REER

Safety, Detection, Control

La 2006/42/CE, RESS 1.2.1 e la EN ISO13849-1/2

La Direttiva macchine 2006/42/CE e l'allegato 1

ALLEGATO I

Requisiti essenziali di sicurezza e di tutela della salute relativi alla progettazione e alla costruzione delle macchine

PRINCIPI GENERALI

1. Il fabbricante di una macchina, o il suo mandatario, deve garantire che sia effettuata una valutazione dei rischi per stabilire i requisiti di sicurezza e di tutela della salute che concernono la macchina. La macchina deve inoltre essere progettata e costruita tenendo conto dei risultati della valutazione dei rischi.

Con il processo iterativo della valutazione dei rischi e della riduzione dei rischi di cui sopra, il fabbricante o il suo mandatario:

- stabilisce i limiti della macchina, il che comprende l'uso previsto e l'uso scorretto ragionevolmente prevedibile,
- individua i pericoli cui può dare origine la macchina e le situazioni pericolose che ne derivano,
- stima i rischi, tenendo conto della gravità dell'eventuale lesione o danno alla salute e della probabilità che si verifichi,
- valuta i rischi al fine di stabilire se sia richiesta una riduzione del rischio conformemente all'obiettivo della presente direttiva,
- elimina i pericoli o riduce i rischi che ne derivano, applicando le misure di protezione nell'ordine indicato nel punto 1.1.2, lettera b).

La Direttiva macchine 2006/42/CE e l'allegato 1

PRINCIPI GENERALI (segue)

2. Gli obblighi previsti dai requisiti essenziali di sicurezza e di tutela della salute si applicano soltanto se esiste il pericolo corrispondente per la macchina in questione, allorché viene utilizzata nelle condizioni previste dal fabbricante, o dal suo mandatario, o nelle condizioni anormali prevedibili. Il principio di integrazione della sicurezza di cui al punto 1.1.2 e gli obblighi relativi alla marcatura e alle istruzioni di cui ai punti 1.7.3 e 1.7.4 si applicano comunque.

3. I requisiti essenziali di sicurezza e di tutela della salute elencati nel presente allegato sono inderogabili. Tuttavia, tenuto conto dello stato della tecnica, gli obiettivi da essi prefissi possono non essere raggiunti. In tal caso la macchina deve, per quanto possibile, essere progettata e costruita per tendere verso questi obiettivi.

4. Il presente allegato si articola in varie parti. La prima ha una portata generale ed è applicabile a tutti i tipi di macchine. Le altre parti si riferiscono a taluni tipi di pericoli più specifici. Tuttavia è indispensabile esaminare il presente allegato in tutte le sue parti, al fine di essere certi di soddisfare tutti i requisiti essenziali pertinenti.

Nel progettare la macchina, conformemente al punto 1 dei presenti principi generali, si tiene conto dei requisiti esposti nella parte generale e di quelli elencati in una o più delle altre parti in funzione dei risultati della valutazione dei rischi.

La Direttiva macchine 2006/42/CE e l'allegato 1

1.1.2. Principi d'integrazione della sicurezza

a) Per progettazione e costruzione, le macchine devono essere atte a funzionare, ad essere azionate, ad essere regolate e a subire la manutenzione senza che tali operazioni espongano a rischi le persone, se effettuate nelle condizioni previste tenendo anche conto dell'uso scorretto ragionevolmente prevedibile.

Le misure adottate devono avere lo scopo di eliminare ogni rischio durante l'esistenza prevedibile della macchina, comprese le fasi di trasporto, montaggio, smontaggio, smantellamento (messa fuori servizio) e rottamazione.

b) Per la scelta delle soluzioni più opportune il fabbricante o il suo mandatario deve applicare i seguenti principi, nell'ordine indicato:

- eliminare o ridurre i rischi nella misura del possibile (integrazione della sicurezza nella progettazione e nella costruzione della macchina),
- adottare le misure di protezione necessarie nei confronti dei rischi che non possono essere eliminati,
- informare gli utilizzatori dei rischi residui dovuti all'incompleta efficacia delle misure di protezione adottate, indicare se è richiesta una formazione particolare e segnalare se è necessario prevedere un dispositivo di protezione individuale.

La Direttiva macchine 2006/42/CE e l'allegato 1

c) In sede di progettazione e di costruzione della macchina, nonché all'atto della redazione delle istruzioni, il fabbricante o il suo mandatario, deve prendere in considerazione non solo l'uso previsto della macchina, ma anche l'uso scorretto ragionevolmente prevedibile.

La macchina deve essere progettata e costruita in modo da evitare che sia utilizzata in modo anormale, se ciò può comportare un rischio. Negli altri casi le istruzioni devono richiamare l'attenzione dell'utilizzatore sulle controindicazioni nell'uso della macchina che potrebbero, in base all'esperienza, presentarsi.

d) La macchina deve essere progettata e costruita tenendo conto delle limitazioni imposte all'operatore dall'uso necessario o prevedibile delle attrezzature di protezione individuale.

e) La macchina deve essere fornita completa di tutte le attrezzature e gli accessori speciali essenziali per poterla regolare, eseguirne la manutenzione e utilizzarla in condizioni di sicurezza.

La Direttiva macchine 2006/42/CE e l'allegato 1

1.2.1. Sicurezza ed affidabilità dei sistemi di comando

I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose. In ogni caso essi devono essere progettati e costruiti in modo tale che:

- resistano alle previste sollecitazioni di servizio e agli influssi esterni,
- un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose,
- errori della logica del sistema di comando non creino situazioni pericolose,
- errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose.

La Direttiva macchine 2006/42/CE e l'allegato 1

Particolare attenzione richiede quanto segue:

- la macchina non deve avviarsi in modo inatteso,
- i parametri della macchina non devono cambiare in modo incontrollato, quando tale cambiamento può portare a situazioni pericolose,
- non deve essere impedito l'arresto della macchina, se l'ordine di arresto è già stato dato,
- nessun elemento mobile della macchina o pezzo trattenuto dalla macchina deve cadere o essere espulso,
- l'arresto manuale o automatico degli elementi mobili di qualsiasi tipo non deve essere impedito,
- i dispositivi di protezione devono rimanere pienamente efficaci o dare un comando di arresto,
- le parti del sistema di controllo legate alla sicurezza si devono applicare in modo coerente all'interezza di un insieme di macchine e/o di quasi macchine.
- In caso di comando senza cavo deve essere attivato un arresto automatico quando non si ricevono i segnali di comando corretti, anche quando si interrompe la comunicazione.

Le Norme ISO 13849-1 e 13849-2

UNI EN ISO 13849-1:2008

Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione

Sommario :

La presente norma è la versione ufficiale della norma europea EN ISO 13849-1 (edizione giugno 2008) e tiene conto della errata corrige del marzo 2009 (AC:2009). La norma specifica i requisiti di sicurezza e le linee guida sui principi di progettazione e integrazione di parti dei sistemi di comando legate alla sicurezza, inclusa la progettazione del software.

UNI EN ISO 13849-2:2013

Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 2: Validazione

Sommario : La presente norma è la versione ufficiale in lingua inglese della norma europea EN ISO 13849-2(edizione ottobre 2012). La norma specifica le procedure e le condizioni da seguire per la validazione mediante analisi e prove delle funzioni di sicurezza specificate, la categoria ottenuta e il livello di prestazione ottenuto dalle parti di un sistema di comando legate alla sicurezza progettate in conformità alla UNI EN ISO 13849-1.

La norma ed il RESS 1.2.1

Annex ZB
(informative)

Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach Directive Machinery 2006/42/EC.

Once this standard is cited in the Official Journal of the European Communities under that Directive and has been implemented as a national standard in at least one Member State, compliance with the normative clauses of this standard confers, within the limits of the scope of this standard, a presumption of conformity with Essential Requirements 1.2.1 of Annex I of that Directive and associated EFTA regulations.

WARNING — Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

Termini e definizione

- **SRP/CS (Safety Related Parts of Command System) – Sistemi di comando legati alla sicurezza**
  - Parte di un sistema di comando che risponde a segnali di ingresso legati alla sicurezza e genera dei corrispondenti segnali di uscita legati alla sicurezza.
- **Fault - Avaria**
  - Stato di un entità caratterizzato dall'incapacità di eseguire una funzione richiesta, esclusa l'inabilità durante la manutenzione preventiva o durante altre azioni programmate o dovute alla mancanza di mezzi esterni
  - Una avaria è spesso il risultato di un guasto, ma, può esistere anche senza il verificarsi dello stesso
- **Failure - Guasto**
  - Cessazione dell'attitudine di un entità ad eseguire una azione richiesta
- **Dangerous Failure – Guasto pericoloso**
  - Guasto che, potenzialmente, può portare la SRP/CS in uno stato pericoloso e/o inibirne la capacità di effettuare la propria funzione
- **PL (Performance Level) - Livello di prestazione**
  - Livello discreto usato per per specificare la capacità di un sistema di comando legato alla sicurezza di effettuare una funzione di sicurezza in determinate condizioni.

Termini e definizione

- **PLr (Performance Level Required) - Livello di prestazione richiesto**
  - Valore di PL minimo da raggiungere dalla SRP/CS, determinato dalla figura A.1 della UNI EN ISO 13849-1
- **MTTFd (Mean Time To Dangerous Failure) - Tempo medio ad un guasto pericoloso.**
  - Tempo medio al verificarsi di un guasto pericoloso, espresso in anni.
- **B10d**
  - Numero dei cicli per il quale il 10% dei componenti ha subito un guasto pericoloso
- **DC (Diagnostic Coverage) – Copertura diagnostica**
  - Valore della capacità del SRP/CS di rilevare i guasti pericolosi, espresso come il rapporto tra la probabilità di guasti pericolosi diagnosticabili ed il totale dei guasti pericolosi che possono avvenire. Valore espresso in percentuale.
- **CCF (Common Cause Failure) – Guasti di causa comune**
  - Guasto di più di un entità, risultato di un singolo evento, dove un guasto non è conseguenza di altri.
- **Tm (Mission Time) – Tempo di utilizzo**
  - Periodo di tempo che copre l'utilizzo previsto di un SRP/CS.

Termini e definizione

- **PLr (Performance Level Required) - Livello di prestazione richiesto**
  - Valore di PL minimo da raggiungere dalla SRP/CS, determinato dalla figura A.1 della UNI EN ISO 13849-1
- **MTTFd (Mean Time To Dangerous Failure) - Tempo medio ad un guasto pericoloso.**
  - Tempo medio al verificarsi di un guasto pericoloso, espresso in anni.
- **B10d**
  - Numero dei cicli per il quale il 10% dei componenti ha subito un guasto pericoloso
- **DC (Diagnostic Coverage) – Copertura diagnostica**
  - Valore della capacità del SRP/CS di rilevare i guasti pericolosi, espresso come il rapporto tra la probabilità di guasti pericolosi diagnosticabili ed il totale dei guasti pericolosi che possono avvenire. Valore espresso in percentuale.
- **CCF (Common Cause Failure) – Guasti di causa comune**
  - Guasto di più di un entità, risultato di un singolo evento, dove un guasto non è conseguenza di altri.
- **Tm (Mission Time) – Tempo di utilizzo**
  - Periodo di tempo che copre l'utilizzo previsto di un SRP/CS.

Il PL (performace level)

Table 2 — Performance levels (PL)

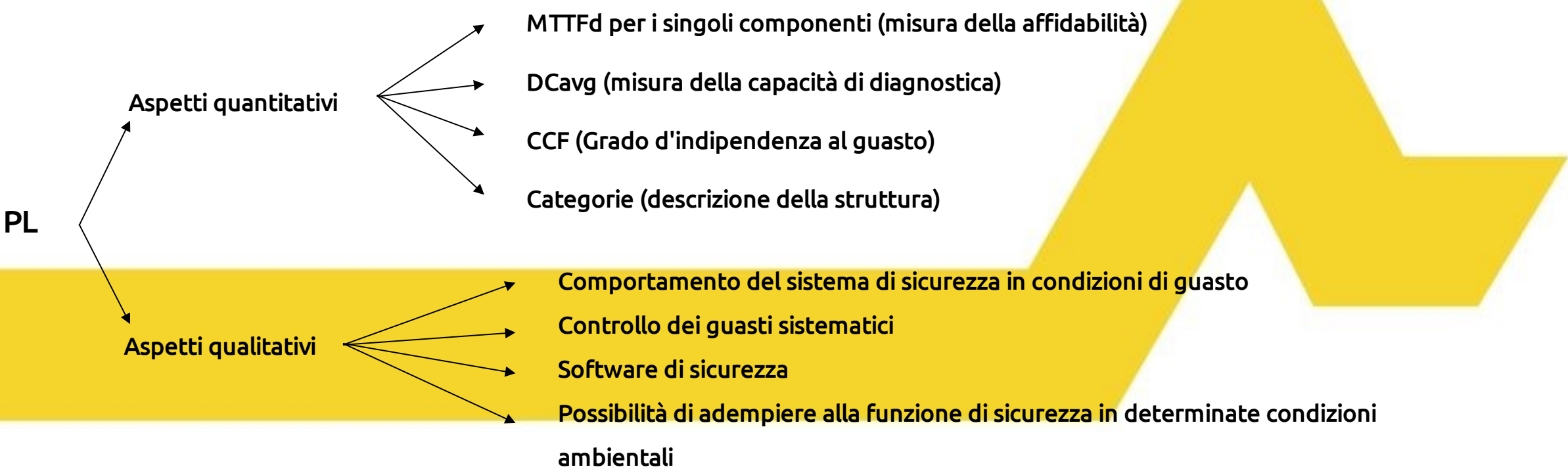
PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

Quanto maggiore è il contributo alla riduzione del rischio tanto più bassa è la **Probabilità media di guasto pericoloso/ora.**

Il PL è funzione della architettura del sistema di controllo, della affidabilità dei componenti, della capacità di rilevare per tempo eventuali guasti interni che potrebbero limitare la funzione di sicurezza e della qualità del progetto.

Il PL (performace level)

Il seguente prospetto riassume gli aspetti qualitativi e quantitativi da rispettare se si vuole progettare un sistema di controllo di sicurezza conforme alla EN13849-1.



PL o Performance Level

Il progettista, per poter dichiarare un determinato valore di PL deve:

Calcolare la Probabilità media di guasto pericoloso/ora del circuito di controllo realizzato, dimostrare di aver ottemperato a tutti i requisiti riguardanti gli aspetti qualitativi stabiliti dalla norma.

Il progetto dovrà poi essere validato utilizzando la
ISO EN13849-2 Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 2: Validazione.

Essa definisce le procedure e le condizioni da seguire per la convalida mediante analisi e prove:

- della funzione di sicurezza fornita
- della categoria raggiunta
- del livello di prestazione raggiunto.

IMPORTANTE!

Il valore PFHd è solo uno dei parametri che contribuiscono all'assegnazione del PL.
Bisogna altresì dimostrare e documentare di aver preso in considerazione e rispettato tutti i requisiti relativi:

- al controllo dei guasti sistematici;
- all'uso di componenti robusti e affidabili (rispondenti a norme di prodotto, ove disponibili);
- all'uso di norme di buona tecnica;
- di aver tenuto conto delle condizioni ambientali in cui dovrà operare il sistema di sicurezza;
- nel caso sia stato necessario scrivere software, di aver adottato tutti gli aspetti di organizzazione esemplificati nel modello di sviluppo a V di Fig. 6 della norma ISO EN13849-1 e di aver rispettato i requisiti di sviluppo sia per il software applicativo che per quello incorporato.

Il processo di progettazione di un SRP/CS secondo la ISO EN13849-1 può essere riassunto nei seguenti otto passi:

1. Individuazione della funzione di sicurezza tramite l'analisi dei rischi
2. Assegnazione del Performance Level richiesto (PLr) tramite il grafico dei rischi
3. Scelta della struttura del sistema (architetture) e delle tecniche di autodiagnosi
4. Realizzazione tecnica del sistema di controllo
5. Calcolo di MTTFd, DCavg e verifica di CCF (non esemplificato in questa presentazione)
6. Calcolo di PL, per esempio tramite la Tabella 5
7. Verifica del PL
   (se il PL calcolato è inferiore al PLr occorre ritornare al passo 3)
8. Validazione

Individuazione della funzione di sicurezza e assegnazione del Performance Level richiesto - PLr

Per ogni funzione di sicurezza individuata (Paragrafo 5 della Norma) il progettista decide il contributo alla riduzione del rischio che essa deve fornire, ossia il PLr.

Questo contributo non copre il rischio complessivo della macchina, ma solo quella parte del rischio legata alla applicazione di quella particolare funzione di sicurezza.

Il Parametro PLr rappresenta il Livello di Prestazione richiesto per quella funzione di sicurezza.

Il parametro PL rappresenta invece il Livello di prestazione dell'hardware che la implementa.

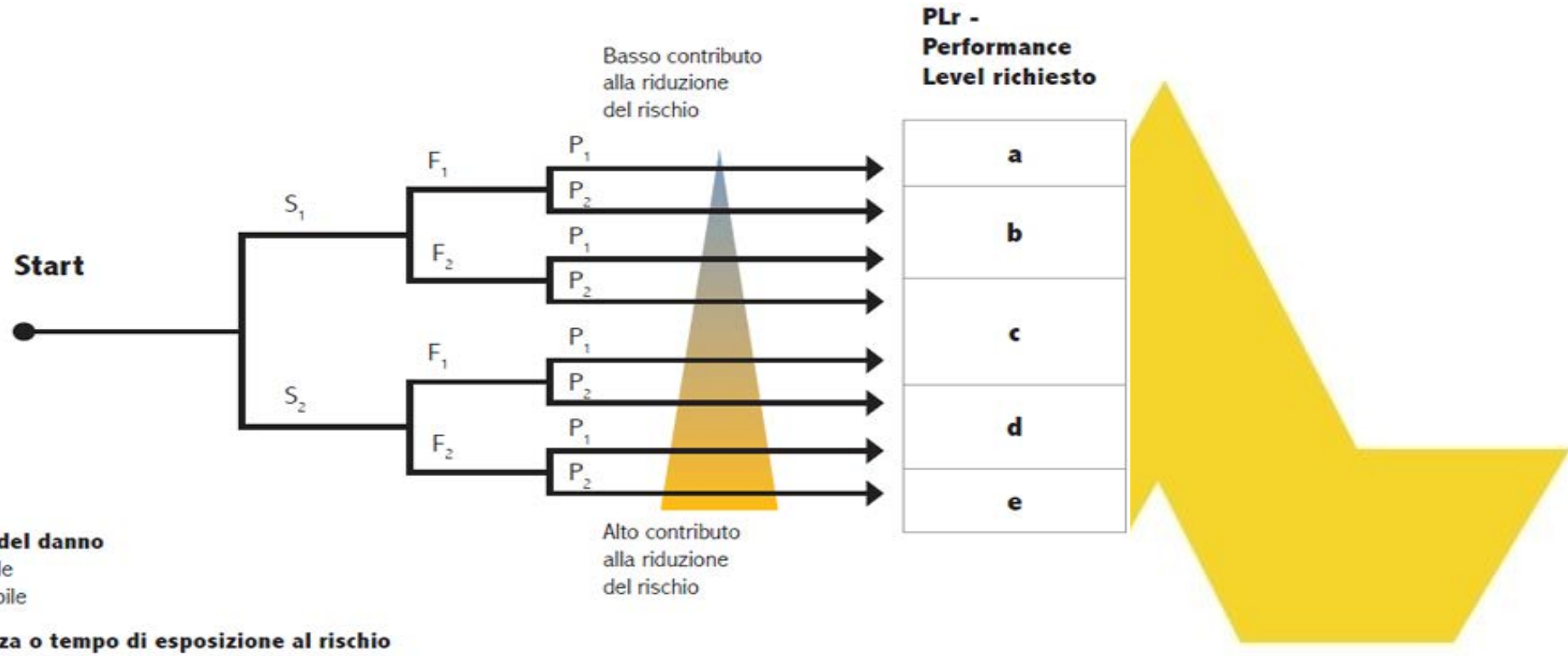
PL>=PLr

Individuazione della funzione di sicurezza e assegnazione del Performance Level richiesto - PLr

Lo strumento che viene utilizzato per stabilire quale dovrà essere il contributo alla riduzione del rischio fornito dalla funzione di sicurezza è un grafico del tipo ad albero delle decisioni che porta ad individuare in modo univoco il valore di PLr (Annesso “A” della norma).

Se vengono individuate più funzioni di sicurezza, per ognuna di esse occorre definire il PLr.

Grafico per individuare in modo univoco il valore di PLr



S gravità del danno
S1 reversibile
S2 irreversibile

F frequenza o tempo di esposizione al rischio
F1 rara / breve
F2 continua / lunga

P possibilità di evitare il rischio o di limitare il danno
P1 possibile entro certe condizioni
P2 scarsamente possibile

Nota: al contrario di quanto veniva detto nella EN954-1 a proposito delle Categorie, qui i PLr sono pienamente gerarchici".
PLr(e) fornisce il più alto contributo alla riduzione del rischio, PLr(a) il più basso.

Dopo aver deciso il valore di PLr necessario bisogna progettare un SRP/CS idoneo, calcolare il PL risultante e verificare che sia maggiore o uguale al PLr.

Dalla **tabella 3** (vedi pag. 19) si vede che per ricavare il valore di PL occorre calcolare la Probabilità media di guasto pericoloso/ora del sistema di controllo progettato.

Esistono diversi metodi per effettuare una stima della Probabilità media di guasto pericoloso/ora di un sistema di controllo di sicurezza.

L'uso di questi metodi presuppone che per ogni componente si conosca:

- il tasso di guasto (λ)
- la percentuale di ripartizione del tasso di guasto per tutte le modalità di guasto del componente (es. per un interruttore ad azione positiva:
  - ✓ il contatto non si apre quando richiesto = 20% dei casi,
  - ✓ il contatto non si chiude quando richiesto = 80% dei casi)
- l'effetto che ha ogni guasto sul comportamento del sistema di Sicurezza (es. guasto pericoloso- λd oppure guasto non pericoloso-λs)
- la percentuale di guasti pericolosi rilevati dalle tecniche automatiche di autodiagnosi implementate rispetto al totale dei guasti pericolosi:

$$\lambda dd = \lambda d \times DC$$

- la percentuale di guasti pericolosi non rilevati dalle tecniche automatiche di autodiagnosi implementate rispetto al totale dei guasti pericolosi:

$$\lambda du = \lambda d \times (1-DC).$$

La ISO EN13849-1 semplifica il calcolo fornendo una tabella basata sulla modellazione di Markov nella quale il valore di probabilità media di guasto pericoloso per ora è già pre-calcolato per diverse combinazioni di Categorie, e di valori di massima di MTTFd e di DCavg che vengono determinati anch'essi tramite tabelle.

Indicazione di MTTFd	Valori espressi in anni
Basso	3 ≤ MTTFd < 10
Medio	10 ≤ MTTFd < 30
Alto	30 ≤ MTTFd < 100

Definizione DCavg	Valore di DC DCavg
Nessuna	DC < 60%
Basso	60% ≤ DC < 90%
Medio	90% ≤ DC < 99%
Alto	99% ≤ DC

Si riconduce tutto a:

- scelta dell'architettura;
- calcolo di DCavg in funzione delle tecniche di autodiagnosi;
- calcolo semplificato di MTTFd del circuito progettato;
- verifica rispettato delle condizioni di indipendenza di funzionamento dei canali (CCF) nel caso di architetture ridondanti.

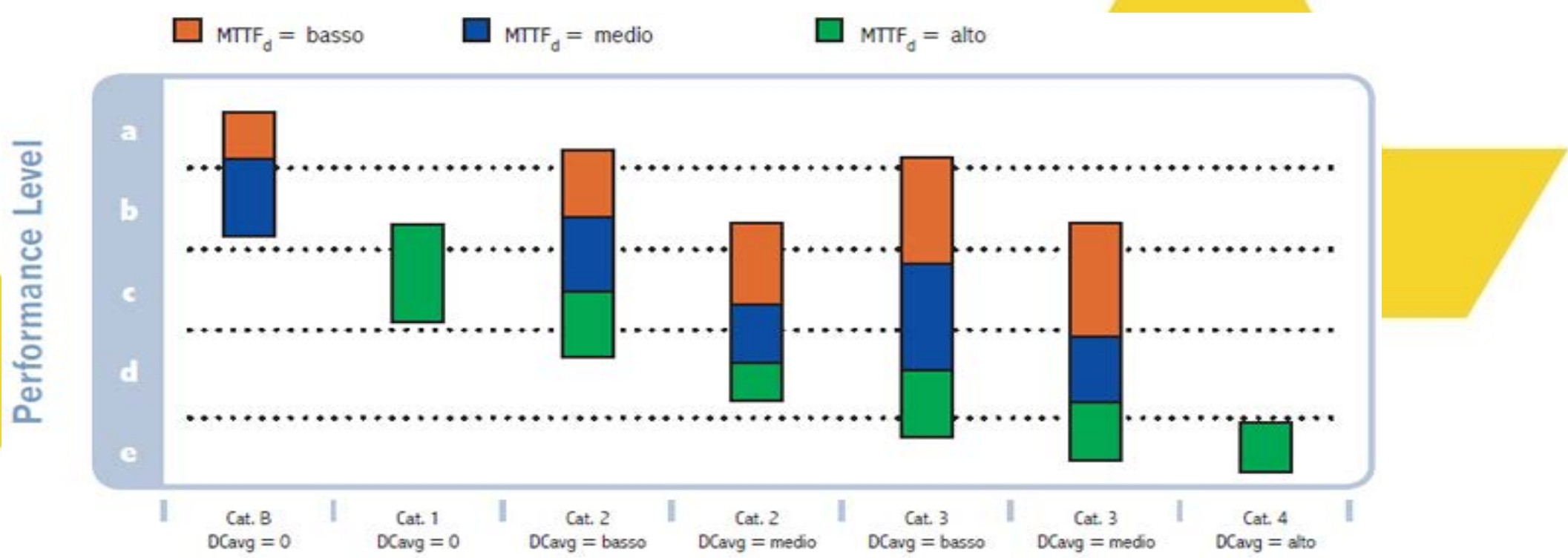


Fig. 5 di ISO 13849-1

Calcolo del PL

Nel caso che la parte di colonna scelta comprenda due possibili valori di PL si può ricavare il valore puntuale di PL dalla tabella **K.1 dell'Annesso K** della Norma.

La Norma può essere usata solo se per il progetto del sistema di controllo ci si avvale di una (o più) delle cinque architetture prefissate.
Ad ogni architettura corrisponde una delle categorie definite nella EN 954-1.
Per ogni Livello di Prestazione richiesto sono possibili più scelte.

Esempio

Per ottenere un sistema con PL pari a "c" sono possibili:

- Categoria 3 con MTTFd = basso e DCavg media
- Categoria 3 con MTTFd = medio e DCavg bassa
- Categoria 2 con MTTFd = medio e DCavg media
- Categoria 2 con MTTFd = alto e DCavg bassa
- Categoria 1 con MTTFd = alto.

Combinazione di più SRP/CS

Una funzione di sicurezza può essere composta da uno o più SRP/CS, e più funzioni di sicurezza possono utilizzare gli stessi SRP/CS.

I singoli SRP/CS poi, potrebbero essere realizzati con architetture diverse.

Se la funzione di sicurezza è realizzata collegando in serie più SRP/CS (es. barriera di sicurezza, logica di controllo, uscita di potenza) e se per ciascuno di essi è
noto il PL, la norma fornisce un modo semplice per calcolare il PL totale.

Si identifica la parte col PL più basso (PL low),
Si identifica il numero di parti che hanno PL = PL low
Si inseriscono i dati nella tabella seguente e si ricava il PL totale

Combinazione di più SRP/CS

PL (low)	n (low)		PL
a	> 3 ≤ 3	→	- a
b	> 2 ≤ 2	→	a b
c	> 2 ≤ 2	→	b c
d	> 3 ≤ 3	→	c d
e	> 3 ≤ 3	→	d e

Tabella 3 della EN ISO 13849-1

Il PL ricavato tramite questa tabella si riferisce a valori di probabilità media di guasto pericoloso per ora che si trovano a meta per ognuno degli intervalli di Tabella 3 della ISO13849-1

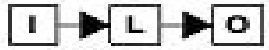
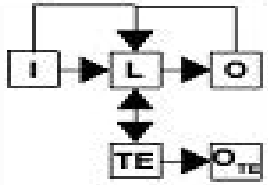
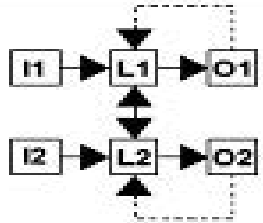
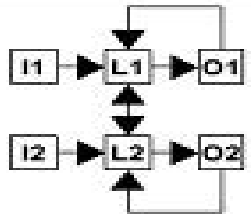
Esempio

Risulta: **PL low = d** **N low = 1 (< 3)**
Quindi: **PL complessivo = d**

Il valore di Probabilità media di guasto pericoloso per ora dell'intero sistema sarà un numero compreso fra $1x10^{-6}$ e $1x10^{-7}$ (vedere Tabella 3 della EN ISO 13849-1).

Le categorie

Requisiti delle categorie di sicurezza e PL possibile

		Categoria B	Categoria 1	Categoria 2	Categoria3	Categoria 4
						
Proprietà	Ridondanza(2 Canali)	No	No	No	SI	SI
	Tolleranza al guasto Accumulo di guasti	0 -	0 -	0 ✗	1 ✗	1 ✓
Requisiti	Monitoraggio(DC)	Nessuno	nessuno	da basso a medio	da basso a medio	alto
	MTTFd dei componenti	da basso a medio	alto	da basso a alto	da basso a alto	alto
	Osservanza CCF	No	No	SI	SI	SI
	Principi di sicurezza	Base	Base & ben provati	Base & ben provati	Base & ben provati	Base & ben provati
	Componenti ben provati	-	Si	-	-	-
	PL (possibile)	a+b	b+c	a+d	a+e	e

I: Ingresso
L: Logica
O: Uscita

TE: Equipaggiamento di test
O_{TE}: Uscita Equipaggiamento di test
$MTTF_d$: Mean time to dangerous failure

DC: Copertura diagnostica
✗ Perdita della funzione di sicurezza

Calcolo MTTFd per componenti con B10d

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad Dove\ n_{op} = numero\ di\ operazioni$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600}{t_{cycle}}$$

$h_{op} = ore\ operative\ al\ giorno\ [\mathrm{h}]$

$d_{op} = giorni\ operativi\ all'anno\ [\mathrm{gg}]$

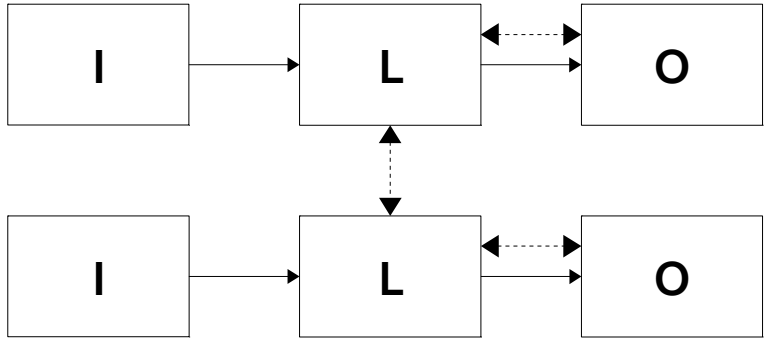
$t_{cycle} = tempo\ che\ intercorre\ tra\ due\ successive\ richieste\ d'intervento\ [\mathrm{s}]$

Metodo semplificato per la stima di MTTFd

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}}$$

$$\frac{1}{MTTF_{dtot}} = \frac{1}{MTTF_{dI}} + \frac{1}{MTTF_{dL}} + \frac{1}{MTTF_{dO}}$$

MTTFd diverso per 2 canali, simmetrizzazione per ciascun canale



$$MTTF_d = \frac{2}{3} \times \left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

La copertura diagnostica

Misure	DC	Dipendente da	Non suff. Per PL
Dispositivi d'ingresso			
Stimolo di prova ciclico mediante variazione dinamica dei segnali d´ingresso.	90	-	-
Controllo di plausibilità, per esempio utilizzo di contatti collegati meccanicamente normalmente aperti e normalmente chiusi.	99	-	-
Monitoraggio incrociato degli ingressi senza prova dinamica.	0÷99	in funzione della frequenza di cambiamento del segnale da parte dell'applicazione	-
Monitoraggio incrociato dei segnali di ingresso con prova dinamica se i cortocircuiti non sono rilevabili (e.s I/O multipli)	90	-	-
Monitoraggio incrociato dei segnali di ingresso e dei risultati all'interno della logica (L), monitoraggio software temporale e logico del flusso di programma e rilevamento della avarie statiche e dei cortocircuiti (per I/O multipli)	99	-	-
Monitoraggio indiretto (per esempio monitoraggio mediante pressostato, monitoraggio elettrico della posizione degli attuatori)	90÷99	in funzione dell'applicazione	-
Monitoraggio diretto (per esempio monitoraggio elettrico di posizione delle valvole di comando, monitoraggio dei dispositivi elettromeccanici mediante elementi di contatto collegati meccanicamente)	99	-	-
Rilevamento delle avarie mediante processo	0÷99	in funzione dell'applicazione	e
Monitoraggio di alcune caratteristiche del sensore (tempo di risposta, intervallo dei segnali analogici, per esempio resistenza elettrica, capacita)	60	-	-

La copertura diagnostica

Misure	DC	Dipendente da	Non suff. Per PL
Logica			
Monitoraggio indiretto (per esempio monitoraggio mediante pressostato, monitoraggio elettrico di posizione degli attuatori)	90÷99	in funzione dell'applicazione	-
Monitoraggio diretto (per esempio monitoraggio elettrico di posizione delle valvole di comando, monitoraggio dei dispositivi elettromeccanici mediante elementi di contatto collegati meccanicamente)	99	-	-
Semplice monitoraggio temporale della logica (per esempio timer come watchdog, in cui i punti di trigger rientrano nel programma della logica)	60	-	-
Monitoraggio temporale e logico della logica mediante il watchdog in cui l´attrezzatura di prova effettua controlli di plausibilità del comportamento della logica.	90	-	-
Autodiagnosi all´avvio per rilevare avarie latenti in parti della logica (per esempio programma e memoria dati, porte di ingresso/uscita, interfacce)	90	(in funzione della tecnica di prova)	-
Controllo della capacita di reazione del dispositivo di monitoraggio (per esempio, watchdog) mediante il canale principale all´avvio od ogniqualvolta e richiesta la funzione di sicurezza o e richiesto da un segnale esterno, attraverso un dispositivo in ingresso.	90	-	-
Principio dinamico (a tutti i componenti della logica e richiesto di cambiare lo stato ON-OFF-ON quando e richiesta la funzione di sicurezza), per esempio circuito di interblocco implementato mediante relè.	99	-	-
Memoria invariabile: sigla di una parola singola (8 bit)	90	-	-
Memoria invariabile: sigla di una parola doppia (16 bit)	99	-	-

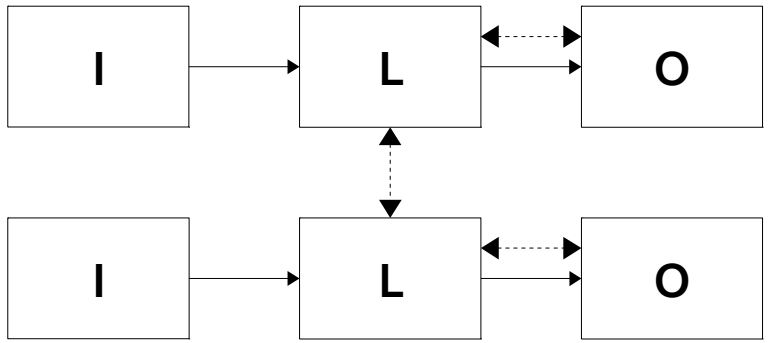
La copertura diagnostica

Misure	DC	Dipendente da	Non suff. Per PL
Logica			
Memoria variabile: Test della RAM mediante l´utilizzo di dati ridondanti, per esempio indicatori, marcatori, costanti, timer e confronto incrociato di questi dati.	60	-	-
Memoria variabile: controllo della leggibilità e della capacita di scrittura delle celle di memoria dati utilizzati.	60	-	-
Memoria variabile: monitoraggio della RAM con codice Hamming modificato o autodiagnosi della RAM (e.s. "galpat" o "Abraham")	99	-	-
Unita di elaborazione:autodiagnosi mediante software	60÷90	-	-
Unita di elaborazione:elaborazione codificata	90÷99	-	-
Rilevamento avarie da parte del processo	0÷99	in funzione dell'applicazione	e

La copertura diagnostica

Misure	DC	Dipendente da	Non suff. Per PL
Dispositivi di uscita			
Monitoraggio delle uscite mediante un canale senza prova dinamica.	0÷99	in funzione della frequenza di cambiamento del segnale da parte dell´applicazione	-
Monitoraggio incrociato delle uscite senza prova dinamica.	0÷99	in funzione della frequenza di cambiamento del segnale da parte dell´applicazione	-
Monitoraggio incrociato dei segnali di uscita con prova dinamica senza rilevamento dei cortocircuiti (per I/O multipli)	90	-	-
Monitoraggio incrociato dei segnali di uscita e dei risultati intermedi all´interno della logica (L), monitoraggio software temporale e logico del flusso di programma e rilevamento delle avarie statiche dei cortocircuiti (per I/O multipli)	99	-	-
Percorso di spegnimento ridondante senza monitoraggio dell´attuatore.	0	-	-
Percorso di spegnimento ridondante con monitoraggio di uno degli attuatori mediante logica o attrezzatura di prova	90	-	-
Percorso di spegnimento ridondante con monitoraggio degli attuatori mediante logica o attrezzatura di prova	99	-	-
Monitoraggio indiretto (per esempio monitoraggio mediante pressostato, monitoraggio elettrico di posizione degli attuatori)	90÷99	in funzione dell´applicazione	-
Rilevamento avarie da parte del processo	0÷99	in funzione dell´applicazione	e
Monitoraggio diretto (per esempio monitoraggio elettrico di posizione delle valvole di comando, monitoraggio dei dispositivi elettromeccanici mediante elementi di contatto collegati meccanicamente)	99	-	-

Stima della copertura diagnostica media DC_{avg}



$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}}$$

prospetto F.1 **Processo di assegnazione di un punteggio e di quantificazione delle misure contro i CCF**

N°	Misure contro i CCF	Punteggio
1	**Separazione/ Segregazione**	
	Separazione fisica tra i percorsi dei segnali: separazione in cablaggi/tubazioni, spazi sufficienti e distanze di scorrimento sulle schede di circuiti stampati.	**15**
2	**Diversità**	
	Si utilizzano tecnologie/progettazione o principi fisici diversi, per esempio: elettronica programmabile nel primo canale e secondo canale cablato, tipo di attuazione, pressione e temperatura. Misurazione di distanza e pressione, digitale e analogica. Componenti di fabbricanti diversi	**20**
3	**Progettazione/applicazione/esperienza**	
3.1	Protezione contro eccesso di tensione, potenza, corrente, ecc.	**15**
3.2	Utilizzo di componenti ben provati	**5**
4	**Valutazione/analisi**	
	Si tiene conto dei risultati dell'analisi delle modalità e degli effetti dei guasti per evitare guasti da causa comune nella progettazione?	**5**

CCF

6	**Ambiente**	
6.1	Prevenzione della contaminazione e compatibilità elettromagnetica (EMC) contro i CCF in conformità alle norme appropriate. Sistemi fluidici: filtrazione del mezzo in pressione, prevenzione dell'assorbimento di sporco, scarico dell'aria compressa, per esempio in conformità ai requisiti del fabbricante del componente concernenti la purezza del mezzo in pressione. Sistemi elettrici: controllo dell'immunità elettromagnetica del sistema, per esempio come specificato nelle norme pertinenti, rispetto ai CCF Per i sistemi fluidici ed elettrici combinati, si dovrebbero considerare entrambi gli aspetti.	**25**
6.2	Altri influssi Considerazione dei requisiti sull'immunità a tutti gli influssi ambientali pertinenti come temperatura, urti, vibrazioni, umidità (per esempio come specificato nelle norme pertinenti).	**10**
	Totale	**[massimo conseguibile 100]**

Punteggio totale	Misure per evitare i CCF[a)]
65 o migliore	Soddisfa i requisiti
Minore di 65	Processo non riuscito ⇒ scegliere misure aggiuntive

GRAZIE PER L'ATTENZIONE