire la funzione di sicurezza,
- Massimo livello di performance raggiungibile: $PL = e$.

La categoria 3 della ISO 13849 corrisponde all'architettura D descritta dalla IEC 62061 e rappresentata in Figura 2.12.

La seguente Figura 2.17 rappresenta un sistema di sicurezza appartenente alla categoria 3 tramite un diagramma. Dal diagramma relativo alla categoria 2, rappresentato in Figura 2.16, differisce per i seguenti punti:

- Sono presenti due elementi di input, definiti come $I1$ ed $I2$,
- Sono presenti due elementi di unità logica, definiti come $L1$ ed $L2$,
- Sono presenti due elementi di output, definiti come $O1$ ed $O2$,

- Viene definita inoltre, con la lettera c, la connessione di monitoraggio mutuale che è presente tra i due canali funzionali. Ogni canale funzionale esegue la diagnostica all'altro canale. È rappresentata da una freccia tratteggiata.
- Sono presenti, rappresentate tramite frecce tratteggiate e con la lettera m, delle ulteriori connessioni che indicano il monitoraggio, tra gli elementi di unità logica ed i rispettivi elementi di output.

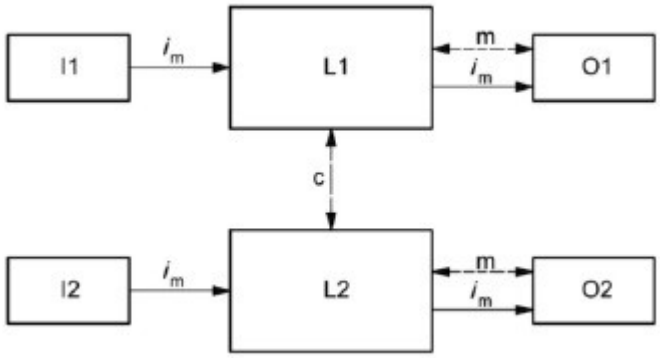


Figura 2.17: Categoria 3 nella normativa ISO 13849.

La **categoria 4** ha le caratteristiche della categoria 3, con le seguenti differenze:

- Copertura diagnostica alta ($DC \geq 99\%$),
- Massimo livello di performance raggiungibile: $PL = e$.

Anche la categoria 4 della ISO 13849-1 corrisponde, come la categoria 3, all'architettura D descritta dalla IEC 62061 e rappresentata in Figura 2.12.

La seguente Figura 2.18 rappresenta un sistema di sicurezza appartenente alla categoria 4 tramite un diagramma a blocchi. Il diagramma corrisponde a quello utilizzato per la categoria 3 con una differenza: le frecce utilizzate per rappresentare i monitoraggi sono continue anziché tratteggiate, questo semplicemente per evidenziare che la copertura diagnostica è più alta rispetto alla categoria 3:

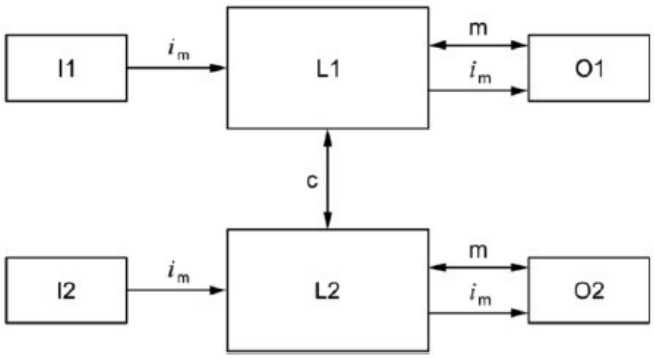


Figura 2.18: Categoria 4 nella normativa ISO 13849.

Non è presente, nella normativa ISO 13849, alcuna categoria corrispondente all'architettura B descritta nella IEC 62061 e rappresentata in Figura 2.10.

Per il calcolo del PFH_D, nella normativa ISO 13849-1, si deve procedere utilizzando la seguente

tabella, considerando un tempo di missione di 20 anni ed un fattore beta delle cause comuni di guasto pari a 2%.

L'utilizzo della tabella è molto semplice: è necessario incrociare il $MTTF_D$ di ogni canale, attraverso la scelta opportuna della riga, con la scelta opportuna della colonna, stabilita in base alla categoria di appartenenza del sottosistema di sicurezza (B, 1, 2, 3 o 4), sempre considerando la copertura diagnostica DC come già descritto (nulla, bassa, media o alta). Per le categorie B, 1, 2 e 3 il limite di $MTTF_D$ considerato è pari a 100 anni mentre, per la categoria 4, è pari a 2500 anni.

Viene riportata, nella seguente Figura 2.19, la tabella da utilizzare:

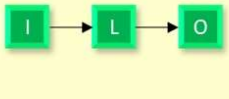
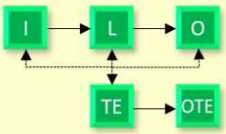
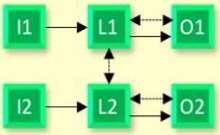
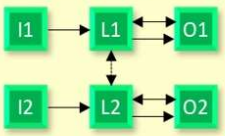
$MTTF_d$ per ogni canale (Anni)	Probabilità di guasto pericoloso all'ora PFH_d [1/h] e livello di Performance Level (PL)								$MTTF_d$ > 100 anni per ogni canale (Anni)
									
	Cat. B PL	Cat. 1 PL	Cat. 2 PL	Cat. 2 PL	Cat. 3 PL	Cat. 3 PL	Cat. 4 PL	Cat. 4 PL	
	DC_{avg} = none (DC < 60%)	DC_{avg} = none (DC < 60%)	DC_{avg} = low (60%≤ DC<90%)	DC_{avg} = med. (90%≤ DC<99%)	DC_{avg} = low (60%≤ DC<90%)	DC_{avg} = med. (90%≤ DC<99%)	DC_{avg} = high (DC≥99%)	DC_{avg} = high (DC≥99%)	
3	$3{,}80 \times 10^{-5}$ a		$2{,}58 \times 10^{-5}$ a	$1{,}99 \times 10^{-5}$ a	$1{,}26 \times 10^{-5}$ a	$6{,}09 \times 10^{-6}$ b		$2{,}23 \times 10^{-8}$ e	110
3.3	$3{,}46 \times 10^{-5}$ a		$2{,}33 \times 10^{-5}$ a	$1{,}79 \times 10^{-5}$ a	$1{,}13 \times 10^{-5}$ a	$5{,}41 \times 10^{-6}$ b		$2{,}03 \times 10^{-8}$ e	120
3.6	$3{,}17 \times 10^{-5}$ a		$2{,}13 \times 10^{-5}$ a	$1{,}62 \times 10^{-5}$ a	$1{,}03 \times 10^{-5}$ a	$4{,}86 \times 10^{-6}$ b		$1{,}87 \times 10^{-8}$ e	130
3.9	$2{,}93 \times 10^{-5}$ a		$1{,}95 \times 10^{-5}$ a	$1{,}48 \times 10^{-5}$ a	$9{,}37 \times 10^{-6}$ b	$4{,}40 \times 10^{-6}$ b		$1{,}61 \times 10^{-8}$ e	150
4.3	$2{,}65 \times 10^{-5}$ a		$1{,}76 \times 10^{-5}$ a	$1{,}33 \times 10^{-5}$ a	$8{,}39 \times 10^{-6}$ b	$3{,}89 \times 10^{-6}$ b		$1{,}50 \times 10^{-8}$ e	160
4.7	$2{,}43 \times 10^{-5}$ a		$1{,}60 \times 10^{-5}$ a	$1{,}20 \times 10^{-5}$ a	$7{,}58 \times 10^{-6}$ b	$3{,}48 \times 10^{-6}$ b		$1{,}33 \times 10^{-8}$ e	180
5.1	$2{,}24 \times 10^{-5}$ a		$1{,}47 \times 10^{-5}$ a	$1{,}10 \times 10^{-5}$ a	$6{,}91 \times 10^{-6}$ b	$3{,}15 \times 10^{-6}$ b		$1{,}19 \times 10^{-8}$ e	200
5.6	$2{,}04 \times 10^{-5}$ a		$1{,}33 \times 10^{-5}$ a	$9{,}87 \times 10^{-6}$ b	$6{,}21 \times 10^{-6}$ b	$2{,}80 \times 10^{-6}$ c		$1{,}08 \times 10^{-8}$ e	220
6.2	$1{,}84 \times 10^{-5}$ a		$1{,}19 \times 10^{-5}$ a	$8{,}80 \times 10^{-6}$ b	$5{,}53 \times 10^{-6}$ b	$2{,}47 \times 10^{-6}$ c		$9{,}81 \times 10^{-9}$ e	240
6.8	$1{,}68 \times 10^{-5}$ a		$1{,}08 \times 10^{-5}$ a	$7{,}93 \times 10^{-6}$ b	$4{,}98 \times 10^{-6}$ b	$2{,}20 \times 10^{-6}$ c		$8{,}67 \times 10^{-9}$ e	270
7.5	$1{,}52 \times 10^{-5}$ a		$9{,}75 \times 10^{-6}$ b	$7{,}10 \times 10^{-6}$ b	$4{,}45 \times 10^{-6}$ b	$1{,}95 \times 10^{-6}$ c		$7{,}76 \times 10^{-9}$ e	300
8.2	$1{,}39 \times 10^{-5}$ a		$8{,}87 \times 10^{-6}$ b	$6{,}43 \times 10^{-6}$ b	$4{,}02 \times 10^{-6}$ b	$1{,}74 \times 10^{-6}$ c		$7{,}04 \times 10^{-9}$ e	330
9.1	$1{,}25 \times 10^{-5}$ a		$7{,}94 \times 10^{-6}$ b	$5{,}71 \times 10^{-6}$ b	$3{,}57 \times 10^{-6}$ b	$1{,}53 \times 10^{-6}$ c		$6{,}44 \times 10^{-9}$ e	360
10	$1{,}14 \times 10^{-5}$ a		$7{,}18 \times 10^{-6}$ b	$5{,}14 \times 10^{-6}$ b	$3{,}21 \times 10^{-6}$ b	$1{,}36 \times 10^{-6}$ c		$5{,}94 \times 10^{-9}$ e	390
11	$1{,}04 \times 10^{-5}$ a		$6{,}44 \times 10^{-6}$ b	$4{,}53 \times 10^{-6}$ b	$2{,}81 \times 10^{-6}$ c	$1{,}18 \times 10^{-6}$ c		$5{,}38 \times 10^{-9}$ e	430
12	$9{,}51 \times 10^{-6}$ b		$5{,}84 \times 10^{-6}$ b	$4{,}04 \times 10^{-6}$ b	$2{,}49 \times 10^{-6}$ c	$1{,}04 \times 10^{-6}$ c		$4{,}91 \times 10^{-9}$ e	470
13	$8{,}78 \times 10^{-6}$ b		$5{,}33 \times 10^{-6}$ b	$3{,}64 \times 10^{-6}$ b	$2{,}23 \times 10^{-6}$ c	$9{,}21 \times 10^{-7}$ d		$4{,}52 \times 10^{-9}$ e	510
15	$7{,}61 \times 10^{-6}$ b		$4{,}53 \times 10^{-6}$ b	$3{,}01 \times 10^{-6}$ b	$1{,}82 \times 10^{-6}$ c	$7{,}44 \times 10^{-7}$ d		$4{,}11 \times 10^{-9}$ e	560
16	$7{,}31 \times 10^{-6}$ b		$4{,}21 \times 10^{-6}$ b	$2{,}77 \times 10^{-6}$ c	$1{,}67 \times 10^{-6}$ c	$6{,}76 \times 10^{-7}$ d		$3{,}70 \times 10^{-9}$ e	620
18	$6{,}34 \times 10^{-6}$ b		$3{,}68 \times 10^{-6}$ b	$2{,}37 \times 10^{-6}$ c	$1{,}41 \times 10^{-6}$ c	$5{,}67 \times 10^{-7}$ d		$3{,}37 \times 10^{-9}$ e	680
20	$5{,}71 \times 10^{-6}$ b		$3{,}26 \times 10^{-6}$ b	$2{,}06 \times 10^{-6}$ c	$1{,}22 \times 10^{-6}$ c	$4{,}85 \times 10^{-7}$ d		$3{,}05 \times 10^{-9}$ e	750
22	$5{,}19 \times 10^{-6}$ b		$2{,}93 \times 10^{-6}$ c	$1{,}82 \times 10^{-6}$ c	$1{,}07 \times 10^{-6}$ c	$4{,}21 \times 10^{-7}$ d		$2{,}79 \times 10^{-9}$ e	820
24	$4{,}76 \times 10^{-6}$ b		$2{,}65 \times 10^{-6}$ c	$1{,}62 \times 10^{-6}$ c	$9{,}47 \times 10^{-7}$ d	$3{,}70 \times 10^{-7}$ d		$2{,}51 \times 10^{-9}$ e	910
27	$4{,}23 \times 10^{-6}$ b		$2{,}32 \times 10^{-6}$ c	$1{,}39 \times 10^{-6}$ c	$8{,}04 \times 10^{-7}$ d	$3{,}10 \times 10^{-7}$ d		$2{,}28 \times 10^{-9}$ e	1000
30		$3{,}80 \times 10^{-6}$ b	$2{,}06 \times 10^{-6}$ c	$1{,}21 \times 10^{-6}$ c	$6{,}94 \times 10^{-7}$ d	$2{,}65 \times 10^{-7}$ d	$9{,}54 \times 10^{-8}$ e	$2{,}07 \times 10^{-9}$ e	1100
33		$3{,}46 \times 10^{-6}$ b	$1{,}85 \times 10^{-6}$ c	$1{,}06 \times 10^{-6}$ c	$5{,}94 \times 10^{-7}$ d	$2{,}30 \times 10^{-7}$ d	$8{,}57 \times 10^{-8}$ e	$1{,}90 \times 10^{-9}$ e	1200
36		$3{,}17 \times 10^{-6}$ b	$1{,}67 \times 10^{-6}$ c	$9{,}39 \times 10^{-7}$ d	$5{,}16 \times 10^{-7}$ d	$2{,}01 \times 10^{-7}$ d	$7{,}77 \times 10^{-8}$ e	$1{,}75 \times 10^{-9}$ e	1300
39		$2{,}93 \times 10^{-6}$ c	$1{,}53 \times 10^{-6}$ c	$8{,}40 \times 10^{-7}$ d	$4{,}53 \times 10^{-7}$ d	$1{,}78 \times 10^{-7}$ d	$7{,}11 \times 10^{-8}$ e	$1{,}51 \times 10^{-9}$ e	1500
43		$2{,}65 \times 10^{-6}$ c	$1{,}37 \times 10^{-6}$ c	$7{,}34 \times 10^{-7}$ d	$3{,}87 \times 10^{-7}$ d	$1{,}54 \times 10^{-7}$ d	$6{,}37 \times 10^{-8}$ e	$1{,}42 \times 10^{-9}$ e	1600
47		$2{,}43 \times 10^{-6}$ c	$1{,}24 \times 10^{-6}$ c	$6{,}49 \times 10^{-7}$ d	$3{,}35 \times 10^{-7}$ d	$1{,}34 \times 10^{-7}$ d	$5{,}76 \times 10^{-8}$ e	$1{,}26 \times 10^{-9}$ e	1800
51		$2{,}24 \times 10^{-6}$ c	$1{,}13 \times 10^{-6}$ c	$5{,}80 \times 10^{-7}$ d	$2{,}93 \times 10^{-7}$ d	$1{,}19 \times 10^{-7}$ d	$5{,}26 \times 10^{-8}$ e	$1{,}13 \times 10^{-9}$ e	2000
56		$2{,}04 \times 10^{-6}$ c	$1{,}02 \times 10^{-6}$ c	$5{,}10 \times 10^{-7}$ d	$2{,}52 \times 10^{-7}$ d	$1{,}03 \times 10^{-7}$ d	$4{,}73 \times 10^{-8}$ e	$1{,}03 \times 10^{-9}$ e	2200
62		$1{,}84 \times 10^{-6}$ c	$9{,}06 \times 10^{-7}$ d	$4{,}43 \times 10^{-7}$ d	$2{,}13 \times 10^{-7}$ d	$8{,}84 \times 10^{-8}$ e	$4{,}22 \times 10^{-8}$ e	$9{,}85 \times 10^{-10}$ e	2300
68		$1{,}68 \times 10^{-6}$ c	$8{,}17 \times 10^{-7}$ d	$3{,}90 \times 10^{-7}$ d	$1{,}84 \times 10^{-7}$ d	$7{,}68 \times 10^{-8}$ e	$3{,}80 \times 10^{-8}$ e	$9{,}44 \times 10^{-10}$ e	2400
75		$1{,}52 \times 10^{-6}$ c	$7{,}31 \times 10^{-7}$ d	$3{,}40 \times 10^{-7}$ d	$1{,}57 \times 10^{-7}$ d	$6{,}62 \times 10^{-8}$ e	$3{,}41 \times 10^{-8}$ e	$9{,}06 \times 10^{-10}$ e	2500
82		$1{,}39 \times 10^{-6}$ c	$6{,}61 \times 10^{-7}$ d	$3{,}01 \times 10^{-7}$ d	$1{,}35 \times 10^{-7}$ d	$5{,}79 \times 10^{-8}$ e	$3{,}08 \times 10^{-8}$ e		
91		$1{,}25 \times 10^{-6}$ c	$5{,}88 \times 10^{-7}$ d	$2{,}61 \times 10^{-7}$ d	$1{,}14 \times 10^{-7}$ d	$4{,}94 \times 10^{-8}$ e	$2{,}74 \times 10^{-8}$ e		
100		$1{,}14 \times 10^{-6}$ c	$5{,}28 \times 10^{-7}$ d	$2{,}29 \times 10^{-7}$ d	$1{,}01 \times 10^{-7}$ d	$4{,}29 \times 10^{-8}$ e	$2{,}47 \times 10^{-8}$ e		

Figura 2.19: Tabella per la valutazione del PFH_D secondo la normativa ISO 13849-1.

Si può notare che, nell'applicazione della normativa ISO 13849-1, i vincoli di architettura sono già presenti all'interno della tabella e non è necessaria, pertanto, una loro apposita definizione, presente nella IEC 62061.

Nella tabella, per valori di $MTTF_D$ compresi tra due di essi presenti, si considera il valore di $MTTF_D$ presente in tabella minore, in via conservativa.

Nell'utilizzo della tabella per sottosistemi appartenenti alla categoria 2, ovvero per sistemi a singolo canale monitorato, non è presente, nel risultato, alcuna dipendenza dal tasso di guasto pericoloso del canale di monitor perché esso non è considerato nel computo.

La normativa ISO 13849-1, tuttavia, specifica che la tabella è utilizzabile se è rispettata la seguente condizione, per quanto concerne la categoria 2: il $MTTF_D$ del canale di monitor deve essere maggiore della metà del $MTTF_D$ del canale funzionale.

Il vincolo di utilizzo equivale, in termini di λ_D, alla condizione che il λ_D del canale di monitor sia minore rispetto al doppio del λ_D del canale funzionale.

3. Analisi dei sistemi di sicurezza con il modello di Markov

Viene ricavato, nei seguenti capitoli 4 e 5, un set di equazioni per il calcolo del PFH_D, relativo alle funzioni di sicurezza facenti parte della modalità di operazione ad alta richiesta e per diverse architetture di sottosistema. Il procedimento descritto è contenuto nel documento intitolato "Calcolo del PFH_D delle funzioni di sicurezza dei macchinari basato sul modello di Markov", pubblicato da Michael Dorra[14] il 30 giugno 2017 e verrà dettagliatamente analizzato e commentato.

Per ricavare il set di equazioni si utilizza una modellazione basata sul modello di Markov e si utilizzano alcune particolari assunzioni, che verranno descritte in seguito, dopo aver introdotto le principali motivazioni del loro sviluppo, che hanno spinto l'autore a ricercare una soluzione alternativa alle due normative per il calcolo del PFH_D.

3.1 Motivazioni dello sviluppo delle equazioni per il calcolo del PFH_D

Gli standard IEC 62061 e ISO 13849-1 forniscono delle Indicazioni riguardanti la sicurezza funzionale dei macchinari. Essi richiedono che la probabilità di guasto sia determinata per ogni funzione di sicurezza, quindi richiedono una stima quantitativa del valore del PFH_D.

Come descritto, le due normative assistono gli utilizzatori nell'accertamento del PFH_D in modalità differenti:

- La normativa IEC 62061 fornisce equazioni per il calcolo del PFH_D. L'approccio utilizzato ha l'inconveniente di non poter affrontare i sistemi a canale singolo testati ad un livello avanzato di analisi e produce, in alcuni casi, dei risultati molto conservativi per i sistemi a due canali testati.
- La normativa ISO 13849-1 impone l'utilizzo di tabelle. L'approccio utilizzato manca di flessibilità a causa della specificazione del tempo di missione T_M e del fattore β. Comporta inoltre una sovrastima del PFH_D nel caso di sistemi asimmetrici a due canali.

I metodi impiegati nei due standard, inoltre, portano ad avere come risultato differenti valori del PFH_D.

L'obiettivo delle equazioni per il calcolo del PFH_D presentate e derivate in seguito è di raggiungere soluzioni più flessibili, ottenute con la tecnica di modellazione più precisa, relativamente al problema oggetto di analisi.

Le equazioni per il PFH_D che verranno ottenute portano da buone a molto buone riproduzioni dei valori in tabella stabiliti dalla ISO 13849-1 ed in alcuni casi particolari assumono la forma delle equazioni già contenute nella IEC 62061. Possono essere considerate pertanto come un ulteriore sviluppo di entrambi gli standard.

[14] Michael Dorra è un matematico tedesco. Ha pubblicato il documento "Markov model-based calculation of the PFHD of safety functions for machines: derivation of a set of PFHD equations for typical machine control subsystem architectures", dal quale sono derivati l'analisi con il modello di Markov ed il set di equazioni.

I modelli di Markov, che sono tra gli strumenti considerati idonei nella normativa IEC 61508, sono stati selezionati come metodo di analisi per le architetture studiate per i seguenti motivi:

- Rendono le equazioni derivabili, a differenza dei metodi numerici, come ad esempio la simulazione Montecarlo.
- Hanno una buona gestione dei processi di guasto con influenza mutuale e del reinserimento dei sistemi riparati, in confronto ad altri strumenti come i diagrammi a blocchi di affidabilità (RBD).

Il modello di Markov, come già descritto, presenta un inconveniente: è in grado di gestire solamente i processi con transizioni di stato distribuite esponenzialmente e quindi con tassi di transizione costanti.

Per consentire di ottenere una coerenza metodica complessiva i casi semplici vengono descritti partendo dai casi più complessi, ovvero sono trattati come dei casi particolari di questi ultimi.

3.2 Assunzioni utilizzate nella modellazione

Nella modellazione utilizzata per lo sviluppo delle equazioni per il calcolo del PFH_D, la richiesta della funzione di sicurezza è alta o continua, infatti il PFH_D è, come già detto, un dato di affidabilità opportuno per sistemi di sicurezza che operano in modalità ad alta richiesta. Nella pratica avviene almeno una richiesta della funzione di sicurezza per anno, quindi è utilizzato un tasso di richiesta, parametro che indica quante volte viene richiesta la funzione di sicurezza nell'unità di tempo e denominato r_d (dall'inglese Demand Rate), che rispetta la seguente relazione: $r_d \geq 1\ anno^{-1}$.

È presente un'implementazione delle funzioni di sicurezza con una disposizione in serie logica comprendente sottosistemi discreti, il quale numero può essere ridotto ad uno.

Riguardo i canali vengono utilizzate le seguenti ipotesi:

- Per modellare un sottosistema sono utilizzate le seguenti architetture:
  - Sistema non testato a canale singolo (1oo1),
  - Sistema testato a canale singolo (1oo1D),
  - Sistema non testato a due canali (1oo2),
  - Sistema testato a due canali (1oo2D).
- I canali funzionali hanno il compito di eseguire la funzione di sicurezza quando richiesto oppure in modo continuo. Nell'architettura 1oo2D sono presenti due canali funzionali che si occupano, oltre che dell'esecuzione della funzione di sicurezza, anche della diagnostica, relativamente all'altro canale. La perdita dell'abilità di eseguire la funzione di sicurezza è descritta come un guasto pericoloso del canale funzionale.
- I canali di test si occupano della diagnostica di un canale funzionale, lo testano ad intervalli di tempo o in modo continuo. La perdita della funzione di test non interferisce con l'esecuzione della funzione di sicurezza, tuttavia, è descritta come un guasto pericoloso perché costituisce una delle situazioni meno favorevoli, in termini di sicurezza.
- I canali costituiti da più elementi collegati logicamente in serie, siano essi funzionali o di test, hanno un tasso di guasto pericoloso che sarà la sommatoria dei tassi di guasto pericoloso di ogni elemento appartenente al canale.

Per quanto riguarda i tassi di guasto, nella modellazione utilizzata, sono valide le seguenti assunzioni:

- I tassi di guasto sicuri vengono ignorati, ovvero non si considerano, nel computo di un tasso di guasto, tutte le tipologie di guasto che portano ad eventi non pericolosi. Questa semplificazione permette di ricavare modelli ed equazioni più semplici e previene un accrescimento indesiderato, in termini matematici, del PFH_D, causato da guasti non riguardanti la sicurezza.
- I tassi di guasto pericoloso dei canali sono costanti nel tempo. Il tempo medio al guasto pericoloso è uguale al reciproco del tasso di guasto pericoloso ($MTTF_D = 1/\lambda_D$).
- Per ottenere un tasso di guasto pericoloso costante anche negli elementi soggetti a wearout, si utilizza la procedura riportata nella ISO 13849-1 e già illustrata in modo dettagliato precedentemente. Si utilizza pertanto il tasso di guasto surrogato $\lambda_{ED} = \frac{n_{op}}{10\, B_{10\ ,E}} = \frac{1}{10\, T_{10D,E}}$, considerando che gli elementi in questione non opereranno per più di un tempo pari a $T_{10D,E}$.
- La probabilità di guasto pericoloso per ora, quindi il PFH_D, è il valore medio nel tempo dell'intensità di guasto, espressa come la frequenza di richieste insoddisfatte della funzione di sicurezza.
- In un sistema formato da più canali, siano essi funzionali o di test, le cause comuni di guasto ed il loro tasso di guasto relativo, λ_{CC}, vengono analizzate con il modello a fattore β, già approfondito precedentemente.

La riparazione, nella modellazione utilizzata, è assunta come segue:

- La riparazione avviene a seguito di eventi pericolosi oppure a seguito di una rilevazione di guasto per mezzo della diagnostica.
- La riparazione è ideale, perfetta: a seguito di una riparazione ogni canale ed ogni elemento ritornano ad eseguire la loro funzione come in origine. A seguito di una riparazione tutti i tassi di guasto restano uguali a quelli originari.
- Il reciproco del tempo medio di riparazione, ovvero del MRT, ed il reciproco del tempo medio alla riparazione, ovvero del MTTR e definito anche tasso di riparazione μ, sono sostanzialmente maggiori dei tassi di guasto pericolosi del canale.

Sono presenti le seguenti assunzioni riguardo la copertura diagnostica:

- La copertura diagnostica (DC) è definita, come già descritto e relativamente ad un canale od elemento, la percentuale di guasti rilevabile. È implementata come descritto nella normativa IEC 61508, anche relativamente ad un canale composto da più elementi in serie, dove si utilizza la media pesata sui tassi di guasto relativamente ad ogni elemento.
- Dopo una rilevazione di guasto per mezzo della diagnostica segue, come già detto, la riparazione.
- La copertura diagnostica viene implementata ed analizzata solamente per i canali funzionali. La diagnostica per i canali di test, quando presente nel sistema da analizzare, viene ignorata, causando un'approssimazione del PFH_D in favore della sicurezza.

4. Architetture a canale singolo

Sono effettuate, in questo capitolo, analisi relative a sistemi di sicurezza che possiedono un solo canale funzionale. In modo particolare viene analizzata l'architettura che prevede, oltre al canale funzionale, anche un canale di test, utilizzato per l'effettuazione della diagnostica (1oo1D). In seguito, da quanto descritto per l'architettura 1oo1D e con opportune semplificazioni, si ricavano risultati anche per l'architettura ad un canale senza diagnostica (1oo1).

4.1 Modello 1oo1D, introduzione

Il sistema descritto in seguito possiede un canale di test, rappresentato con la lettera M (Monitor), in aggiunta al canale funzionale F. La seguente Figura 4.1 mostra il corrispondente diagramma a blocchi con alcune delle variabili impiegate. A queste ultime deve essere aggiunto il tasso di richiesta

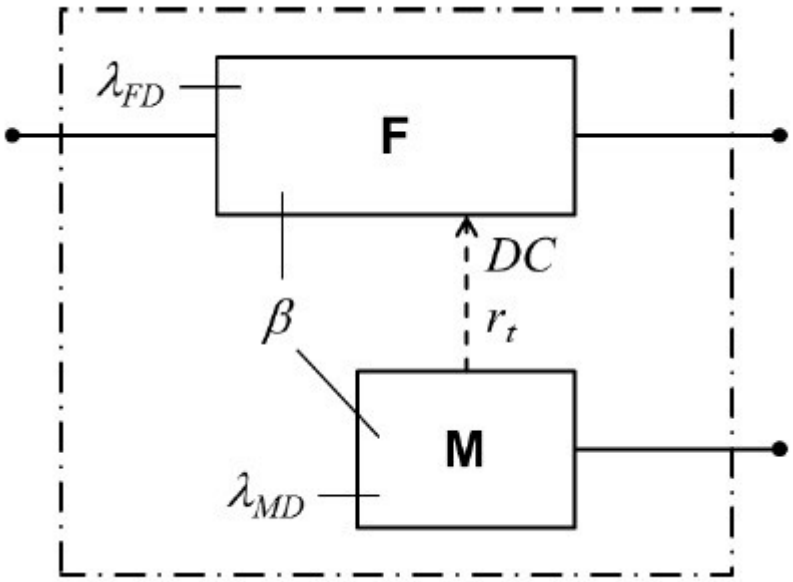


Figura 4.1: Sistema a canale singolo testato (1oo1D).

della funzione di sicurezza (r_d) ed il tempo di missione (T_M):
Il canale funzionale F esegue la funzione di sicurezza ed ha un tasso di guasto pericoloso definito come λ_{FD}.

Il canale di test, definito come M e chiamato anche canale di monitor, effettua dei test al canale F, con una copertura diagnostica DC ed un tasso di test, parametro che indica quanti test vengono effettuati nell'unità di tempo, pari a r_t. Il canale di test ha un tasso di guasto pericoloso definito come λ_{MD}. Nel caso in cui il canale di test rilevi un guasto pericoloso del canale F, il sistema viene portato ad uno stato sicuro dallo stesso. Non è eseguita diagnostica al canale M.

Il sistema è soggetto a richieste regolari della funzione di sicurezza, che avvengono in momenti casuali nel tempo e con un tasso come già detto pari a (r_d). Viene effettuata, come da ipotesi, almeno una richiesta della funzione di sicurezza all'anno.

Vengono introdotte due diverse tipologie di analisi relative ad un sistema 1oo1D, in relazione all'efficienza del test effettuato dal canale di monitor. Sono elencate in seguito, verranno analizzate entrambe e porteranno a diversi risultati in termini di PFH_D:

- Architettura 1oo1D senza test tempo ottimale: è presente una vera e propria corsa contro il tempo tra il test del canale funzionale e la richiesta della funzione di sicurezza: il test è efficace solamente se viene effettuato dopo il guasto del canale funzionale e prima della richiesta della funzione di sicurezza. Se la richiesta della funzione di sicurezza avviene prima del test il canale funzionale non può essere riparato ed il sistema non può essere portato in uno stato sicuro. La funzione di sicurezza richiesta non sarà eseguita ed avverrà pertanto un evento indesiderato.
- Architettura 1oo1D con test tempo ottimale, definito anche TOT (dall'inglese Time-Optimal Testing): il test è molto più frequente della richiesta della domanda della funzione di sicurezza e si può considerare, idealmente, che dopo un guasto avviene sempre un test prima della richiesta della funzione di sicurezza.

L'efficienza di un test verrà analizzata meglio in seguito, tramite un parametro quantitativo definito efficienza del test correlata al tempo, o TRTE (dall'inglese Time Related Test Efficiency).

Un test, anche se eseguito in un intervallo di tempo compreso tra il guasto del canale funzionale e la richiesta della funzione di sicurezza, può risultare inefficace se il guasto occorso al canale funzionale non rientra nella copertura diagnostica.

La seguente Figura 4.2 rappresenta il grafico di transizione degli stati relativo ad un'architettura 1oo1D:

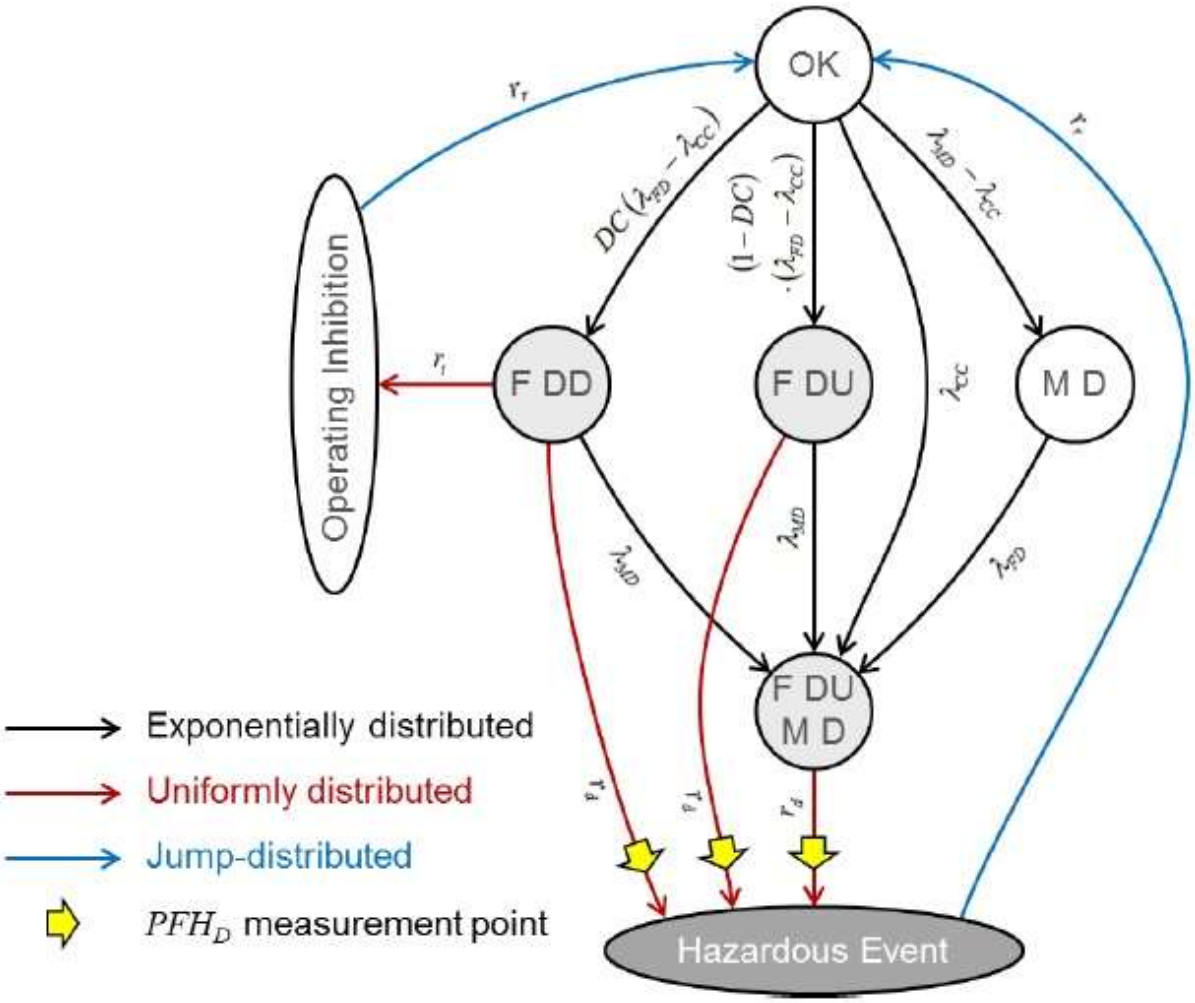


Figura 4.2: Modello di transizione degli stati per un sistema 1oo1D.

Il modello rappresentato in Figura 4.2 è composto da stati, transizioni di stato e punti di misurazione del PFH_D. Ogni entità presente nel modello viene descritta dettagliatamente in seguito.

Le transizioni di stato sono rappresentate da delle frecce e sono caratterizzate da un tasso di transizione e da un colore, che ne indica come è distribuita la probabilità di transizione. In seguito, vengono descritte le tipologie di transizioni di stato presenti nel modello:

- Transizioni di stato dovute a guasti: sono rappresentate in nero e sono distribuite esponenzialmente. I tassi di transizione sono combinazioni dei tassi di guasto presenti nel sistema e della copertura diagnostica.
- Transizioni di stato dovute al test del canale funzionale: sono rappresentate in rosso e sono distribuite uniformemente (distribuzione con densità costante). Hanno un tasso di transizione pari a r_t.
- Transizioni di stato dovute alla richiesta della funzione di sicurezza: sono rappresentate in rosso e sono distribuite uniformemente (distribuzione con densità costante). Hanno un tasso di transizione pari a r_d.
- Transizioni di stato dovute alla riparazione del sistema: sono rappresentate in blu e caratterizzate da una distribuzione a gradino. Hanno un tasso di transizione pari a r_r.

Le distribuzioni non distribuite esponenzialmente rendono impossibile l'analisi tramite il modello di Markov.

Nel modello rappresentato in Figura 4.2 gli stati sono rappresentati da cerchi o ellissi e si suddividono in stati sicuri, stati pericolosi ed uno stato di evento indesiderato. L'evento indesiderato avviene esclusivamente quando viene richiesta la funzione di sicurezza ed il sistema non è in grado di eseguirla. In genere gli stati sono nominati dai guasti in corso nei canali del sistema (gli stati non presenti nella denominazione si intendono funzionanti), dalla tipologia di guasto presente oppure da una condizione particolare nella quale si trova il sistema. Le tipologie di guasto presenti sono due: guasto pericoloso e rilevabile, indicato con DD (dall'inglese Dangerous Detectable) oppure guasto pericoloso e non rilevabile (dall'inglese Dangerous Undetectable).

Gli stati sicuri sono colorati, all'interno della Figura 4.2, in bianco. Sono caratterizzati dal fatto che, se il sistema si trova in uno di essi, non è possibile il verificarsi dell'evento indesiderato con una sola transizione di stato. Gli stati sicuri presenti sono i seguenti:

- Stato "OK": è caratterizzato dall'assenza di qualsiasi tipologia di guasto del sistema. Questo stato è sicuro perché se viene richiesta la funzione di sicurezza il sistema è in grado di eseguirla, evitando l'evento indesiderato. È lo stato inziale di un sistema conforme posto in operazione. Il sistema può raggiungere nuovamente lo stato "OK", da un altro stato, a seguito di una riparazione. Trovandosi nello stato "OK" ed a seguito di un guasto qualsiasi, il sistema abbandona lo stato "OK".
- Stato "Operating Inhibition": è caratterizzato dall'inibizione del macchinario (ad esempio l'arresto dello stesso), che smette di richiedere la funzione di sicurezza, rendendo questo stato uno stato sicuro. A seguito dell'inibizione avviene la riparazione, che riporta il sistema allo stato "OK". Il sistema può trovarsi in questo stato esclusivamente a seguito di un test effettuato dal canale di monitor che rileva un guasto del canale funzionale. Il guasto del canale funzionale deve rientrare nella copertura diagnostica, ovvero deve essere rilevabile, il test deve avvenire prima della richiesta della funzione di sicurezza ed ovviamente il canale di monitor deve essere funzionante.
- Stato "M D": è caratterizzato dal solo guasto pericoloso del canale di monitor. Il canale di monitor, non essendo dotato di diagnostica, può subire esclusivamente guasti non rilevabili, non c'è necessità di distinzione tra rilevabili e non e, pertanto, lo stato è indicato semplicemente come "M D". È uno stato sicuro perché, se viene richiesta la funzione di sicurezza, può essere eseguita correttamente dal canale funzionale, che è funzionante se il sistema si trova in questo stato. Il sistema, pur trovandosi in una condizione abbastanza critica, non può portare all'evento indesiderato se si trova in questo stato. Nell'unico tasso di transizione per questo stato, dallo stato "OK" allo stato "M DU", è escluso dal computo il tasso di guasto per cause comuni, che comprende guasti che portano ad un altro stato: il tasso di transizione è pertanto pari a $\lambda_{MD} - \lambda_{CC}$. Il sistema abbandona questo stato se si verifica un guasto al canale funzionale.

Gli stati pericolosi sono colorati, all'interno della Figura 4.2, in grigio chiaro. Sono caratterizzati dal fatto che, se il sistema si trova in uno di essi, a seguito di una richiesta della funzione di sicurezza, essa non potrà essere eseguita e si verificherà l'evento indesiderato. Gli stati pericolosi presenti hanno in comune la presenza di un guasto al canale funzionale e sono i seguenti:

- Stato “F DD”: indica la presenza esclusiva di un guasto pericoloso e rilevabile del canale funzionale. È uno stato pericoloso perché, se viene richiesta la funzione di sicurezza, il sistema non è in grado di eseguirla, portando all’evento indesiderato. Il sistema può trovarsi in questo stato solamente dallo stato “OK”, con un tasso di transizione che comprende l’esclusione della componente dovuta a guasti da cause comuni e con un fattore moltiplicativo pari alla copertura diagnostica, che serve per comprendere nel computo esclusivamente i guasti rilevabili. Il tasso di transizione, per quanto detto, è pari a $DC(\lambda_{FD} - \lambda_{CC})$. È l’unico stato presente nel modello dove la diagnostica può essere efficace, data la contemporaneità delle due seguenti condizioni: il canale funzionale ha subito un guasto rilevabile ed il canale di monitor è funzionante. Se il sistema si trova in questo stato è presente una vera e propria corsa contro il tempo tra la richiesta della funzione di sicurezza e l’effettuazione di un test. Se avviene prima il test, con tasso di transizione r_t, il sistema viene portato nello stato di inibizione, che, come spiegato precedentemente, è uno stato sicuro. Se avviene prima la richiesta della funzione di sicurezza, con tasso di transizione r_d, si verifica l’evento indesiderato. Il sistema abbandona questo stato anche se si verifica un guasto al canale di monitor.
- Stato “F DU”: indica la presenza di un guasto pericoloso e non rilevabile del canale funzionale. È uno stato pericoloso perché, se viene richiesta la funzione di sicurezza, con tasso di transizione r_d, essa non può essere eseguita e si verifica l’evento indesiderato. Può essere raggiungo dallo stato “OK” a seguito del guasto caratteristico dello stato e nel computo del tasso di transizione vengono sempre escluse le cause comuni di guasto, che portano ad un altro stato, e si considera come fattore moltiplicativo la frazione di guasti che non rientra nella copertura diagnostica. Il tasso di transizione dallo stato “OK” allo stato “F DU” è quindi pari a $(1 - DC)(\lambda_{FD} - \lambda_{CC})$. Il sistema abbandona questo stato anche in seguito ad un guasto al canale di monitor.
- Stato “F DU, M D”: indica la presenza contemporanea nel sistema di un guasto del canale funzionale e di un guasto del canale di monitor. Entrambi i guasti non sono rilevabili: quello del canale funzionale perché il canale di monitor non è funzionante e quello del canale di monitor perché non è dotato di diagnostica. È uno stato pericoloso perché, se viene richiesta la funzione di sicurezza, con tasso di transizione r_d, essa non può essere eseguita e si verifica l’evento indesiderato. Può essere raggiunto direttamente dallo stato “OK” per mezzo delle cause comuni di guasto, con tasso di transizione pari a λ_{CC}, dallo stato “F DD” o “F DU” per mezzo di un guasto al canale di monitor, con tasso λ_{MD} oppure dallo stato “M D” per mezzo di un guasto (rilevabile o non) del canale funzionale, con tasso quindi pari a λ_{FD}.

Lo stato dell’evento indesiderato, denominato “Hazardous Event”, indica l’avvenimento dello stesso ed è rappresentato in Figura 4.2 colorato in grigio scuro. Può essere raggiunto da uno stato nel quale non è operativo il canale funzionale (“F DD”, “F DU” o “F DU, MD”), con delle transizioni di stato, contenenti i punti di misurazione del PFH_D, rappresentate da frecce gialle ed aventi come tasso di transizione r_d. A seguito dell’evento pericoloso avviene una riparazione del sistema di sicurezza, la quale riporta il sistema allo stato “OK” ed ha un tasso di transizione a gradino pari a r_r.

Riassumendo, un sistema completamente funzionante può portare al verificarsi dell’evento indesiderato a seguito di due eventi in sequenza: il guasto del canale funzionale e la richiesta della funzione di sicurezza. Un sistema può tornare completamente funzionante attraverso riparazioni, che avvengono a seguito di un’inibizione o a seguito di un evento indesiderato. Il canale di monitor può rilevare dei guasti del canale funzionale, in particolare i guasti rientranti nella copertura diagnostica, ed inibire il macchinario per evitare il verificarsi di un evento indesiderato. Il guasto del

canale di monitor porta il sistema ad essere in una condizione svantaggiosa: non essendo a sua volta dotato di diagnostica non sarà riparabile fino al verificarsi di un evento indesiderato e non sarà più possibile rilevare guasti al canale funzionale.

4.2 Modello 1oo1D, semplificazione

Per ricavare delle equazioni per il calcolo del PFH_D il più possibili compatte e funzionali è necessario semplificare il modello rappresentato in Figura 4.2, considerando anche che un'eliminazione delle transizioni di stato non distribuite esponenzialmente può consentire l'utilizzo del modello di Markov. Vengono illustrate in seguito le semplificazioni attuate, descritte a step.

Il **primo step** nella semplificazione del modello è rappresentato nella seguente Figura 4.3: vengono uniti gli stati "F DU" ed "F DU, MD", presenti nel modello rappresentato in Figura 4.2, in un unico stato:

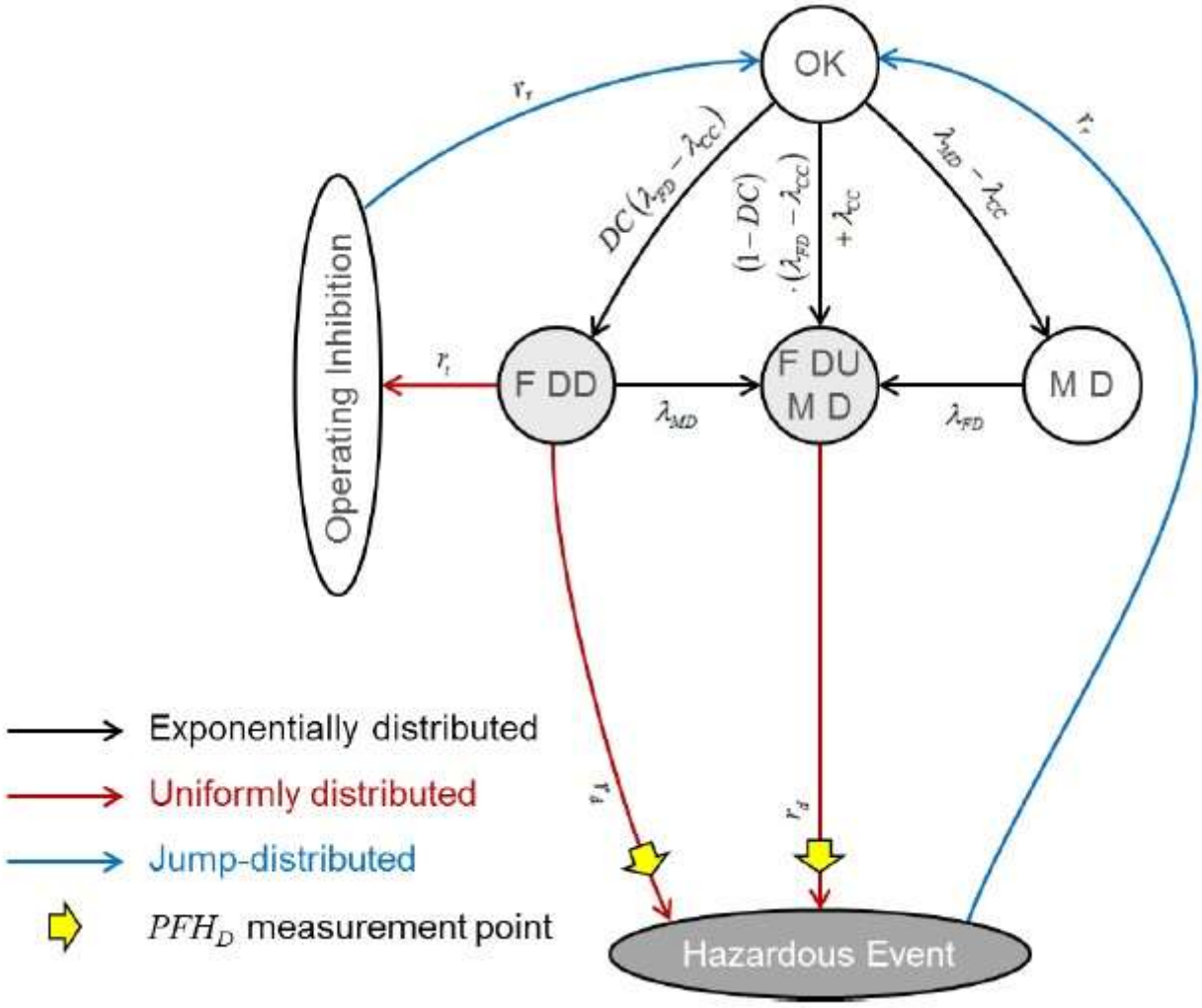


Figura 4.3: Modello 1oo1D, primo step nella semplificazione.

Gli stati oggetto dell'unione, se raggiunti dal sistema, portano al verificarsi dell'evento indesiderato a seguito di una richiesta della funzione di sicurezza, con lo stato "F DU" che può portare il sistema allo stato "F DU, MD" a seguito di un guasto del canale di monitor.

Il funzionamento o meno del canale di monitor è ininfluente per il sistema, se avviene un guasto non rilevabile. Per questo, la transizione che porta il sistema allo stato “F DU, MD” dallo stato “F DU” può essere eliminata e gli stati uniti.

Il tasso di transizione dallo stato “OK” al nuovo stato “F DU, MD” deve essere uguale alla somma dei tassi di transizione, sempre dallo stato “OK”, ai vecchi stati “F DU” ed “F DU, MD”: sarà pertanto pari a $(1 - DC)(\lambda_{FD} - \lambda_{CC}) + \lambda_{CC}$. Dato che i due vecchi stati, escludendo l’unica transizione tra di loro che, come detto, è stata semplificata, portano all’evento indesiderato a seguito della richiesta della funzione di sicurezza, anche il nuovo stato “F DU, MD” avrà una transizione con tasso r_d verso lo stato di evento indesiderato. Vengono riportate, inoltre, le transizioni già presenti, ovvero quelli dagli stati “M D” ed “F DD”, verso il vecchio stato “F DU, MD”, che saranno presenti anche nel nuovo modello.

Questa unione di stati non ha influenza sui flussi passanti per i punti di misurazione del PFH_D, perché la probabilità del nuovo stato “F DU, MD” è uguale alla somma delle probabilità dei vecchi stati “F DU” e “F DU, MD”. Il punto di misurazione di destra nella Figura 4.3 misura lo stesso flusso del punto di destra sommato con quello di mezzo nella configurazione antecedente alla prima semplificazione del modello, riportata in Figura 4.2.

In sostanza vengono uniti due stati che porterebbero in ogni caso alla stessa conseguenza, ovvero all’evento indesiderato. L’avvenimento di un guasto non rilevabile porta il sistema nello stesso stato in cui si trova a seguito del guasto contemporaneo dei canali funzionali e di monitor, sia che avvenga in modo contemporaneo con le cause di guasto comuni, sia passando dal solo guasto rilevabile del canale funzionale e sia passando dal solo guasto del canale di monitor.

Il **secondo step** nella semplificazione consiste nell’unione dello stati indicante l’inibizione e dello stato di evento indesiderato con lo stato “OK”. Vengono trascurate le transizioni di riparazione. l risultato è rappresentato nella seguente Figura 4.4:

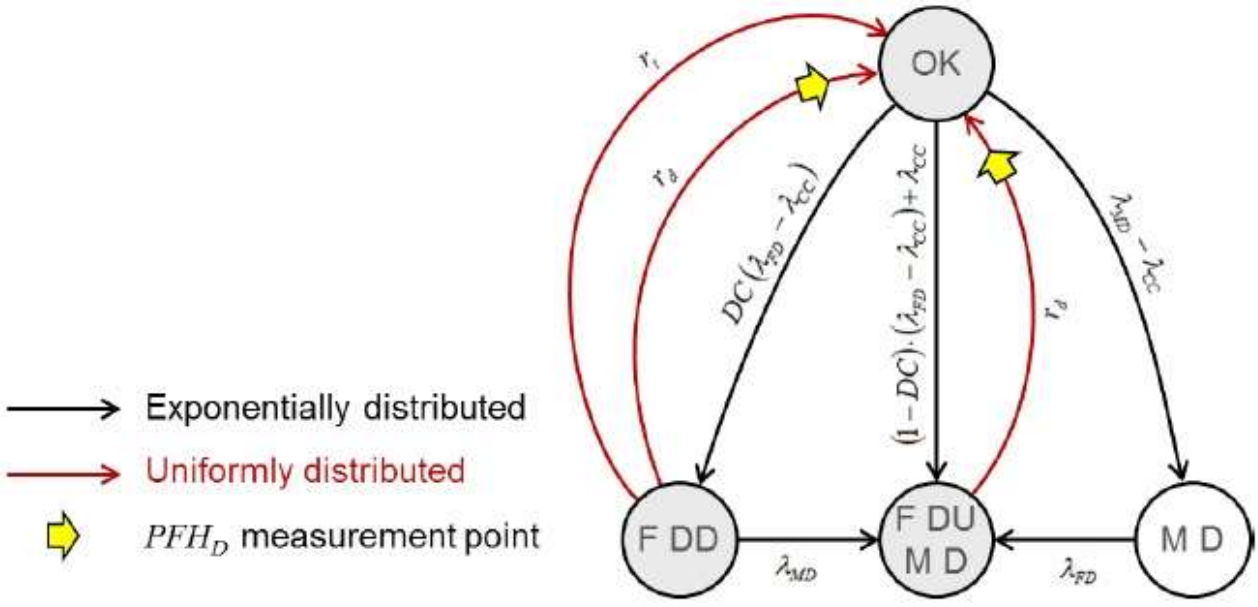


Figura 4.4: Modello 1oo1D, secondo step nella semplificazione.

Nel modello introdotto nel secondo step di semplificazione viene ignorato il tasso di riparazione r_r e quindi il tempo medio alla riparazione MTTR è considerato pari a zero. La riparazione viene considerata istantanea, portando ad essere vuoti gli stati che vengono abbandonati dal sistema a seguito di essa: vengono esclusi dal modello gli stati relativi all'evento indesiderato ed alla inibizione e le transizioni di stato che portavano il sistema in questi stati: nel modello in Figura 4.3 portano direttamente allo stato "OK".

Gli stati eliminati vengono raggiunti dal sistema per via dei guasti dei canali presenti, oltre che per via di test o di richieste della funzione di sicurezza, e gli stessi vengono abbandonati dal sistema in seguito alla riparazione. Si può notare intuitivamente che, come viene dichiarato nel documento di Michael Dorra e dalle assunzioni fatte nel modello, i processi che portano il sistema in tali stati sono molto poco frequenti in relazione ai processi che fanno abbandonare al sistema sempre tali stati. In altre parole, il tasso di riparazione r_r, essendo considerabilmente più elevato di tutti i tassi di guasto presenti nel modello, consente al sistema di non trovarsi quasi mai negli stati "inibizione del macchinario" o "evento indesiderato", che sono degli stati quasi vuoti (il sistema ci transita ma non ci permane per un tempo rilevante) ed in questa semplificazione considerati completamente vuoti ed eliminati dal modello.

Per quanto riguarda la misurazione del PFH_D, tale semplificazione costituisce una piccola stima dalla parte della sicurezza perché, ponendo a zero le probabilità, seppur piccole, che ha il sistema di trovarsi negli stati "inibizione del macchinario" ed "evento indesiderato", viene aumentata, marginalmente la probabilità che ha il sistema di trovarsi nello stato "OK", stato nel quale può, a seguito di transizioni, provocare l'evento indesiderato. Omettere questi stati nel modello provoca pertanto un aumento di flusso nei punti di misurazione del PFH_D che può ritenersi, per quanto detto, solo minimale.

Un effetto secondario della semplificazione è l'eliminazione delle transizioni di stato distribuite a gradino dovute alle riparazioni.

Il **terzo step** nella semplificazione del modello combina le due transizioni parallele dallo stato "F DD" allo stato "OK", presenti in Figura 4.4. Il risultato delle due transizioni è un'unica transizione, con un tasso pari alla somma dei due tassi originari e quindi pari a $r_t + r_d$. Solo le transizioni collegate al tasso di richiesta della funzione di sicurezza (r_d) hanno effetto sulla misura del PFH_D, mentre le transizioni relative al test del canale funzionale (r_t) non ne hanno. Il punto di misurazione del PFH_D deve essere, per quanto detto, pesato, al fine di considerare solo la componente relativa alla domanda della funzione di sicurezza, rispetto a quella totale. Il fattore di peso sarà pertanto pari a $\frac{r_d}{r_t+r_d}$.

Il modello ricavato è rappresentato nella seguente Figura 4.5:

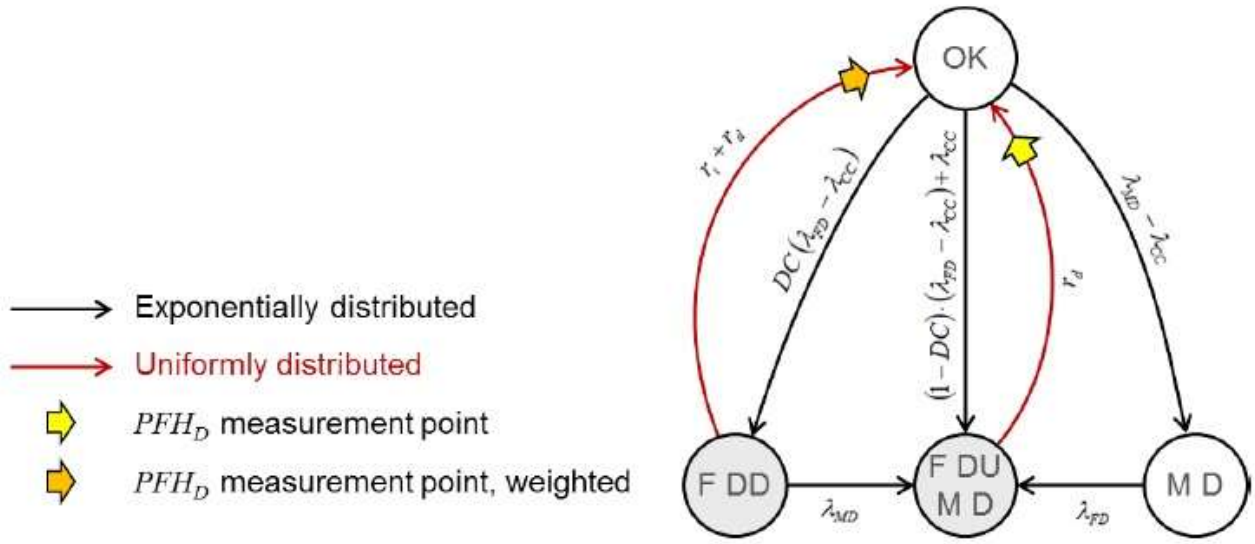


Figura 4.5: Modello 1oo1D, terzo step nella semplificazione.

Utilizzare la frazione descritta come fattore di peso è permesso in quanto le due transizioni hanno lo stesso tipo di distribuzione (distribuzione uniforme). Il terzo step nella semplificazione non ha alcuna influenza, rispetto al modello del secondo step, sul calcolo del valore del PFH_D.

Per procedere nella semplificazione del modello con il **quarto step** è indispensabile il concetto di nodo di partizione del flusso o FPN (dall'inglese Flow Partitioning Node).

Un **nodo di partizione del flusso** è uno stato del sistema con le seguenti caratteristiche:

- Può essere raggiunto dal sistema attraverso processi poco frequenti (ad esempio da un guasto hardware).
- Una volta raggiunto, può essere abbandonato dal sistema da almeno un processo frequente (ad esempio, in questo caso di studio, da un test da parte del canale di monitor, dalla domanda della funzione di sicurezza o da una riparazione). Il sistema che si trova in tale stato, pertanto, lo abbandona attraverso una transizione con un tasso elevato e quindi con un tempo trascurabile.
- Come conseguenza delle due precedenti caratteristiche, è uno stato nel quale il sistema può trovarsi con una probabilità molto bassa ($p_{FPN} << 1$). Tale stato è quasi sempre vuoto.

Queste proprietà essenziali di un nodo di partizione del flusso sono rappresentate nella seguente Figura 4.6:

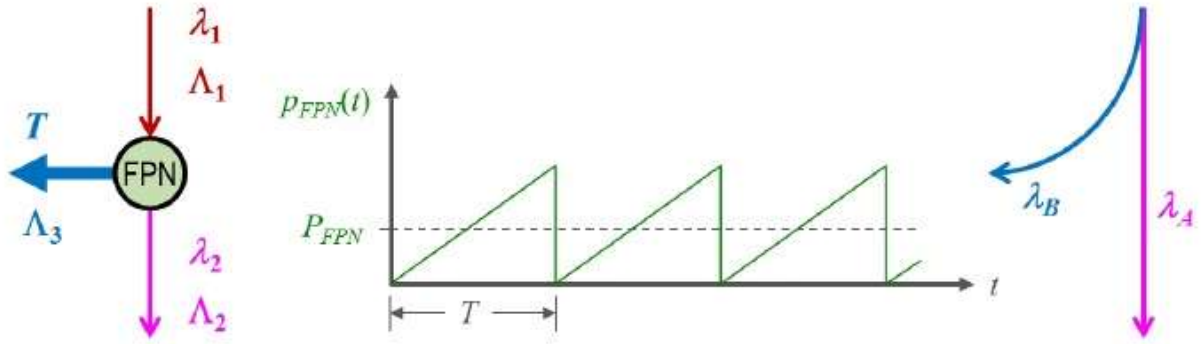


Figura 4.6: Nodo di partizione del flusso o FPN (Flow Partitioning Node).

Nella parte sinistra della Figura 4.6 viene rappresentato un generico nodo di partizione del flusso, con alcune transizioni relative ad esso, che vengono in seguito elencati e descritti:

- λ_1 rappresenta il tasso nominale di flusso entrante, associato ad un processo distribuito esponenzialmente,
- Λ_1 rappresenta il tasso assoluto di flusso entrante, ricavato dal rispettivo flusso nominale, λ_1, pesato con la probabilità dello stato sorgente di tale flusso,
- λ_2 rappresenta il tasso nominale di flusso uscente, associato ad un processo distribuito esponenzialmente,
- Λ_2 rappresenta il tasso assoluto di flusso uscente, ricavato dal rispettivo flusso nominale, λ_2, pesato con la probabilità dello stato sorgente di tale flusso, in questo caso del nodo di partizione stesso,
- Λ_3 rappresenta il tasso assoluto di flusso uscente, associato ad un processo frequente e con distribuzione uniforme,
- T rappresenta il tempo medio tra due liberazioni del nodo di partizione del flusso dovute al processo frequente.

L'incremento di probabilità del nodo di partizione del flusso, in un piccolo intervallo di tempo Δt, è espresso dalla seguente equazione, considerando la probabilità ad un tempo t e le componenti dovute ai flussi entranti ed uscenti dal nodo di partizione:

$$p_{FPN}(t + \Delta t) = p_{FPN}(t) + \Lambda_1 \cdot \Delta t - p_{FPN}(t) \cdot \lambda_2 \cdot \Delta t \tag{4.1}$$

Dividendo entrambi i termini della precedente equazione 4.1 per Δt si ottiene:

$$\frac{p_{FPN}(t + \Delta t) - p_{FPN}(t)}{\Delta t} = \Lambda_1 - \lambda_2 \cdot p_{FPN}(t) \tag{4.2}$$

Ponendo $\Delta t \to 0$ si ottiene la derivata nel tempo della probabilità del nodo di partizione del flusso; si ricava pertanto la seguente equazione differenziale:

$$\dot{p}_{FPN}(t) = \Lambda_1 - \lambda_2 \cdot p_{FPN}(t) \tag{4.3}$$

Ad un generico tempo t che rispetta la seguente condizione: $0 \leq t \leq T$ e, se come condizione iniziale viene posto che $p_{FPN}(0) = 0$, la soluzione alla precedente equazione differenziale 4.3 è la seguente:

$$p_{FPN}(t) = \frac{\Lambda_1}{\lambda_2}\left(1 - e^{-\lambda_2 t}\right) \tag{4.4}$$

La probabilità media del nodo di partizione del flusso è calcolata integrando su un intervallo di tempo della durata T la precedente equazione 4.4, ricordando di dividere sempre per T il risultato:

$$P_{FPN} = \frac{1}{T}\int_0^T p_{FPN}(t)dt = \frac{\Lambda_1}{\lambda_2} + \frac{\Lambda_1}{\lambda_2^2 \cdot T}\left(e^{-\lambda_2 T} - 1\right) \tag{4.5}$$

Il tasso assoluto di flusso uscente, causato dalla distribuzione uniformemente distribuita, può essere calcolato dall'equazione 4.4, che rappresenta la probabilità dello stato sorgente. Tale valore deve essere moltiplicato per l'inverso del tempo medio di liberazione, T, ovvero per il rispettivo tasso nominale di flusso:

$$\Lambda_3 = \frac{p_{FPN}(T)}{T} = \frac{\Lambda_1}{\lambda_2 \cdot T}\left(1 - e^{-\lambda_2 T}\right) \tag{4.6}$$

Si può ricavare un'espressione del tasso assoluto di flusso uscente causato dal processo distribuito esponenzialmente (Λ_2), considerandolo inizialmente come la differenza tra il tasso assoluto di flusso entrante ed il tasso assoluto di flusso uscente relativo al processo distribuito uniformemente (Λ_3) ed in seguito sostituendo a quest'ultimo l'equazione 4.6:

$$\Lambda_2 = \Lambda_1 - \Lambda_3 = \lambda_2 P_{FPN} = \Lambda_1\left(1 - \frac{1 - e^{-\lambda_2 T}}{\lambda_2 T}\right) \tag{4.7}$$

Il nodo di partizione del flusso mostrato in Figura 4.6 può essere semplificato come mostrato nella parte destra della stessa figura: il nodo viene eliminato perché virtualmente vuoto e restano solamente due transizioni che dalla sorgente del nodo portano il sistema ad altri stati.

Per calcolare i tassi nominali λ_A e λ_B, i quali sono relativi alle due transizioni della semplificazione del nodo, come già detto rappresentata nella parte destra della Figura 4.6, è necessario utilizzare le equazioni 4.6 e 4.7, sostituendo al tasso assoluto di flusso entrante (Λ_1) il tasso nominale di flusso entrante (λ_1). In questo modo anche i tassi assoluti Λ_2 e Λ_3 assumono nelle equazioni il tasso nominale relativo, partendo sempre dallo stato sorgente del nodo di partizione del flusso.

Le equazioni per λ_A e λ_B, ricavate come descritto, portano alle seguenti equazioni:

$$\lambda_A = \lambda_1\left(1 - \frac{1 - e^{-\lambda_2 T}}{\lambda_2 T}\right) \tag{4.8}$$

$$\lambda_B = \frac{\lambda_1}{\lambda_2 T}\left(1 - e^{-\lambda_2 T}\right) \tag{4.9}$$

Riassumendo, come mostrato nella parte destra della Figura 4.6, la partizione del flusso inizia dallo stato sorgente ed il nodo di partizione, che è virtualmente vuoto ($P_{FPN} << 1$), può essere eliminato.

Dopo aver introdotto il concetto di nodo di partizione del flusso è necessario analizzare attentamente lo stato "F DD", presente nel modello relativo al terzo step di semplificazione (Figura 4.5).

Lo stato oggetto di osservazione è alimentato da un processo di transizione distribuito esponenzialmente, con tasso pari a $DC(\lambda_{FD} - \lambda_{CC})$, proveniente dallo stato "OK" e che indica un guasto rilevabile del canale funzionale. Inoltre, lo stato "F DD", alimenta due processi di transizione: uno è distribuito esponenzialmente, porta il sistema nello stato "F DU, MD" con un tasso pari a λ_{MD} ed indica un guasto al canale di monitor; l'altro invece è distribuito uniformemente, porta il sistema allo stato "OK" con un tasso pari a $r_t + r_d$ ed indica un test o una domanda della funzione di sicurezza.

Avendo descritto il concetto di nodo di partizione del flusso e la sua semplificazione, si nota che lo stato "F DD" ne costituisce un esempio, pertanto potrà essere eliminato in accordo con i principi appena descritti.

Come già detto sono presenti due processi, distribuiti uniformemente, che liberano frequentemente il nodo di partizione del flusso (lo stato "F DD"): il test effettuato dal canale di monitor, con tasso r_t, e la domanda della funzione di sicurezza, con tasso r_d. Questi due processi agiscono contemporaneamente ed è possibile calcolare il tempo medio tra due liberazioni del nodo tramite il reciproco della somma dei due tassi, come illustrato nella seguente equazione 4.10:

$$T = \frac{1}{r_t + r_d} \tag{4.10}$$

Sostituendo nelle equazioni 4.8 e 4.9 il parametro appena trovato nell'equazione 4.10 ed i tassi di transizione relativi allo stato "F DD" agli stati generici λ_1 e λ_2, si possono ricavare le seguenti equazioni, che forniscono i tassi delle due transizioni che sostituiranno lo stato "F DD" nella semplificazione:

$$\lambda_A = DC(\lambda_{FD} - \lambda_{CC}) \left[1 - \frac{r_t + r_d}{\lambda_{MD}} \left(1 - e^{-\frac{\lambda_{MD}}{r_t + r_d}}\right)\right] \tag{4.11}$$

$$\lambda_B = \frac{DC(\lambda_{FD} - \lambda_{CC})(r_t + r_d)}{\lambda_{MD}} \left(1 - e^{-\frac{\lambda_{MD}}{r_t + r_d}}\right) \tag{4.12}$$

L'eliminazione del nodo di partizione del flusso "F DD", che consiste nel quarto step di semplificazione, porta al seguente modello, rappresentato in Figura 4.7:

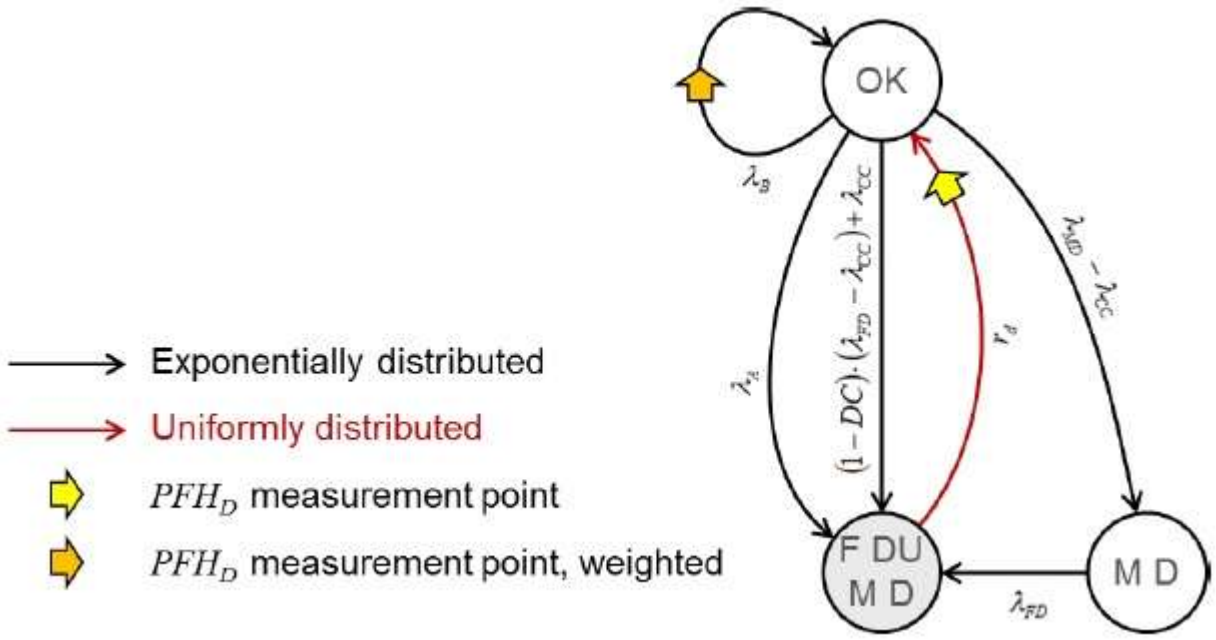


Figura 4.7: Modello 1oo1D, quarto step di semplificazione.

Nel modello si può notare l'assenza dello stato "F DD", considerato virtualmente vuoto, e la presenza di due transizioni, dallo stato sorgente "OK", agli stati "F DU, MD" ed ancora allo stato "OK". La seconda transizione, non facendo cambiare stato al sistema, è esclusivamente utilizzata come punto di misurazione pesato del PFH_D.

Dopo questa semplificazione, seguendo le stesse considerazioni sull'eliminazione degli stati "inibizione del macchinario" ed "evento indesiderato" apportati nel secondo step, porterà ad un leggero aumento del PFH_D, dovuto all'aumento solo minimale, secondo quanto riportato da Michael Dorra nel suo documento, delle probabilità degli stati "OK" ed "F DU, MD". Ciò porta ad una semplificazione in favore della sicurezza.

Nel **quinto step** nella semplificazione del modello viene analizzato lo stato "F DU, MD". Si può notare, dalla Figura 4.7, che il sistema raggiunge tale stato attraverso transizioni che comportano l'avvenimento di un guasto ed abbandona lo stesso, tornando allo stato "OK", attraverso la domanda della funzione di sicurezza.

I tassi di guasto, per assunzioni fatte relative a questa modellazione, sono molto minori del tasso di domanda r_d, che è maggiore o uguale ad una domanda per anno, essendo la domanda della funzione di sicurezza relativa alla modalità di operazione alta o continua, sempre per assunzione.

Da quanto detto lo stato "F DU, MD" è uno stato virtualmente vuoto, come un nodo di partizione del flusso, presenta tuttavia un solo flusso uscente, con tasso r_d. Per questo stato non c'è necessità di calcolare una partizione del flusso e la media del flusso uscente è la somma dei flussi entranti.

Lo stato "F DU, MD" è unito, in questo step, con lo stato "OK". Le tre transizioni che, in Figura 4.7, portano il sistema a raggiungere lo stato "F DU, MD" sono originati da due stati sorgente: due dallo stato "OK" ed una dallo "MD". La transizione uscente dallo stato "F DU, MD" porta il sistema allo stato "OK".

Si possono ricavare, dalle precedenti osservazioni, le transizioni da inserire nel nuovo modello: le due transizioni originate dallo stato "OK" saranno sommate mentre ci sarà una nuova transizione che comporterà l'aggiunta di un nuovo punto di misurazione del PFH_D, dallo stato "M D" allo stato "OK".

Quanto descritto è rappresentato nella seguente Figura 4.8:

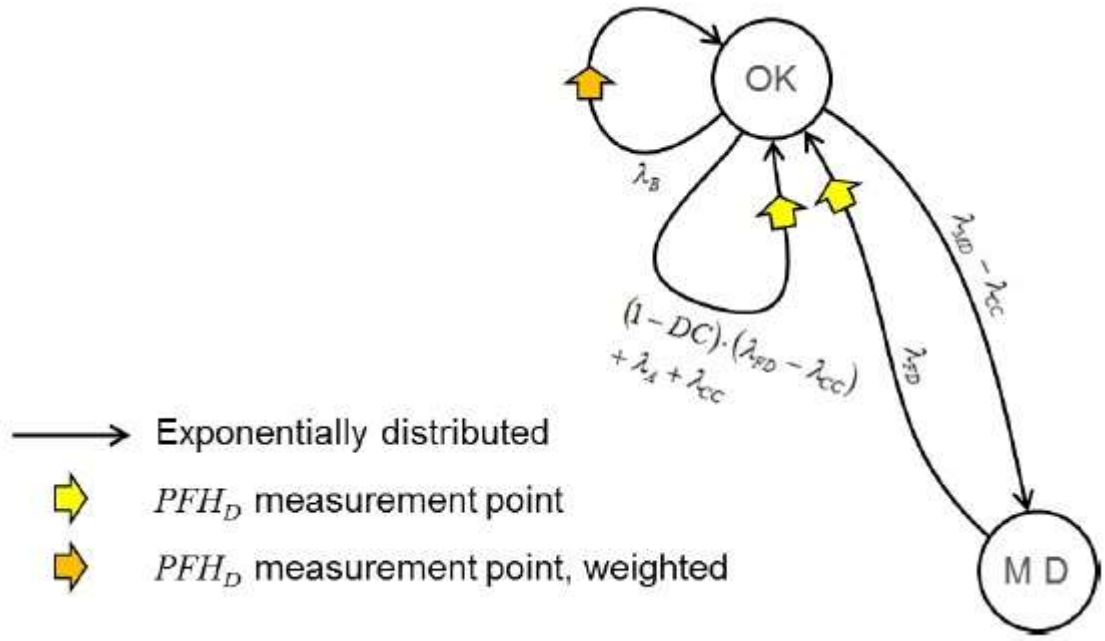


Figura 4.8: Modello 1oo1D, quinto step di semplificazione.

Come per gli altri stati virtualmente vuoti, anche lo stato "F DU, MD" ($P_{F\,DU,MD} << 1$) porta ad un aumento marginale nel computo del PFH_D, che porta ad una semplificazione dalla parte della sicurezza.

Il modello di transizioni di stato mostrato in Figura 4.8 contiene solamente processi di transizione distribuiti esponenzialmente: è quindi un modello di Markov.

Le due transizioni presenti nel modello dallo stato "OK" allo stesso stato "OK" sono importanti nell'analisi, a causa del punto di misurazione del PFH_D che contengono. Esse, tuttavia, non provocano un cambiamento di probabilità tra stati e pertanto non hanno influenza sulle probabilità che ha il sistema di trovarsi in uno dei due stati rimanenti, "OK" ed "MD".

Le probabilità dei due stati rimanenti possono essere analizzate tramite un modello di Markov, come descritto nel seguente paragrafo.

4.3 Utilizzo del modello di Markov a due stati

Per il calcolo delle probabilità dei due stati rimanenti, nel modello rappresentato in Figura 4.8, può essere utilizzato il modello generale di Markov a due stati, il quale procedimento risolutivo è già stato trattato nel paragrafo relativo nel capitolo d'introduzione all'affidabilità.

È riportato in seguito, in Figura 4.9, il modello generale di Markov a due stati:

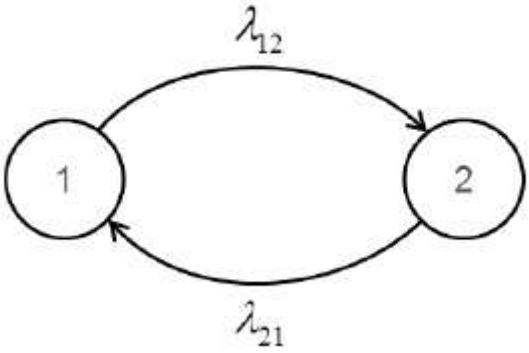


Figura 4.9: Modello di Markov a due stati.

Il modello è descritto dal seguente sistema di equazioni differenziali:

$$\dot{p_1}(t) = -\lambda_{12} \cdot p_1(t) + \lambda_{21} \cdot p_2(t) \tag{4.13}$$

$$\dot{p_2}(t) = \lambda_{12} \cdot p_1(t) - \lambda_{21} \cdot p_2(t) \tag{4.14}$$

Il sistema sarà inizialmente nello stato 1, le condizioni iniziali saranno pertanto le seguenti:

$$p_1(0) = 1 \tag{4.15}$$

$$p_2(0) = 0 \tag{4.16}$$

La soluzione delle equazioni differenziali 4.13 e 4.14, con le condizioni iniziali indicate nelle equazioni 4.15 e 4.16, è la seguente:

$$p_1(t) = \frac{\lambda_{21}}{\lambda_{12} + \lambda_{21}} + \frac{\lambda_{12}}{\lambda_{12} + \lambda_{21}} e^{-(\lambda_{12}+\lambda_{21})t} \tag{4.17}$$

$$p_2(t) = \frac{\lambda_{12}}{\lambda_{12} + \lambda_{21}} - \frac{\lambda_{12}}{\lambda_{12} + \lambda_{21}} e^{-(\lambda_{12}+\lambda_{21})t} \tag{4.18}$$

La soluzione riportata nelle equazioni 4.17 e 4.18 è relativa al modello di Markov generale, rappresentato in Figura 4.9.

Per ottenere la soluzione relativa al modello in Figura 4.8 si tralasciano nella rappresentazione le transizioni dallo stato “OK” allo stesso, perché, come è stato descritto, sono ininfluenti nel computo delle probabilità degli stati. Vengono sostituiti inoltre, ai generici tassi di transizione del modello di Markov generale, i relativi tassi di transizione presenti nel modello in Figura 4.8. Il modello di Markov ricavato è rappresentato nella figura seguente:

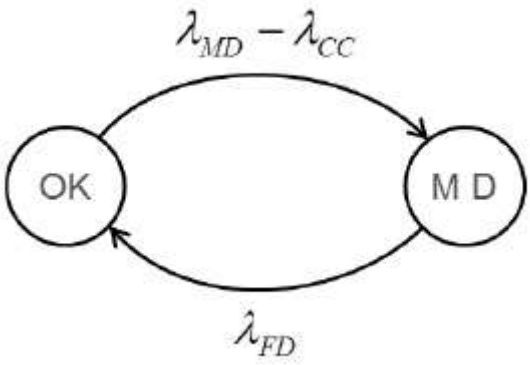


Figura 4.10: Modello di Markov per il calcolo delle probabilità degli stati.

Il sistema, inizialmente, non avrà guasti e si troverà nello stato "OK", le condizioni iniziali saranno pertanto le seguenti:

$$p_{OK}(0) = 1 \tag{4.19}$$

$$p_{M\,D}(0) = 0 \tag{4.20}$$

La soluzione del modello di Markov ha una corrispondenza con la soluzione del modello generale, riportata nelle equazioni 4.17 e 4.18. Ad esse è sufficiente sostituire ai generici tassi di transizione λ_{12} e λ_{21} rispettivamente i tassi di transizione ($\lambda_{MD} - \lambda_{CC}$)e λ_{FD}.

La soluzione del modello di Markov rappresentato in Figura 4.10 è composta dalle seguenti equazioni:

$$p_{OK}(t) = \frac{\lambda_{FD}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} + \frac{\lambda_{MD} - \lambda_{CC}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} e^{-(\lambda_{MD} + \lambda_{FD} - \lambda_{CC})t} \tag{4.21}$$

$$p_{M\,D}(t) = \frac{\lambda_{MD} - \lambda_{CC}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} - \frac{\lambda_{MD} - \lambda_{CC}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} e^{-(\lambda_{MD} + \lambda_{FD} - \lambda_{CC})t} \tag{4.22}$$

4.4 Modello 1oo1D, calcolo PFH_D con test non tempo ottimale

Viene riportato, nella seguente Figura 4.11, il modello di Markov ricavato dalla semplificazione, con tutti i suoi punti di misurazione del PFH_D e con l'espressione del fattore di peso da considerare nel calcolo, per uno di essi:

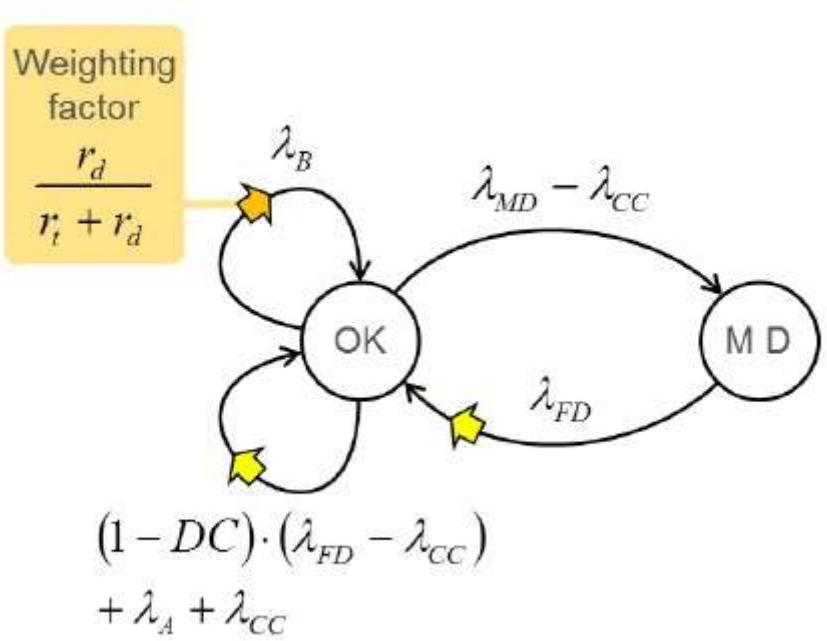


Figura 4.11: 1oo1D, modello di Markov per il calcolo del PFH_d.

Il valore del PFH_D istantaneo, definito in seguito come $pfh_D(t)$, può essere calcolato tramite la sommatoria dei tassi relativi alle transazioni che contengono misuratori del PFH_D, moltiplicati per la probabilità dello stato sorgente relativo, tenendo conto del fattore di peso presente:

$$pfh_D(t) = \lambda_B \frac{r_d}{r_t + r_d} p_{OK}(t) + [(1 - DC)(\lambda_{FD} - \lambda_{CC}) + \lambda_A + \lambda_{CC}] p_{OK}(t) + \lambda_{FD} p_{M\,D}(t) \quad (4.23)$$

Sostituendo alla precedente equazione le probabilità degli stati "OK" ed "M D", riportate nelle equazioni 4.21 e 4.22, si sviluppa la stessa, che viene resa più compatta tramite l'utilizzo di variabili di semplificazione, denominate L_α, L_β ed L_γ.

Le variabili di semplificazione hanno il solo scopo di rendere più semplice e compatta l'espressione del $pfh_D(t)$ e, essendo derivate da tassi di guasto, hanno la loro stessa unità di misura, $tempo^{-1}$.

Viene riportata in seguito l'espressione del $pfh_D(t)$, ricavata con l'ausilio delle variabili di semplificazione e susseguita dalle espressioni relative alle stesse:

$$pfh_D(t) = L_\alpha + L_\beta e^{-L_\gamma t} \quad (4.24)$$

$$L_\alpha = \left[(1 - DC)(\lambda_{FD} - \lambda_{CC}) + \lambda_A + \frac{r_d}{r_t + r_d}\lambda_B + \lambda_{CC}\right] \frac{\lambda_{FD}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} + \lambda_{FD} \frac{\lambda_{MD} - \lambda_{CC}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} \quad (4.25)$$

$$L_\beta = \left[(1 - DC)(\lambda_{FD} - \lambda_{CC}) + \lambda_A + \frac{r_d}{r_t + r_d}\lambda_B - \lambda_{FD} + \lambda_{CC}\right] \frac{\lambda_{MD} - \lambda_{CC}}{\lambda_{MD} + \lambda_{FD} - \lambda_{CC}} \quad (4.26)$$

$$L_\gamma = \lambda_{MD} + \lambda_{FD} - \lambda_{CC} \tag{4.27}$$

Per il calcolo del PFH_D si utilizza la media del suo valore istantaneo, calcolata su un tempo pari alla durata del tempo di missione T_M. La seguente equazione è prodotta in accordo con l'equazione 4.24:

$$PFH_D = \frac{1}{T_M}\int_0^{T_M} pfh_D(t)dt = \frac{1}{T_M}\int_o^{T_M}\left(L_\alpha + L_\beta e^{-L_\gamma t}\right)dt = L_\alpha + \frac{L_\beta}{L_\gamma T_M}(1 - e^{-L_\gamma T_M}) \tag{4.28}$$

Nell'equazione 4.28 vengono reintrodotte le espressioni relative alle variabili di semplificazione, ovvero a L_α, L_β ed L_γ, come riportato nelle equazioni 4.25, 4.26 e 4.27 e vengono reintrodotte le espressioni relative a λ_A e λ_B, in accordo con quanto riportato nelle equazioni 4.11 e 4.12.

L'equazione risultante e relativa al PFH_D è la seguente:

$$PFH_D = \lambda_{FD} - \left\{ DC\,\frac{r_t}{\lambda_{MD}}\left(1 - e^{-\frac{\lambda_{MD}}{r_t + r_d}}\right)\cdot \right.$$

$$\left. \cdot\ \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2 T_M} \right\} \tag{4.29}$$

Il test del canale funzionale, idealmente, per essere tempo ottimale, deve essere sempre eseguito, a seguito di un guasto, prima della domanda della funzione di sicurezza. Nelle condizioni di test tempo ottimale, indicate anche come TOT (dall'inglese Time-Optimal Testing), il tasso di test del canale funzionale è molto elevato, nel caso ideale è valida la seguente relazione: $r_t \to \infty$.

Sotto la condizione di test tempo ottimale il PFH_d assume un valore particolare definito come $PFH_{d\,TOT}$. Viene dapprima analizzata la parte dell'equazione 4.29 contenente il tasso di test r_t. Nella seguente equazione è calcolato il limite con la condizione imposta per test tempo ottimali ($r_t \to \infty$):

$$\lim_{r_t \to \infty} \frac{r_t}{\lambda_{MD}}\left(1 - e^{-\frac{\lambda_{MD}}{r_t + r_d}}\right) = 1 \tag{4.30}$$

Sostituendo quando ricavato dal limite contenuto nell'equazione 4.30 all'equazione 4.29 si ottiene l'espressione del $PFH_{D\,TOT}$:

$$PFH_{D\,TOT} = \lambda_{FD} - DC \cdot$$

$$\cdot\ \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2 T_M} \tag{4.31}$$

L'altra condizione estrema, completamente opposta al test tempo ottimale, è l'assenza totale di test

del canale funzionale, indicata anche come NT (dall'inglese No Testing). Per ottenere questa condizione tramite delle variabili si può porre pari a zero sia la copertura diagnostica che il tasso di test, ovvero si deve considerare $r_t = 0$ oppure, ottenendo lo stesso risultato, $DC = 0$.

Sostituendo una delle due condizioni nell'equazione 4.29 si ottiene la seguente, relativa al calcolo del $PFH_{D\ NT}$, ovvero del PFH_D in assenza di test:

$$PFH_{D\ NT} = \lambda_{FD} \tag{4.32}$$

Il PFH_D sarà certamente compreso tra i due valori ottenuti dalle due condizioni estreme, tra il valore ottenuto in assenza di test (equazione 4.32) ed il valore ottenuto con test tempo ottimale (equazione 4.31):

$$PFH_{D\ NT} \geq PFH_D \geq PFH_{D\ TOT} \tag{4.33}$$

Se in un sistema viene introdotto il test del canale funzionale, come risultato diminuirà il valore del PFH_D, rispetto al $PFH_{D\ NT}$, che è relativo alla condizione caratterizzata dall'assenza del test.

Il miglioramento relativo atteso dall'introduzione del test è dato dal seguente rapporto:

$$Miglioramento\ relativo\ atteso = \frac{PFH_{D\ NT} - PFH_D}{PFH_{D\ NT}} \tag{4.34}$$

Il seguente rapporto descrive, in modo analogo, il massimo miglioramento, in termini di PFH_D, ottenibile con un test. Il miglioramento massimo si ottiene in condizioni di test tempo ottimale:

$$Massimo\ miglioramento\ ottenibile = \frac{PFH_{d\ NT} - PFH_{d\ TOT}}{PFH_{d\ NT}} \tag{4.35}$$

Viene definita l'efficienza di test correlata al tempo, indicata come $TRTE$, come il rapporto tra i due fattori appena descritti, che nell'equazione vengono poi rimpiazzati dalle loro espressioni, presenti nelle equazioni 4.34 e 4.35:

$$TRTE = \frac{Miglioramento\ relativo\ atteso}{Massimo\ miglioramento\ ottenibile} = \frac{\frac{PFH_{D\ NT} - PFH_D}{PFH_{D\ NT}}}{\frac{PFH_{D\ NT} - PFH_{D\ TOT}}{PFH_{D\ NT}}} = \frac{PFH_{D\ NT} - PFH_D}{PFH_{D\ NT} - PFH_{D\ TOT}} \tag{4.36}$$

Vengono ora inserite, nell'equazione 4.36 appena ottenuta, le espressioni relative al PFH_D, al $PFH_{D\ TOT}$ ed al $PFH_{D\ NT}$, contenute rispettivamente nelle equazioni 4.29, 4.31 e 4.32. Si ricava, a seguito di ciò, la seguente espressione della $TRTE$:

$$TRTE = \frac{r_t}{\lambda_{MD}}\left(1 - e^{-\frac{\lambda_{MD}}{r_t + r_d}}\right) \tag{4.37}$$

Per un tasso di test tendente a zero l'efficienza di test sarà anch'essa pari a zero:

$$\lim_{r_t \to 0} TRTE = 0 \tag{4.38}$$

Per un tasso di test tendente a infinito l'efficienza di test sarò pari ad uno:

$$\lim_{r_t \to \infty} TRTE = 1 \tag{4.39}$$

La $TRTE$, similmente alla copertura diagnostica DC, è una variabile adimensionale che può assumere valori compresi tra zero ed uno ($0 \leq TRTE \leq 1$).

Un test può essere valutato tramite questi due parametri: se entrambi si avvicinano all'unità il test può essere ritenuto elevatamente efficiente.

La funzione esponenziale presente nell'equazione 4.37 e relativa alla $TRTE$ può essere rimpiazzata dalla sua approssimazione lineare, riportata in forma generale nella seguente equazione 4.40:

$$e^x \approx 1 + x \tag{4.40}$$

L'approssimazione non porta a notevoli perdite di precisione per la relazione $\lambda_{MD} << r_t + r_d$, presente grazie alle assunzioni fatte per la modellazione. Il risultato ottenuto tramite l'applicazione dell'approssimazione lineare nell'equazione 4.37 porta alla seguente espressione della $TRTE$, che non contiene più la variabile λ_{MD}:

$$TRTE = \frac{r_t}{r_t + r_d} \tag{4.41}$$

Per tassi di test esclusivamente maggiori di zero ($r_t > 0$) l'equazione 4.41 può essere riformulata come segue, dividendo numeratore e denominatore per lo stesso r_t:

$$TRTE = \frac{1}{1 + \frac{r_d}{r_t}} \tag{4.42}$$

L'equazione 4.42 indica che il $TRTE$ dipende esclusivamente dal rapporto tra il tasso della domanda della funzione di sicurezza ed il tasso di test. Sempre tramite l'equazione 4.42 si può notare che, se $r_t/r_d = 100$, allora $TRTE \approx 99\%$.

La seguente Figura 4.12 rappresenta, per mezzo di un grafico, la dipendenza tra $TRTE$ ed r_t/r_d:

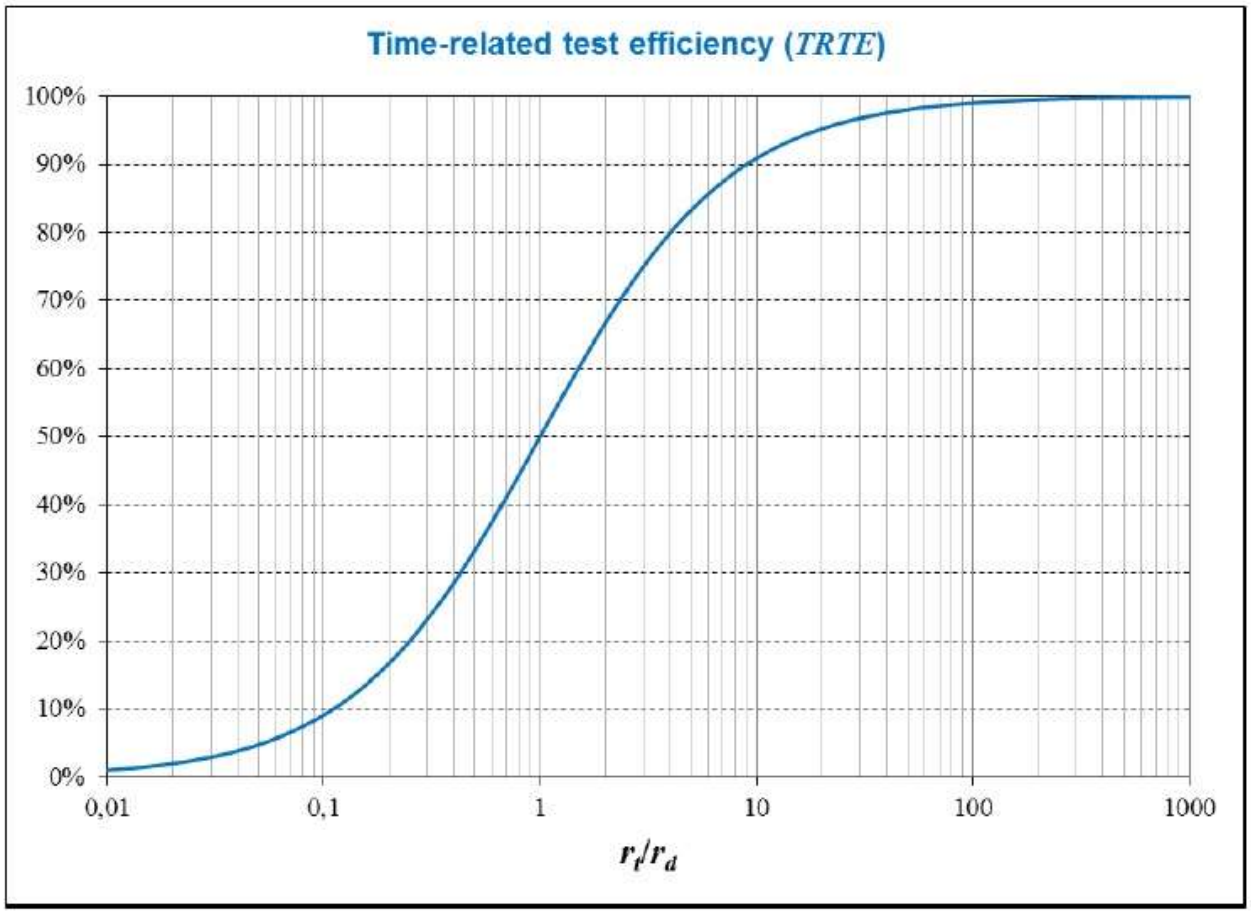


Figura 4.12: Dipendenza tra $TRTE$ ed r_t/r_d.

All'interno dell'equazione 4.29 relativa al PFH_D, si può sostituire l'espressione del $TRTE$ presente e descritta dall'equazione 4.37 con la sua forma più semplice e compatta, ricavata con l'approssimazione lineare del termine esponenziale e descritta dall'equazione 4.41.

Così facendo si ottiene la seguente equazione, relativa al PFH_D ed utilizzata in caso di modello 1oo1D senza test tempo ottimale:

$$PFH_d = \lambda_{FD} - DC\frac{r_t}{r_t + r_d} \cdot \cdot \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2 T_M} \quad (4.43)$$

4.5 Modello 1oo1D, calcolo PFHD con test tempo ottimale

Riassumendo quanto descritto relativamente al test tempo ottimale, si ricorda che un test, in questa condizione, avviene sempre prima della domanda della funzione di sicurezza, a seguito di un guasto. Più in generale, un test tempo ottimale indica che la sua efficienza di test correlata al tempo ($TRTE$) è tendente, se non pari, ad 1.

All'interno di un caso pratico ci si può ritenere in condizioni di test tempo ottimale nei seguenti casi:

- Il tasso di test è più grande del tasso di domanda della funzione di sicurezza ed il loro rapporto è maggiore o uguale a 100: $r_t/r_d \geq 100$.
- Il test del canale funzionale è eseguito in maniera continua oppure viene eseguito immediatamente a seguito di ogni richiesta della funzione di sicurezza. In questo caso il tempo impiegato per il rilevamento del guasto, sommato con il tempo necessario per portare il sistema in uno stato sicuro (inibizione), deve essere minore del tempo di reazione del sistema (o del tempo di sicurezza del processo) perché, se fosse maggiore, non ci sarebbe abbastanza tempo per evitare il verificarsi dell'evento indesiderato.
- Il test del canale funzionale viene eseguito periodicamente e la somma dell'intervallo di test con il tempo richiesto per il rilevamento di un guasto e con il tempo necessario per portare il sistema in uno stato sicuro (inibizione delle operazioni), deve essere minore del tempo di reazione del sistema (o del tempo di sicurezza del processo) perché, se fosse maggiore, non ci sarebbe abbastanza tempo per evitare il verificarsi dell'evento indesiderato.

In questi casi la competizione tra il test del canale funzionale e la domanda della funzione di sicurezza pende nettamente in favore del test, che non avrà alcuna riduzione dell'efficienza ($TRTE = 1$).

Di conseguenza, l'equazione 4.43, relativa al PFH_D, assume la seguente forma, in accordo con l'equazione 4.31, relativa al PFH_D con test tempo ottimale:

$$PFH_D = PFH_{D\,TOT} \;= \lambda_{FD} - DC \cdot$$

$$\cdot \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2 T_M} \tag{4.44}$$

Se la funzione di monitoraggio del canale funzionale viene implementata all'esterno del sottosistema 1oo1D ma in un altro blocco dello stesso sistema di sicurezza, è possibile, nel calcolo del PFH_D, stabilire che non può avvenire la perdita del monitoraggio. Nel computo vengono pertanto esclusi i guasti del canale di monitor, settando $\lambda_{MD} = 0$.

Secondo l'analisi delle cause comuni di guasto tramite il modello a fattore beta, se è nullo il tasso di guasto relativo ad un canale (in questo caso quello di monitor), allora anche il tasso relativo alle cause comuni di guasto sarà nullo: $\lambda_{CC} = 0$.

In altri termini, questa semplificazione può essere utilizzata nel caso in cui uno stesso dispositivo è utilizzato per eseguire diagnostica ad un sottosistema e, contemporaneamente, è usato per l'esecuzione della funzione di sicurezza in questione. Il guasto del dispositivo è già considerato nel relativo contributo di PFH_D del sistema di sicurezza.

Relativamente a questo caso particolare è possibile ottenere la seguente espressione del PFH_D, derivata dall'equazione 4.43 e settando le variabili λ_{MD} e λ_{CC} come descritto:

$$PFH_D = \left(1 - DC\frac{r_t}{r_t + r_d}\right)\lambda_{FD} \tag{4.45}$$

Nell'equazione 4.45 è di facile identificazione l'espressione semplificata utilizzata per il $TRTE$ nell'equazione 4.41. In caso di test tempo ottimale, come definito precedentemente, tale espressione assume il valore 1, portando alla seguente equazione:

$$PFH_D = (1 - DC)\lambda_{FD} \tag{4.46}$$

È possibile ricavare un'altra equazione, semplificata, del PFH_D relativo al modello 1oo1D con test tempo ottimale, con l'approssimazione quadratica di una funzione esponenziale, che non porta a notevoli perdite di precisione per argomenti di x con $|x| << 1$. Viene riportata in seguito la forma generica:

$$e^x \approx 1 + x + \frac{1}{2}x^2 \tag{4.47}$$

La sostituzione della funzione esponenziale presente nell'equazione 4.44 con l'approssimazione quadratica (come da equazione 4.47) porta alla seguente soluzione semplificata:

$$PFH_D = \lambda_{FD} - DC(\lambda_{FD} - \lambda_{CC})\left[1 - \frac{1}{2}(\lambda_{MD} - \lambda_{CC})T_M\right] \tag{4.48}$$

Viene utilizzata l'approssimazione quadratica perché l'utilizzo dell'approssimazione lineare, descritta nell'equazione 4.40, non è conveniente in quanto produrrebbe un'eccessiva semplificazione del PFH_D, dovuta all'eliminazione delle variabili di input λ_{MD} e T_M.

4.6 Modello 1oo1

Il modello 1oo1 rappresenta il caso più semplice relativo ai sistemi a canale singolo: non è presente un canale di monitor e la diagnostica per il canale funzionale non è implementata.

Nella seguente Figura 4.13 è rappresentato il corrispondente diagramma a blocchi:

Figura 4.13: Sistema a canale singolo non testato (1oo1)

Il PFH_D può essere calcolato dall'equazione più generale relativa al modello 1oo1D, ovvero dall'equazione 4.43, riferita ad una condizione che non comprende il test tempo ottimale. L'assenza del canale di monitor può essere espressa in egual modo ponendo pari a zero il tasso di test o la copertura diagnostica: $DC = 0$ oppure $r_t = 0$.

Ponendo una o entrambe le variabili pari a zero nell'equazione 4.43 si ottiene la seguente espressione del PFH_D , relativa al modello 1oo1:

$$PFH_D = \lambda_{FD} \tag{4.49}$$

5. Architetture a due canali

Sono effettuate, in questo capitolo, analisi relative a sistemi di sicurezza che possiedono due canali funzionali collegati logicamente in parallelo, i quali consentono a questa tipologia di sistemi di avere ridondanza nell'esecuzione della funzione di sicurezza. In modo particolare viene analizzata l'architettura che prevede la presenza della copertura diagnostica (1oo2D). In seguito, da quanto descritto per l'architettura 1oo2D e con opportune semplificazioni, si ricavano risultati anche per l'architettura a due canali senza diagnostica (1oo2).

5.1 Modello 1oo2D, introduzione

Nei sistemi modellizzati con architettura 1oo2D sono presenti due canali funzionali, definiti genericamente in seguito come canale A e canale B. Ciascuno dei due canali, se funzionante, oltre ad eseguire la funzione di sicurezza è impegnato nel testare l'altro canale, offrendo una certa copertura diagnostica. La seguente Figura 5.1 mostra il diagramma a blocchi corrispondente al modello, con le variabili di input utilizzate. A queste deve essere aggiunto il tempo di missione T_M:

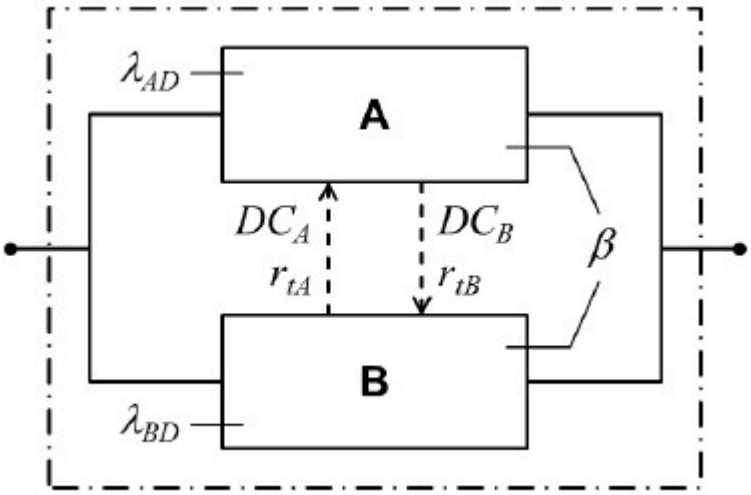


Figura 5.1: Sistema a due canali testato (1oo2D).

È presente, per ciascun canale funzionale, il rispettivo tasso di guasto pericoloso, definiti come λ_{AD} e λ_{BD}. I guasti dovuti a cause comuni sono gestiti con il modello a fattore beta, presente come input del modello (β).

La diagnostica effettuata è rappresentata, in Figura 5.1, da delle frecce tratteggiate, in particolare, il canale A è testato dal canale B con un certo tasso r_{tA} ed una certa copertura diagnostica DC_A. In modo analogo, per il canale B è implementata la diagnostica, eseguita dal canale A, con un certo tasso di test r_{tB} ed una certa copertura diagnostica DC_B. È assunto che, in caso di guasto pericoloso di un canale, esso perde sia la capacità di eseguire la funzione di sicurezza che di eseguire diagnostica all'altro canale, che ne rimarrà sprovvisto.

Il modello è ritenuto adatto per rappresentare i seguenti casi:

a) I canali A e B eseguono ciascuno diagnostica all'altro canale, includendo il raggiungimento di uno stato sicuro in caso di rilevamento di un guasto.
b) A e B sono sensori ridondanti, i quali segnali di output sono comparati con lo scopo di eseguire diagnostica in un controllore a valle che non è parte del sottosistema costituito da A e B.
c) A e B formano un sistema di attuatori ridondanti che servono come elementi di output per la funzione di sicurezza. In questa modalità un controllore esterno rileva i guasti di un attuatore e porta il sistema a uno stato sicuro per mezzo dell'attuatore ancora intatto.

È da considerare che il controllore esterno, presente nei casi b) e c), non rientra nel calcolo del PFH_D descritto in seguito per sottosistemi costituiti dai blocchi A e B. Il controllore esterno deve essere considerato separatamente nel calcolo del PFH_D totale per la funzione di sicurezza, per esempio nella forma di una componente di PFH_D additivo dovuto esclusivamente ad esso.

La seguente Figura 5.2 mostra il grafico delle transizioni degli stati relativo al modello 1oo2D:

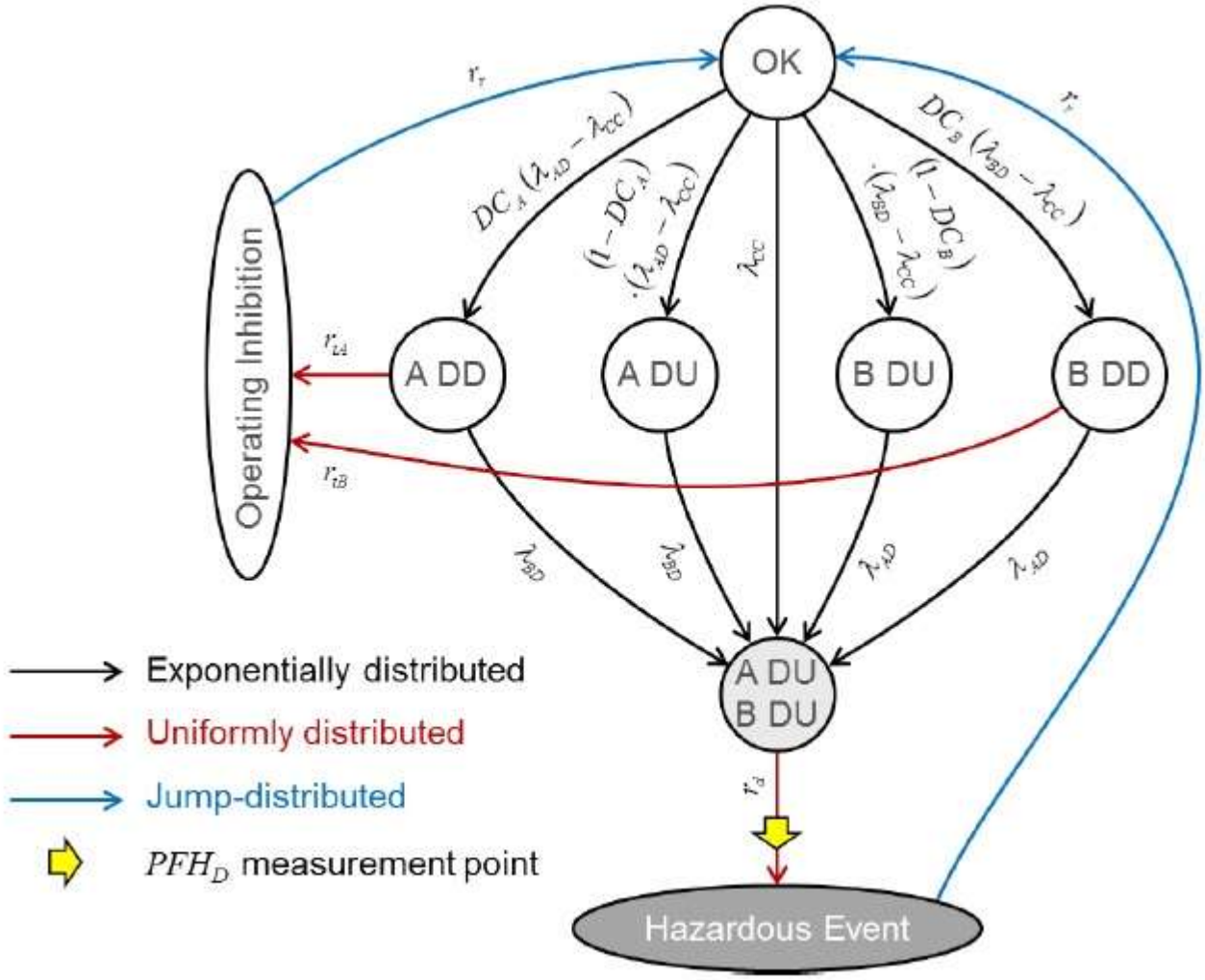


Figura 5.2: Modello di transizione degli stati per un sistema *1oo2D.*

Il modello rappresentato in Figura 5.2 è composto da stati, transizioni di stato e punti di misurazione del PFH_D. Ogni entità presente nel modello viene descritta dettagliatamente in seguito.

Le transizioni di stato sono rappresentate da delle frecce e sono caratterizzate da un tasso di transizione e da un colore, che ne indica come è distribuita la probabilità di transizione. In seguito, vengono descritte le tipologie di transizioni di stato presenti nel modello, che seguono la logica utilizzata anche per il modello 1oo1D, rappresentato in Figura 4.2:

- Transizioni di stato dovute a guasti: sono rappresentate in nero e sono distribuite esponenzialmente. I tassi di transizione sono combinazioni dei tassi di guasto presenti nel sistema e della due coperture diagnostiche.
- Transizioni di stato dovute al test del canale funzionale: sono rappresentate in rosso e sono distribuite uniformemente (distribuzione con densità costante). Hanno un tasso di transizione pari a $r_{tA}\ o\ r_{tB}$.
- Transizioni di stato dovute alla domanda della funzione di sicurezza: sono rappresentate in rosso e sono distribuite uniformemente (distribuzione con densità costante). Hanno un tasso di transizione pari a r_d.
- Transizioni di stato dovute alla riparazione del sistema: sono rappresentate in blu e caratterizzate da una distribuzione a gradino. Hanno un tasso di transizione pari a r_r.

Le distribuzioni non distribuite esponenzialmente rendono impossibile l'analisi tramite il modello di Markov.
Nel modello rappresentato in Figura 5.2 gli stati sono rappresentati da cerchi o ellissi e si suddividono in stati sicuri, stati pericolosi ed uno stato di evento indesiderato. L'evento indesiderato avviene esclusivamente quando viene richiesta la funzione di sicurezza ed il sistema non è in grado di eseguirla, ovvero nel caso in cui entrambi i canali funzionali siano guasti. In genere gli stati sono nominati dai guasti in corso nei canali del sistema (gli stati non presenti nella denominazione si intendono funzionanti), dalla tipologia di guasto presente oppure da una condizione particolare nella quale si trova il sistema. Le tipologie di guasto presenti sono due: guasto pericoloso e rilevabile, indicato con DD (dall'inglese Dangerous Detectable) oppure guasto pericoloso e non rilevabile (dall'inglese Dangerous Undetectable).

Gli stati sicuri sono colorati, all'interno della Figura 5.2, in bianco. Sono caratterizzati dal fatto che, se il sistema si trova in uno di essi, non è possibile il verificarsi dell'evento indesiderato con una sola transizione di stato. Gli stati sicuri presenti sono i seguenti:

- Stato "OK": è caratterizzato dall'assenza di qualsiasi tipologia di guasto del sistema. Questo stato è sicuro perché se viene richiesta la funzione di sicurezza il sistema è in grado di eseguirla, evitando l'evento indesiderato. È lo stato inziale di un sistema conforme posto in operazione. Il sistema può raggiungere nuovamente lo stato "OK", da un altro stato, a seguito di una riparazione. Trovandosi nello stato "OK" ed a seguito di un guasto qualsiasi, il sistema abbandona lo stato "OK".
- Stato "Operating Inhibition": è caratterizzato dall'inibizione del macchinario che, pertanto, smette di richiedere la funzione di sicurezza, rendendo questo stato uno stato sicuro. A seguito dell'inibizione delle operazioni avviene la riparazione, che riporta il sistema allo stato "OK". Nella modellazione, per ipotesi cautelativa, non è ammesso il funzionamento degradato, ovvero il funzionamento con solo un canale funzionante. Pertanto, a seguito di una rilevazione di guasto di un canale funzionale, per mezzo dell'altro, il sistema viene inibito immediatamente, in modo che non potrà più richiedere la funzione di sicurezza. Il sistema di sicurezza può trovarsi in questo stato esclusivamente a seguito di un test con la presenza di un guasto rilevabile di uno dei due canali.

- Stato “A DD”: è caratterizzato da un guasto pericoloso e rilevabile del canale A. Le richieste della funzione di sicurezza, mentre il sistema si trova in tale stato, saranno eseguite dal canale B, ancora funzionante: è pertanto uno stato sicuro. Può essere raggiunto esclusivamente dallo stato “OK” con un tasso di transizione, per quanto descritto ed escludendo dal computo le cause comuni di guasto, pari a $DC_A(\lambda_{AD} - \lambda_{CC})$. La diagnostica è fornita dal canale B, che porterà il sistema allo stato di inibizione delle operazioni, con un tasso di transizione pari al tasso di test del canale A, r_{tA}. Il sistema abbandona questo stato anche se si verifica un guasto all’altro canale funzionale.
- Stato “B DD”: analogamente a quanto descritto per lo stato “A DD”, è caratterizzato da un guasto pericoloso e rilevabile del canale B. Le richieste della funzione di sicurezza, mentre il sistema si trova in tale stato, saranno eseguite dal canale A, ancora funzionante: è pertanto uno stato sicuro. Può essere raggiunto esclusivamente dallo stato “OK” con un tasso di transizione, per quanto descritto ed escludendo dal computo le cause comuni di guasto, pari a $DC_B(\lambda_{BD} - \lambda_{CC})$. La diagnostica è fornita dal canale A, che porterà il sistema allo stato di inibizione delle operazioni, con un tasso di transizione pari al tasso di test del canale B, r_{tB}. Il sistema abbandona questo stato anche se si verifica un guasto all’altro canale funzionale.
- Stato “A DU”: è caratterizzato da un guasto pericoloso e non rilevabile del canale A. Le richieste della funzione di sicurezza, mentre il sistema si trova in tale stato, saranno eseguite dal canale B, ancora funzionante: è pertanto uno stato sicuro. Può essere raggiunto esclusivamente dallo stato “OK” con un tasso di transizione, per quanto descritto ed escludendo dal computo le cause comuni di guasto, pari a $(1 - DC_A) \cdot (\lambda_{AD} - \lambda_{CC})$. La diagnostica, in questo stato, è inefficace. Il sistema abbandona questo stato se si verifica un guasto all’altro canale funzionale.
- Stato “B DU”: analogamente a quanto descritto per lo stato “A DU”, è caratterizzato da un guasto pericoloso e non rilevabile del canale B. Le richieste della funzione di sicurezza, mentre il sistema si trova in tale stato, saranno eseguite dal canale A, ancora funzionante: è pertanto uno stato sicuro. Può essere raggiunto esclusivamente dallo stato “OK” con un tasso di transizione, per quanto descritto ed escludendo dal computo le cause comuni di guasto, pari a $(1 - DC_B) \cdot (\lambda_{BD} - \lambda_{CC})$. La diagnostica, in questo stato, è inefficace. Il sistema abbandona questo stato se si verifica un guasto all’altro canale funzionale.

È presente, in Figura 5.2, un unico stato pericoloso, colorato in grigio chiaro. Se il sistema si trova in questo stato non potrà eseguire la funzione di sicurezza e, pertanto, a seguito di una richiesta della stessa si verificherà l’evento indesiderato. La funzione di sicurezza non può essere eseguita esclusivamente se entrambi i canali funzionali sono guasti, in seguito è descritto lo stato “A DU, B DU”:

- Stato “A DU, B DU”: indica la presenza di un guasto pericoloso ad entrambi i canali funzionali, A e B. Il sistema, se si trova in questo stato, non sarà in grado di eseguire la funzione di sicurezza né tantomeno nessun tipo di diagnostica, per questo i guasti vengono indicati, per entrambi i canali, come non rilevabili. È uno stato pericoloso perché, a seguito di una richiesta della funzione di sicurezza, che avviene con tasso di domanda r_d, si verifica l’evento indesiderato. Questo stato può essere raggiunto direttamente dallo stato “OK” tramite le cause comuni di guasto, con tasso λ_{CC}. Può essere raggiunto, inoltre, se il sistema si trova in uno stato con un canale funzionale già guasto ed avviene il guasto dell’altro canale, in particolare, se il sistema si trova nello stato “A DD” o nello stato “A DU”, può essere raggiunto tramite un guasto pericoloso qualsiasi dell’altro canale funzionale B, con un tasso pari a λ_{BD}. Parimenti, se il sistema si trova nello stato “B DD” o nello stato “B DU”, può raggiungere lo

stato “A DU, B DU” tramite un guasto pericoloso qualsiasi dell’altro canale funzionale, in questo caso A, con un tasso pari a λ_{AD}.

Lo stato di evento indesiderato, denominato “Hazardous Event”, indica l’avvenimento dello stesso ed è rappresentato in Figura 5.2 colorato in grigio scuro. Può essere raggiunto esclusivamente dallo stato “A DU, B DU”, essendo l’unico stato nel quale entrambi i canali funzionali sono guasti, con delle transizioni di stato, contenenti i punti di misurazione del PFH_D, rappresentate da frecce gialle ed aventi come tasso di transizione r_d. A seguito dell’evento pericoloso avviene una riparazione del sistema di sicurezza, la quale riporta il sistema allo stato “OK” ed ha un tasso di transizione a gradino pari a r_r.

Riassumendo, un sistema completamente funzionante può portare al verificarsi dell’evento indesiderato a seguito di due eventi in sequenza: il guasto di entrambi i canali funzionali e la richiesta della funzione di sicurezza. Il guasto di entrambi i canali funzionali può avvenire in modo diretto, per mezzo delle cause comuni di guasto, o in sequenza, con un primo guasto relativo ad uno dei due canali ed un secondo guasto relativo all’altro canale. Un sistema può tornare completamente funzionante attraverso riparazioni, che avvengo dopo un’inibizione delle operazioni o dopo un evento indesiderato. La diagnostica è efficace se avviene un guasto rilevabile ad un canale e l’altro canale effettua un test prima di subire un guasto.

5.2 Modello 1oo2D, semplificazione

Per ricavare delle equazioni per il calcolo del PFH_D il più possibili compatte e funzionali è necessario semplificare il modello rappresentato in Figura 5.2, considerando anche che un’eliminazione delle transizioni di stato non distribuite esponenzialmente può consentire l’utilizzo del modello di Markov. Vengono illustrate in seguito le semplificazioni attuate, descritte a step.

Nel **primo step** di semplificazione del modello si può notare che, essendo in modalità di operazione alta o continua, ogni tasso di guasto presente nel modello in Figura 5.2 è molto minore rispetto al tasso di domanda, r_d, che per assunzione è maggiore o uguale ad una domanda per anno.

Il tasso di domanda porta il sistema, dallo stato “A DU, B DU”, allo stato di evento indesiderato, pertanto lo stato pericoloso oggetto di studio è virtualmente vuoto, come un nodo di partizione del flusso (FPN), anche se ha solamente un flusso uscente, la richiesta della funzione di sicurezza con tasso r_d. Per quanto detto non è necessario calcolare la partizione del flusso ed il flusso uscente è la somma dei flussi entranti.

Lo stato “A DU, B DU” è unito, in questo step di semplificazione, con lo stato di evento indesiderato (Hazardous Event), alla luce di quanto descritto. La seguente Figura 5.3 illustra il primo step nella semplificazione del modello:

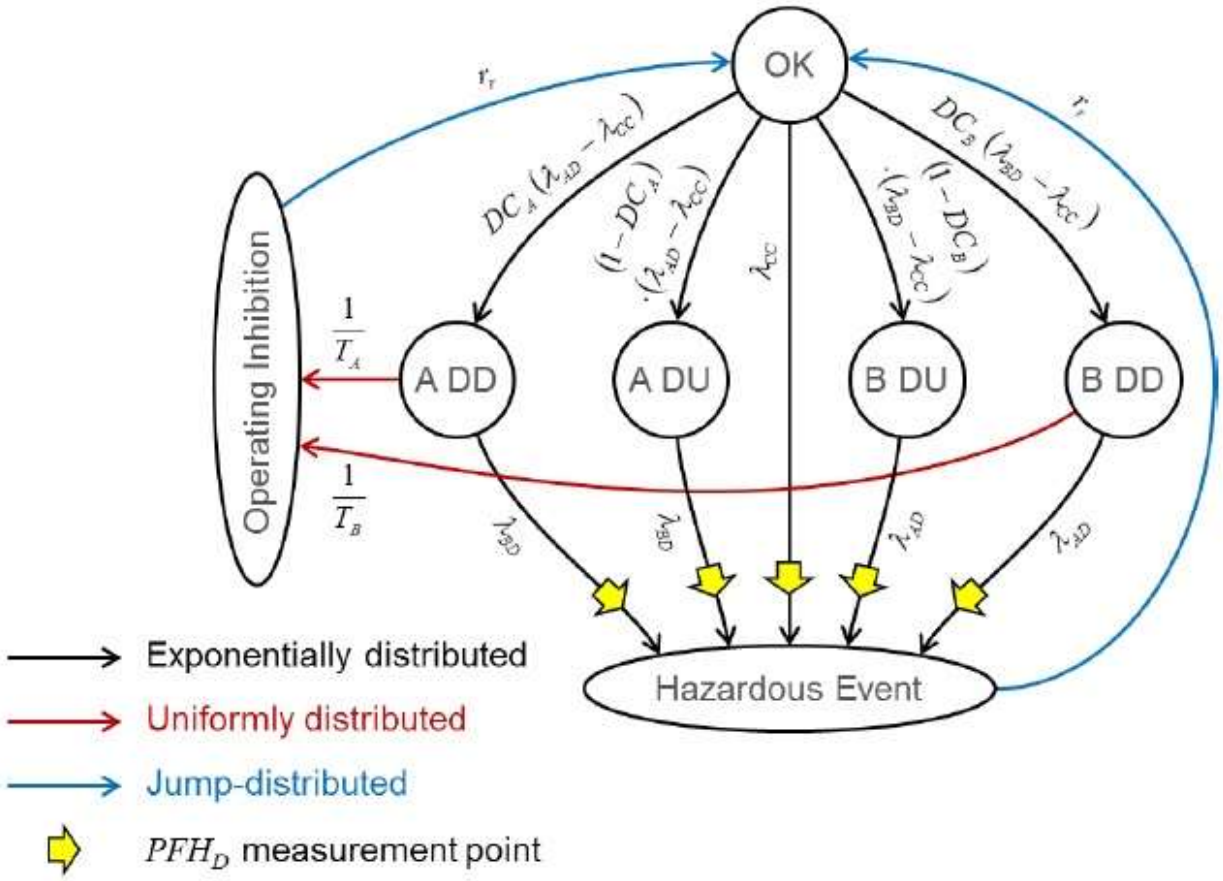


Figura 5.3: Modello 1oo2D, primo step di semplificazione.

Dopo questa semplificazione, al posto dell'unico punto di misurazione del PFH_D presente in Figura 5.2 originario, ve ne sono ora presenti cinque, uno per ogni transizione che porta all'evento indesiderato da un diverso stato sorgente. Gli stati sorgente, quindi, sono diventati cinque: "A DD", "A DU", "B DD", "B DU" e "OK" e, per ognuno di essi, è presente una transizione che porta all'evento indesiderato e che pertanto necessita di un punto di misurazione del PFH_D. In sostanza, le transizioni che portavano allo stato "A DU, B DU" nel modello in Figura 5.2 ora portano direttamente al verificarsi dell'evento indesiderato.

I tassi di test, r_{tA} ed r_{tB}, vengono espressi, sempre in Figura 5.2, tramite l'inverso degli intervalli di tempo medi di test, denominati T_A e T_B e descritti dalle seguenti equazioni:

$$r_{tA} = \frac{1}{T_A} \tag{5.1}$$

$$r_{tB} = \frac{1}{T_B} \tag{5.2}$$

Per quanto riguarda la misurazione del PFH_D, tale semplificazione costituisce una piccola stima dalla parte della sicurezza perché, ponendo a zero la probabilità, seppur piccola, che ha il sistema di trovarsi nello stato "A DU, B DU", viene aumentato, in modo marginale, il flusso verso lo stato di evento indesiderato. Omettere questo stato nel modello provoca pertanto un aumento di flusso nei

punti di misurazione del PFH_D che può ritenersi, per quanto detto, solo minimale.

Un effetto secondario della semplificazione è l'eliminazione della transizione distribuita uniformemente e dovuta alla richiesta della funzione di sicurezza.

Il **secondo step** di semplificazione del modello consiste nell'unione dello stato di inibizione delle operazioni con lo stato "OK". Questa riformulazione in pratica consiste nel trascurare il tempo medio alla riparazione, il MTTR, una volta assunto lo stato di inibizione delle operazioni. Il modello risultante è mostrato nella seguente Figura 5.4:

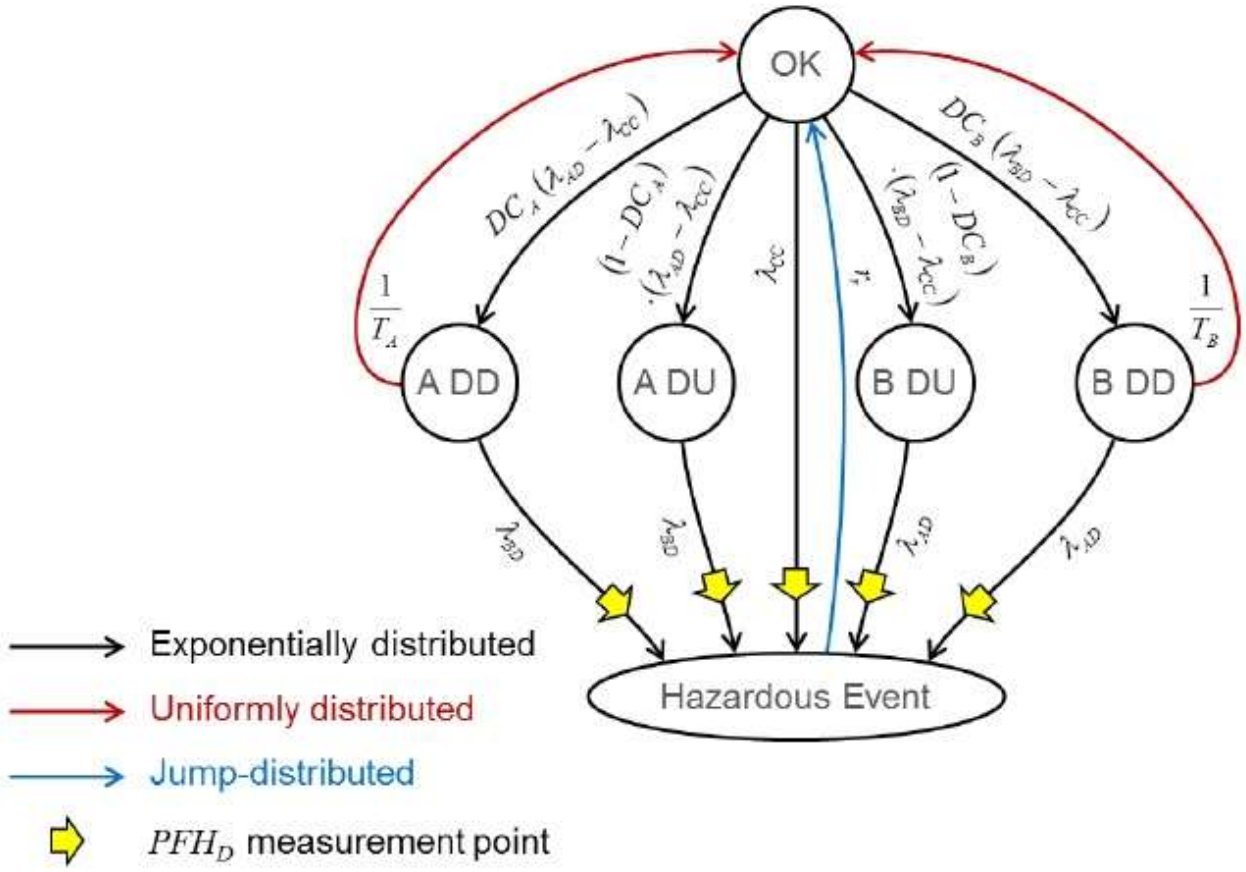


Figura 5.4: Modello 1oo2D, secondo step nella semplificazione.

Come si può notare nella Figura 5.4, le transizioni relative al test di uno dei due canali, comprendente la rilevazione di un guasto, non portano più allo stato di inibizione delle operazioni, che viene considerato virtualmente vuoto, ma portano il sistema direttamente allo stato "OK".

Rispetto alla misura del PFH_D costituisce una piccola stima dalla parte della sicurezza, perché, essendo il tasso di riparazione r_r considerabilmente più alto di tutti i tassi di guasto si può ritenere lo stato di inibizione delle operazioni virtualmente vuoto. Omettere questo stato nel modello in Figura 5.3 produce una crescita dei flussi nei punti di misura del PFH_D solo minimale, causata dall'aumento della probabilità che ha il sistema di trovarsi nello stato "OK".

Un effetto secondario della semplificazione è l'eliminazione delle transizioni distribuite a gradino e relative alle riparazioni esclusivamente a seguito dell'inibizione delle operazioni.

Le sole transizioni non distribuite esponenzialmente contenute nel modello in Figura 5.4 sono ora quelle relative ai test dei canali A e B che rilevano un guasto pericoloso e quella relativa alla riparazione che segue l'evento indesiderato.

Per il **terzo step** di semplificazione è necessario effettuare alcune considerazioni riguardo il modello rappresentato in Figura 5.4.

Le probabilità degli stati presenti in tale modello possono essere determinate da un'analisi eseguita attraverso l'utilizzo di un modello di Markov multifase. Procedendo in questa determinata maniera il tempo, all'interno del modello, deve essere fermato non appena avviene un test efficace in uno dei due canali funzionali, ovvero non appena viene rilevato un guasto attraverso la diagnostica. La probabilità ottenuta, nel momento in cui viene fermato il tempo per il test, deve essere in seguito trasferita da uno dei due stati dove è possibile che la diagnostica sia efficace, ovvero da "A DD" o da "B DD", allo stato "OK". Una volta trasferita la probabilità allo stato "OK" è necessario considerare il modello come viene fatto inizialmente, con una nuova distribuzione di probabilità.

La procedura appena descritta deve essere utilizzata fino al raggiungimento del tempo di missione T_M. Il $pfh_D(t)$, valore istantaneo del PFH_D, deve essere calcolato dalle probabilità ricavate dalla procedura, suddividendolo in intervalli di tempo, ed il PFH_D si ricava la sua media per l'intero tempo di missione.

Con questa procedura il numero di intervalli di tempo da utilizzare fino alla fine del tempo di missione varia in modo considerevole in base agli intervalli di test, T_A e T_B. Un elevato numero di cicli produce un elevato numero di suddivisione nel calcolo del PFH_D.

Questo approccio non può essere utilizzato in modo efficace, data l'elevata variabilità nel numero e nella lunghezza delle suddivisioni del PFH_D, che crea una coesione di equazioni difficili da realizzare e da analizzare.

Viene introdotto, per quanto descritto, un differente approccio di calcolo, comprendente il terzo step di semplificazione del modello, nel quale gli stati "A DD" e "B DD", presenti nel modello in Figura 5.4, vengono eliminati.

L'eliminazione degli stati "A DD" e "B DD" viene effettuata con l'ausilio di una procedura, applicata in maniera identica per tutti e due gli stati. La stessa viene descritta in seguito, per compattezza, solamente per lo stato "A DD", prendendolo come esempio.

Tra lo stato "OK" e lo stato "A DD" sono presenti due transizioni di stato, una dallo stato "OK" ad "A DD" che rappresenta l'avvenimento di un guasto rilevabile del canale A ed una dallo stato "A DD" allo stato "OK" che rappresenta il test del canale A. La procedura consiste nel sostituire, a queste due transizioni, una sola transizione, dallo stato "OK" allo stato "A DD", avente un tasso surrogato, denominato $\lambda_{A\,SI}$. Come risultato dell'eliminazione della transizione relativa al test, lo stato "A DD" è raggiunto a seguito di guasti non rilevabili del canale A ed il sistema si comporta di conseguenza, non essendo più possibile ricorrere alla diagnostica. Lo stato "A DD" viene rinominato pertanto "A DU 2".

La seguente Figura 5.5 mostra quanto appena descritto, nella sua parte sinistra è rappresentato il modello a seguito del secondo step di semplificazione, con un focus sugli stati relativi ai guasti del canale A, nella parte destra della figura è rappresentata la stessa parte di grafico di transizione degli stati con le modifiche appena descritte, ovvero la ridenominazione dello stato "A DD" in "A DU 2", l'eliminazione della transizione relativa al test e l'implementazione del tasso di guasto surrogato $\lambda_{A\,SI}$:

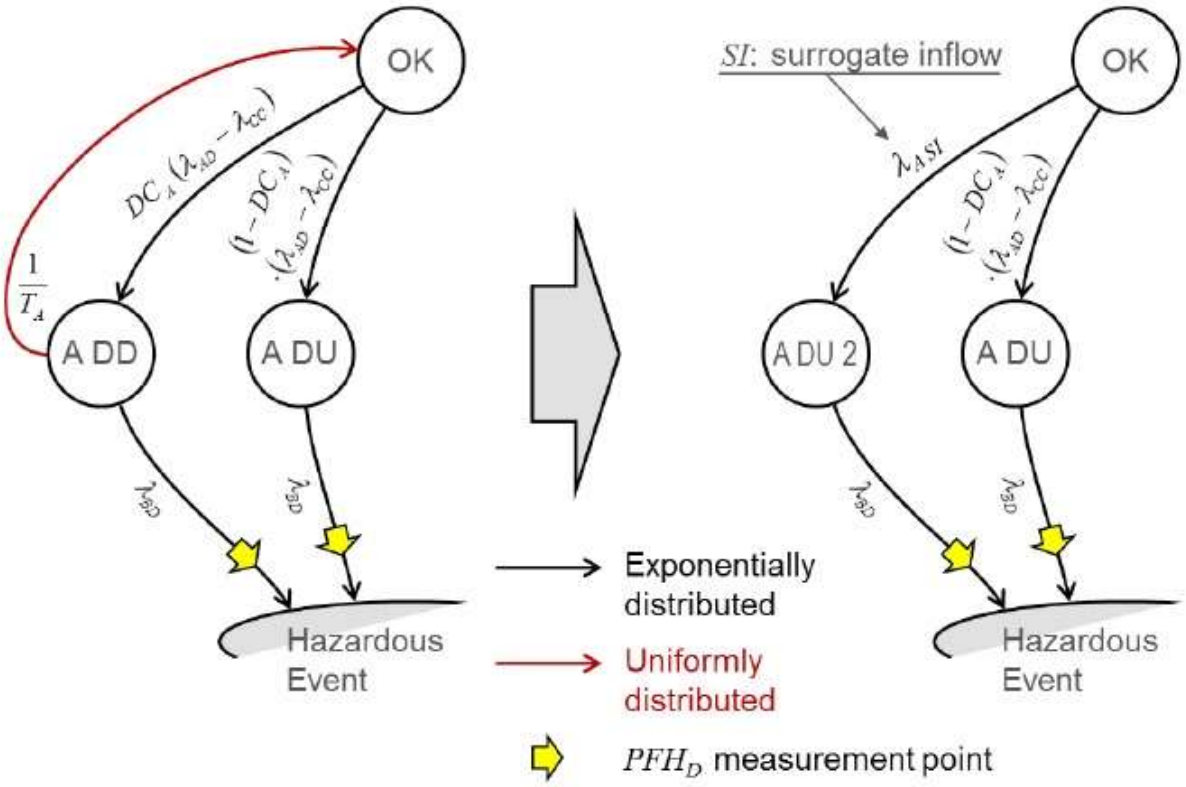


Figura 5.5: Tasso di transizione surrogato verso lo stato "A DD".

Per ricavare un valore approssimato del tasso surrogato $\lambda_{A\,SI}$ è necessario il valore medio nel tempo della probabilità dello stato "A DD", che è calcolato in base alla parte sinistra della Figura 5.5, ignorando la transizione di stato uscente, con tasso λ_{BD}. Per approssimazione lineare della funzione esponenziale (con la quale in generale si descrive l'inaffidabilità di un dispositivo), si può stabilire che la probabilità dello stato "A DD" sia la probabilità dello stato "OK" moltiplicata per il tasso di transizione e per il tempo, come mostrato nella seguente equazione:

$$P_{A\,DD}(t) \approx P_{OK}(t) \cdot DC_A(\lambda_{AD} - \lambda_{CC}) \cdot t \tag{5.3}$$

Per ricavare la probabilità media è necessario integrare la probabilità istantanea. Considerando che il sistema abbandona lo stato "A DD", una volta entrato in esso, in modo frequente con un tempo pari a T_A, la probabilità media sarà calcolata su di un tempo pari allo stesso T_A. Dalla precedente equazione 5.3 si ricava per integrazione un'approssimazione della probabilità media dello stato "A DD", considerando costante la probabilità dello stato "OK":

$$P_{A\,DD} \approx \frac{1}{T_A} \cdot \int_0^{T_A} P_{OK} \cdot DC_A(\lambda_{AD} - \lambda_{CC}) \cdot t\, dt = \frac{1}{2} P_{OK} DC_A(\lambda_{AD} - \lambda_{CC}) T_A \quad (5.4)$$

È necessario, al fine di ricavare $\lambda_{A\,SI}$, il valore medio nel tempo della probabilità dello stato "A DU 2", che è calcolato in base alla parte destra della Figura 5.5, ignorando la transizione di stato uscente, con tasso λ_{BD}. Per approssimazione lineare della funzione esponenziale si può stabilire che la probabilità dello stato "A DU 2" sia la probabilità dello stato "OK" moltiplicata per il tasso di transizione e per il tempo, come mostrato nella seguente equazione:

$$P_{A\,DU\,2}(t) \approx P_{OK}(t) \cdot \lambda_{A\,SI} \cdot t \quad (5.5)$$

Per ricavare la probabilità media è necessario integrare la probabilità istantanea. La media è effettuata su tutta la durata del tempo di missione T_M, dato che lo stato "A DU 2" non ha nessuna transizione verso altri stati, viste le semplificazioni introdotte sulla transizione con tasso λ_{BD}. Dalla precedente equazione 5.5 si ricava per integrazione un'approssimazione della probabilità media dello stato "A DU 2", considerando costante la probabilità dello stato "OK":

$$P_{A\,DU\,2} \approx \frac{1}{T_M} \cdot \int_0^{T_M} P_{OK} \cdot \lambda_{A\,SI} \cdot t\, dt = \frac{1}{2} P_{OK} \lambda_{A\,SI} T_M \quad (5.6)$$

Eguagliando la probabilità degli stati "A DD" ed "A DU 2", espressa nelle equazioni 5.4 e 5.6, si ricava la seguente equazione:

$$\frac{1}{2} P_{OK} DC_A(\lambda_{AD} - \lambda_{CC}) T_A = \frac{1}{2} P_{OK} \lambda_{A\,SI} T_M \quad (5.7)$$

Semplificando quanto compare in entrambi i membri dell'equazione 5.7 ed isolando il tasso surrogato $\lambda_{A\,SI}$, si ottiene l'espressione dello stesso utilizzata nella semplificazione:

$$\lambda_{A\,SI} = DC_A(\lambda_{AD} - \lambda_{CC}) \frac{T_A}{T_M} \quad (5.8)$$

Questo approccio molto semplice, che ha prodotto l'equazione 5.8 per il tasso surrogato $\lambda_{A\,SI}$, in alcuni casi, produce dei risultati non ottimali, per le seguenti motivazioni:

- Ad alti tassi di guasto, alta copertura diagnostica e con alcuni test efficaci e riparazioni durante il tempo di missione, la probabilità dello stato "OK" è soggetta ad una fluttuazione non ininfluente, interferendo con le probabilità degli altri stati. Le riparazioni, con il tasso surrogato, non sono emulate in modo efficiente ma sono livellate nel tempo.
- L'incremento di probabilità degli stati "A DD" e "A DU 2", ovvero di $P_{A\,DD}(t)$ e $P_{A\,DU\,2}(t)$, implicati nelle equazioni 5.3 e 5.5, è sostanzialmente più debole che lineare perché, in realtà, la probabilità dello stato sorgente "OK", ovvero $P_{OK}(t)$, non è costante nel tempo ma bensì decrescente.

- L'approssimazione lineare applicata alla funzione esponenziale può non essere sufficientemente precisa nel modello, perché l'argomento della stessa, ovvero il tasso di guasto moltiplicato per il tempo, non sempre è $<< 1$ e, in alcuni casi, può anche essere > 1.

Gli indicatori mostrano comunque che l'approccio di semplificazione selezionato è molto più preciso di quanto possa far pensare in primo luogo la sua semplicità:

- L'approccio lineare per le probabilità degli stati "A DD" e "A DU 2", espresso nelle equazioni 5.3 e 5.4, è di fatto non rappresentativo nel modello surrogato come un incremento lineare di $P_{A\,DU\,2}(t)$, perché la $P_{OK}(t)$, in realtà diventa minore senza di essa nel corso del tempo di missione T_M.
- I primi guasti del canale A, teoricamente rilevabili ma rimasti non rilevati a causa della sequenza di eventi, sono trattati in modo completamente corretto come primi guasti pericolosi non rilevabili, e pertanto contribuiscono come tali al calcolo del PFH_D.
- Il fatto che i primi guasti pericolosi rilevabili, i quali vengono rilevati e riparati con successo entro un tempo trascurabilmente breve, non vengono recuperati correttamente dallo stato "OK" riflette la loro riparazione e quindi la stabilizzazione della probabilità dello stato "OK".
- Le fluttuazioni di probabilità causate da processi di riparazione a tempo discreto non sono considerate come uno svantaggio, perché solo il valore medio del PFH_D nel tempo di missione T_M deve essere calcolato e non il PFH_D caratteristico nel corso del tempo.
- I casi limite, ovvero $T_A = 0$ e $T_A = T_M$, sono modellati correttamente. Nel primo caso, lo stato "A DD" rimane vuoto e lo stato "A DU 2" anche, nel modello surrogato, perché il tasso surrogato $\lambda_{A\,SI} = 0$. Nel secondo caso, la prima componente di guasto $DC_A(\lambda_{AD} - \lambda_{CC})$, la quale è di fatto la componente rilevabile, produce un flusso dal canale A allo stato "A DU 2" nel modello surrogato, com'è plausibile quando il test non viene effettuato durante tutto il tempo di missione.

Questa procedura, che prevede la modellazione con il tasso surrogato, è ritenuta adatta per l'analisi, sulla base di quanto appena descritto. Si procede pertanto utilizzandola nei calcoli successivi.

Nella seguente Figura 5.6, corrispondente al terzo step di semplificazione, viene applicato quanto descritto per lo stato "A DD". In modo del tutto analogo anche per lo stato "B DD" è applicata la stessa procedura. I due stati vengono sostituiti dagli stati "A DU 2" e "B DU 2", con i tassi di transizione surrogati dallo stato "OK" e senza più la transizione relativa al test:

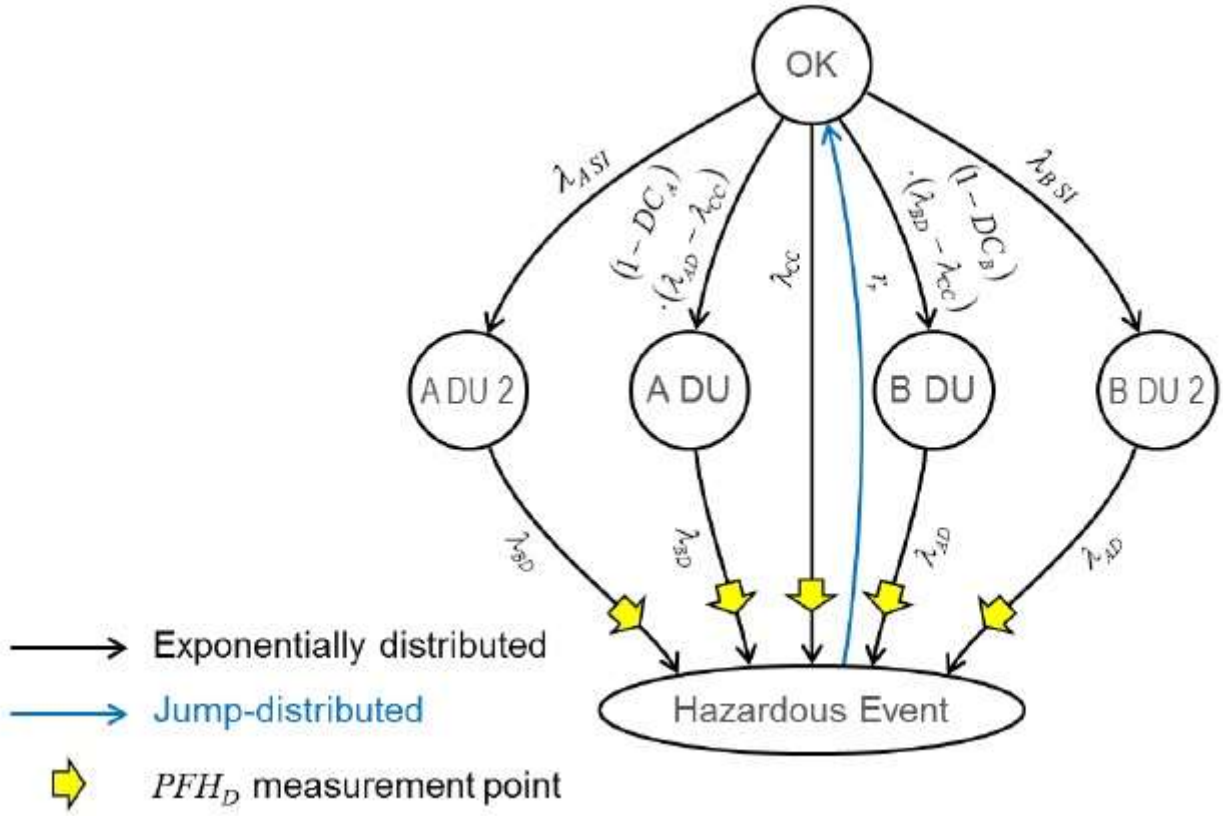


Figura 5.6: Modello 1oo2D, terzo step nella semplificazione.

In modo analogo al tasso surrogato $\lambda_{A\,SI}$, viene espresso il tasso surrogato anche per lo stato "B DU 2". La seguente equazione è ricavata direttamente dalla 5.8:

$$\lambda_{B\,SI} = DC_B(\lambda_{BD} - \lambda_{CC})\frac{T_B}{T_M} \tag{5.9}$$

Nel **quarto step** di semplificazione, si nota che gli stati "A DU" ed "A DU 2" hanno entrambi una transizione verso lo stato di evento indesiderato ed entrambe hanno lo stesso tasso di transizione, ovvero λ_{BD}. Essendo "A DU" ed "A DU 2" alimentati dallo stesso stato sorgente, ovvero "OK", il nuovo stato, denominato ancora "A DU" e composto dall'unione dei due, avrà un tasso di transizione dallo stato "OK" pari alla somma dei due tassi di transizione originari. Il tasso di transizione verso lo stato di evento indesiderato rimane uguale a quello già presente.

Le stesse considerazioni sono valide per gli stati "B DU" e "B DU 2", che vengono pertanto uniti come gli stati "A DU" ed "A DU 2", applicando le stesse osservazioni.

Il risultato è rappresentato nella seguente Figura 5.7:

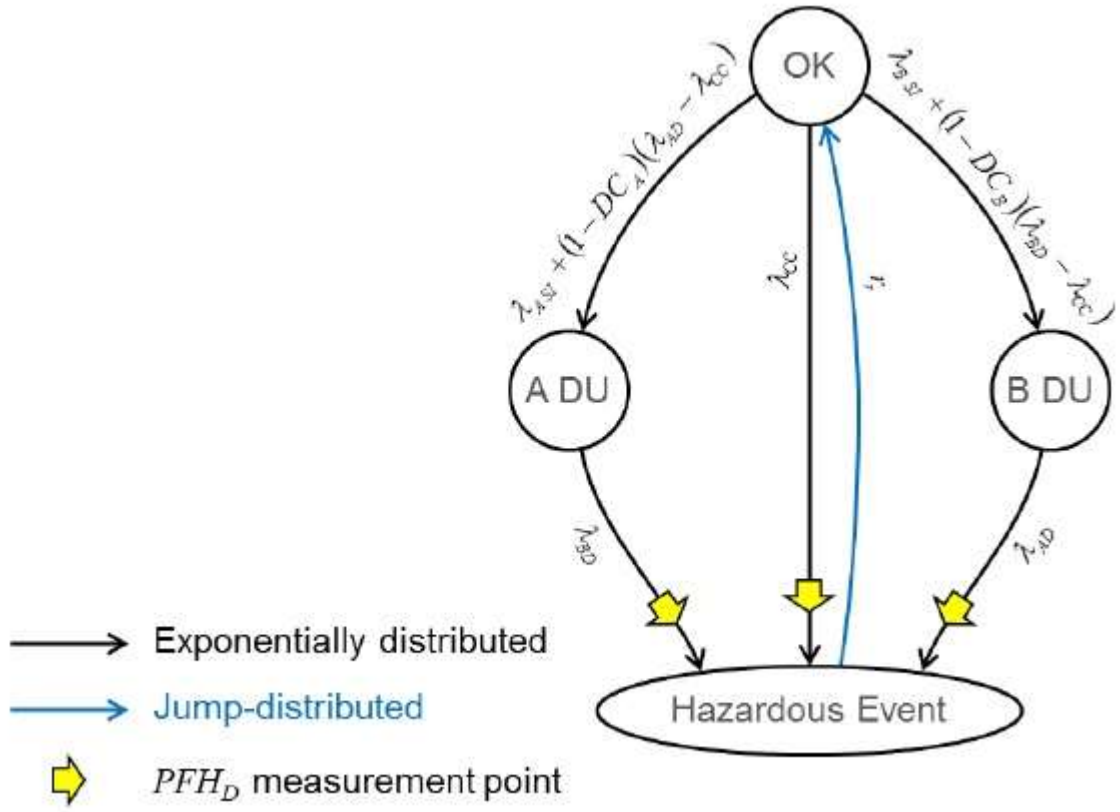


Figura 5.7: Modello 1oo2D, quarto step nella semplificazione.

Analizzando il tasso della transizione tra lo stato "OK" e lo stato "A DU", rappresentata in Figura 5.7, si può sostituire l'espressione di $\lambda_{A\,SI}$ con quella contenuta nell'equazione 5.8 e raccogliere prima $(\lambda_{AD} - \lambda_{CC})$ e poi DC_A. L'equazione ricavata è la seguente:

$$\lambda_{A\,SI} + (1 - DC_A)(\lambda_{AD} - \lambda_{CC}) = \left[1 - \left(1 - \frac{T_A}{T_M}\right) DC_A\right](\lambda_{AD} - \lambda_{CC}) \tag{5.10}$$

Si può introdurre la copertura diagnostica generalizzata del canale A, denominata $\overline{DC_A}$. Essa è sempre un valore adimensionale influenzata, oltre che dalla copertura diagnostica DC_A, anche dal rapporto tra l'intervallo di test medio del canale, T_A, ed il tempo di missione:

$$\overline{DC_A} = \left(1 - \frac{T_A}{T_M}\right) DC_A \tag{5.11}$$

Inserendo la copertura diagnostica generalizzata, descritta nell'equazione 5.11, nel risultato dell'equazione 5.10, si può ricavare una forma più compatta della stessa equazione, indicante il tasso di transizione tra lo stato "OK" ed "A DU" nel modello in Figura 5.7:

$$\lambda_{A\,SI} + (1 - DC_A)(\lambda_{AD} - \lambda_{CC}) = (1 - \overline{DC_A})(\lambda_{AD} - \lambda_{CC}) \tag{5.12}$$

Viene introdotta ora una variabile di semplificazione, denominata L_A ed utilizzata per indicare in maniera compatta il tasso di transizione tra lo stato "OK" e lo stato "A DU". Deriva da dei tassi di guasto e quindi ne prende la stessa unità di misura, $tempo^{-1}$. È descritta dalla seguente equazione, in accordo con la 5.10:

$$L_A = \left[1 - \left(1 - \frac{T_A}{T_M}\right) DC_A\right] (\lambda_{AD} - \lambda_{CC}) \tag{5.13}$$

Analizzando, in modo analogo, il tasso della transizione tra lo stato "OK" e lo stato "B DU", rappresentata in Figura 5.7, si può sostituire l'espressione di $\lambda_{B\,SI}$ con quella contenuta nell'equazione 5.9 e raccogliere prima $(\lambda_{BD} - \lambda_{CC})$ e poi DC_B. L'equazione ricavata è la seguente:

$$\lambda_{B\,SI} + (1 - DC_B)(\lambda_{BD} - \lambda_{CC}) = \left[1 - \left(1 - \frac{T_B}{T_M}\right) DC_B\right] (\lambda_{BD} - \lambda_{CC}) \tag{5.14}$$

Si può introdurre la copertura diagnostica generalizzata anche per il canale B, denominata $\overline{DC}_B$, che considera, oltre alla copertura diagnostica del canale B DC_B, anche il rapporto tra l'intervallo di test medio del canale, T_B, ed il tempo di missione:

$$\overline{DC}_B = \left(1 - \frac{T_B}{T_M}\right) DC_B \tag{5.15}$$

Inserendo la copertura diagnostica generalizzata, descritta nell'equazione 5.15, nel risultato dell'equazione 5.14, si può ricavare una forma più compatta della stessa equazione, indicante il tasso di transizione tra lo stato "OK" ed "B DU" nel modello in Figura 5.7:

$$\lambda_{B\,SI} + (1 - DC_B)(\lambda_{BD} - \lambda_{CC}) = (1 - \overline{DC}_B)(\lambda_{AD} - \lambda_{CC}) \tag{5.16}$$

Viene introdotta ora una variabile di semplificazione, denominata L_B ed utilizzata per indicare in maniera compatta il tasso di transizione tra lo stato "OK" e lo stato "B DU". Deriva da dei tassi di guasto e quindi ne prende la stessa unità di misura, $tempo^{-1}$. È descritta dalla seguente equazione, in accordo con la 5.14:

$$L_B = \left[1 - \left(1 - \frac{T_B}{T_M}\right) DC_B\right] (\lambda_{BD} - \lambda_{CC}) \tag{5.17}$$

La seguente Figura 5.8 mostra il modello nel quarto step di semplificazione, corrispondente al modello in Figura 5.7 ma con l'utilizzo delle variabili di semplificazione L_A ed L_B, introdotte nelle equazioni 5.13 e 5.17 ed indicanti i tassi delle transizioni dallo stato "OK" agli stati "A DU" e "B DU":

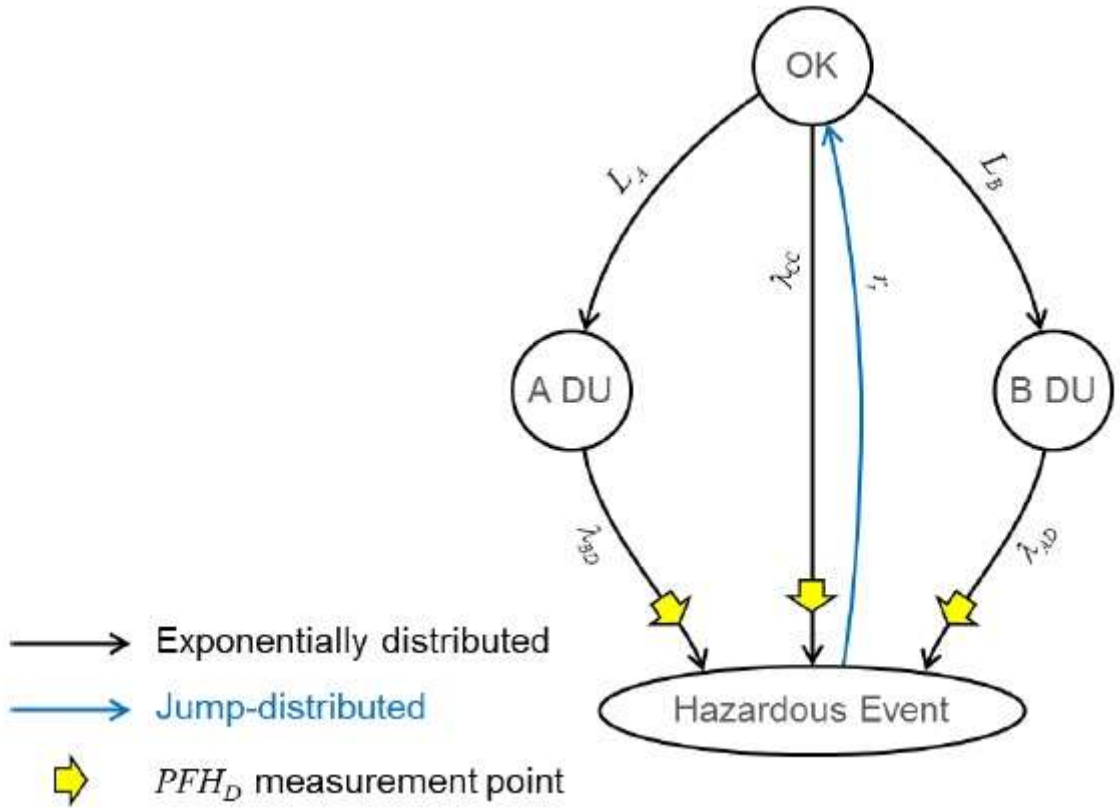


Figura 5.8: Modello 1oo2D, quarto step nella semplificazione con variabili di semplificazione.

Nel **quinto step** di semplificazione, viene ignorato il MTTR della riparazione ancora presente del modello, ovvero quella che avviene dopo che avviene l'evento indesiderato e che riporta il sistema allo stato "OK".

Il risultato della semplificazione è l'unione dello stato di evento indesiderato con lo stato "OK", come mostrato nella seguente Figura 5.9:

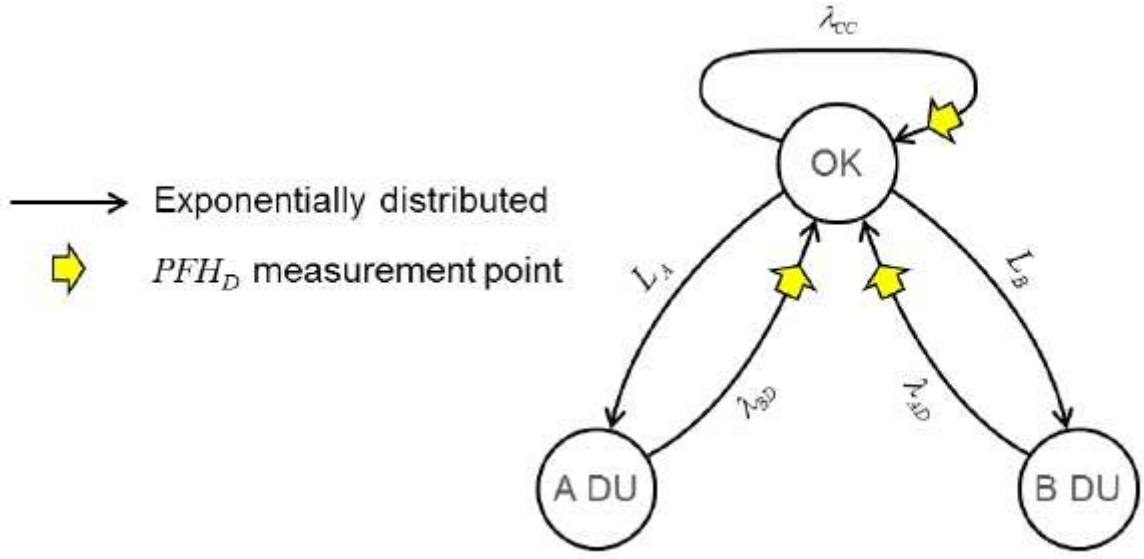


Figura 5.9: Modello 1oo2D, quinto step nella semplificazione.

La transizione relativa alle cause comuni di guasto porta ora il sistema dallo stato "OK" allo stesso stato "OK", non viene eliminata perché contiene un punto di misurazione del PFH_D, che è mantenuto. La semplificazione implica che lo stato di evento indesiderato sia virtualmente vuoto, ne consegue, come già descritto più volte, un piccolo aumento del PFH_D tramite questa semplificazione in favore della sicurezza.

Dopo l'eliminazione della transizione dovuta alla riparazione distribuita a gradino, il modello rappresentato in Figura 5.9 contiene ora solamente processi di transizione distribuiti esponenzialmente ed è pertanto definibile come un modello di Markov.

5.3 Utilizzo del modello di Markov a tre stati

Per l'utilizzo del modello di Markov a tre stati si considera il modello semplificato rappresentato in Figura 5.9. In tale modello la transizione dallo stato "OK" allo stesso non viene considerata, in quanto non ha influenza sulle probabilità dei tre stati rimanenti ma solo nella valutazione del PFH_D.

Inizialmente verrà analizzato un modello di Markov a tre stati generalizzato, rappresentato nella seguente Figura 5.10 ed utilizzato in seguito per il calcolo della probabilità che avrà il sistema di trovarsi in ogni stato:

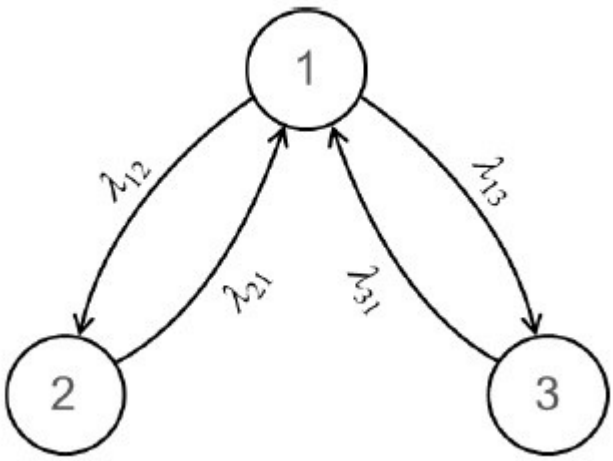


Figura 5.10: Modello di Markov a tre stati.

Il modello di Markov rappresentato in Figura 5.10 è descritto da un sistema composto dalle seguenti tre equazioni differenziali:

$$\dot{p_1}(t) = -(\lambda_{12} + \lambda_{13}) \cdot p_1(t) + \lambda_{21} \cdot p_2(t) + \lambda_{31} \cdot p_3(t) \quad (5.18)$$

$$\dot{p_2}(t) = \lambda_{12} \cdot p_1(t) - \lambda_{21} \cdot p_2(t) \quad (5.19)$$

$$\dot{p_3}(t) = \lambda_{13} \cdot p_1(t) - \lambda_{31} \cdot p_3(t) \quad (5.20)$$

Il sistema, inizialmente (a $t = 0$) si troverà nello stato 1, pertanto le condizioni iniziali saranno le seguenti:

$$p_1(0) = 1 \tag{5.21}$$

$$p_2(0) = 0 \tag{5.22}$$

$$p_3(0) = 0 \tag{5.23}$$

La soluzione del sistema di equazioni differenziali (equazioni 5.18, 5.19 e 5.20) è trovata con l'ausilio delle condizioni iniziali (equazioni 5.21, 5.22 e 5.23) ed applicando uno dei metodi per la soluzione di sistemi di equazioni differenziali, come ad esempio il metodo, già descritto, comprendente la trasformata di Laplace e le espansioni di Heaviside. In alternativa la soluzione può essere ricercata in letteratura:

$$\begin{aligned} p_1(t) = {} & \frac{\lambda_{21} \cdot \lambda_{31}}{\lambda_{12} \cdot \lambda_{31} + \lambda_{13} \cdot \lambda_{21} + \lambda_{21} \cdot \lambda_{31}} + \frac{(L_1 + L_2 - 2\lambda_{21})(L_1 + L_2 - 2\lambda_{31})}{2L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1+L_2)t} \\ & - \frac{(L_2 - L_1 - 2\lambda_{21})(L_2 - L_1 - 2\lambda_{31})}{2L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2-L_1)t} \end{aligned} \tag{5.24}$$

$$\begin{aligned} p_2(t) = {} & \frac{\lambda_{12} \cdot \lambda_{31}}{\lambda_{12} \cdot \lambda_{31} + \lambda_{13} \cdot \lambda_{21} + \lambda_{21} \cdot \lambda_{31}} - \frac{\lambda_{12}(L_1 + L_2 - 2\lambda_{31})}{L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1+L_2)t} \\ & + \frac{\lambda_{12}(L_2 - L_1 - 2\lambda_{21})}{L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2-L_1)t} \end{aligned} \tag{5.25}$$

$$\begin{aligned} p_3(t) = {} & \frac{\lambda_{13} * \lambda_{21}}{\lambda_{12} * \lambda_{31} + \lambda_{13} * \lambda_{21} + \lambda_{21} * \lambda_{31}} - \frac{\lambda_{13}(L_1 + L_2 - 2\lambda_{21})}{L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1+L_2)t} \\ & + \frac{\lambda_{13}(L_2 - L_1 - 2\lambda_{21})}{L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2-L_1)t} \end{aligned} \tag{5.26}$$

Nella soluzione del modello di Markov generalizzato, descritta dalle precedenti equazioni 5.24, 5.25 e 5.26, sono state inserite delle variabili di semplificazione, denominate L_1 ed L_2. Esse derivano da dei tassi di guasto e quindi ne assumono la stessa unità di misura, $tempo^{-1}$. Sono esplicitate nelle seguenti equazioni:

$$L_1 = \sqrt{(\lambda_{12} + \lambda_{13})^2 + 2(\lambda_{12} - \lambda_{13})(\lambda_{21} - \lambda_{31}) + (\lambda_{21} - \lambda_{31})^2} \tag{5.27}$$

$$L_2 = \lambda_{12} + \lambda_{13} + \lambda_{21} + \lambda_{31} \tag{5.28}$$

Comparando il modello di Markov generalizzato, rappresentato in Figura 5.10, con il modello semplificato relativo all'architettura 1oo2D, rappresentato in Figura 5.9, si possono ottenere le seguenti correlazioni:

$$p_1(t) = p_{OK}(t) \tag{5.29}$$

$$p_2(t) = p_{A\,DU}(t) \tag{5.30}$$

$$p_3(t) = p_{B\,DU}(t) \tag{5.31}$$

$$\lambda_{12} = L_A \tag{5.32}$$

$$\lambda_{13} = L_B \tag{5.33}$$

$$\lambda_{21} = \lambda_{BD} \tag{5.34}$$

$$\lambda_{31} = \lambda_{AD} \tag{5.35}$$

Le condizioni iniziali relative al modello semplificato corrispondo a quelle del modello di Markov generalizzato (equazioni 5.21, 5.22 e 5.23), con la sostituzione delle variabili per mezzo delle correlazioni riportate nelle equazioni 5.29, 5.30 e 5.31. Il sistema, inizialmente (a $t = 0$) si troverà nello stato "OK":

$$p_{OK}(0) = 1 \tag{5.36}$$

$$p_{A\,DU}(0) = 0 \tag{5.37}$$

$$p_{B\,DU}(0) = 0 \tag{5.38}$$

La soluzione del modello concreto, specifico per la modellazione semplificata dell'architettura 1oo2D, è riportata nelle seguenti equazioni, che corrispondono a quelle del modello generalizzato (equazioni 5.24, 5.25 e 5.26) con inserite le correlazioni presenti (equazioni dalla 5.29 alla 5.35):

$$\begin{aligned} p_{OK}(t) = {} & \frac{\lambda_{AD} \cdot \lambda_{BD}}{L_A \cdot \lambda_{AD} + L_B \cdot \lambda_{BD} + \lambda_{AD} \cdot \lambda_{BD}} \\ & + \frac{(L_1 + L_2 - 2\lambda_{AD})(L_1 + L_2 - 2\lambda_{BD})}{2L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1 + L_2)t} \\ & - \frac{(L_2 - L_1 - 2\lambda_{AD})(L_2 - L_1 - 2\lambda_{BD})}{2L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2 - L_1)t} \end{aligned} \tag{5.39}$$

$$\begin{aligned} p_{A\,DU}(t) = {} & \frac{L_A \cdot \lambda_{AD}}{L_A \cdot \lambda_{AD} + \lambda_B \cdot \lambda_{BD} + \lambda_{AD} \cdot \lambda_{BD}} - \frac{L_A(L_1 + L_2 - 2\lambda_{AD})}{L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1 + L_2)t} \\ & + \frac{L_B(L_2 - L_1 - 2\lambda_{BD})}{L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2 - L_1)t} \end{aligned} \tag{5.40}$$

$$p_{B\,DU}(t) = \frac{L_B \cdot \lambda_{BD}}{L_A \cdot \lambda_{AD} + \lambda_B \cdot \lambda_{BD} + \lambda_{AD} \cdot \lambda_{BD}} - \frac{L_B(L_1 + L_2 - 2\lambda_{BD})}{L_1(L_1 + L_2)} e^{-\frac{1}{2}(L_1+L_2)t} + \frac{L_B(L_2 - L_1 - 2\lambda_{BD})}{L_1(L_2 - L_1)} e^{-\frac{1}{2}(L_2-L_1)t} \quad (5.41)$$

L'espressione delle variabili di semplificazione, denominate L_1 ed L_2 ed utilizzate nelle precedenti equazioni 5.39, 5.40 e 5.41, sono ricavate sostituendo, alle rispettive espressioni del modello generalizzato (equazioni 5.27 e 5.28), le correlazioni presenti tra i due modelli e descritte nelle equazioni 5.32, 5.33, 5,34 e 5,35:

$$L_1 = \sqrt{(L_A + L_B)^2 + 2(L_A - L_B)(\lambda_{BD} - \lambda_{AD}) + (\lambda_{BD} - \lambda_{AD})^2} \quad (5.42)$$

$$L_2 = L_A + L_B + \lambda_{AD} + \lambda_{BD} \quad (5.43)$$

5.4 Modello 1oo2D, calcolo PFH_D con test a tempo discreto

Il valore istantaneo del PFH_D, il $pfh_D(t)$, può essere calcolato, in accordo con la Figura 5.9, tramite la sommatoria delle probabilità dei tre stati presenti, moltiplicate per i tassi relativi alle transizioni contenenti punti di misurazione del PFH_D. Il risultato è espresso nella seguente equazione:

$$pfh_D(t) = \lambda_{CC} p_{OK}(t) + \lambda_{BD} p_{A\,DU}(t) + \lambda_{AD} p_{B\,DU}(t) \quad (5.44)$$

L'equazione per il calcolo del PFH_D è ricavata dal $pfh_D(t)$, espresso nella precedente equazione 5.44. Essendo il suo valore medio, valutato durante il tempo di missione T_M, l'equazione risultante è la seguente:

$$PFH_D = \frac{1}{T_M}\int_0^{T_M} pfh_D(t)dt = \frac{1}{T_M}\int_0^{T_M} [\lambda_{CC} p_{OK}(t) + \lambda_{BD} p_{A\,DU}(t) + \lambda_{AD} p_{B\,DU}(t)]dt \quad (5.45)$$

Risolvendo l'equazione 5.45, raccogliendo i termini e con l'ausilio di variabili di semplificazione, che verranno trattate in seguito, si ottiene la seguente espressione del PFH_d:

$$PFH_D = \frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_A\lambda_{AD} + L_B\lambda_{BD} + \lambda_{AD}\lambda_{BD}} + \frac{C_P}{T_M}\left[1 - e^{-\frac{1}{2}(L_1+L_2)T_M}\right] - \frac{C_N}{T_M}\left[1 - e^{-\frac{1}{2}(L_1-L_2)T_M}\right] \quad (5.46)$$

Nell'equazione 5.46 sono utilizzate le variabili di semplificazione L_A ed L_B, già definite nelle equazioni 5.13 e 5.17. Con il supporto delle equazioni 5.1 e 5.2 è possibile ricavare delle espressioni di tali variabili di semplificazione contenenti i tassi di test dei canali A e B: r_{tA} ed r_{tB}:

$$L_A = (\lambda_{AD} - \lambda_{CC})\left[1 - \left(1 - \frac{1}{r_{tA}T_M}\right) DC_A\right] \quad (5.47)$$

$$L_B = (\lambda_{BD} - \lambda_{CC})\left[1 - \left(1 - \frac{1}{r_{tB}T_M}\right)DC_B\right] \quad (5.48)$$

Nell'equazione 5.46 sono utilizzate inoltre le variabili di semplificazione L_1 ed L_2, introdotte nelle equazioni 5.42 e 5.43. Tali equazioni vengono riportate in seguito per completezza nell'esposizione della soluzione:

$$L_1 = \sqrt{(L_A + L_B)^2 + 2(L_A - L_B)(\lambda_{BD} - \lambda_{AD}) + (\lambda_{BD} - \lambda_{AD})^2} \quad (5.42)$$

$$L_2 = L_A + L_B + \lambda_{AD} + \lambda_{BD} \quad (5.43)$$

Per completare la descrizione dell'equazione 5.46 è necessario esprimere altre due nuove variabili di semplificazione che sono state utilizzate in essa. Le due variabili adimensionali, denominate C_P e C_N, sono definite dalle seguenti equazioni:

$$C_P = \frac{\lambda_{CC}}{L_1} - 2\frac{\lambda_{AD}L_B + \lambda_{BD}L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1(L_1 + L_2)} + 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1(L_1 + L_2)^2} \quad (5.49)$$

$$C_N = \frac{\lambda_{CC}}{L_1} - 2\frac{\lambda_{AD}L_B + \lambda_{BD}L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1(L_2 - L_1)} + 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1(L_2 - L_1)^2} \quad (5.50)$$

5.5 Modello 1oo2D, calcolo PFH_D con test continuo

Se, in un'architettura 1oo2D (rappresentata in Figura 5.1), i due canali vengono testati in modo continuo, è possibile calcolare il PFH_D sempre utilizzando l'equazione 5.46 con le variabili di semplificazione relative.

Se il test viene effettuato in modo continuo i tassi di test dei due canali, A e B, tenderanno ad infinito, quindi $r_{tA} \to \infty$ ed $r_{tB} \to \infty$. Grazie e queste considerazioni è possibile ottenere una forma ancora più compatta delle variabili di semplificazione L_A ed L_B, semplicemente inserendo le condizioni di test continuo nelle equazioni 5.47 e 5.48.

Le equazioni ottenute sono le seguenti:

$$L_A = (1 - DC_A)(\lambda_{AD} - \lambda_{CC}) \quad (5.51)$$

$$L_B = (1 - DC_B)(\lambda_{BD} - \lambda_{CC}) \quad (5.52)$$

5.6 Modello 1oo2D, soluzione semplificata per test a tempo discreto e continuo

È possibile ottenere una soluzione più semplice e compatta per il calcolo del PFH_D, sempre relativa ad architetture 1oo2D, che può essere utilizzata come alternativa alla soluzione già introdotta ed

esplicitata dall'equazione 5.46, con l'ausilio delle opportune variabili di semplificazione.

La soluzione semplificata, che viene illustrata in seguito, necessita di stime che includono semplificazioni dal lato della sicurezza; per questa ragione il valore del PFH_D ottenuto sarà sempre maggiore rispetto al valore dello stesso ottenuto tramite la metodologia già mostrata.

Per procedere con questa semplificazione alternativa è necessario prendere in considerazione il sistema a due canali già considerato ed il relativo diagramma di transizione degli stati, modellizzato fino al secondo step di semplificazione. Il grafico risultante viene riportato nella seguente Figura 5.11, ed è identico a quello già rappresentato nella precedente Figura 5.4:

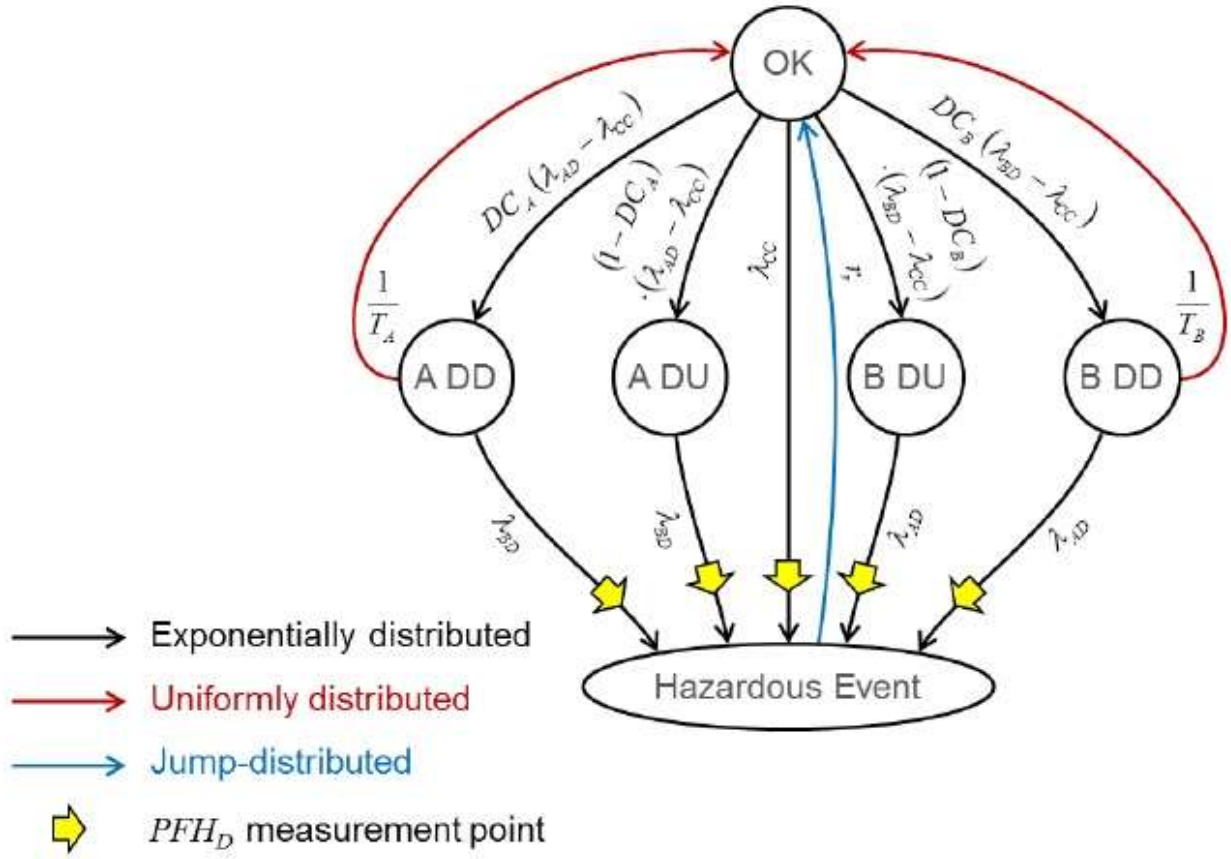


Figura 5.11: Modello 1oo2D, secondo step nella semplificazione (ripete la Figura 5.4).

Si effettua ora una scomposizione dei tassi di transizione che portano il sistema, dagli stati "A DD", "A DU", "B DD" e "B DU", allo stato di evento indesiderato. Ad ogni tasso di transizione viene sottratto il tasso di guasto per cause comuni, λ_{CC} e, ad ogni stato in questione, viene aggiunta una nuova transizione verso lo stato di evento indesiderato, avente come tasso di transizione lo stesso λ_{CC}.

Per gli stati "A DD", "A DU", "B DD" e "B DU" è semplice notare come questa operazione non cambi il tasso di transizione effettivo verso lo stato di evento indesiderato, infatti, sommando i due tassi di transizione ora presenti per ogni stato, si ottiene il tasso di transizione relativo che era presente nel modello in Figura 5.11. Il modello risultante è rappresentato nella seguente Figura 5.12, con le modifiche ai tassi di transizione e le nuove transizioni, definite ausiliari, rappresentati in color lilla:

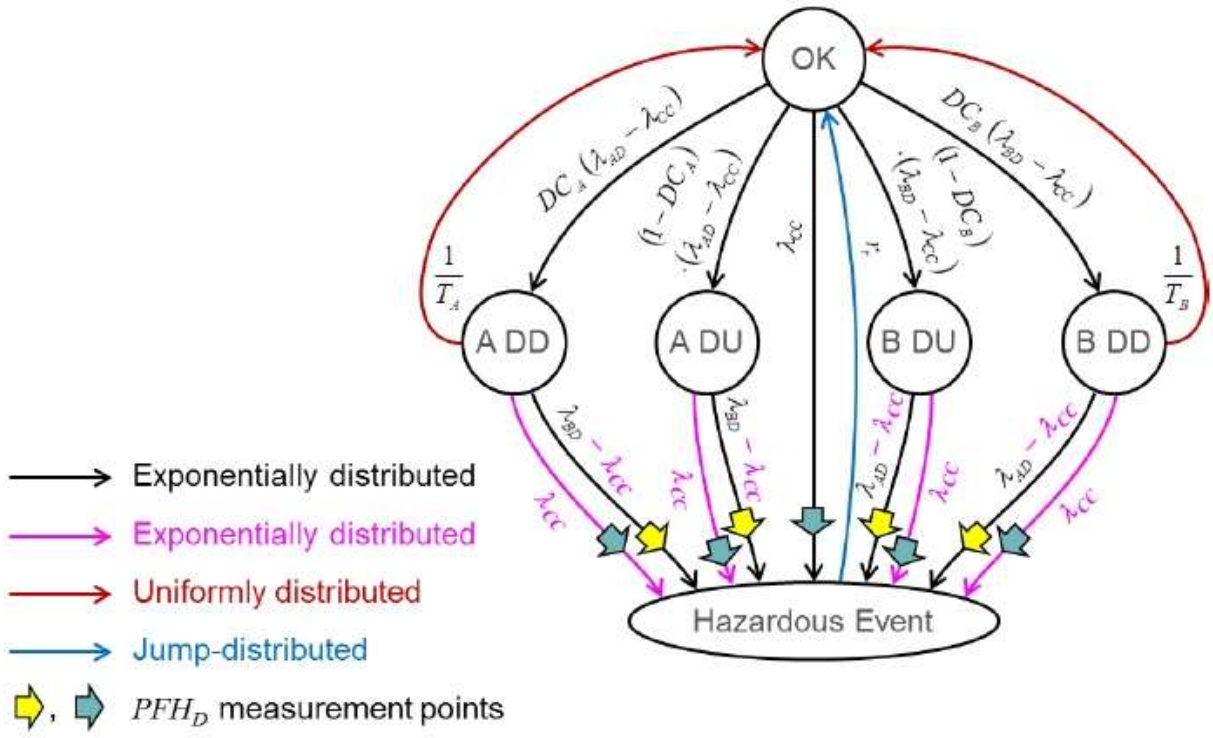


Figura 5.12: Modello 1oo2D, semplificazione con le transizioni ausiliari.

Lo stato relativo all'evento indesiderato possiede, in Figura 5.12, un totale di cinque transazioni entranti aventi tutte tasso pari a λ_{CC}. Le cinque sorgenti di tali transizioni sono gli stati "OK", "A DD", "A DU", "B DD" e "B DU". Essendo ogni transazione diretta allo stato di evento indesiderato è presente per ognuna di esse un punto di misurazione del PFH_d, rappresentati, per differenziarli e sempre in Figura 5.12, in azzurro anziché in giallo, compreso il punto di misurazione già presente relativo alla transizione con sorgente lo stato "OK".

In un grafico di transizione degli stati la somma delle probabilità di ogni stato presente è sempre pari ad 1. Nel modello rappresentato si può ritenere leggermente inferiore a 1 la somma delle probabilità dei soli stati "OK", "A DD", "A DU", "B DD" e "B DU", ovvero la somma delle probabilità degli stati sorgente delle transizioni con tasso pari a λ_{CC}.

La somma di tali probabilità si può ritenere inferiore a 1 di una quantità accettabile, dato che lo stato di evento indesiderato, abbandonato dal sistema a seguito di riparazioni, aventi tasso più elevato di tutte le transizioni relative a guasti, è quasi sempre vuoto. Ciò, tuttavia, costituisce una stima dalla parte della sicurezza perché, semplificando in questo modo, aumentano le probabilità degli altri stati e quindi il PFH_d calcolato sarà maggiorato.

Riassumendo, si ritiene la somma delle cinque sorgenti pari ad 1, escludendo dal computo la piccola componente relativa allo stato di evento pericoloso.

A questo punto, le cinque transizioni, con tasso pari a λ_{CC} ed aventi come origine gli stati sorgenti la cui somma di probabilità è stata assunta pari a 1, vengono sostituite da un'unica transizione di stato, avente sempre tasso di transizione pari a λ_{CC} ma generata da un nuovo stato sorgente,

aggiunto nel modello e chiamato stato ausiliario.

Lo stato ausiliario, indicato come "AUX" (dall'inglese Auxiliary), avendo lo scopo di sostituire i precedenti cinque stati sorgente, ha una probabilità costante e pari ad 1.

Il modello risultante è rappresentato nella seguente Figura 5.13. I punti di misurazione del PFH_d sono ora complessivamente cinque e vengono numerati, in particolare, quello relativo al nuovo stato ausiliario "AUX" è rappresentato ancora in azzurro, in quanto sostituisce i cinque che erano rappresentati in azzurro nella Figura 5.12:

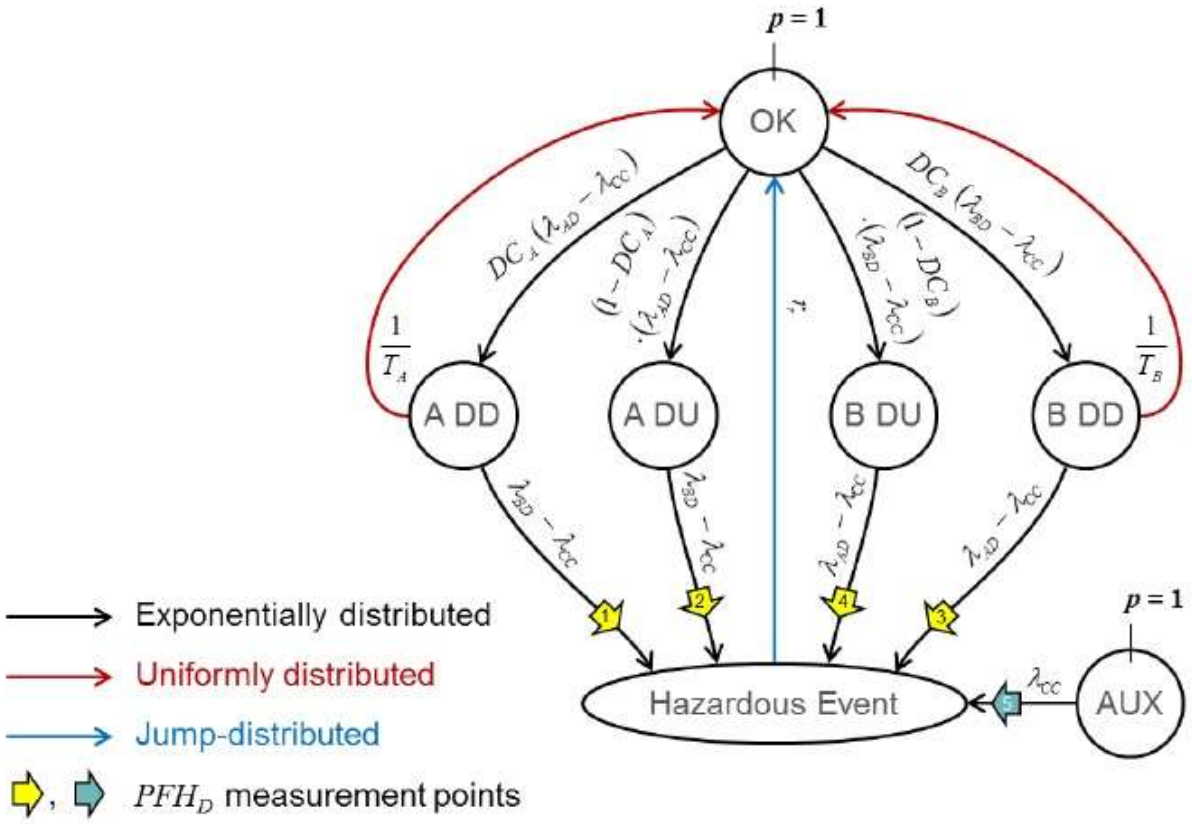


Figura 5.13: Modello 1oo2D, semplificazione con lo stato ausiliario.

Come ulteriore semplificazione, che costituisce un'ulteriore stima dalla parte della sicurezza, è assunto nel modello rappresentato in Figura 5.13, che lo stato "OK" abbia una probabilità costante nel tempo e pari a 1.

È importante sottolineare come, in un caso pratico, alti tassi di guasto ed un test con bassa efficienza facciano scendere significativamente la probabilità dello stato "OK" nel corso del tempo di missione T_M e come, pertanto, questa assunzione semplificativa conduca ad una sovrastima del PFH_D nelle equazioni che verranno derivate in seguito, nei sistemi con le caratteristiche appena descritte.

Settare arbitrariamente le probabilità degli stati "OK" ed "AUX" al valore costante di 1 consente di calcolare indipendentemente le cinque componenti del PFH_D, una per ogni percorso plausibile che causi l'evento indesiderato, percorso inteso come susseguirsi di transazioni dallo stato "OK".

Viene considerato, nella seguente Figura 5.14, un percorso generico, descritto dettagliatamente in seguito:

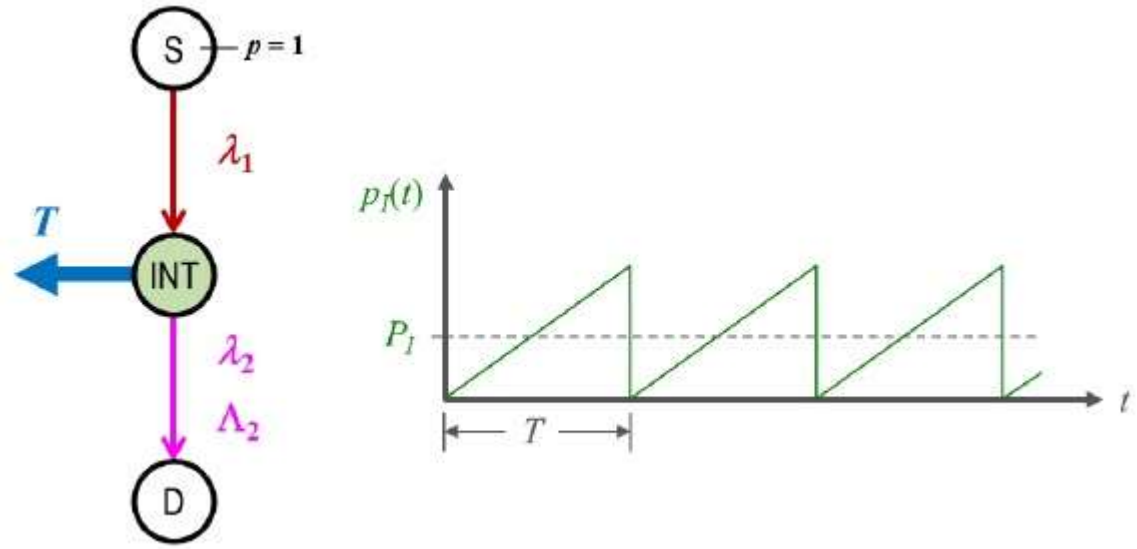


Figura 5.14: Generico stato "INT" con pulizia periodica.

In Figura 5.14 sono presenti tre stati:

- Stato "S": è lo stato sorgente, ha una probabilità pari ad 1,
- Stato "INT": è lo stato intermedio, è raggiunto, dallo stato "S", tramite una transizione con tasso λ_1 ed il sistema lo abbandona ad intervalli di durata T, come rappresentato in Figura 5.14,
- Stato "D": è lo stato di drenaggio, è raggiunto, dallo stato "INT", tramite una transizione con tasso nominale pari a λ_2 e tasso assoluto (tasso nominale moltiplicato per la probabilità dello stato "INT", lo stato sorgente) pari a Λ_2.

Nel procedimento seguente è ricercata un'espressione per il tasso assoluto di flusso uscente dallo stato "INT", ovvero Λ_2.

L'equazione differenziale applicabile per il calcolo della probabilità dello stato "INT", tra due pulizie è la seguente, considerando che lo stato sorgente della transizione con tasso λ_1, lo stato "S", ha una probabilità pari ad 1, $p_S(t) = 1$:

$$\dot{p}_{INT}(t) = \lambda_1 - \lambda_2 p_{INT}(t) \tag{5.53}$$

Inizialmente il sistema generico non si trova nello stato "INT", la condizione iniziale è pertanto:

$$p_{INT}(0) = 0 \tag{5.54}$$

La soluzione all'equazione differenziale 5.53, con la condizione iniziale riportata nell'equazione 5.54

è la seguente:

$$p_{INT}(t) = \frac{\lambda_1}{\lambda_2}\left(1 - e^{-\lambda_2 t}\right) \tag{5.55}$$

Il flusso uscente medio assoluto dallo stato "INT", ovvero Λ_2, è, su un intervallo di tempo pari a T, dato dal prodotto tra la probabilità media dello stato "INT", calcolata tramite integrale, ed il tasso di transizione nominale relativo alla transizione in questione, ovvero λ_2:

$$\Lambda_2 = \frac{\lambda_2}{T}\int_0^T p_{INT}(t)dt = \lambda_1\left(1 - \frac{1 - e^{-\lambda_2 T}}{\lambda_2 T}\right) \tag{5.56}$$

Utilizzando l'approssimazione quadratica della funzione esponenziale, riportata nella seguente equazione 5.57, si può ottenere un valore approssimato di Λ_2, il quale calcolo è riportato nell'equazione 5.58:

$$e^x \approx 1 + x + \frac{1}{2}x^2 \tag{5.57}$$

$$\Lambda_2 = \lambda_1\left(1 - \frac{1 - 1 + \lambda_2 T + \frac{1}{2}{\lambda_2}^2 T^2}{\lambda_2 T}\right) = \lambda_1\left(1 - 1 + \frac{1}{2}\lambda_2 T\right) = \frac{1}{2}\lambda_1\lambda_2 T \tag{5.58}$$

Per il calcolo del PFH_D è conveniente considerare separatamente ogni contributo dello stesso dovuto ai cinque punti di misurazione presenti in Figura 5.13. I contributi sono numerati coerentemente da PFH_{D1} a PFH_{D5} in base alla denominazione numerica riportata nei punti di misurazione sempre in Figura 5.13. Il risultato complessivo sarà la somma dei cinque contributi.

Il risultato dell'equazione 5.58 è utilizzato per determinare i quattro contributi dovuti alle transizioni che hanno lo stato "OK" come sorgente, ovvero a quelli rappresentati in giallo in Figura 5.13. L'equazione 5.58 e l'esempio riportato in Figura 5.14 permettono di analizzare correttamente tali contributi.

Si considera, nel calcolo del PFH_{D1}, una correlazione tra gli stati "OK", "A DD" e di evento indesiderato con gli stati "S", "INT" e "D" dell'esempio generico. Sono da utilizzare quindi i tassi di transizione presenti in Figura 5.13 tra questi stati e bisogna considerare inoltre che lo stato "A DD" è abbandonato dal sistema con intervalli di tempo pari al tempo di test del canale A, ovvero a T_A.

Sostituendo, come descritto, i tassi di transizione e l'intervallo di tempo di abbandono dello stato "A DD", nell'equazione 5.58, si ricava il primo contributo in termini di PFH_D:

$$PFH_{D1} = \frac{1}{2}DC_A(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})T_A \tag{5.59}$$

Nel calcolo del secondo contributo, che considera “A DU” come stato intermedio valgono le stesse considerazioni espresse precedentemente per lo stato “A DD”, con l’accorgimento che, al contrario di quest’ultimo stato, lo stato “A DU” non è soggetto a diagnostica e quindi non ha un intervallo di tempo di abbandono. Il tempo da considerare per la formazione della media è esteso pertanto fino al tempo di missione T_M.

In accordo con l’equazione 5.58 e con quanto appena espresso viene ricavato il secondo contributo in termini di PFH_D:

$$PFH_{D2} = \frac{1}{2}(1 - DC_A)(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})T_M \tag{5.60}$$

Il terzo contributo in termini di PFH_D, relativo alle transizioni ed al punto di misurazione che vedono coinvolto lo stato “B DD”, è determinato in modo analogo a quanto descritto per il primo contributo, nell’equazione 5.59:

$$PFH_{D3} = \frac{1}{2}DC_B(\lambda_{BD} - \lambda_{CC})(\lambda_{AD} - \lambda_{CC})T_B \tag{5.61}$$

Il quarto contributo in termini di PFH_D, relativo alle transizioni ed al punto di misurazione che vedono coinvolto lo stato “B DU”, è determinato in modo analogo a quanto descritto per il secondo contributo, nell’equazione 5.60:

$$PFH_{D4} = \frac{1}{2}(1 - DC_B)(\lambda_{BD} - \lambda_{CC})(\lambda_{AD} - \lambda_{CC})T_M \tag{5.62}$$

Il quinto contributo è ricavato semplicemente moltiplicando la probabilità dello stato “AUX”, che è pari a 1, per il tasso di transizione contenente il punto di misurazione del PFH_D, ovvero λ_{CC}:

$$PFH_{D5} = \lambda_{CC} \tag{5.63}$$

Il PFH_d totale è dato dalla somma dei cinque contributi appena esplicitati:

$$PFH_D = PFH_{D1} + PFH_{D2} + PFH_{D3} + PFH_{D4} + PFH_{D5} \tag{5.64}$$

Sostituendo, nell’equazione 5.64, le espressioni dei cinque contributi, contenuti nelle equazioni dalla 5.59 alla 5.63, e raccogliendo i termini comuni, si ottiene la seguente equazione:

$$PFH_D = \frac{1}{2}(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})[DC_A T_A + DC_B T_B + (2 - DC_A - DC_B)T_M] + \lambda_{CC} \tag{5.65}$$

Vengono riportate le equazioni 5.11 e 5.15, contenenti la già descritta copertura diagnostica generalizzata:

$$\overline{DC_A} = \left(1 - \frac{T_A}{T_M}\right) DC_A \tag{5.11}$$

$$\overline{DC_B} = \left(1 - \frac{T_B}{T_M}\right) DC_B \tag{5.15}$$

L'equazione 5.65 può essere riformulata con l'ausilio delle coperture diagnostiche generalizzate, descritte nelle equazioni 5.11 e 5.15:

$$PFH_d = \frac{1}{2}(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})(2 - \overline{DC_A} - \overline{DC_B})T_M + \lambda_{CC} \tag{5.66}$$

Nell'equazione 5.66, moltiplicando semplicemente la frazione per il terzo fattore dell'equazione, si più ottenere la seguente riformulazione:

$$PFH_d = (\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})\left(1 - \frac{\overline{DC_A} + \overline{DC_B}}{2}\right)T_M + \lambda_{CC} \tag{5.67}$$

L'equazione 5.65 può essere riformulata inoltre con la reintroduzione dei tassi di test dei canali A e B, ovvero r_{tA} ed r_{tB}, al posto dei tempi medi di test T_A e T_B, utilizzando le equazioni 5.1 e 5.2 in seguito riportate nuovamente:

$$r_{tA} = \frac{1}{T_A} \tag{5.1}$$

$$r_{tB} = \frac{1}{T_B} \tag{5.2}$$

La seguente equazione del PFH_D è prodotta con la procedura di sostituzione appena descritta (equazioni 5.1 e 5.2), applicata all'equazione 5.65:

$$PFH_D = \frac{1}{2}(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})\left[\frac{DC_A}{r_{tA}} + \frac{DC_B}{r_{tB}} + (2 - DC_A - DC_B)T_M\right] + \lambda_{CC} \tag{5.68}$$

È possibile semplificare ulteriormente l'equazione 5.68 in caso di completa simmetria del sistema, quindi nel caso in cui i due canali abbiamo identici i seguenti parametri:

- Tasso di guasto pericoloso: $\lambda_{AD} = \lambda_{BD}$, in seguito definiti genericamente come λ_D,
- Copertura diagnostica: $DC_A = DC_B$, in seguito definita genericamente come DC,
- Tasso di test: $r_{tA} = r_{tB}$, in seguito definito genericamente come r_t.

L'equazione 5.68, in caso di completa simmetria, può essere semplificata come segue:

$$PFH_D = (\lambda_D - \lambda_{CC})^2 \left[\frac{DC}{r_t} + (1 - DC)T_M\right] + \lambda_{CC} \quad (5.69)$$

Se entrambi i canali, A e B, sono testati in modo continuo, ovvero se $r_{tA} \to \infty$ ed $r_{tB} \to \infty$, è possibile ricavare la seguente espressione per il calcolo del PFH_d, ponendo le condizioni di test continuo nell'equazione 5.68 oppure, in modo equivalente, ponendo pari a zero gli intervalli di test T_A e T_B nell'equazione 5.65:

$$PFH_D = \frac{1}{2}(\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})(2 - DC_A - DC_B)T_M + \lambda_{CC} \quad (5.70)$$

In caso di sistema completamente simmetrico è possibile ricavare un'ulteriore semplificazione in presenza di test continuo, procedendo per l'equazione 5.70 in modo analogo a quanto descritto per un sistema senza test continuo, ovvero nella equazione 5.69:

$$PFH_D = (\lambda_D - \lambda_{CC})^2(1 - DC)T_M + \lambda_{CC} \quad (5.71)$$

5.7 Modello 1oo2

In caso di architettura 1oo2, i canali non sono dotati di diagnostica, pertanto è possibile ricavare la seguente rappresentazione grafica direttamente dalla Figura 5.1, rappresentante un sistema a due canali testato (1oo2D); la rappresentazione grafica seguente, in Figura 5.15, coincide con quest'ultima con le interconnessioni dovute alla diagnostica ed i tassi di test che non vengono riportati perché non più presenti:

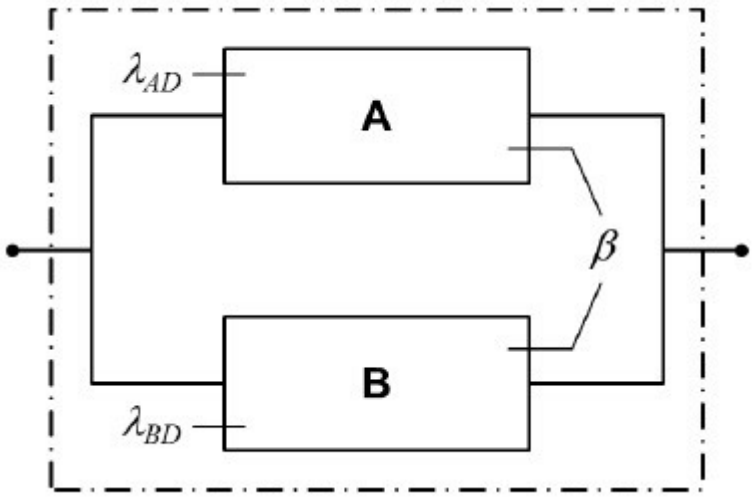


Figura 5.15: Sistema a due canali non testato (1oo2).

Il PFH_D può essere calcolato, analogamente al modello 1oo2D, tramite l'equazione 5.46. Le variabili di semplificazione L_1, L_2, C_P e C_N restano sempre definite dalle equazioni 5.42, 5.43, 5.49 e 5.50.

Le variabili di semplificazione espresse dalle equazioni 5.47 e 5.48, ovvero L_A ed L_B, diversamente dalle altre quattro appena citate, dipendono intrinsecamente dalla copertura diagnostica. Nel

modello 1oo2 la diagnostica non implementata può essere espressa settando a zero le coperture diagnostiche dei due canali ($DC_A = DC_B = 0$) nelle equazioni 5.47 e 5.48.

Le variabili L_A ed L_B vengono semplificate, in accordo con quanto appena descritto, come riportato nelle seguenti equazioni:

$$L_A = (\lambda_{AD} - \lambda_{CC}) \tag{5.72}$$

$$L_B = (\lambda_{BD} - \lambda_{CC}) \tag{5.73}$$

Con l'assenza di diagnostica, espressa sempre dal settaggio a zero delle coperture diagnostiche ($DC_A = DC_B = 0$), è possibile rendere ancora più compatta l'equazione per il calcolo del PFH_D ottenuta con la soluzione semplificata, semplicemente sostituendo le condizioni appena citate nell'equazione 5.65 oppure, in modo equivalente, nell'equazione 5.68:

$$PFH_D = (\lambda_{AD} - \lambda_{CC})(\lambda_{BD} - \lambda_{CC})T_M + \lambda_{CC} \tag{5.74}$$

In caso di sistema completamente simmetrico i tassi di guasto pericolosi dei due canali saranno identici ($\lambda_{AD} = \lambda_{BD}$, definito in seguito come λ_D). L'equazione risultante è la seguente:

$$PFH_D = (\lambda_D - \lambda_{CC})^2 T_M + \lambda_{CC} \tag{5.75}$$

6. Applicazione

6.1 Caso di studio

Il caso di studio analizzato in seguito è una semplice area con un macchinario in funzione che presenta intrinsecamente il pericolo di causare danno all'operatore che accede all'area di funzionamento dello stesso. Il macchinario, in questo esempio, si considera dotato di una lama o una componente similare che può produrre lacerazioni, contusioni o amputazioni delle dita dell'operatore. L'evento indesiderato può avvenire se l'operatore entra nell'area di funzionamento del macchinario mentre quest'ultimo è in funzione.

È assunto che un operatore deve accede all'area mediamente ogni ora per effettuare il cambio del pezzo da trattare o per manutenzione. L'impianto è assunto in funzione per 16 ore al giorno e per 260 giorni all'anno. Il rischio prodotto dalla presenza e dal funzionamento del macchinario è inaccettabile ed è necessario, pertanto, introdurre un sistema di sicurezza che si assicuri che, nel momento in cui un operatore abbia bisogno di accedere all'area di funzionamento del macchinario, esso sia spento.

Il sistema di sicurezza per la diminuzione del rischio, che ha come scopo quello di arrestare il funzionamento del macchinario quando richiesto, è formato da un elettroserratura (interblocco con blocco del riparo), un PLC (un controllore logico programmabile) ed un contattore (chiamato anche teleruttore).

L'elettroserratura costituisce il sottosistema di input ed ha il compito di rilevare la richiesta di ingresso dell'operatore nell'area di funzionamento del macchinario e di trasmetterla al PLC. Nel sistema di sicurezza in fase di progettazione è utilizzata l'elettroserratura Schmersal AMZ 201. Le sue caratteristiche verranno analizzate meglio per la valutazione del sottosistema di input. Il dispositivo utilizzato è riportato nella seguente Figura 6.1:

Figura 6.1: Elettroserratura Schmersal AMZ 201.

Il PLC costituisce il sottosistema di logica ed ha il compito di ricevere il segnale dall'elettroserratura, di elaborarlo e di produrre un segnale di output, che servirà come segnale di input per il contattore. Nel sistema di sicurezza in fase di progettazione vengono utilizzate delle componenti Siemens per il PLC, che sarà assemblato con i seguenti dispositivi:

- CPU: 1511F-1PN,
- Modulo di ingresso: 138 4/8 F-DI,
- Modulo di uscita: 138 4 F-DO.

Le caratteristiche del PLC e quindi del sottosistema di logica verranno analizzate meglio in seguito, considerando che esso è composto da tre elementi connessi logicamente in serie e quindi i tassi di guasto pericolosi del sottosistema e le componenti di PFH_D relative ai singoli componenti andranno sommate per ricavare il dato riferito all'intero sottosistema.

I dispositivi utilizzati per il sottosistema di logica sono rappresentati nella seguente Figura 6.2:

Figura 6.2: PLC (controllore logico programmabile) con dispositivi Siemens.

Il contattore costituisce il sottosistema di output, riceve un segnale dal PLC e si occupa fisicamente dello spegnimento del macchinario, quando richiesto. È l'attuatore del sistema di sicurezza. Il contattore è utilizzato ogni due minuti dall'automazione del macchinario, oltre che dal sistema di sicurezza, questo comporterà un'elevata frequenza di commutazioni del contattore. Nel sistema di sicurezza in fase di progettazione viene utilizzato un contattore Siemens 3RT2017, che sarà analizzato meglio in seguito. È rappresentato nella seguente Figura 6.3:

Figura 6.3: Contattore Siemens 3RT2017.

6.2 Analisi di rischio

Dopo aver introdotto il macchinario ed il rischio ad esso correlato si procede trovando di quanto è necessario ridurre tale rischio, con l'introduzione di un sistema di sicurezza. Si procede applicando le analisi di rischio già discusse e presenti nelle normative, trovando un PL richiesto (ISO 13849-1) ed un SIL richiesto (IEC 62061). Come verrà descritto in seguito le due normative porteranno allo stesso risultato in termini di affidabilità del sistema di sicurezza.

6.2.1 Analisi di rischio con normativa IEC 62061

Per l'applicazione della normativa IEC 62061 sono necessari i seguenti dati di input:

- La frequenza di esposizione è di un'esposizione per ora: $F = 1/h \geq 1/h$,
- La durata di ogni singola esposizione è ridotta ed è certamente $\leq 10\ min$,
- La probabilità di accadimento viene considerata come "possibile": si ricava che $P = 3$, dalla Tabella 2.8,
- L'evitabilità viene considerata come "possibile": si ricava che $E = 3$, tramite la Tabella 2.9,
- La gravità rientra nella classificazione 3 (lesione irreversibile, rottura di arti o perdita di dita): $G = 3$.

Dalla frequenza e dalla durata di esposizione si ricava, tramite la Tabella 2.7, che il parametro D è pari a 5.

Il calcolo della classe di rischio, definita C, è effettuato, come già descritto, sommando la durata, la probabilità di accadimento e l'evitabilità delle conseguenze. Il risultato è espresso nella seguente equazione:

$$C = D + P + E = 5 + 3 + 3 = 11 \quad (6.1)$$

Il SIL richiesto è ottenuto dall'apposita Tabella 2.10, considerando la classe di rischio ottenuta nell'equazione 6.1 e la gravità delle conseguenze: $SIL_r = SIL\ 2$.

Il procedimento utilizzato, che consiste nell'utilizzo delle apposite tabelle, è riportato nella seguente Figura 6.4, che evidenzia in verde le scelte effettuate per la quantificazione dei parametri e del SIL richiesto:

Frequenza dell'esposizione	Durata esposizione <= 10 min	Durata esposizione > 10 min
$F \geq 1/ora$	5	5
$1/giorno \leq F < 1/ora$	4	5
$2/settimana \leq F < 1/giorno$	3	4
$1/anno \leq F < 2/settimana$	2	3
$F < 1/anno$	1	2

Probabilità di accadimento	(P)
Molto alta	5
Probabile	4
Possibile	3
Scarsa	2
Trascurabile	1

Evitabilità o limitazione	(E)
Impossibile	5
Possibile	3
Probabile	1

Conseguenze	Gravità	Classe				
		3-4	5-7	8-10	11-13	14-15
Irreversibile: morte o perdita di un braccio o di un occhio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Irreversibile: rottura di uno o più arti, perdita di dita	3		Altre misure	SIL 1	SIL 2	SIL 3
Reversibile: richiede l'intervento di un medico	2			Altre misure	SIL 1	SIL 2
Reversibile: richiede cure di un pronto soccorso	1				Altre misure	SIL 1

Figura 6.4: Valutazione del SIL richiesto secondo la normativa IEC 62061.

6.2.2 Analisi di rischio con normativa ISO 13849-1

Per l'applicazione della normativa ISO 13849-1 sono necessari i seguenti dati di input:

- Severità della lesione: $S = S2$, per via dell'irreversibilità della stessa, che può comprendere amputazioni di dita,
- Frequenza e/o tempo di esposizione: $F = F2$, come stabilito dalla normativa, in caso di alte frequenze di esposizione come nel caso in esame, si ritiene opportuno prediligere $F2$,
- Possibilità di evitare il pericolo o di limitarne il danno: $P = P1$, per la capacità oggettiva dell'operatore di accorgersi del funzionamento del macchinario, per via del rumore prodotto e del movimento macroscopico che l'operatore può notare. L'operatore, accorgendosi del pericolo, può evitarlo allontanandosi.

Dal grafico contenuto nella normativa, rappresentato nella Figura 2.5, si ottiene, con i dati appena descritti, un livello di performance richiesto pari a "d": $PL_r = d$.

L'applicazione dell'albero decisionale riportato nella normativa ISO 13849-1 e le iterazioni scelte per la valutazione del PL_r, effettuate in base ai parametri di input, sono rappresentate in verde nella seguente Figura 6.5:

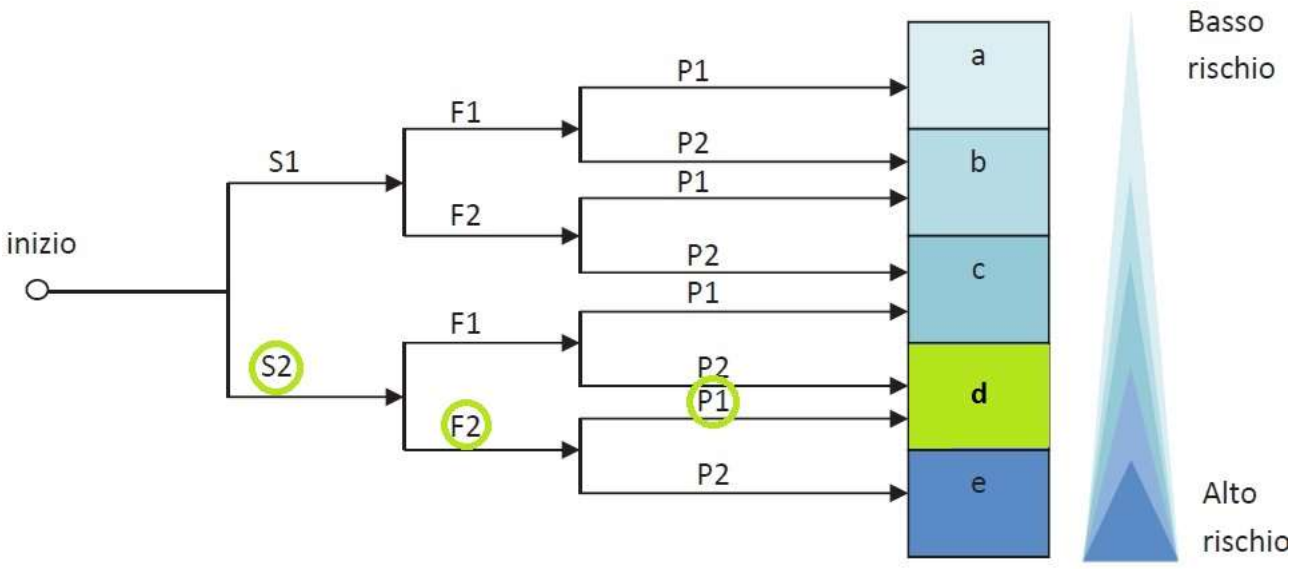


Figura 6.5: Valutazione del PL richiesto secondo la normativa ISO 13849-1.

Si può notare, come anticipato, che le due normative producono lo stesso risultato, sarà pertanto richiesto, dal sistema di sicurezza, almeno un SIL 2, che equivale ad un PL=d.

6.3 Analisi del sistema di sicurezza

Per la valutazione dell'affidabilità del sistema di sicurezza bisogna considerare i suoi sottosistemi: di input, di logica e di output. In termini di PFH_D sarà necessaria una valutazione di ogni singolo sottosistema ed il PFH_D totale sarà semplicemente la somma dei valori di esso relativi ad ogni sottosistema.

Bisogna considerare che il sistema, per raggiungere il SIL/PL richiesto, dovrà avere un valore di PFH_D che rientri nel range ammissibile sancito dalla normativa: $PFH_D < 10^{-6}$, per raggiungere almeno SIL 2/ PL=d.

Dato che il PFH_D dell'intero sistema sarà la somma dei PFH_D dei sottosistemi, una condizione necessaria affinché il sistema possa essere ritenuto adatto è che ogni sottosistema abbia un SIL/PL pari o superiore a quanto richiesto per l'intero sistema di sicurezza.

6.3.1 Sottosistema di input

Viene analizzata l'**elettroserratura**, tramite il foglio dati relativo fornito dal costruttore, dal quale si ricavano le seguenti informazioni:

- $\mathrm{PL}_{\max} =$ "e": il dispositivo è adatto per l'utilizzo in sistemi di sicurezza fino ad un livello di performance pari ad "e",
- Adatto per SIL 3: il dispositivo è adatto per l'utilizzo in sistemi di sicurezza con affidabilità pari a SIL 3,
- $PFH_D = 1{,}90 \cdot 10^{-9}\ h^{-1}$,
- Durata di utilizzo pari a 20 anni.

Le precedenti caratteristiche dell'elettroserratura la rendono idonea per il sistema di sicurezza in questione, avendo delle caratteristiche di affidabilità addirittura superiori di un SIL/PL rispetto a quelle richieste.

L'elettroserratura, tecnicamente, ha un'architettura 1oo2D, ma è trattato come un cosiddetto "sistema incapsultato", ovvero un sistema che non viene analizzato ulteriormente in quanto il produttore fornisce il valore di PFH_D e le caratteristiche di affidabilità; viene considerato come un unico componente.

6.3.2 Sottosistema di logica

Viene ora analizzato il **PLC**, tramite il foglio dati di ogni suo componente, forniti dal costruttore. Bisogna considerare il PLC, ovvero il sottosistema di logica, come formato da tre elementi connessi in serie, ovvero il modulo di ingresso, la CPU ed il modulo di uscita. Il PFH_D del sottosistema di logica sarà pari alla somma dei PFH_D dei componenti.

Per il modulo di ingresso, tramite il foglio dati relativo, si ricavano le seguenti informazioni:

- Adatto per SIL 3,
- Adatto per PL=e,
- $PFH_D = 1 \cdot 10^{-9}\ h^{-1}$,
- Durata di utilizzo pari a 20 anni.

Per la CPU, tramite il foglio dati relativo, si ricavano le seguenti informazioni:

- Adatta per SIL 3,
- Adatta per PL=e,
- $PFH_D = 2 \cdot 10^{-9}\ h^{-1}$,
- Durata di utilizzo pari a 20 anni.

Per il modulo di uscita, tramite il foglio dati relativo, si ricavano le seguenti informazioni:

- Adatto per SIL 3,
- Adatto per PL=e,
- $PFH_D = 1 \cdot 10^{-9}\ h^{-1}$,
- Durata di utilizzo pari a 20 anni.

Ogni componente del sottosistema di logica ha un SIL/PL maggiore rispetto a quello richiesto dalla progettazione ed il suo PFH_D sarà pari alla somma dei tre contributi, come riportato nella seguente equazione:

$$PFH_D = PFH_{D,mod.IN} + PFH_{D,CPU} + PFH_{D,mod.OUT} = 4 \cdot 10^{-9}\ h^{-1} \quad (6.2)$$

I dati di affidabilità relativi al PLC sono pertanto SIL 3 e PL=e, pertanto, il PLC è ritenuto adatto per il sistema di sicurezza, avendo delle caratteristiche di affidabilità addirittura superiori di un SIL/PL rispetto a quelle richieste.

Il PLC, tecnicamente, ha un'architettura 1oo2D, ma è trattato come un cosiddetto "sistema incapsultato", come avviene per l'elettroserratura.

6.3.3 Sottosistema di output

Viene ora analizzato il **contattore**, tramite il foglio dati relativo fornito dal costruttore, dal quale si ricavano le seguenti informazioni:

- $B_{10} = 1\,000\,000$, per alto tasso di richiesta. È simile al già discusso B_{10D}, con la differenza che include ogni tipo di guasto e non solamente i guasti pericolosi,
- $Frazione\ di\ guasti\ pericolosi = 73\%$, per alto tasso di richiesta,
- Durata di utilizzo ed intervallo di prova pari a 20 anni.

È necessario procedere con il calcolo del PFH_D tramite il tasso di guasto pericoloso, come descritto nella trattazione dei dispositivi soggetti a wearout. Il procedimento è elencato e descritto in seguito:

- Calcolo del B_{10D}. È sufficiente dividere il B_{10} fornito dal costruttore per la frazione di guasti pericolosi, anch'essa fornita dal costruttore. Il valore è ricavato dalla seguente equazione:

$$B_{10D} = B_{10} \,/\, Frazione\ di\ guasti\ pericolosi = 1369\,863 \quad (6.3)$$

- Calcolo della frequenza di operazione n_{op}, espressa in operazioni all'anno. È necessario utilizzare i periodi di funzionamento del macchinario ed il numero di operazioni al minuto,

considerando, oltre alle operazioni dovute alla sicurezza, anche le operazioni dovute all'automazione:

$$n_{op} = 0.5/min \cdot 60\ min/h \cdot 16\ h/giorno \cdot 260\ giorni/anno = 124\,800\ op./anno \quad (6.4)$$

- Calcolo del tasso di guasto pericoloso λ_D, espresso in h^{-1}. Si utilizza la formula apposita e già descritta, considerando i risultati ottenuti nelle equazioni 6.3 e 6.4. Per ottenere l'unità di misura richiesta è necessario dividere il risultato per le ore presenti in un anno, ovvero 8760:

$$\lambda_D = \frac{n_{op}}{10\ B_{10D}} = \frac{124\,800\ anni^{-1}}{10 \cdot 1\,369\,863} \cdot \frac{1\ anno}{8760\ h} = 1{,}04 \cdot 10^{-6}\ h^{-1} \quad (6.5)$$

- Calcolo del PFH_D del sottosistema di output e quindi del contattore. Sarà pari al tasso di guasto pericoloso, ricavato nella precedente equazione 6.5, perché in questo caso, come per gli altri sottosistemi, si considera un'architettura 1oo1, ovvero composta semplicemente da un dispositivo:

$$PFH_D = \lambda_D = 1{,}04 \cdot 10^{-6}\ h^{-1} \quad (6.6)$$

Il sottosistema di output non è in grado di raggiungere un'affidabilità sufficiente, infatti dal PFH_D ottenuto si ricava che raggiunge SIL 1/PL=c, anche senza considerare i vincoli di architettura.

Il sottosistema di output non è adeguato e pertanto, se viene utilizzato nel sistema di sicurezza, quest'ultimo non ridurrà il rischio del necessario.

Il sottosistema di output appena valutato corrisponde al modello 1oo1. Nella seguente Figura 6.6 è rappresentato il sistema di sicurezza, tramite un diagramma a blocchi, con un sottosistema di output 1oo1:

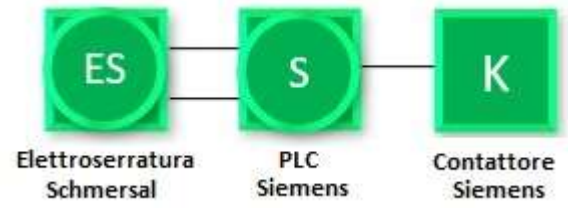


Figura 6.6: Sistema di sicurezza con sottosistema di output 1oo1.

Il sistema di sicurezza, dunque, presenta una mancanza di affidabilità nel sottosistema di output, mentre sono adatti i sottosistemi di input e di logica. È necessario ricorrere a delle modifiche esclusivamente al sottosistema di output, applicando della ridondanza o implementando del monitoraggio su di esso.

È possibile considerare tutte architetture analizzate precedentemente con l'aggiunta, dovuta a possibili configurazioni pratiche, di una nuova tipologia di architettura, denominata 1oo2(1D),

un'architettura a due canali funzionali dove la diagnostica è implementata esclusivamente per uno di essi.

Ogni architettura, dopo una breve introduzione, sarà analizzata con la normativa IEC 62061, la normativa ISO 13849-1 ed il set di equazioni ricavato nei capitoli 4 e 5.

6.3.4 Sottosistema di output 1oo2

L'architettura 1oo2 è ottenibile aggiungendo semplicemente al sottosistema di output un altro contattore, che sarà connesso in parallelo all'altro già presente. In questo caso entrambi i contattori, se funzionanti, svolgono la loro funzione e, pertanto, avranno la stessa frequenza di operazione e di conseguenza lo stesso tasso di guasto pericoloso.

L'architettura 1oo2 è rappresentata nella seguente Figura 6.7, che comprende l'intero sistema di sicurezza:

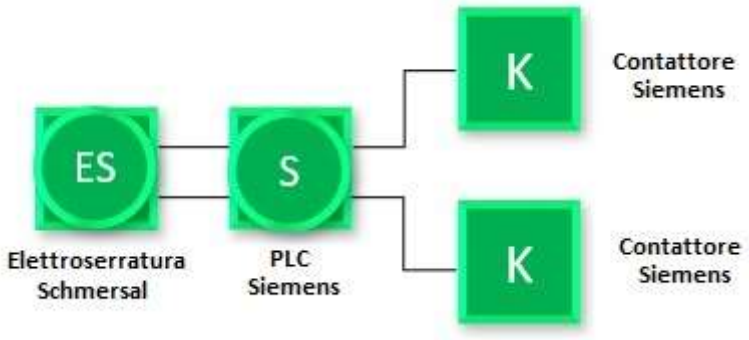


Figura 6.7: Sistema di sicurezza con sottosistema di output 1oo2.

6.3.5 Sottosistema di output 1oo1D

L'architettura 1oo1D è ottenibile aggiungendo una bobina di minima, ovvero un dispositivo che ha lo scopo di portare il macchinario in uno stato sicuro quando viene rilevato un guasto, facendo scattare un interruttore a cui è associata. Il funzionamento della bobina di minima avviene attraverso il PLC, essa può essere considerata, come da normativa ISO 13849-1, come l'OTE dell'architettura (elemento di output del canale di monitor).

Non è in grado di eseguire la funzione di sicurezza ma è in grado semplicemente di inibire il funzionamento del macchinario, dopo che viene rilevato un guasto ed evitando il verificarsi dell'evento indesiderato.

Viene rappresentata, nella seguente Figura 6.8, la bobina di minima ABB A428401, che viene utilizzata nella progettazione del sistema di sicurezza per consentire l'applicazione dell'architettura 1oo1D:

Figura 6.8: Bobina di minima ABB A428401.

L'unico parametro d'interesse della bobina è il B_{10} , che in questo caso non è fornito dal costruttore ma viene stabilito dalle normative ISO 13849-1 (allegato C) ed IEC 62061 (allegato C). Le due normative stabiliscono valori conservativi per diverse tipologie di componenti. Per la bobina di minima risulta che: $B_{10D} = 400\ 000$.

Il PLC non rientrerà nell'analisi di questa architettura perché è il suo PFH_D è già considerato nel computo totale, nel sottosistema di logica.

L'architettura 1oo2 è rappresentata nella seguente Figura 6.9, che comprende l'intero sistema di sicurezza:

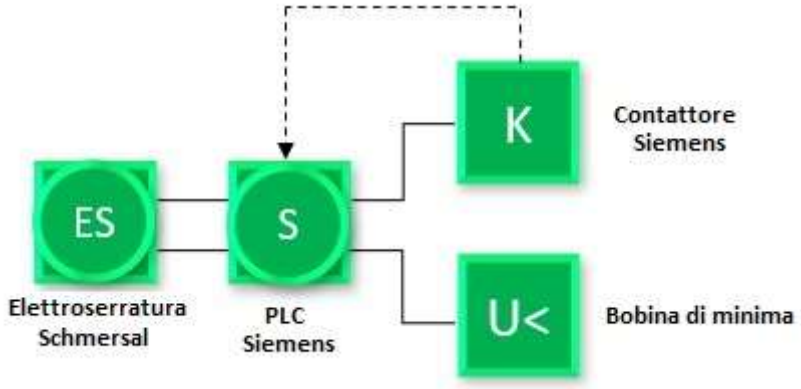


Figura 6.9: Sistema di sicurezza con sottosistema di output 1oo1D.

6.3.6 Sottosistema di output 1oo2(1D)

L'architettura **1oo2(1D)** è ottenuta implementando la diagnostica per solamente uno dei due contattori: il sistema di sicurezza è in grado di rilevare un guasto pericoloso avvenuto al solo contattore monitorato e può portare il macchinario in uno stato sicuro attraverso l'altro contattore, se funzionante. Questa architettura non è descritta nelle normative IEC 62061 ed ISO 13849-1.

È possibile considerare l'architettura 1oo2(1D) come un'architettura 1oo2D degradata. La degradazione consiste nella mancanza di copertura diagnostica per uno dei due contattori. L'architettura sarà indicata brevemente come $1oo2D^{-}$, se considerata in questo modo. Ciò è possibile per via del fatto che i due contattori formano un sistema di attuatori ridondanti nel sottosistema di output ed il controllore esterno, ovvero il PLC, rileva i guasti di un contattore e porta ad uno stato sicuro per mezzo dell'altro se funzionante.

È possibile, inoltre, considerare l'architettura 1oo2(1D) come un'architettura 1oo1D migliorata. Il miglioramento consiste nel fatto che il contattore non monitorato viene considerato come canale di test, come la bobina di minima nell'esempio 1oo1D, quando, in realtà è anche in grado di eseguire la funzione di sicurezza. L'architettura sarà indicata brevemente come $1oo1D^{+}$, se considerata in questo modo.

Il PLC partecipa attivamente ma non rientra nel computo del sottosistema perché è considerato separatamente nel calcolo del PFH_D totale del sistema di sicurezza, sotto forma di una componente di PFH_D additiva, dovuta esclusivamente ad esso e già valutata precedentemente.

L'architettura 1oo2(1D) è rappresentata nella seguente Figura 6.10, che comprende l'intero sistema di sicurezza:

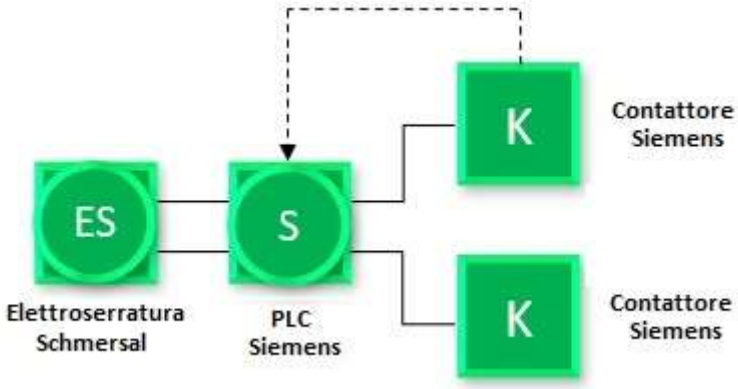


Figura 6.10: Sistema di sicurezza con sottosistema di output 1oo2(1D).

6.3.7 Sottosistema di output 1oo2D

L'architettura **1oo2D** è ottenuta implementando la diagnostica per entrambi i contattori: il sistema di sicurezza è ora in grado, attraverso il PLC, di rilevare un guasto pericoloso avvenuto ad uno dei due contattori e può portare il macchinario in uno stato sicuro attraverso l'altro.

È possibile considerare il sistema come 1oo2D perché i due contattori formano un sistema di attuatori ridondanti nel sottosistema di output ed il controllore esterno, ovvero il PLC, rileva i guasti di entrambi i contattori e porta ad uno stato sicuro per mezzo dell'altro contattore ancora intatto.

È possibile questa applicazione perché il PLC è considerato separatamente nel calcolo del PFH_D totale del sistema di sicurezza, sotto forma, in questo caso, di una componente di PFH_D additivo dovuto esclusivamente ad esso e già valutato precedentemente.

È rappresentata nella seguente Figura 6.11, che comprende l'intero sistema di sicurezza:

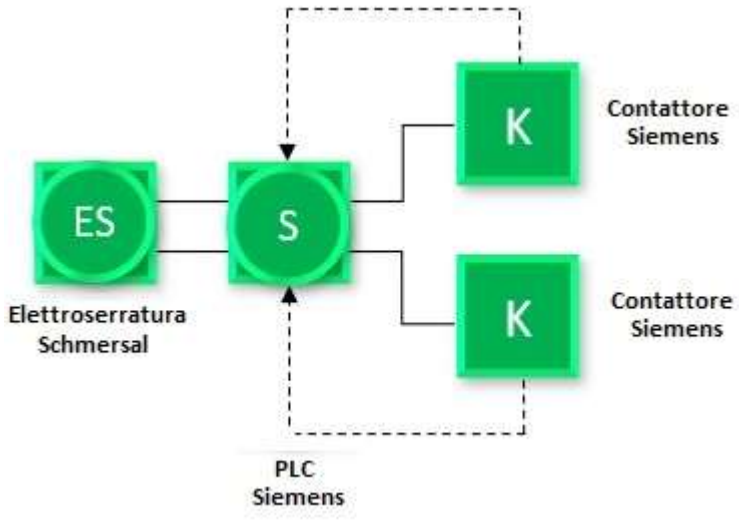


Figura 6.11: Sistema di sicurezza con sottosistema di output 1oo2D.

Dopo l'analisi di ogni architettura con la normativa IEC 62061, la normativa ISO 13849-1 ed il set di equazioni ottenuto nei capitoli 4 e 5, verranno confrontati i risultati ottenuti e valutate le architetture utilizzabili per la progettazione del sistema di sicurezza.

6.4 Procedura con applicazione della normativa IEC 62061

La normativa IEC 62061, per le analisi del sottosistema di output, fornisce un set di equazioni da utilizzare in modo specifico, in base alla corrispondenza tra il caso trattato e le quattro architetture presenti nella stessa normativa (A, B, C e D). Le corrispondenze presenti sono le seguenti:

- 1oo1: Architettura A.
- 1oo2: Architettura B.
- 1oo1D: Architettura C.
- 1oo2(1D): non è modellizzata nella IEC 62061. Si può correlare all'architettura C considerandola come 1oo1D migliorata, ovvero $1oo1D^{+}$, oppure all'architettura D considerandola come 1oo2D degradata, ovvero $1oo2D^{-}$**.**
- 1oo2D: Architettura D.

Per effettuare tutte le analisi è necessario il tasso di guasto pericoloso del canale funzionale, ovvero del contattore. Questo parametro è già stato ricavato in precedenza con l'equazione 6.5, come funzione di n_{op} e B_{10D}: $\lambda_D = 1{,}04 \cdot 10^{-6}\ h^{-1}$.

6.4.1 IEC 62061: 1oo1

Per l'architettura **1oo1** si utilizza l'equazione relativa all'architettura A, relativa ad un sottosistema composto da più elementi in serie e che viene riportata in seguito:

$$PFH_D = \lambda_{De1} + \ldots + \lambda_{Den} \quad (2.16)$$

Per il calcolo del PFH_D bisogna considerare la presenza di un solo elemento. Il PFH_D sarà pari, pertanto, al tasso di guasto pericoloso del contattore, come già descritto nell'equazione 6.6, che viene pertanto riportata:

$$PFH_D = \lambda_D = 1{,}04 \cdot 10^{-6}\ h^{-1} \quad (6.6)$$

6.4.2 IEC 62061: 1oo2

Per l'architettura **1oo2**, per la quale analisi si utilizza l'architettura B presente nella normativa, è necessario aggiungere i seguenti parametri:

- Fattore beta: indice della suscettibilità alle cause comuni di guasto. Viene considerato pari al 2% perché si ritiene, tramite la procedura descritta, che siano state adottate sufficienti misure contro i CCF: $\beta = 2\%$.
- T_{10D}, ovvero il tempo dopo il quale il contattore deve essere sostituito per wearout. Questo parametro, già descritto, può essere ricavato con la seguente equazione, considerando i risultati ottenuti nelle equazioni 6.3 e 6.4:

$$T_{10D} = B_{10D}/n_{op} = 1\,369\,863/124800\ anni^{-1} = 10.98\ anni\ \cong 11\ anni \quad (6.7)$$

- T_1, ovvero l'intervallo di tempo minore tra la vita utile e l'intervallo di prova del contattore, con la vita utile che è il minore tra il T_{10D} ed il tempo di missione, considerato pari a 20 anni. Per quanto descritto il T_1 sarà pari al T_{10D}, ovvero a 11 anni.

L'equazione utilizzata è quella relativa all'architettura B, che viene riportata in seguito:

$$PFH_D = [(1-\beta)^2(\lambda_{De1} \cdot \lambda_{De2} \cdot T_1)] + [\beta(\lambda_{De1} + \lambda_{De2})/2] \quad (2.17)$$

Sostituendo, nell'equazione 2.17, il fattore beta ricavato, i tassi di guasto pericoloso dei due contattori, già ricavati ed uguali, ed il T_1, ricordando che deve essere espresso in ore e non in anni e quindi che necessita di essere moltiplicato per 8760, il numero di ore di un anno, si ottiene il seguente valore di PFH_D:

$$PFH_D = 1{,}21 \cdot 10^{-7} \quad (6.8)$$

6.4.3 IEC 62061: 1oo1D

Per l'architettura **1oo1D**, per la quale analisi si utilizza l'architettura C presente nella normativa, è necessario aggiungere i seguenti parametri:

- La copertura diagnostica del contattore, che è ricavabile dalla modalità di esecuzione della stessa tramite le tabelle già descritte: $DC = 99\%$, per "monitoraggio dei dispositivi elettromeccanici per mezzo di contatti meccanicamente legati".
- Il tasso di guasto pericoloso della bobina di minima, indicato come $\lambda_{D\,FH}$, che è il dispositivo che si occupa di portare il sistema in uno stato sicuro dopo la rilevazione di un guasto. Si calcola tramite il B_{10D} della bobina fornito dalle normative e considerando, in via altamente cautelativa, una operazione al mese e quindi una frequenza di operazione pari a 12 operazioni all'anno: $n_{op} = 12/anno$. L'equazione è la stessa utilizzata per il tasso di guasto pericoloso del contattore e porta al seguente risultato:

$$\lambda_{D\,FH} = \frac{n_{op}}{10\,B_{10D}} = \frac{12\ anni^{-1}}{10 \cdot 400\,000} \cdot \frac{1\ anno}{8760\ h} = 3{,}42 \cdot 10^{-10}\ h^{-1} \tag{6.8}$$

Per l'applicabilità dell'equazione sono presenti dei vincoli. Dalla Tabella 2.11 si ricava il vincolo $1/\ \lambda_{D\,FH} \geq 5\,900\ anni$. Si procede, alla verifica del vincolo di applicabilità:

$$1/\lambda_{D\,FH} = 1/3{,}42 \cdot 10^{-10}\ h^{-1} = \ 333\,787\ anni \geq 5\,900\ anni \tag{6.9}$$

Il vincolo è rispettato, assieme agli altri vincoli riguardanti il fattore beta ($\leq 2\%$) e la copertura diagnostica ($\leq 99\%$). Il vincolo relativo al tasso di guasto del canale funzionale è rispettato in quanto $1/\lambda_{De} = \ 111\ anni\ \leq 1\,000\ anni$. È possibile utilizzare l'equazione relativa all'architettura C, dato che tutti i vincoli sono rispettati. Viene riportata in seguito:

$$PFH_D = \lambda_{De} - DC[\lambda_{De} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})] \cdot [1 - \frac{1}{2} \cdot (\lambda_{D\,FH} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})T_1)] \tag{2.20}$$

Sostituendo tutte le variabili presenti nell'equazione si ottiene come risultato:

$$PFH_D = 1{,}04 \cdot 10^{-8} \tag{6.10}$$

6.4.4 IEC 62061: 1oo2(1D)

Per l'architettura **1oo2(1D)** è possibile procedere considerandola 1oo1D$^+$ e quindi applicando l'equazione relativa all'architettura C. Il procedimento è già stato effettuato per il modello 1oo1D, comprendente la bobina di minima.

L'unico accorgimento è relativo al $\lambda_{D\,FH}$, che non sarà più quello della bobina ma quello del contattore non monitorato. Nel computo è necessario considerare tutte le operazioni svolte dal contattore non monitorato, siano essere relative all'automazione oppure alla sicurezza. Il tasso di guasto pericoloso del contattore non monitorato sarà uguale a quello già considerato in precedenza e ricavato nell'equazione 6.5.

Anche in questo caso è necessaria la verifica dei vincoli di applicabilità, effettuata in seguito:

$$1/\lambda_{D\,FH} = 1/\lambda_D = 1/1{,}04 \cdot 10^{-6}\ h^{-1} = \ 109\ anni < 5\,900\ anni \tag{6.11}$$

Il vincolo ($1/\ \lambda_{D\,FH} \geq 5\,900\ anni$) non è rispettato. È possibile, tuttavia, utilizzare l'equazione perché gli altri vincoli sono tutti rispettati. Vengono rispettati infatti i vincoli riguardanti il fattore beta ($\leq 2\%$), la copertura diagnostica ($\leq 99\%$) ed il vincolo relativo al tasso di guasto del canale funzionale è rispettato in quanto $1/\lambda_{De} = \ 111\ anni\ \leq 1\,000\ anni$. È possibile utilizzare l'equazione relativa all'architettura C, dato che solamente un vincolo non viene rispettato. Il risultato ottenuto è il seguente:

$$PFH_D = 8{,}05 \cdot 10^{-8} \tag{6.12}$$

Per l'architettura **1oo2(1D)** è possibile, inoltre, procedere considerandola 1oo2D⁻ e quindi applicando l'equazione relativa all'architettura D.

È necessario aggiungere i seguenti parametri:

- T_2, ovvero l'intervallo del test diagnostico. Può essere considerato pari a zero e quindi trattare il test come se fosse continuo, viste le caratteristiche che presenta il monitoraggio del contattore: il test viene effettuato immediatamente prima di eseguire ogni richiesta della funzione di sicurezza ed il sistema di sicurezza è in grado, in caso di rilevare un guasto di inibire il macchinario in un tempo minore rispetto al tempo di reazione dello stesso, evitando sempre e comunque, in caso di rilevazione di guasto, il verificarsi dell'evento indesiderato. Si considera $T_2 = 0$.
- DC_1 è la copertura diagnostica del contattore monitorato, che sarà pari al 99% per quanto già descritto nell'architettura 1oo1D: $DC_1 = 99\%$.
- DC_2 è la copertura diagnostica del contattore non monitorato, che ovviamente sarà pari a zero: $DC_2 = 0$.

L'equazione utilizzata è quella relativa all'architettura D, che viene riportata in seguito:

$$PFH_D = (1-\beta)^2[\lambda_{De1}\lambda_{De2}(DC_1 + DC_2)\frac{T_2}{2} + \lambda_{De1}\lambda_{De2}(2 - DC_1 - DC_2)\frac{T_1}{2}] + \beta\frac{\lambda_{De1} + \lambda_{De2}}{2} \tag{2.21}$$

Sostituendo ad ogni variabile contenuta nell'equazione il suo rispettivo valore, ottenuto precedentemente, si ottiene il seguente PFH_D:

$$PFH_D = 7{,}13 \cdot 10^{-8} \tag{6.13}$$

6.4.5 IEC 62061: 1oo2D

Per il modello **1oo2D** è possibile procedere analogamente a quanto fatto per il modello 1oo2(1D) considerato 1oo2D⁻**,** con l'accorgimento di porre entrambe le coperture diagnostiche pari a 99%, in

quanto per entrambi i contattori, in questo caso, è implementato il monitoraggio.

Il risultato ottenuto, considerando $DC_1 = DC_2 = 99\%$, è il seguente:

$$PFH_D = 2{,}18 \cdot 10^{-8} \tag{6.14}$$

6.4.6 Vincoli di architettura

Alla valutazione del PFH_D devono essere aggiunti i vincoli di architettura.

La tolleranza al guasto hardware è pari a zero nelle architetture 1oo1 e 1oo1D ed è pari ad uno nei modelli 1oo2 e 1oo2D. Per il modello 1oo2(1D) è pari a zero se viene considerato 1oo1D$^+$ oppure pari ad uno se viene considerato 1oo2D$^-$.

La frazione di guasti sicuri, essendo il contattore un componente elettromeccanico, è pari alla copertura diagnostica.

Nell'esempio trattato, la SSF, che coincide quindi con la DC, è maggiore o uguale a 99% nei modelli 1oo1D e 1oo2D, dove è uguale a 99% ed è minore del 60% nei modelli 1oo1 e 1oo2, dove non è presente diagnostica e quindi è pari a zero. Per il modello 1oo2(2D) è maggiore o uguale a 99% se viene considerato 1oo1D$^+$ oppure è minore del 60% se viene considerato 1oo2D$^-$. In quest'ultimo caso la copertura diagnostica sarà pari alla media aritmetica delle coperture diagnostiche dei due contattori, quindi pari a $(99\% + 0\%)/2 \cong 50\%$. Non è necessario pesare la media sui tassi di guasto pericoloso perché sono uguali.

Viene ricavato il SIL massimo raggiungibile per ogni modello tramite l'opportuna Tabella 2.12 ed i risultati sono riportati in seguito, i componenti sono ben provati e quindi l'architettura 1oo1 si considera in grado di raggiungere SIL 1:

Architettura	SFF=DC	HFT	SIL massimo raggiungibile
1oo1	$< 60\%$	0	SIL 1
1oo2	$< 60\%$	1	SIL 1
1oo1D	$\geq 99\%$	1	SIL 3
1oo2(1D) come 1oo1D$^+$	$\geq 99\%$	0	SIL 3
1oo2(1D) come 1oo2D$^-$	$< 60\%$	1	SIL 1
1oo2D	$\geq 99\%$	1	SIL 3

Tabella 6.1: Applicazione dei vincoli di architettura.

6.4.7 Risultati con IEC 62061

Nella seguente tabella vengono riassunti i risultati ottenuti con la normativa IEC 62061 e vengono indicati due SIL, uno relativo strettamente al PFH_D definito SIL teorico ed uno considerando i vincoli

di architettura:

Architettura	PFH_D [h^{-1}]	SIL teorico	SIL con vincoli di architettura
1oo1	$1{,}04 \cdot 10^{-6}$	SIL 1	SIL 1
1oo2	$1{,}21 \cdot 10^{-7}$	SIL 2	SIL 1
1oo1D	$1{,}04 \cdot 10^{-8}$	SIL 3	SIL 3
1oo2(1D) come 1oo1D^{+}	$8{,}05 \cdot 10^{-8}$	SIL 3	SIL 3
1oo2(1D) come 1oo2D^{-}	$7{,}13 \cdot 10^{-8}$	SIL 3	SIL 1
1oo2D	$2{,}18 \cdot 10^{-8}$	SIL 3	SIL 3

Tabella 6.2: Risultati ottenuti con la procedura descritta nella normativa IEC 62061.

6.5 Procedura con applicazione della normativa ISO 13849-1

La normativa ISO 13849-1, per l'analisi del sottosistema di output, fornisce una soluzione tabellare, dove è necessario individuare una corrispondenza tra l'architettura in esame ed una delle cinque Categorie presenti nella stessa normativa (B, 1, 2, 3 e 4). Le corrispondenze presenti sono le seguenti:

- 1oo1: Categoria B oppure, se il valore del $MTTF_D$ del contattore è sufficientemente elevato ($MTTF_D \geq 30\ anni$), Categoria 1.
- 1oo2: non è presente alcuna categoria corrispondente, non può essere analizzato con la normativa ISO 13849-1.
- 1oo1D: Categoria 2.
- 1oo2(1D): non è modellizzata nella ISO 13849-1. Si può correlare alla categoria 2 considerandola 1oo1D^{+}, oppure alla categoria 3 o categoria 4 considerandola come 1oo2D^{-}.
- 1oo2D: Categoria 3 oppure, se il $MTTF_D$ e la DC sono entrambi sufficientemente elevati ($MTTF_D \geq 30\ anni$ e $DC \geq 99\%$), Categoria 4.

Per effettuare tutte le analisi è necessario il tempo medio al guasto pericoloso del contattore, ovvero il $MTTF_D$. Questo parametro, avendo già ricavato il tasso di guasto pericoloso, è semplicemente il reciproco di quest'ultimo. È oltremodo calcolabile dal B_{10} e dal n_{op}, come riporta la seguente equazione:

$$MTTF_D = \frac{10\ B_{10D}}{n_{op}} = \frac{1}{\lambda_D} = 110\ anni \tag{6.15}$$

Per applicare la ISO 13849-1 bisogna considerare inoltre il fattore beta, indice della suscettibilità alle cause comuni di guasto, che deve essere pari al 2%, ovvero devono essere sufficienti le misure adottate contro i CCF, cosa che in questo caso pratico è già stata considerata.

Per l'applicare la ISO 13849-1 un altro parametro è il tempo di missione, che deve essere considerato pari a 20 anni. In questo caso si procede sostituendo il contattore dopo un tempo pari al T_{10D}, già calcolato e pari a 11 anni.

L'ultimo parametro di input necessario, oltre al $MTTF_D$ ed alla Categoria, è la copertura diagnostica. La DC viene considerata nulla ($DC < 60\%$) per l'architettura 1oo1, mentre viene considerata alta ($DC \geq 99\%$) per l'architettura 1oo2D.

Per l'architettura 1oo1D la copertura diagnostica viene considerata media ($90\% \leq DC < 99\%$) anche se $DC = 99\%$, in quanto, per analizzare una categoria 2, non è possibile considerare una copertura diagnostica alta. Ciò costituisce una piccola stima dalla parte della sicurezza nella valutazione del PFH_D con questa normativa. Per l'architettura 1oo2(1D), se considerata 1oo1D$^+$, vale lo stesso e si considera, come stima dalla parte della sicurezza, una copertura diagnostica media.

Per l'architettura 1oo2(1D), se considerata 1oo2D$^-$, la copertura diagnostica sarà $DC \cong 50\%$, come già illustrato. Non si può procedere con l'analisi perché, nella ISO 13849-1, non si può analizzare un'architettura 1oo2D con una copertura diagnostica nulla ($DC < 60\%$), in questo caso non si possono effettuare stime dalla parte della sicurezza per procedere ugualmente con l'analisi, come è stato descritto per la 1oo2(1D) considerata 1oo1D$^+$.

Prima dell'utilizzo della tabella bisogna considerare il vincolo di applicazione presente per il monitoraggio: il $MTTF_{D\ FH}$ del canale di monitor deve essere maggiore della metà del $MTTF_D$ del canale funzionale, già valutato. Deve essere maggiore della metà di 110 anni, ovvero 55 anni.

Per il modello 1oo1D si procede con la verifica utilizzando il tasso di guasto pericoloso della bobina:

$$MTTF_{D\ FH} = \frac{1}{\lambda_{D\ FH}} = \frac{1}{3{,}42 \cdot 10^{-10}\ h^{-1}} = 333\,787\ anni > 55\ anni \tag{6.16}$$

Per il modello 1oo2(1D) considerato 1oo1D$^+$ si procede in modo analogo con la verifica utilizzando il tasso di guasto pericoloso del contattore non monitorato:

$$MTTF_{D\ FH} = \frac{1}{\lambda_D} = \frac{1}{1{,}04 \cdot 10^{-6}\ h^{-1}} = 111\ anni > 55\ anni \tag{6.17}$$

Il $MTTF_D$ è pari a 110 anni ma è soggetto a limitazioni relative alla Categoria considerata, elencate in seguito:

- Categoria B: 30 anni,
- Categorie 1, 2 e 3: 100 anni,
- Categoria 4: 2500 anni.

Nella seguente figura viene riportata la soluzione ricavata dalla tabella. Per semplicità vengono riportate le sole righe che sono state considerate:

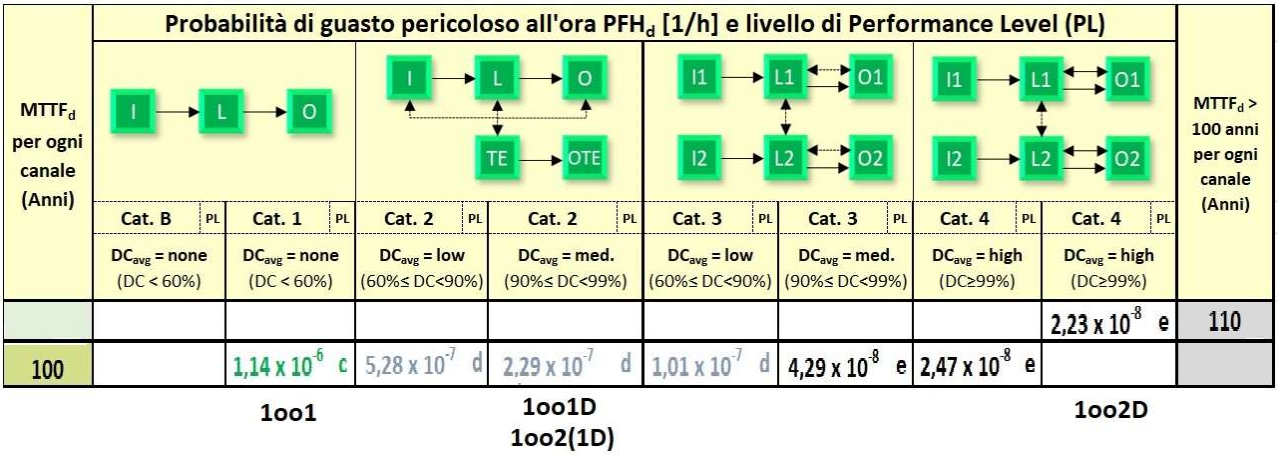


Figura 6.12: Utilizzo della tabella presente nella normativa ISO 13849-1 per il calcolo del PFH_D.

Si può notare come il $MTTF_D$ maggiore di 30 anni consenta all'architettura 1oo1 di rientrare nella Categoria B ed all'architettura 1oo2D di rientrare nella categoria 4, congiuntamente alla copertura diagnostica alta. Le architetture 1oo1D e 1oo2(1D) considerata 1oo1D$^+$ hanno portato allo stesso risultato. Ottenere maggiore affidabilità aumentando il $MTTF_D$, con l'utilizzo di un migliore contattore o una riduzione della frequenza di operazione, è possibile esclusivamente con l'architettura 1oo2D, perché nella tabella utilizzata sono già considerati i vincoli di architettura della ISO 13849-1.

La soluzione fornita dalla ISO 13849-1 è semplice da applicare: è sufficiente ricercare il valore di PFH_D nella tabella, partendo dal valore di $MTTF_D$ che indica la riga e dalla categoria, la quale, congiuntamente alla copertura diagnostica, indica la colonna.

6.5.1 Risultati con ISO 13849-1

I risultati ottenuti sono riportati nella seguente tabella:

Architettura	PFH_D [h^{-1}]	PL
1oo1	$1{,}14 \cdot 10^{-6}$	c
1oo2	/	/
1oo1D	$2{,}29 \cdot 10^{-7}$	d
1oo2(1D) come 1oo1D$^+$	$2{,}29 \cdot 10^{-7}$	d
1oo2(1D) come 1oo2D$^-$	/	/
1oo2D	$2{,}23 \cdot 10^{-8}$	e

Tabella 6.3: Risultati ottenuti con la procedura descritta nella normativa ISO 13849-1.

6.6 Procedura con applicazione del set di equazioni ottenuto nei capitoli 4 e 5

Le analisi effettuate nei capitoli 4 e 5 hanno consentito di ottenere una soluzione per il calcolo del PFH_D basata su un set di equazioni. Verranno utilizzate le equazioni non semplificate.

Ogni modello da analizzare è stato trattato ed ha delle equazioni specifiche, ad eccezione del modello 1oo2(1D), che viene trattato, come già descritto, come 1oo1D$^+$ oppure 1oo2D$^-$.

Vista la modalità con la quale viene effettuata la diagnostica è possibile considerare il sottosistema di output come operante, per le architetture ad un canale funzionale monitorato, in TOT e, per i modelli a due canali funzionali monitorati, operante con test continuo. Questa semplificazione è possibile perché il test viene effettuato prima di ogni esecuzione della funzione di sicurezza e, in caso di rilevazione di un guasto, il canale di monitor, o l'altro canale funzionale, sono in grado di inibire il macchinario e quindi di portare ad uno stato sicuro dove non è possibile il verificarsi dell'evento indesiderato. Nella pratica si utilizzano equazioni che non computano un aumento in termini di PFH_D dovuto al tasso (o ai tassi) di test**.**

6.6.1 Set di equazioni: 1oo1

Per il modello **1oo1** viene riportata l'equazione da utilizzare:

$$PFH_D = \lambda_{FD} \tag{4.49}$$

Le variabili presenti nell'equazione sono valutate come segue:

- λ_{FD} è il tasso di guasto pericoloso del canale funzionale. È pari al tasso di guasto pericoloso del contattore, già valutato e pari a $1{,}04 \cdot 10^{-6}\ h^{-1}$.

Si ottiene il seguente risultato:

$$PFH_D = 1{,}04 \cdot 10^{-6}\ h^{-1} \tag{6.18}$$

6.6.2 Set di equazioni: 1oo1D

Per il modello **1oo1D** viene riportata l'equazione da utilizzare che, per quanto descritto, è l'equazione che considera il test del canale come TOT:

$$PFH_D = PFH_{D\,TOT} = \lambda_{FD} - DC \cdot \cdot \frac{(\lambda_{FD} - \lambda_{CC})\left[\lambda_{FD}(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})T_M + (\lambda_{MD} - \lambda_{CC})\left(1 - e^{-(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M}\right)\right]}{(\lambda_{FD} + \lambda_{MD} - \lambda_{CC})^2 T_M} \tag{4.44}$$

Le variabili presenti nell'equazione sono valutate come segue:

- λ_{FD} è il tasso di guasto pericoloso del canale funzionale. È pari al tasso di guasto pericoloso del contattore, già valutato e pari a $1{,}04 \cdot 10^{-6}\ h^{-1}$.
- λ_{MD} è il tasso di guasto pericoloso del canale di monitor. È pari al tasso di guasto pericoloso della bobina di minima, già valutato e pari a $3{,}42 \cdot 10^{-10}\ h^{-1}$.
- λ_{CC} è il tasso di guasto pericoloso dovuto alle CCF. È pari al tasso di guasto pericoloso minimo, considerando il contattore e la bobina di minima, moltiplicato per il fattore beta, già valutato e pari a 2%. In questo caso λ_{CC} è pari a $2{,}08 \cdot 10^{-8}\ h^{-1}$.
- T_M è il tempo di missione. È pari al T_{10D} del contattore, già valutato pari a 11 anni.
- DC è la copertura diagnostica del contattore. È pari al 99%.

Si ottiene il seguente risultato:

$$PFH_D = 1{,}12 \cdot 10^{-7}\ h^{-1} \tag{6.19}$$

6.6.3 Set di equazioni: 1oo2D

Per il modello **1oo2D** viene riportata l'equazione da utilizzare e le equazioni di corredo, che esprimono le variabili di semplificazione contenute in essa. Le variabili di semplificazione L_A ed L_B vengono espresse tramite le equazioni relative al test continuo:

$$PFH_D = \frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_A\lambda_{AD} + L_B\lambda_{BD} + \lambda_{AD}\lambda_{BD}} + \frac{C_P}{T_M}\left[1 - e^{-\frac{1}{2}(L_1+L_2)T_M}\right] - \frac{C_N}{T_M}\left[1 - e^{-\frac{1}{2}(L_1-L_2)T_M}\right] \tag{5.46}$$

$$L_A = (1 - DC_A)(\lambda_{AD} - \lambda_{CC}) \tag{5.51}$$

$$L_B = (1 - DC_B)(\lambda_{BD} - \lambda_{CC}) \tag{5.52}$$

$$L_1 = \sqrt{(L_A + L_B)^2 + 2(L_A - L_B)(\lambda_{BD} - \lambda_{AD}) + (\lambda_{BD} - \lambda_{AD})^2} \tag{5.42}$$

$$L_2 = L_A + L_B + \lambda_{AD} + \lambda_{BD} \tag{5.43}$$

$$C_P = \frac{\lambda_{CC}}{L_1} - 2\frac{\lambda_{AD}L_B + \lambda_{BD}L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1(L_1 + L_2)} + 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1(L_1 + L_2)^2} \tag{5.49}$$

$$C_N = \frac{\lambda_{CC}}{L_1} - 2\frac{\lambda_{AD}L_B + \lambda_{BD}L_A + (\lambda_{AD} + \lambda_{BD})\lambda_{CC}}{L_1(L_2 - L_1)} + 4\frac{\lambda_{AD}\lambda_{BD}(L_A + L_B + \lambda_{CC})}{L_1(L_2 - L_1)^2} \tag{5.50}$$

Le variabili presenti nell'equazione sono valutate come segue:

- λ_{AD} e λ_{BD} sono i tassi di guasto pericoloso dei due canali funzionali. Sono pari entrambi al tasso di guasto pericoloso del contattore, già valutato e pari a $1{,}04 \cdot 10^{-6}\ h^{-1}$.
- λ_{CC} è il tasso di guasto pericoloso dovuto alle CCF. È pari al tasso di guasto pericoloso del contattore, considerando che i due canali funzionali sono identici, moltiplicato per il fattore beta, già valutato e pari a 2%. In questo caso λ_{CC} è pari a $6{,}84 \cdot 10^{-12}\ h^{-1}$.
- T_M è il tempo di missione. È pari al T_{10D} del contattore, già valutato e pari a 11 anni.
- DC_A e DC_B sono le coperture diagnostiche dei due contattori. Sono pari entrambe a 99%.

Si ottiene il seguente risultato:

$$PFH_D = 1{,}04 \cdot 10^{-8}\ h^{-1} \tag{6.20}$$

6.6.4 Set di equazioni: 1oo2

Per il modello **1oo2** viene utilizzato il set di equazioni proposto per il modello 1oo2D, con la differenza che, per le variabili di semplificazione L_A ed L_B, vengono utilizzate le equazioni semplificative che considerano la copertura diagnostica di entrambi i canali funzionali, in questo caso dei contattori, pari a zero ($DC_A = DC_B = 0$):

$$L_A = (\lambda_{AD} - \lambda_{CC}) \tag{5.75}$$

$$L_B = (\lambda_{BD} - \lambda_{CC}) \tag{5.76}$$

Si ottiene il seguente risultato:

$$PFH_D = 1{,}12 \cdot 10^{-7}\ h^{-1} \tag{6.21}$$

6.6.5 Set di equazioni: 1oo2(1D)

Per il modello **1oo2(1D)** considerato 1oo2D⁻ viene utilizzato il set di equazioni utilizzato anche per i modelli 1oo2D e 1oo2. Per le variabili di semplificazione L_A ed L_B viene utilizzata un'equazione comprendente la copertura diagnostica ed un'equazione che la considera pari a zero. Vista la simmetria del sottosistema è indifferente quale dei due canali funzionali, in questo caso quale dei contattori, si considera monitorato. Nelle equazioni proposte in seguito il canale monitorato viene considerato A mentre B viene considerato quello non monitorato ($DC_A = 99\%$, $DC_B = 0$):

$$L_A = (1 - DC_A)(\lambda_{AD} - \lambda_{CC}) \tag{5.51}$$

$$L_B = (\lambda_{BD} - \lambda_{CC}) \tag{5.76}$$

Sostituendo le variabili presenti come descritto si ottiene il seguente risultato:

$$PFH_D = 6{,}81 \cdot 10^{-8}\ h^{-1} \tag{6.22}$$

Per il modello **1oo2(1D)** considerato 1oo1D⁺ viene utilizzata l'equazione utilizzata per il modello 1oo1D. Come unico accorgimento è necessario considerare il tasso di guasto pericoloso del canale di monitor pari al tasso di guasto pericoloso del contattore: $\lambda_{MD} = 1{,}04 \cdot 10^{-6}\ h^{-1}$, invece che considerarlo pari al tasso di guasto pericoloso della bobina di minima, come è stato fatto per il modello 1oo1D.

Si ottiene il seguente risultato:

$$PFH_D = 7{,}74 \cdot 10^{-8}\ h^{-1} \tag{6.23}$$

6.6.6 Risultati ottenuti con set di equazioni

I risultati ottenuti con il set di equazioni ricavato nei capitoli 4 e 5 sono riportati nella seguente tabella, con anche la relativa corrispondenza al PL teorico ed al SIL teorico:

Architettura	PFH_D [h^{-1}]	PL teorico	SIL teorico
1oo1	$1{,}04 \cdot 10^{-6}$	c	SIL 1
1oo2	$1{,}12 \cdot 10^{-7}$	d	SIL 2
1oo1D	$1{,}04 \cdot 10^{-8}$	e	SIL 3
1oo2(1D) come 1oo1D⁺	$7{,}74 \cdot 10^{-8}$	e	SIL 3
1oo2(1D) come 1oo2D⁻	$6{,}81 \cdot 10^{-8}$	e	SIL 3
1oo2D	$2{,}17 \cdot 10^{-8}$	e	SIL 3

Tabella 6.4: Risultati ottenuti con il set di equazioni ottenute nei capitoli 4 e 5.

6.7 Soluzione con confronto dei risultati ottenuti

Vengono riportati, nella seguente tabella, i valori di PFH_D ottenuti con le tre metodologie illustrate, relativamente al sottosistema di output:

Architettura	IEC 62061	ISO 13849-1	Set di equazioni
1oo1	$1{,}04 \cdot 10^{-6}$	$1{,}14 \cdot 10^{-6}$	$1{,}04 \cdot 10^{-6}$
1oo2	$1{,}21 \cdot 10^{-7}$	/	$1{,}12 \cdot 10^{-7}$
1oo1D	$1{,}04 \cdot 10^{-8}$	$2{,}29 \cdot 10^{-7}$	$1{,}04 \cdot 10^{-8}$
1oo2(1D) come 1oo1D⁺	$8{,}05 \cdot 10^{-8}$	$2{,}29 \cdot 10^{-7}$	$7{,}74 \cdot 10^{-8}$
1oo2(1D) come 1oo2D⁻	$7{,}13 \cdot 10^{-8}$	/	$6{,}81 \cdot 10^{-8}$
1oo2D	$2{,}18 \cdot 10^{-8}$	$2{,}23 \cdot 10^{-8}$	$2{,}17 \cdot 10^{-8}$

Tabella 6.5: Confronto dei risultati ottenuti, in termini di PFH_D, per il sottosistema di output.

Si può notare la discrepanza tra le normative IEC 62061 e ISO 13849-1: le due hanno portato a differenti valori in termini di PFH_D per tutte le architetture considerate. La ISO 13849-1 non è utilizzabile per le architetture 1oo2 e 1oo2D⁻. Il set di equazioni, non presentando alcun vincolo, è utilizzabile per modellizzare ogni architettura. In questo caso la normativa IEC 62061 è utilizzabile per ogni analisi, essendo rispettati i vincoli di applicazione presenti in essa.

Il set di equazioni consente di ottenere risultati meno conservativi, se confrontati con entrambe le normative, per tutte le architetture considerate, ad eccezione dell'architettura 1oo1 dove la semplicità della stessa causa l'utilizzo di una semplice equazione sia per la IEC 62061 che per il set di equazioni, portando allo stesso risultato.

Le prestazioni migliori, in termini di PFH_D, sono ottenute dall'architettura 1oo1D, considerando il set di equazioni e la IEC 62061, a causa dell'elevata affidabilità della bobina di minima. Considerando la ISO 13849-1, dove non è presente una dipendenza diretta tra l'affidabilità del canale di monitor ed il risultato (se non attraverso il vincolo da rispettare), l'architettura migliore, in termini di PFH_D, è la 1oo2D.

Come era intuitivo attendere, considerando i sottosistemi a due canali funzionali, è presente un'affidabilità crescente in base al numero di canali monitorati, ciò è osservabile dai risultati ottenuti con la IEC 62061 ed il set di equazioni.

Per ottenere il PFH_D relativo all'intero sistema di sicurezza è sufficiente sommare le tre componenti di PFH_D ottenute, relative al sottosistema di input, di logica e di output. Le componenti ottenute per i primi due sottosistemi avranno un peso specifico molto limitato nella determinazione del PFH_D totale visto il loro minore ordine di grandezza. Viene ricordato che il PFH_D relativo all'elettroserratura è pari a $1{,}90 \cdot 10^{-9}\ h^{-1}$ mentre quello relativo al PLC è pari a $4 \cdot 10^{-9}\ h^{-1}$.

I sottosistemi di input e di logica, nella valutazione complessiva di SIL e di PL del sistema di sicurezza, non comportano un cambiamento perché hanno un SIL ed un PL maggiori rispetto a quanto richiesto dall'analisi di rischio, entrambi i sottosistemi sono caratterizzata da SIL 3 e PL=e, mentre è richiesta una riduzione del rischio pari a SIL 2 e PL=d.

Nella seguente tabella vengono riportati i valori di PFH_D relativi all'intero sistema di sicurezza, ottenuti come descritto:

Architettura output	IEC 62061	ISO 13849-1	Set di equazioni
1oo1	$1{,}05 \cdot 10^{-6}$	$1{,}15 \cdot 10^{-6}$	$1{,}05 \cdot 10^{-6}$
1oo2	$1{,}27 \cdot 10^{-7}$	/	$1{,}18 \cdot 10^{-7}$
1oo1D	$1{,}63 \cdot 10^{-8}$	$2{,}35 \cdot 10^{-7}$	$1{,}63 \cdot 10^{-8}$
1oo2(1D) come 1oo1D⁺	$8{,}64 \cdot 10^{-8}$	$2{,}35 \cdot 10^{-7}$	$8{,}33 \cdot 10^{-8}$
1oo2(1D) come 1oo2D⁻	$7{,}72 \cdot 10^{-8}$	/	$7{,}40 \cdot 10^{-8}$
1oo2D	$2{,}77 \cdot 10^{-8}$	$2{,}82 \cdot 10^{-8}$	$2{,}76 \cdot 10^{-8}$

Tabella 6.6: Confronto dei risultati ottenuti, in termini di PFH_D, per l'intero sistema di sicurezza.

Il sottosistema che stabilisce l'affidabilità dell'intero sistema è quello peggiore, che, in tutte le tipologie di architettura analizzate, è sempre il sottosistema di output. In altri termini la presenza dei sottosistemi di input e di logica non è in grado di produrre un abbassamento dell'affidabilità rilevante, dovuto alla disposizione in serie dei tre sottosistemi.

Nella seguente tabella viene riportata la valutazione in termini di SIL/PL di ogni tipologia di sistema di sicurezza analizzato. Viene evidenziato in rosso il SIL 1/PL=c per sottolineare l'inadeguatezza del sistema di sicurezza in questione mentre il SIL 2/PL=d ed il SIL 3/PL=e vengono evidenziati in verde perché adatti, con due gradazioni differenti per sottolineare la maggior affidabilità del SIL 3/PL=e:

Architettura output	ISO 13849-1	PLmax per ISO 13849-1	IEC 62061	Vincoli di architettura per IEC 62061	Set di equazioni
1oo1	PL=c	PL=c	SIL 1	SIL 1	SIL 1/PL=c
1oo2	/	/	SIL 2	SIL 1	SIL 2/PL=d
1oo1D	PL=d	PL=d	SIL 3	SIL 3	SIL 3/PL=e
1oo2(1D) come 1oo1D^{+}	PL=d	PL=d	SIL 3	SIL 3	SIL 3/PL=e
1oo2(1D) come 1oo2D^{-}	/	/	SIL 3	SIL 1	SIL 3/PL=e
1oo2D	PL=e	PL=e	SIL 3	SIL 3	SIL 3/PL=e

Tabella 6.7: Confronto dei risultati in termini di affidabilità ottenuti con diverse procedure, per il sistema di sicurezza.

Il PL massimo raggiungibile, per la ISO 13849-1 è relativo alla Categoria di riferimento, in questo caso corrisponde al valore ottenuto nel caso pratico dato l'elevato $MTTF_D$.

Si può notare un'ulteriore discrepanza tra le normative IEC 62061 e ISO 13849-1: le due hanno portato a differenti valori in termini di PL massimo raggiungibile e SIL massimo raggiungibile con i vincoli di architettura, considerando le architetture 1oo1D e 1oo2(1D).

Per la progettazione del sistema di sicurezza non è sufficiente, come già detto, un contattore con architettura 1oo1. In ogni analisi effettuata si ottiene la conferma di una riduzione del rischio insufficiente, ottenibile con questa architettura.

Dalla tabella si può notare che le architetture 1oo1D e 1oo2D sono adatte nella realizzazione del sistema di sicurezza: esse portano a risultati sufficienti con qualsiasi tipologia di analisi effettuata e rispettano i vincoli di architettura.

L'architettura 1oo2 non è utilizzabile anche se ottiene dei valori di PFH_D adeguati con l'applicazione del set di equazioni e della normativa IEC 62061: non rispetta i vincoli di architettura.

L'architettura 1oo2(1D) presenta, quando analizzabile, sia come 1oo1D^{+} che come 1oo2D^{-}, dei valori di PFH_D adeguati, con l'applicazione di tutte le metodologie. È possibile ritenere che soddisfi i vincoli di architettura considerandola come 1oo1D^{+}.

In conclusione, si può ritenere che, per ottenere una riduzione del rischio accettabile, è possibile, utilizzando i dispositivi descritti, applicare al macchinario uno dei seguenti sistemi di sicurezza già analizzati dettagliatamente nel loro funzionamento:

- Elettroserratura, PLC di sicurezza, contattore monitorato e bobina di minima (Figura 6.9).
- Elettroserratura, PLC di sicurezza e due contattori ridondanti di cui uno monitorato (Figura 6.10).
- Elettroserratura, PLC di sicurezza e due contattori ridondanti monitorati (Figura 6.11).

7. Considerazioni sulle normative

7.1 Considerazioni sulla normativa ISO 13849-1

La procedura tabellare riportata nella normativa ISO 13849-1 è molto semplice da applicare e necessita di pochi parametri di input, ovvero il $MTTF_D$, la DC e la definizione della Categoria relativa (B, 1, 2, 3 oppure 4). Può avere una discreta precisione, come dimostrato nell'esempio trattato, ma presenta alcune limitazioni, descritte in seguito.

Non è presente la definizione del tempo di missione, che è considerato pari a 20 anni per tutti i risultati ottenibili. Ciò può causare un risultato maggiore in termini di PFH_D se si considerano dispositivi soggetti a wearout aventi un T_{10D} minore di 20 anni. Minore è il T_{10D} e più sarà conservativo il PFH_D calcolato con questa normativa.

Non è presente la definizione del fattore beta, che è considerato pari a 2% per tutti i risultati ottenibili. Ciò non è di per sé una grande limitazione perché nella pratica il fattore beta è considerato sempre pari a 2%, ma potrebbe esserlo nel caso in cui si volesse procedere all'analisi di un sottosistema senza aver preso tutte le misure contro i CCF e considerando quindi un fattore beta maggiore; oppure nel caso di un nuovo sviluppo dello stato della tecnica che possa prevedere, sotto opportune condizioni, un fattore beta minore.

Non è definita in alcun modo l'efficienza di test legata al tempo (TRTE), che provoca un aumento in termini di PFH_D quando non è possibile considerare il test come tempo ottimale (TOT) in un'architettura 1oo1D. Non è possibile modellizzare nemmeno con test non continuo l'architettura 1oo2D.

Non è presenta la definizione del tasso di guasto pericoloso del canale di monitor per la Categoria 2 e, pertanto, si otterranno risultati identici con diversi canali di monitor applicati allo stesso canale funzionale. Ciò lo si è potuto notare anche nel caso pratico trattato dove, monitorando un contattore con una bobina di minima o con un altro contattore, si sono ricavati risultati uguali, anche se i due dispositivi presentavano dati di affidabilità differenti. Per non produrre risultati troppo imprecisi è stata aggiunto il già descritto vincolo di applicabilità sul tasso di guasto pericoloso del canale di monitor.

La copertura diagnostica è definibile solo attraverso una classificazione qualitativa (nulla, bassa, media, alta). Ciò può provocare una valutazione identica di due sottosistemi aventi copertura diagnostica differente ma appartenente alla stessa classe.

Non è possibile analizzare architetture 1oo2 o 1oo2(1D) simmetriche con le Categorie 3 o 4 ed è possibile analizzare architetture 1oo1D con copertura diagnostica alta solo in via ulteriormente conservativa, come mostrato nel caso di studio.

La definizione del $MTTF_D$ comporta una perdita di precisione nella valutazione del PFH_D perché deve essere correlato a valori predefiniti. Si ottiene lo stesso risultato per due sottosistemi con

caratteristiche di affidabilità differenti ma che, nell'applicazione della normativa, comportano l'utilizzo, nella tabella, dello stesso valore di $MTTF_D$.

Non è in grado di analizzare in modo accurato sottosistemi a due canali monitorati attraverso le Categorie 3 e 4: viene considerato in via conservativa il $MTTF_D$ minore.

I risultati conservativi ottenuti con la ISO 13849-1 sono validi anche considerando la peggiore delle ipotesi (condizione in genere definita in inglese come Worst Case Scenario) per i valori di PFH_D inseriti nella tabella. Un esempio pratico di ciò è descritto in seguito:

Viene considerato il Worst Case Scenario relativo alla Categoria 2, con $MTTF_D = 100\ anni$ e con DC alta. Il risultato, in termini di PFH_D, è già stato valutato nell'esempio ed è pari a $2{,}29 \cdot 10^{-7}$.

Per analizzare la peggiore delle ipotesi, con l'equazione relativa all'architettura 1oo1D del set di equazioni ricavato, è necessario considerare i seguenti parametri:

- DC come la minore che rientri nella classificazione "media": $DC = 90\%$,
- $MTTF_D$ come il minore che possa essere considerato in tabella pari a 100 anni, che corrisponde allo stesso valore: $MTTF_D = 100\ anni$,
- $MTTF_D$ del canale di monitor come il minore che possa rispettare la condizione di applicabilità: $MTTF_D = 100/2\ anni\ =\ 50\ anni$.

Il risultato è il seguente, utilizzando il set di equazioni: $PFH_D = 2{,}24 \cdot 10^{-7} < 2{,}29 \cdot 10^{-7}$.

Il caso studiato per il sottosistema con architettura 1oo2D nell'esempio pratico rappresenta, con una piccola approssimazione del $MTTF_D$, la peggiore delle ipotesi che può portare al PFH_D ottenuto con la ISO 13849-1. Anche in questo caso sono stati ottenuti risultati conservativi.

La normativa ISO 13849-1 porterà quindi a risultati sempre conservativi per sottosistemi monitorati, in confronto ai risultati ottenuti con il set di equazioni ricavate, anche nel caso in cui è necessario analizzare la peggiore delle ipotesi.

Il $MTTF_D$ da considerare nell'utilizzo della tabella ha un limite massimo, pari a 30 anni per la Categoria B, a 100 anni le Categorie 1, 2, 3 ed a 2500 anni per la Categoria 4. Ciò non costituisce una limitazione, per la normativa ISO 13849-1, in quanto questo limite nel $MTTF_D$ è l'equivalente dei vincoli di architettura presenti nella IEC 62061.

7.2 Considerazioni sulla normativa IEC 62061

La procedura riportata nella normativa IEC 62061 consiste in un set di equazioni molto simile al set di equazioni semplificato ottenuto nei capitoli 4 e 5. Necessita degli stessi parametri di input e porta, nel caso dell'architettura 1oo1, all'utilizzo della stessa equazione. La normativa IEC 62061 è stata applicata tramite un set di fogli elettronici. Può avere una discreta precisione, come dimostrato

nell'esempio trattato, ma presenta alcune limitazioni, descritte in seguito.

Presenta dei risultati leggermente conservativi per le architetture 1oo2, 1oo1D (al terzo decimale, nell'esempio trattato, non riportato in tabella), 1oo2(1D) e 1oo2D.

Non è definita in alcun modo l'efficienza di test legata al tempo (TRTE), che provoca un aumento in termini di PFH_D quando non è possibile considerare il test come tempo ottimale (TOT) in un'architettura 1oo1D. Non è possibile analizzare un'architettura 1oo2D con tassi di test differenti tra i due canali funzionali.

Per le architetture 1oo2 e 1oo2D viene calcolato il tasso di guasto per cause comuni utilizzando la media dei tassi di guasto pericoloso dei due canali. In caso di simmetria il risultato è uguale mentre, in caso di asimmetria, si ha una sovrastima del PFH_D dovuta ad una maggiorazione ingiustificata del tasso di guasto per cause comuni. È sempre corretto moltiplicare, al fattore beta, il minore dei tassi di guasto pericoloso.

È presente, per l'architettura 1oo1D, un importante vincolo sull'affidabilità del canale di monitor, che non viene rispettato nel caso trattato. Il vincolo è necessario perché l'equazione presente non modellizza correttamente la presenza di un canale di monitor poco affidabile. Intuitivamente, a livello teorico, un'architettura 1oo1D con un canale di monitor avente tasso di guasto pericoloso elevato, converge all'architettura 1oo1 perché, considerando la facilità che ha il canale di monitor di guastarsi, è come se non fosse presente nel modello.

Il set di equazioni ricavato nei capitoli 4 e 5 modellizza in modo corretto un canale di monitor poco affidabile, anche nel caso dove il tasso di guasto pericoloso di esso tenda ad infinito. Nella seguente equazione è riportato il limite appena discusso, come si può notare, il PFH_D dell'architettura 1oo1D converge a λ_{FD}, ovvero il PFH_D relativo all'architettura 1oo1:

$$\lim_{\lambda_{MD}\to\infty} PFH_D = \lim_{\lambda_{MD}\to\infty} \lambda_{FD} - DC \cdot \cdot \frac{(\lambda_{FD}-\lambda_{CC})\left[\lambda_{FD}(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M + (\lambda_{MD}-\lambda_{CC})\left(1-e^{-(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})T_M}\right)\right]}{(\lambda_{FD}+\lambda_{MD}-\lambda_{CC})^2 T_M} = \lambda_{FD} \quad (7.1)$$

Nell'equazione presente nella IEC 62061 non è presente questo riscontro pratico che rende inesistente un canale di monitor con un livello molto basso di affidabilità.

Nel calcolo dell'analogo limite si può notare che il PFH_D divergerà, ingiustificatamente, ad infinito:

$$\lim_{\lambda_{D\,FH}\to\infty} PFH_D = \lim_{\lambda_{D\,FH}\to\infty} \lambda_{De} - DC[\lambda_{De} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})] \cdot [1 - \frac{1}{2} \cdot (\lambda_{D\,FH} - \beta \cdot min(\lambda_{De}, \lambda_{D\,FH})T_1)] = +\infty \quad (7.2)$$

È possibile ottenere un esempio considerando l'architettura 1oo1D dell'esempio trattato nel caso pratico ed un tasso di guasto molto elevato del canale di monitor, pari ad esempio a $1 \cdot 10^{-3}$. I risultati ottenuti sono i seguenti:

- Con il set di equazioni si ottiene un PFH_D pari a $1{,}03 \cdot 10^{-6}$, valore che conferma la giusta convergenza all'architettura 1oo1 ($PFH_D = 1{,}04 \cdot 10^{-6}$).
- Con la IEC 62061 si ottiene un PFH_D pari a $4{,}86 \cdot 10^{-5}$, un valore maggiore di un ordine di grandezza rispetto all'architettura 1oo1. Questo aumento di PFH_D è assurdo per come è stata trattata l'architettura 1oo1D: aggiungendo un canale di monitor ad un canale funzionale è impossibile ottenere un peggioramento in termini di PFH_D.

Questa problematica nell'equazione relativa all'architettura 1oo1D non permette l'analisi nel caso di canali di monitor poco efficienti e giustifica la presenza del vincolo di applicabilità relativo, che potrebbe per altro non essere sufficiente per evitare l'applicabilità dell'equazione, vista la presenza di altri tre vincoli indipendenti che, se rispettati, permetterebbero l'utilizzo della stessa.

8. Conclusioni

Per l'applicazione del set di equazioni per il calcolo del PFH_D ottenuto nei capitoli 4 e 5 è stato implementato un set di fogli elettronici, che può essere utilizzato nella pratica aziendale in modo preciso, veloce e versatile. Produce risultati di una precisione più elevata e meno conservativi rispetto all'applicazione delle normative ISO 13849-1 ed IEC 62061 ed anche con una maggiore flessibilità. Con il suo utilizzo vengono risolte tutte le limitazioni descritte nel capitolo precedente, relative alle normative ISO 13849-1 ed IEC 62061.

I risultati minori, in termini di PFH_D, potrebbero permettere una valutazione diversa in termini di SIL e di PL per un sistema di sicurezza. È possibile considerare adatto, per il sistema di sicurezza, un certo dispositivo o l'utilizzo di una certa architettura che, con le normative ISO ed IEC, verrebbe considerata inadatta.

I risultati ottenibili con il set di equazioni, anche se meno conservativi rispetto a quelli ottenibili con la normativa ISO 13849-1 ed IEC 62061, possono essere ritenuti adatti all'utilizzo pratico, nell'ambito della sicurezza funzionale. Ciò è dovuto al fatto che, nella modellazione descritta nei capitoli 4 e 5, ogni semplificazione è stata fatta dal lato della sicurezza, garantendo un aumento di PFH_D.

Le analisi condotte nello svolgimento di questo lavoro di tesi hanno permesso di ottenere due importanti risultati:

- Analisi di una nuova architettura funzionale, presentata nei capitoli precedenti come 1oo2(1D), particolarmente interessante per alcune applicazioni di sicurezza funzionale ad alta richiesta (per questo scopo è stato analizzato un sistema di taglio confinato).
- È stato realizzato un software basato su Excel che, implementando le equazioni ricavate nei capitoli 4 e 5, consente di analizzare le architetture funzionali anche con la realizzazione di un confronto quantitativo con le normative IEC 62061 e ISO 13849-1.
- Le equazioni ricavate nei capitoli 4 e 5 consentono l'analisi di particolari architetture non analizzabili seguendo l'approccio IEC 62061 o ISO 13849-1.

Bibliografia

A. Birolini, "*Reliability Engineering – Theory and Practice*", Springer, 2010.

M. Catelani, L. Cristaldi, M. Lazzaroni, L. Peretto, P. Rinaldi, "*Reliability Engineering: basic concept and application in ICT*", Springer, 2011.

M. Dorra, "*Markov model-based calculation of the PFH_D of safety functions for machines: derivation of a set of PFH_D equations for typical machine control subsystem architectures*", Institute for Occupationa-l Safety and Health of the German Social Accident Insurance (IFA), 2017.

IEC 61508, "*Functional safety of electrical/electronic/programmable electronic safety-related systems*", IEC, 2010.

IEC 61708, "*Analysis techniques for dependability – Reliability block diagram and boolean methods*", IEC, 2006.

IEC 62061, "*Safety of machinery – Functional safety of safety-related control system*", IEC, 2020.

ISO 13849-1, "*Safety of machinery – Safety-related parts of control systems*", ISO, 2020.

G. Nano, R. Rota, "*Introduzione all'Affidabilità e Sicurezza nell'Industria di Processo*", Pitagora Editrice Bologna, 2007.

M. Rausand, A. Hoyland, "*System Reliability Theory: models, statistical methods and applications*", Wiley, 2004.