PL e probabilità di guasto

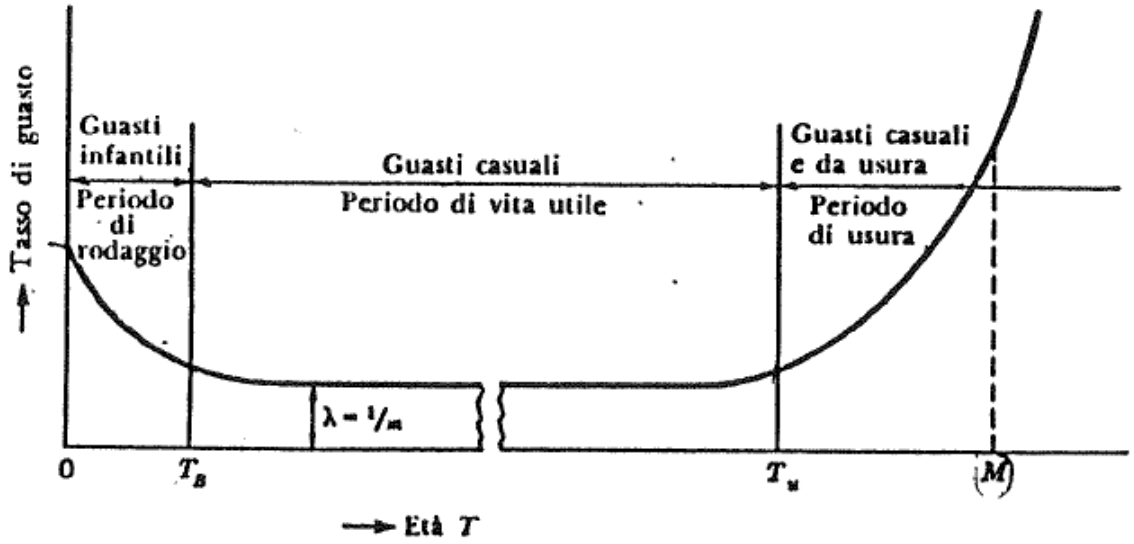
La EN ISO 13849-1 richiede che per valutare il livello di prestazione PL di un sistema di controllo di sicurezza si calcoli fra l'altro la sua probabilità di guasto pericoloso/ora (PFHd) :

PL	RRF	PFHd
a	1 - 10	10^{-4} - 10^{-5}
b	10 - 33	10^{-5} - 3×10^{-6}
c	33 - 100	3×10^{-6} – 10^{-6}
d	100 - 1000	10^{-6} - 10^{-7}
e	1000 - 10000	10^{-7} - 10^{-8}

Relazione che esiste fra PL , PFHd e fattore di riduzione del rischio RRF.

Per il calcolo del PFHd occorre conoscere il tasso di guasto dei guasti casuali di ogni componente del sistema di controllo di sicurezza.

Andamento del tasso di guasto dei componenti in funzione dell'età



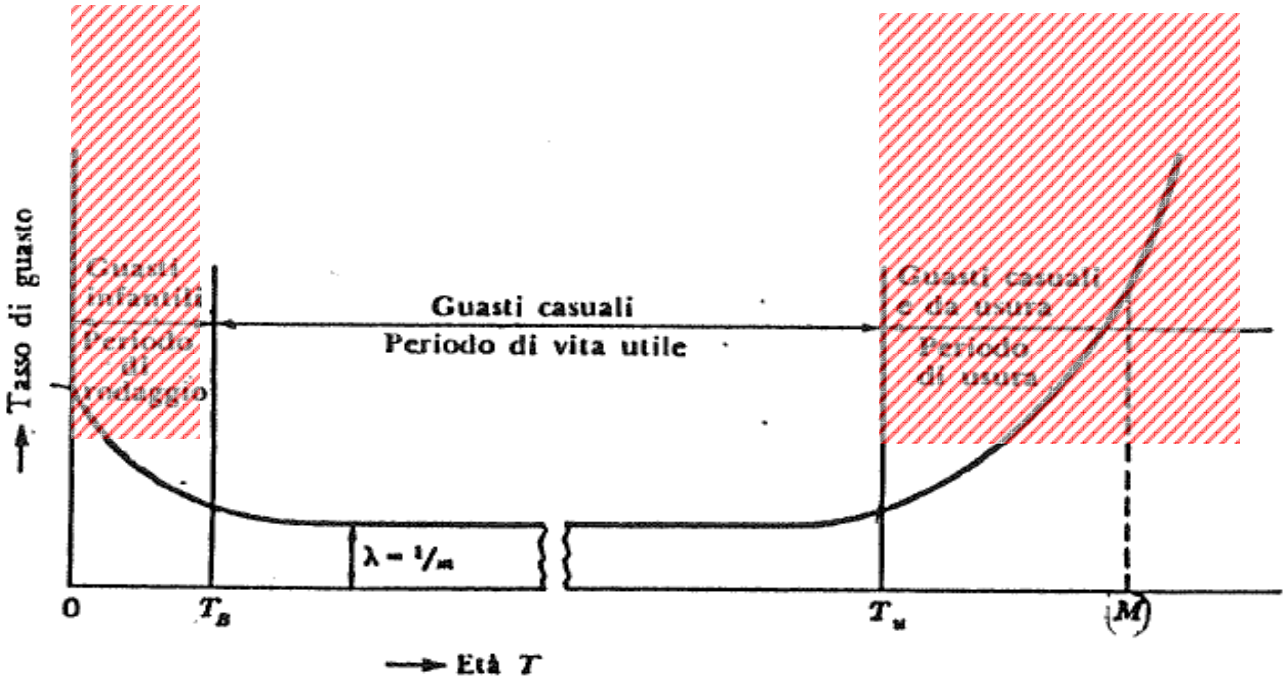
Dopo il rodaggio il valore di tasso di guasto rimane approssimativamente costante per un certo periodo di tempo (T*u* – T*a*) cui si dà il nome di vita utile.

Nell'intervallo di tempo che va da T*u* a M circa la metà dei componenti sopravissuti subirà guasti. Il tempo M è la vita media per usura.

I metodi descritti nelle norme EN 62061 e EN ISO 13849-1 si riferiscono solo alla stima dei guasti casuali.

I guasti per usura vanno eliminati adottando adeguate procedure di manutenzione preventiva.

I guasti infantili vanno eliminati tramite la tecnica del rodaggio.



Al contrario, non c'è tecnica di sostituzione che possa eliminare i guasti casuali, in ragione del tasso di guasto costante durante il periodo di vita utile.

La miglior cosa che si può fare durante il periodo di vita utile è sostituire i componenti appena si guastano.

Nessun componente dovrebbe essere mantenuto in servizio dopo il periodo di vita utile, in caso contrario l'affidabilità del sistema scenderebbe a valori ridicoli.

Regola aurea dell'affidabilità:

Nel periodo di vita utile sostituire i componenti appena si guastano; un po' prima della fine del periodo di vita utile effettuare una sostituzione preventiva di tutti i componenti, benché non guasti.

MTBF , MTTF, MTTFd

MTBF

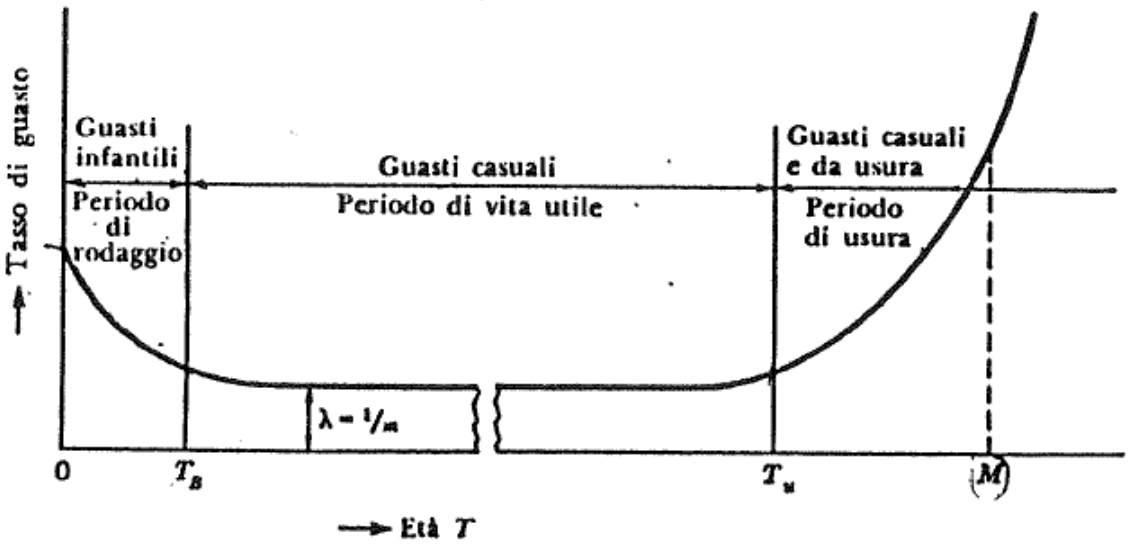
La probabilità di un componente o di un sistema di non guastarsi durante tutta la sua vita utile è misurata dal suo tasso di guasto λ (n° di guasti per ora). Il suo inverso, detto tempo medio fra i guasti, è misurato in ore ed è comunemente indicato con la sigla MTBF (mean time between failures)

$$MTBF = 1/\lambda$$

Relazione valida per valori di λ costanti e sufficientemente bassi

Se il tasso di guasto **λ** è molto basso *(come in genere accade),* il tempo medio tra i guasti (**MTBF**) può arrivare a valori dell'ordine di milioni di ore, quindi è generalmente molto più grande della vita media M.

Questo non vuol dire che il componente può essere usato per milioni di ore perché interviene il fattore legato all'usura a limitarne la vita.



L' MTBF è relativo al periodo di vita utile e va distinto dalla vita media!

Esempio:

caratteristiche del componente:

vita utile =100.000 ore e MTBF= 1.000.000 ore

Il componente potrà essere usato per un tempo T*u* di circa 100.000 ore perché solo entro le prime 100.000 ore è garantito l'MTBF = 1.000.000 ore.

Qual è allora il significato di MTBF?

Indica semplicemente quanto il componente sia affidabile nel suo periodo di vita utile.

Se dopo 100.000 ore il componente continua a funzionare (come molto probabile) e si vuole continuare a garantire lo stesso MTBF, il componente va sostituito con un altro di pari qualità.

MTTF

Per MTBF si intende la somma di due tempi:

MTBF = MTTF (Mean Time To Failure) + **MTTR** (Mean Time To Repair).

Nel settore del macchinario industriale si può confondere MTBF con MTTF perché MTTR è trascurabile rispetto al MTTF, per cui:

MTTF = MTBF

Quindi ricordando che **MTBF = 1/ λ** sarà anche **MTTF = 1/ λ**

MTTFd

Per ricavare MTTFd (tasso di guasto dei guasti pericolosi) da MTTF, occorre condurre una analisi FMEA determinando quindi per ogni componente, nel contesto dell'applicazione in esame, l'effettiva percentuale di guasti pericolosi rispetto a tutti i guasti possibili.

Per semplicità di calcolo la EN ISO 13849-1 consente di valutare , per ogni componente, come pericolosi il 50% dei guasti, quindi

$$MTTFd = 2 \times MTTF$$

Se per un componente è possibile escludere guasti pericolosi, il loro contributo al MTTFd = 0

$MTTF_d$: dove reperire i dati?

Il procedimento gerarchico per trovare i dati dovrebbe essere, nell'ordine:

a) utilizzo dei dati del fabbricante

b) utilizzo dei dati contenuti nelle tabelle dell'annesso C della EN ISO 13849-1

c) scelta di dieci anni

prospetto C.1 **Norme internazionali concernenti l'$MTTF_d$ o B_{10d} dei componenti**

	Principi di sicurezza di base e ben provati secondo la ISO 13849-2:2003	Altre norme pertinenti	Valori tipici: $MTTF_d$ (anni) B_{10d} (cicli)
Componenti meccanici	Prospetti A.1 e A.2	-	$MTTF_d = 150$
Componenti idraulici	Prospetti C.1 e C.2	EN 982	$MTTF_d = 150$
Componenti pneumatici	Prospetti B.1 e B.2	EN 983	$B_{10d} = 20\,000\,000$
Relè e relè contattori con carico ridotto (carico meccanico)	Prospetti D.1 e D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 20\,000\,000$ **20% del carico**
Relè e relè contattori con carico massimo	Prospetti D.1 e D.2	EN 50205 IEC 61810 IEC 60947	$B_{10d} = 400\,000$ **Pieno carico**

$MTTF_d$ di componenti elettrici

Per componenti elettrici/elettronici non elencati nelle tabelle dell'annesso C della EN ISO 13849-1 o per condizioni di funzionamento diverse da quelle specificate si possono usare i valori forniti dalla norma SN 29500.

Tutti i valori sono specificati alla temperatura di funzionamento di 40° e con corrente e tensione nominale.

Se le condizioni di funzionamento sono diverse, occorre correggere i valori tramite fattori di stress forniti dalla stessa SN 29500.

L'unità di misura usata nella SN 29500 è il FIT (failure in time) e corrisponde a un guasto per miliardo di ore di funzionamento.

$1\ FIT = 10^{-9}$ ore

Es: 3 FIT → $\lambda = 3 \times 10^{-9}$ ore → MTTFd = 76103 anni

$MTTF_d$ di relè ed elettrovalvole

Per tutti i componenti elettromeccanici, idraulici e meccanici soggetti a usura (es. relè ed elettrovalvole) il tasso di guasto aumenta con il numero di cicli lavorati, pertanto la loro affidabilità non viene in genere riferita al tempo per cui hanno lavorato bensì al numero di cicli effettuati.

Il parametro fornito dai costruttori è il B10 (numeri di manovre dopo le quali si verificano guasti nel 10 % dei componenti esaminati durante una prova della durata di esercizio sotto carico specificato).

La percentuale di B10 per cui si hanno guasti pericolosi nell'applicazione considerata viene indicata con B10d.

In assenza di informazioni dettagliate la EN ISO 13849-1 consiglia di considerare come pericolosi il 50% dei guasti, quindi **B10d = 2 x B10**.

Conoscendo il **B10d** e il numero medio di operazioni in un anno (N_{op}) si ricava il valore di **MTTFd** nel seguente modo:

$$MTTF_d = \frac{B10_d}{0{,}1 \times N_{op}}$$

La vita utile del componente deve poi essere limitata a **T10d = B10d / Nop** (tempo entro il quale il 10% dei componenti può subire un guasto pericoloso).

Questo tempo va confrontato col tempo di servizio della macchina (20 anni, stabilito dalla norma). Se risulta inferiore, il componente va sostituito un po' prima della fine della sua vita utile.

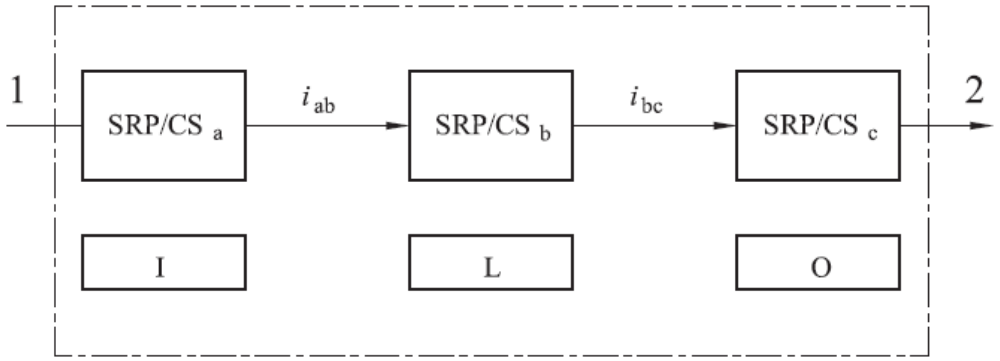
Funzioni di sicurezza

Parte del processo di riduzione del rischio consiste nel determinare le funzioni di sicurezza della macchina

Esempio:

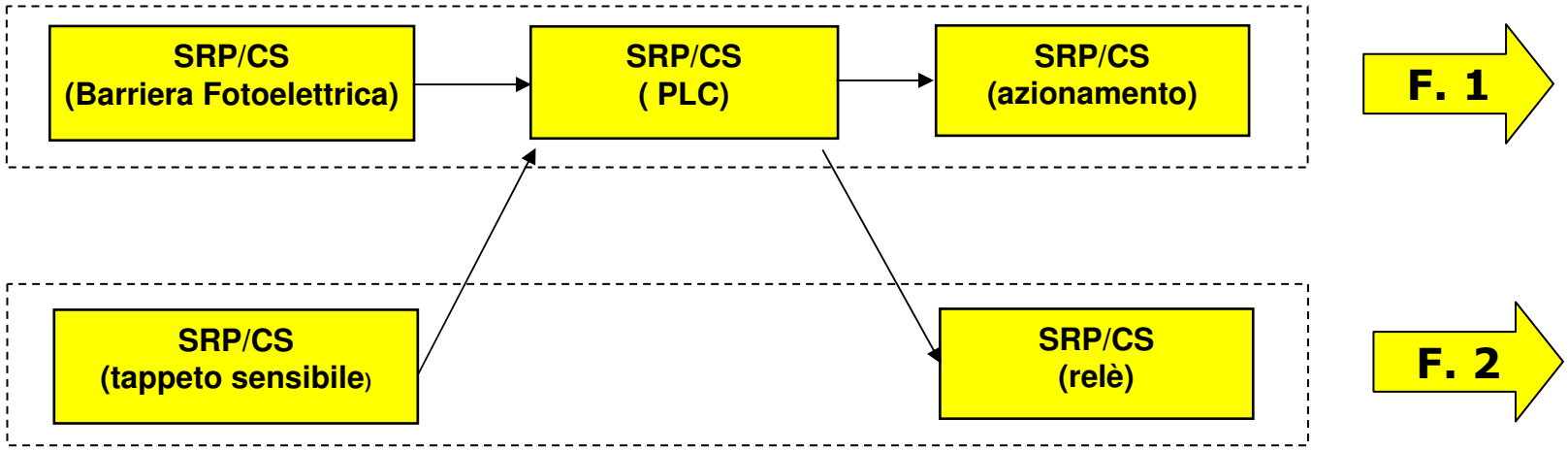
Funzione di arresto legata alla sicurezza, prevenzione dell'avviamento inatteso, funzione di ripristino manuale, funzione di inibizione, funzione di azione mantenuta, funzione di comando locale, funzione di avvio/riavvio.

Rappresentazione schematica tipica delle funzioni di sicurezza



Una funzione di sicurezza può essere implementata mediante una o più SRP/CS e

diverse funzioni di sicurezza possono condividere una o più SRP/CS



È anche possibile che una SRP/CS implementi funzioni di sicurezza e normali funzioni di comando.

Selezione delle funzioni di sicurezza

Per ogni funzione di sicurezza individuata dalla analisi di rischio, devono essere stabiliti

- **requisiti funzionali**
- **contributo alla riduzione del rischio che essa deve fornire (PL).**

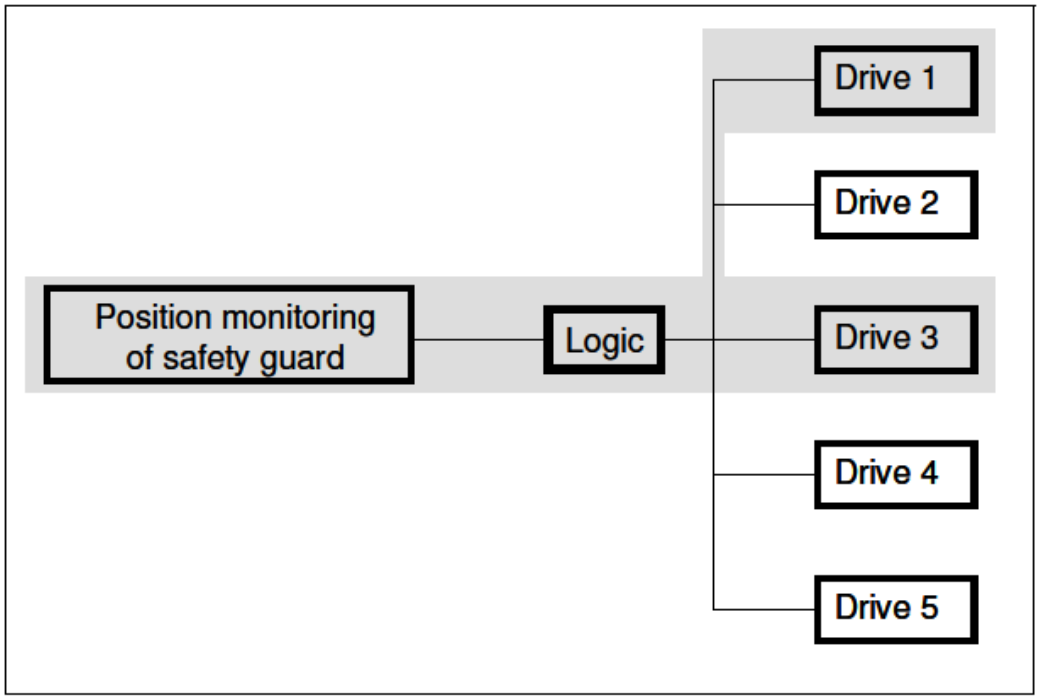
Questo contributo non copre il rischio complessivo della macchina, ma solo quella parte del rischio che deriva dalla applicazione di quella particolare funzione di sicurezza.

La valutazione del PL va fatta quindi separatamente per ogni singola funzione di sicurezza.

Questo accorgimento agevola l'esecuzione dei calcoli e evita di penalizzare eccessivamente il valore di PFHd ottenuto poiché non si introducono nel calcolo dati di affidabilità di componenti che non contribuiscono a quella funzione di sicurezza.

Esempio:

Funzione di sicurezza: Comando di stop generato dall'apertura di un cancello. Il comando blocca il movimento di tutti e cinque gli azionamenti del robot

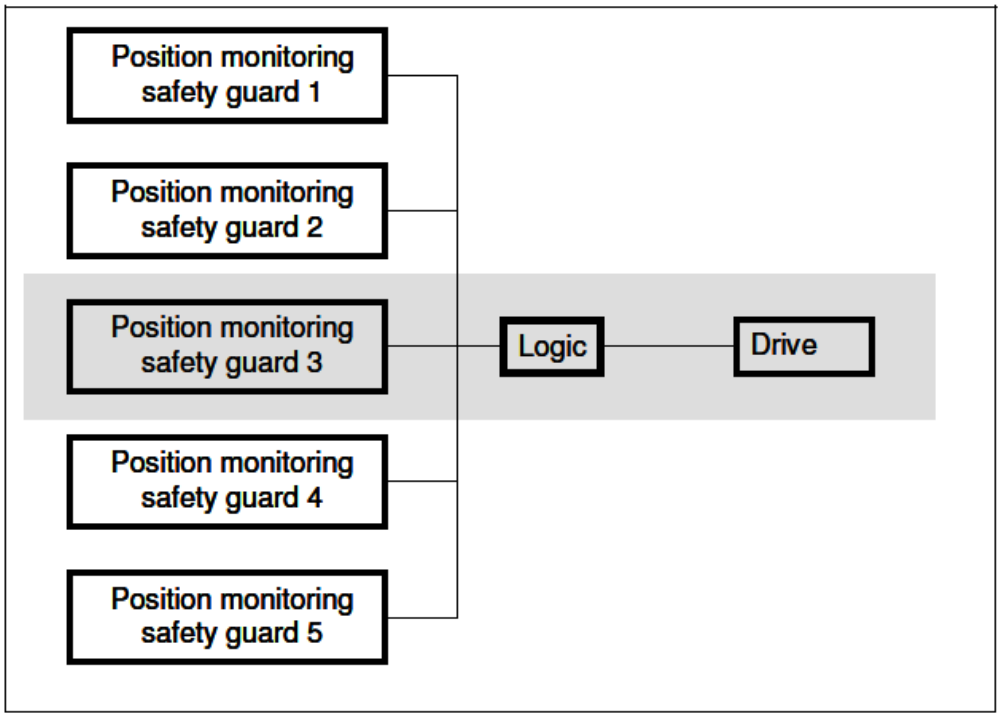


I movimenti relativi ai motori 1 e 2 sono quelli pericolosi , i motori 2,4,5 vengono fermati solo per ragioni funzionali.

Ai fini del calcolo del PFHd vanno considerati solo i blocchi evidenziati.

Esempio:

Funzione di sicurezza: E' possibile accedere all'area pericolosa tramite uno di cinque cancelli. L'apertura di un cancello qualsiasi genera il comando di stop per il motore.

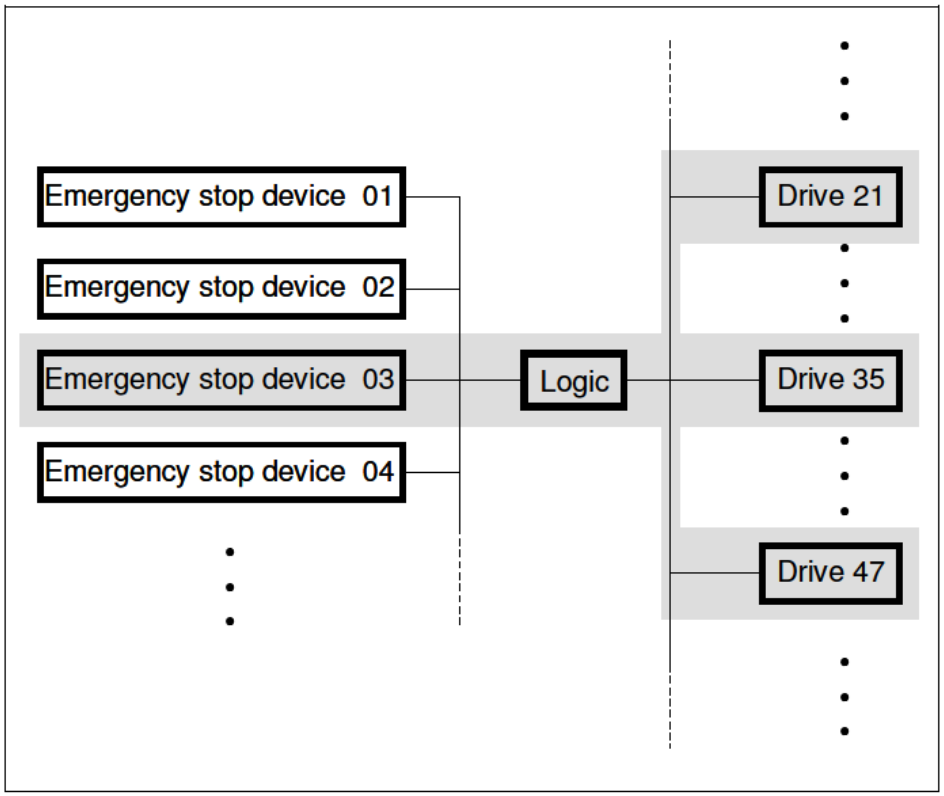


Le funzioni di sicurezza da calcolare sono 5 perché ogni cancello, preso singolarmente, garantisce la protezione

Per ogni funzione di sicurezza, ai fini del calcolo del PFHd, vanno considerati solo i blocchi evidenziati.

Esempio:

Funzione di sicurezza: Arresto d'emergenza. L'attuazione di uno qualsiasi di 20 comandi di arresto d'emergenza blocca nel tempo più breve possibile 50 azionamenti.



Le funzioni di sicurezza da calcolare sono 20 perché si suppone che venga azionato un solo ES per volta.

Poiché non è nota la posizione della persona esposta quando viene azionato un ES e poiché si suppone che non tutti i 50 motori possano rappresentare un pericolo, per il calcolo del PFHd si valuta la combinazione peggiore.

Nell'esempio, i blocchi evidenziati

Rappresentazione schematica a blocchi dello SRP/CS

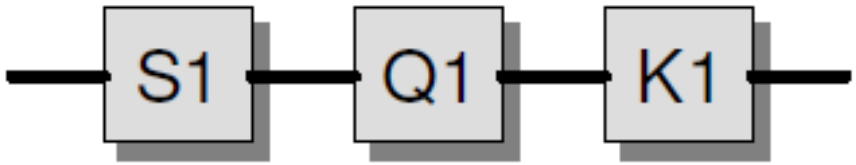
Per la valutazione del $MTTF_d$ e del DC_{avg} la EN ISO 13849-1 propone un approccio semplificato.

Il metodo richiede una rappresentazione a blocchi - logica non funzionale.

Ogni unità hardware della SRP/CS deve appartenere esattamente a un blocco, consentendo così di calcolare l'MTTFd del blocco in base all'MTTFd dei componenti appartenenti al blocco.

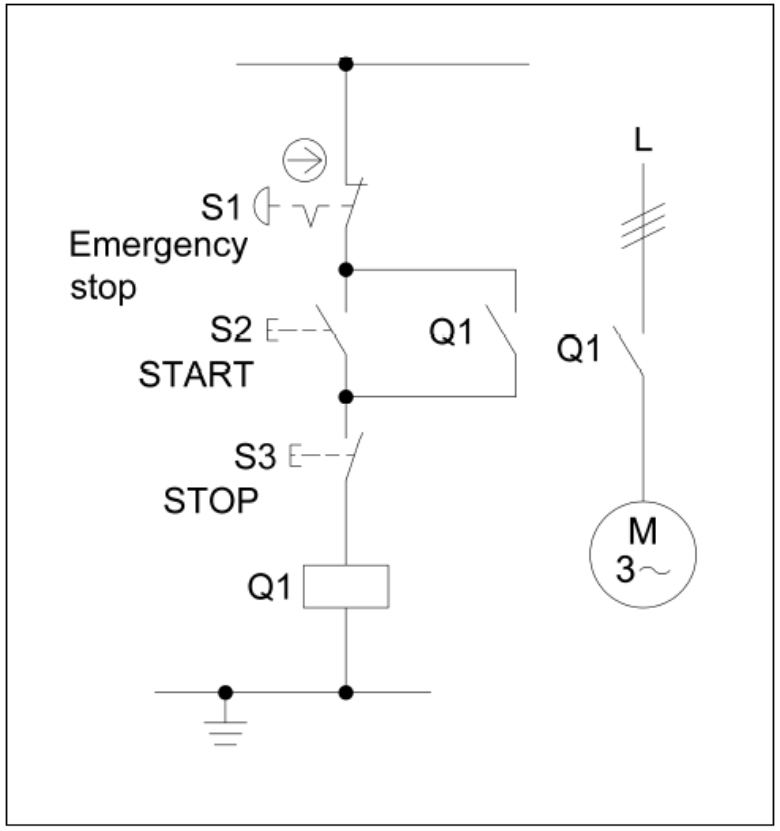
Una sequenza di uno o più blocchi allineati in serie (es. input, logica, output) costituisce un canale.

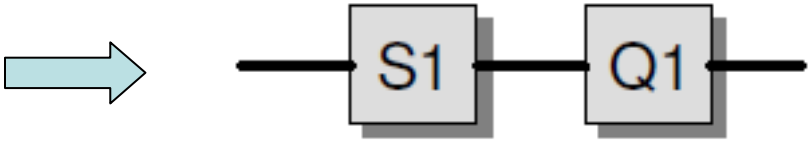
Il guasto di un blocco in un canale causa il guasto dell'intero canale.



Esempio

Funzione di sicurezza: arresto di emergenza





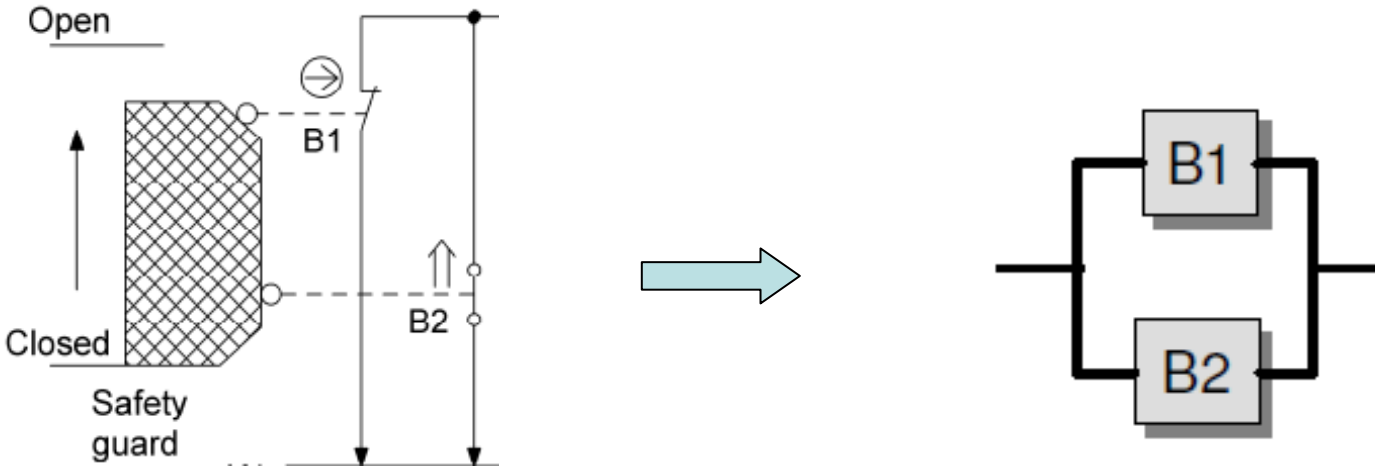
Il comando di Marcia/Arresto non è coinvolto nella funzione di sicurezza quindi il suo contributo al valore di MTTFd non deve essere conteggiato

Sistemi ridondanti

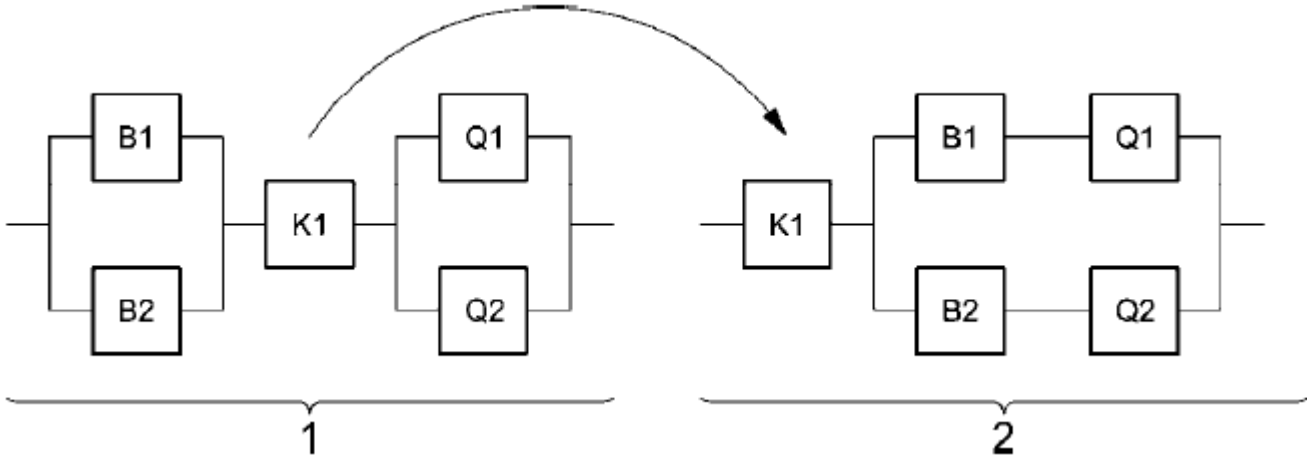
Si dicono ridondanti o parallelo quei sistemi dove la stessa funzione è eseguita da più dispositivi o canali.

In un allineamento in parallelo solo il guasto pericoloso di tutti i canali causa la perdita della funzione di sicurezza.

Eventuali blocchi utilizzati solo per diagnostica e che non influiscono sull'esecuzione della funzione di sicurezza nei diversi canali possono essere indicati a parte e non vengono conteggiati nel calcolo del MTTFd.



Rappresentazione logica a blocchi

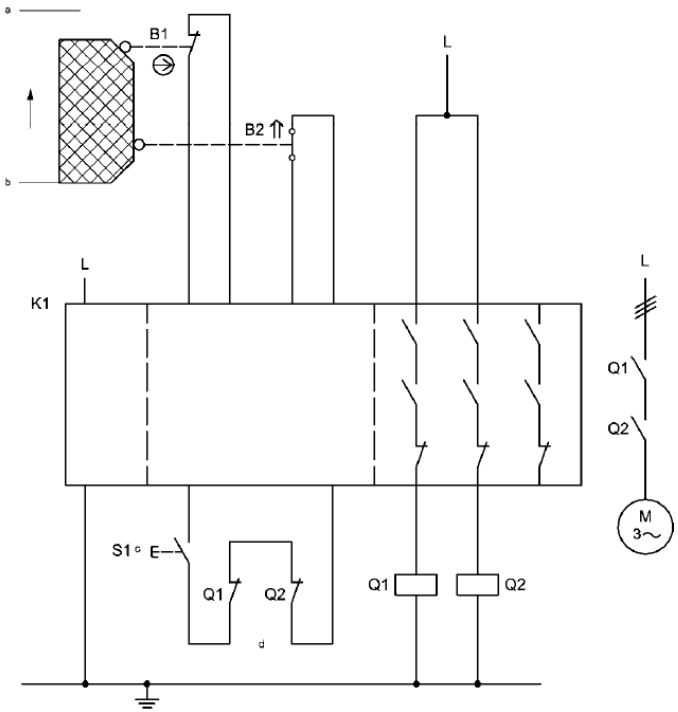


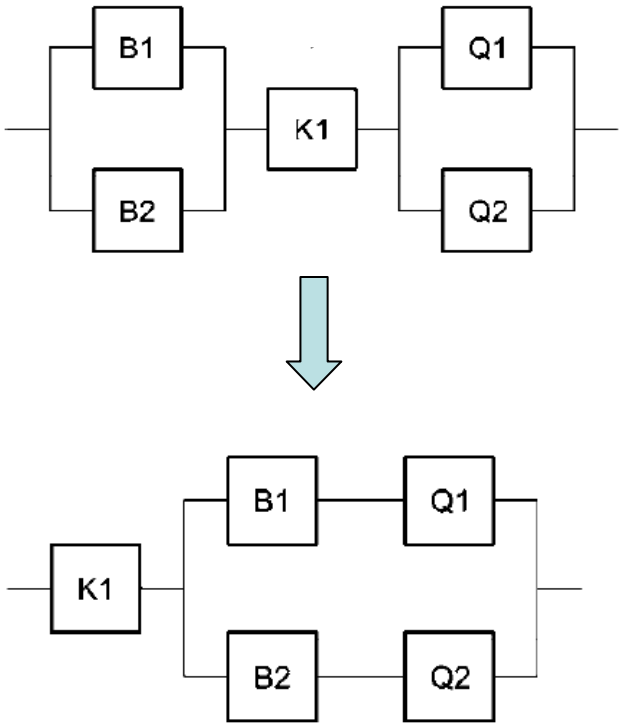
corrispondente all'hardware **semplificata**

La sequenza dei sottosistemi è in linea di principio intercambiabile. Conviene pertanto raggruppare sottosistemi che condividono la stessa struttura (se per esempio B1/B2 e Q1/Q2 sono entrambi realizzati in Cat.4). Questo rende il calcolo del PL più semplice.

Esempio:

Funzione sicurezza: l'apertura del riparo mobile comanda lo stop del motore.





K1 è un modulo di sicurezza commerciale.
PL, PFHd, Cat. specificati dal costruttore.
Es. PLe, Cat. 4, PFHd = 2,31 x 10^{-9}

Esempio - Specifiche funzionali

B1 e B2 sono monitorati per plausibilità da K1.

I guasti in Q1 e Q2 sono rilevati da K1 tramite uno start-up test (il comando di start può avvenire solo se nel ciclo precedente sia Q1 che Q2 sono stati de-energizzati).

Possibili guasti pericolosi vengono rilevati sia durante il normale funzionamento che durante l'apertura o la chiusura del riparo.

Il rilevamento di guasti pericolosi provoca l'immediata apertura di Q1 e Q2.

Q1 e Q2 vanno scelti in modo che la corrente nominale dei contatti sia almeno il 50% superiore alla corrente assorbita dal carico (well tried safety principles).

I contatti vanno protetti tramite opportuni dispositivi di protezione.

B1 e B2 devono essere montati in modo solido in modo tale da sopportare le naturali vibrazioni della macchina.

I conduttori di collegamento di B1 e B2 dovranno essere tenuti separati gli uni dagli altri.

B1 è un interruttore di posizione ad apertura positiva conforme a IEC 60947-5-1 An. K

Q1 e Q2 sono contattori a contatti legati conformi a IEC 60947-5-1 Annesso L.

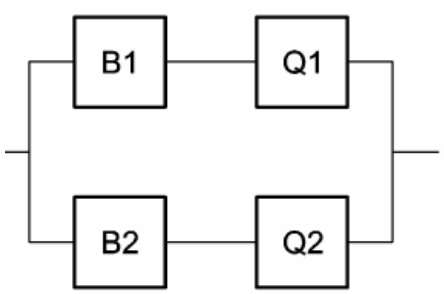
Metodo di calcolo proposto da ISO/TR 23849:2010

La stima del PFHD per una combinazione serie di SRP/CS può essere eseguita anche sommando i valori di PFHD (ad esempio, derivati da allegato K della norma ISO 13849-1) di ciascun SRP/CS in modo simile a quello utilizzato con i sottosistemi in IEC 62061.

L'allegato K descrive la relazione che esiste tra MTTFd e PFHd di un SRP/CS per le 4 architetture classificate in termini di Categoria e DC.

	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)											
$MTTF_d$ di ogni canale anni	Cat. B PL DC_{avg} = nessuna		Cat. 1 PL DC_{avg} = nessuna		Cat. 2 PL DC_{avg} = bassa		Cat. 2 PL DC_{avg} = media		Cat. 3 PL DC_{avg} = bassa		Cat. 3 PL DC_{avg} = media		Cat. 4 PL DC_{avg} = alta	
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		
16	$7{,}13 \times 10^{-6}$	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		
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		
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		
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		
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		
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		
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
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
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

Si calcola quindi in un primo momento il valore di **MTTFd e DCavg,** del sistema:



poi, incrociando i valori così ottenuti sulla tabella K.1 di EN ISO 13849-1, si ricava il valore di PFHd.

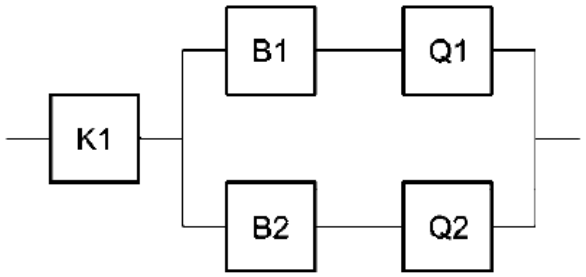
Se ad esempio si fosse ottenuto:

Cat. 4 **MTTFd = 100 anni** **DCavg = 99%** **CCF > 65 punti**

Dalla tabella K.1 risulta **PFHd = 2,47 × 10^{-8}** e **PL = e**

	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)													
$MTTF_d$ di ogni canale anni	Cat. B PL DC_{avg} = nessuna		Cat. 1 PL DC_{avg} = nessuna		Cat. 2 PL DC_{avg} = bassa		Cat. 2 PL DC_{avg} = media		Cat. 3 PL DC_{avg} = bassa		Cat. 3 PL DC_{avg} = media		Cat. 4 PL DC_{avg} = alta	
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		
16	$7{,}13 \times 10^{-6}$	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		
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		
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		
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		
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		
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		
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
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
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
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
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
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
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
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
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
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
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
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

Il valore di PFHd del sistema serie totale



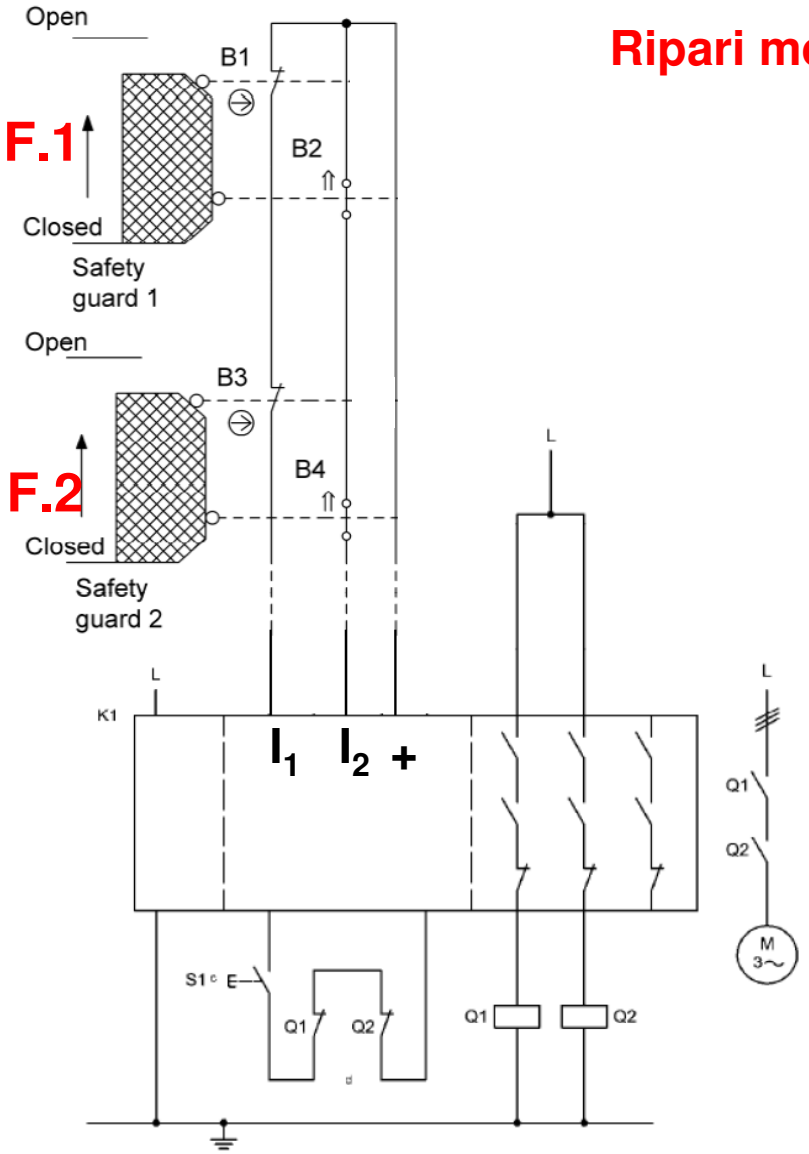
si ottiene infine sommando 2,47 x 10^{-8} al valore PFHd del modulo K1

$$PFHd_{(SRP/CS)} = 2{,}47 \times 10^{-8} + 2{,}31 \times 10^{-9} = 2{,}70 \times 10^{-8}$$

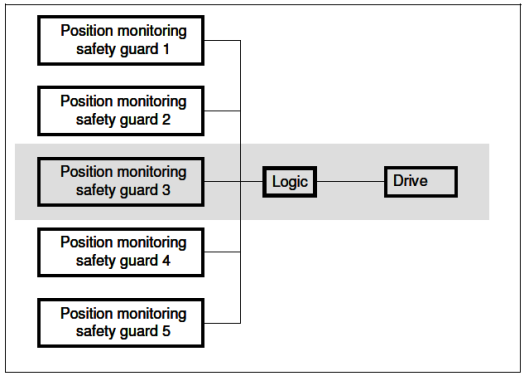
e dalla Tabella 3: PL $_{(SRP/CS)}$ = e

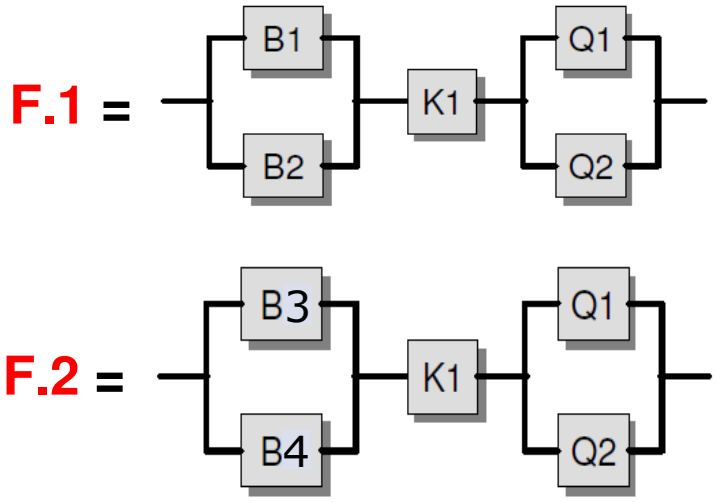
PL	Probabilità media di guasto pericoloso per ora 1/h
a	$\geq 10^{-5}$ fino a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ fino a $< 10^{-5}$
c	$\geq 10^{-6}$ fino a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ fino a $< 10^{-6}$
e	$\geq 10^{-8}$ fino a $< 10^{-7}$

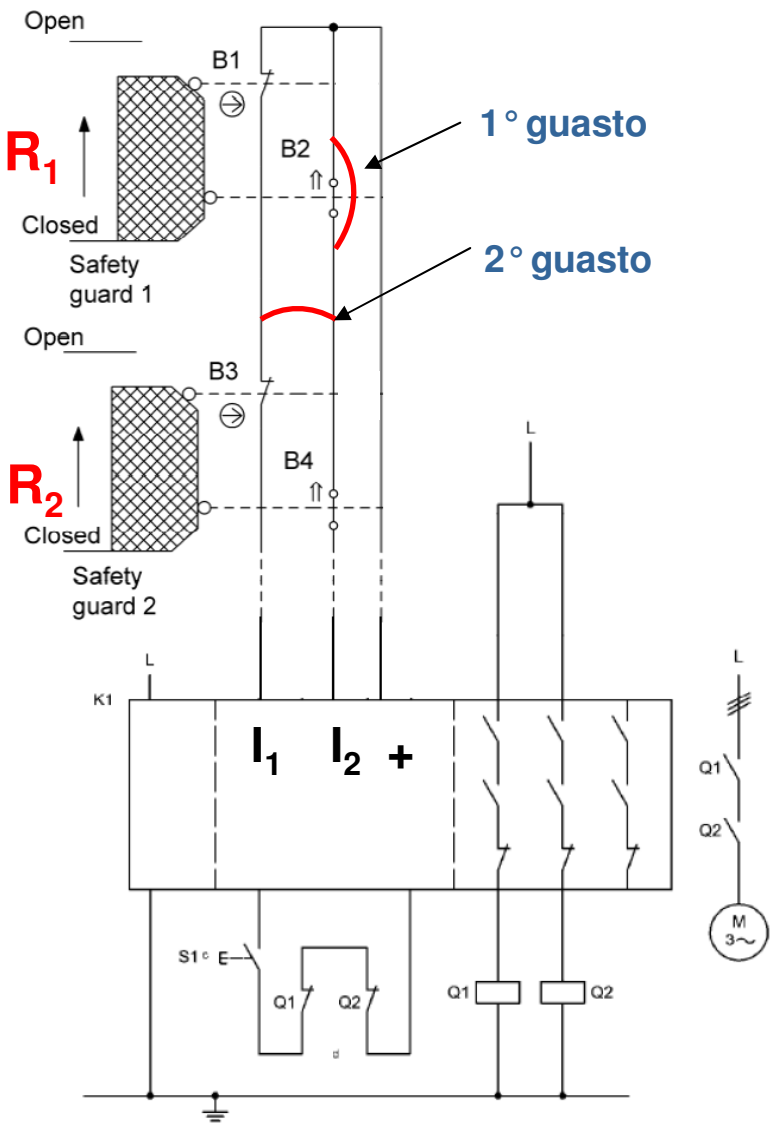
Ripari mobili collegati in serie



I due ripari mobili proteggono la stessa zona e arrestano lo stesso motore







Ripari mobili collegati in serie

Il rilevamento di un singolo guasto può essere mascherato dall'attivazione di ogni interruttore collegato tra il guasto e il modulo di controllo.

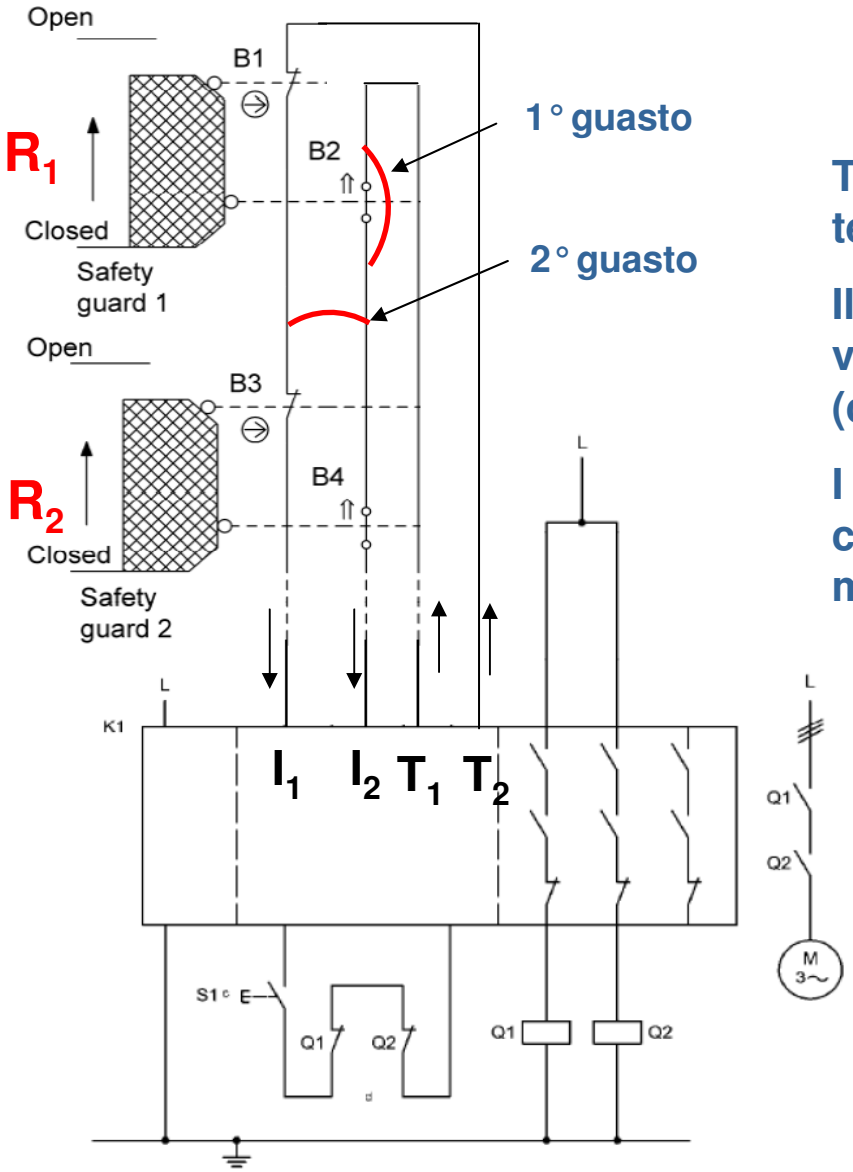
Esempio:

La successione di eventi:
1° guasto - apertura di R_1,
provoca l'arresto del motore M.

La successiva combinazione:
chiusura di R_1 – apertura e chiusura di R_2,
resetta l'informazione di guasto e abilita di nuovo il comando di Start

L'ulteriore 2° guasto impedisce l'arresto del motore M all'apertura di R_1

Non è possibile raggiungere la Categoria 3 perché DC < 60% (Annesso R di ISO 14119)



Possibile Modifica

T_1 e T_2 sono segnali di test dinamici separati nel tempo.

Il guasto n°2 e possibili guasti verso massa vengono rilevati dal modulo di sicurezza (controllo di plausibilità I_1-T_1 , I_2-T_2).

I rimanenti possibili guasti nei cavi di collegamento (cortocircuiti) vengono esclusi mediante appropriato cablaggio (es. guaina prot.)

I guasti di natura meccanica di B1 e B3 possono essere esclusi fino a PLd solo se vengono prese appropriate misure (ultimo periodo di par. 6.2.4 di EN ISO 13849-1 e Tabelle A.4 e D.8 di EN ISO 13849-2).

Con queste condizioni DC > 60%.
I sotto-assiemi B1/B2 e B3/B4 sono così conformi ai requisiti della Categoria 3.

Il valore di PL dipende dal valore di MTTFd raggiunto.

PL b se MTTFd = basso

PL c se MTTFd = medio

PL d se MTTFd = alto

figura 5 **Rapporto tra categorie, DC_{avg}, $MTTF_d$ di ogni canale e PL**

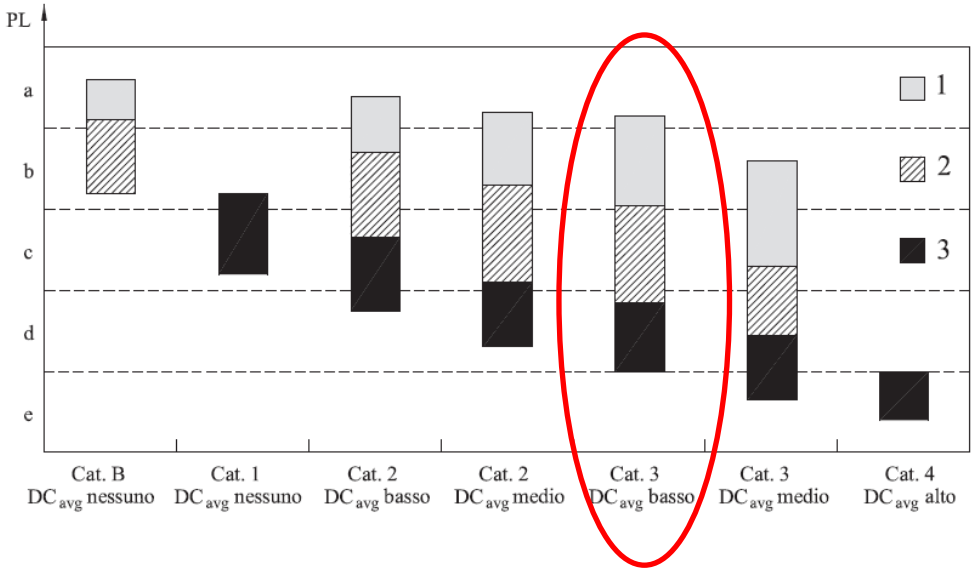
Legenda

PL Livello di prestazione

1 $MTTF_d$ di ogni canale = basso

2 $MTTF_d$ di ogni canale = medio

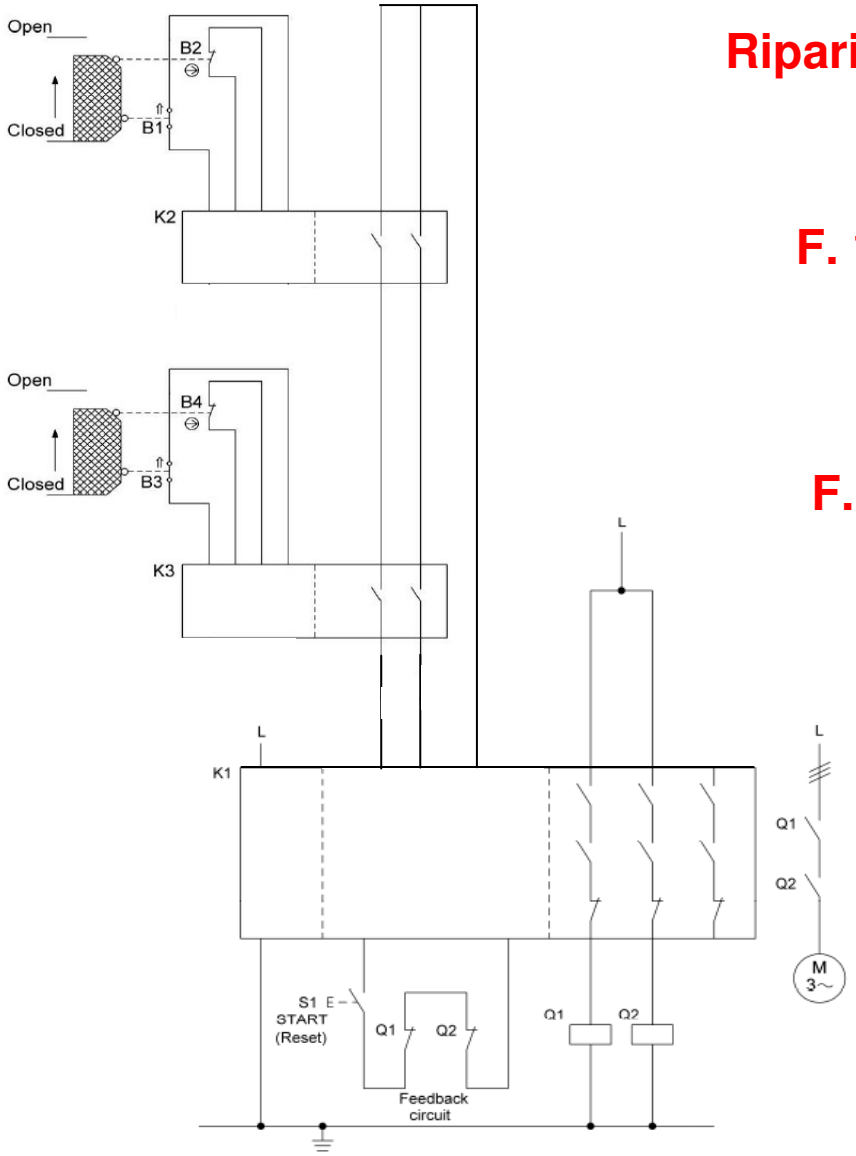
3 $MTTF_d$ di ogni canale = alto



Estratto da ISO TR 23849

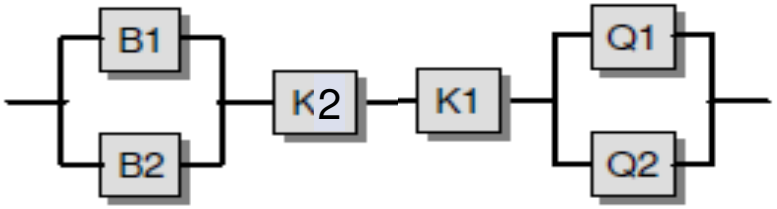
8.2.5 The following observation can be made on the design of SRP/CS and/or SRECS:

Category 4 can only be achieved where several mechanical position switches for different protective devices are not connected in a series arrangement (i. e. no cascading). This is necessary as faults in the switches cannot otherwise be detected.

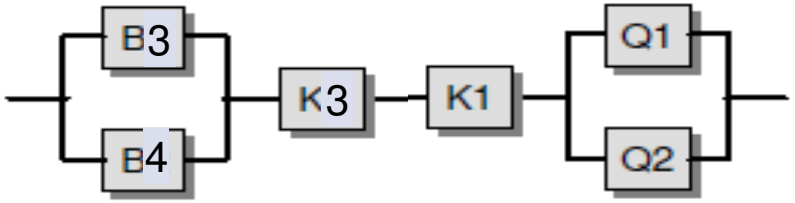


Ripari mobili collegati in serie

F. 1 =



F. 2=

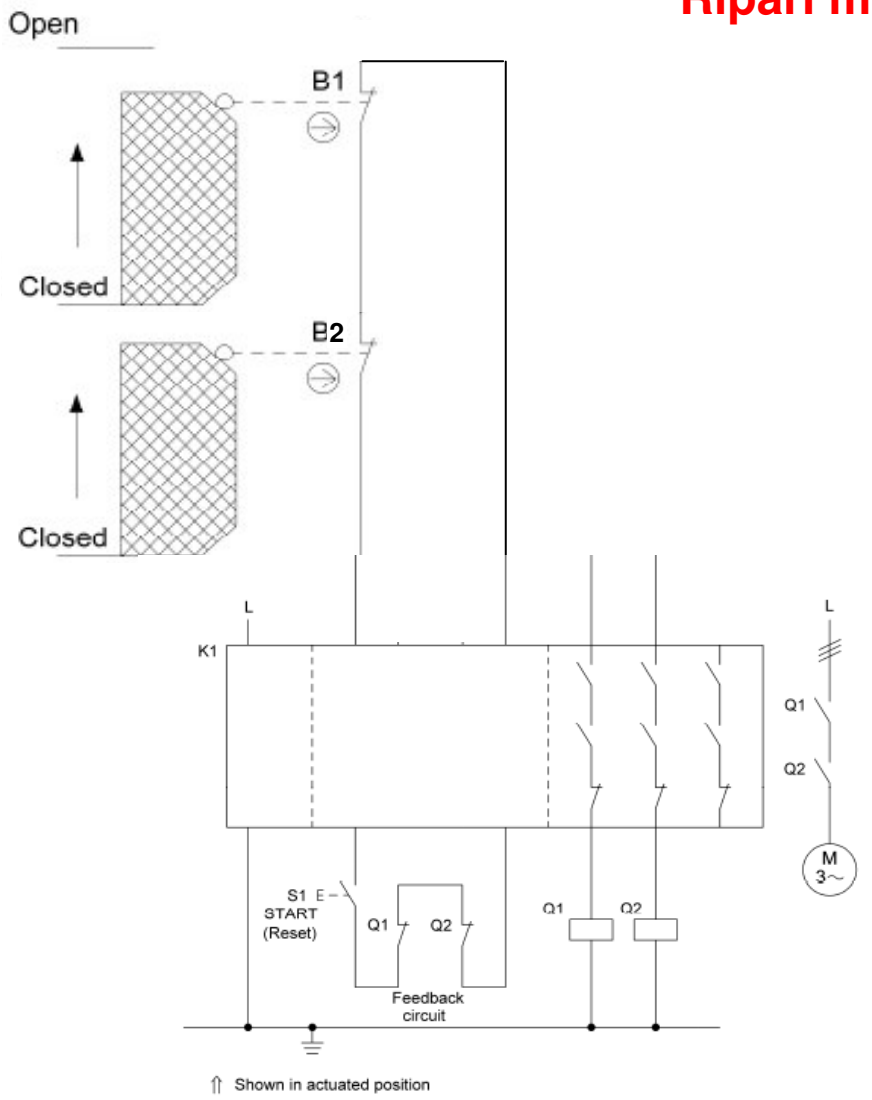


Si esclude il cortocircuito nel cablaggio fra i moduli all'interno del quadro se quadro e cablaggio sono conformi a EN 60204-1 (EN ISO 13849-2 Tab. D.4)

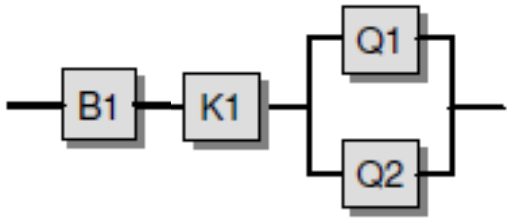
Se K1, K2, K3, sono conformi a Cat. 4, PLe allora DCavg = 99%,

Se anche MTTFd = alto, per le due funzioni F.1 e F.2 sarà PL = e

Ripari mobili collegati in serie



F.1 =



La funzione di sicurezza non può essere mantenuta per tutti i guasti.

Non sono implementati metodi per il rilevamento dei guasti (DC = 0).

Guasti verso massa nei cavi di collegamento di B1 e B2 sono rilevati dal modulo K1 e i cortocircuiti sono evitati per esempio mediante l'uso di cavi schermati con lo schermo collegato a PE (principi di sicurezza ben provati – EN ISO 13849-2 Tab. D.2).

B1 (e B2) sono conformi alla Cat. 1 per cui PL = c se MTTFd = alto

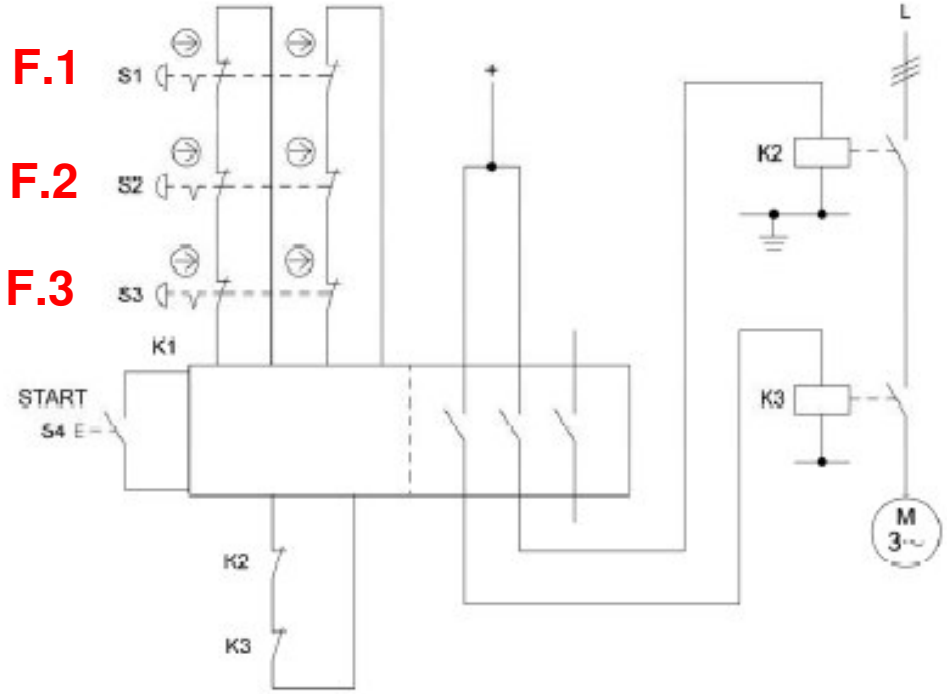
Collegamento in cascata di E-Stop

L'arresto d'emergenza è definita "misura di protezione complementare", tuttavia poiché deve essere disponibile nel caso di avaria degli altri dispositivi protezione, ad essa va applicata la EN ISO 13849-1.

F.1

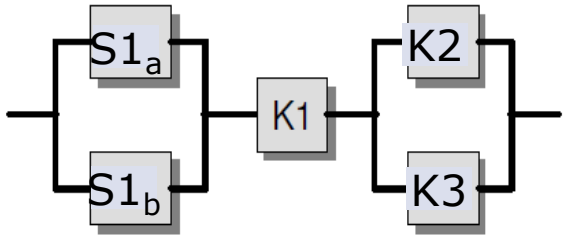
F.2

F.3



Si assume che non venga premuto più di un E-Stop contemporaneamente.

Tre funzioni di sicurezza, uguale schema logico



Se S1, S2, S3 sono conformi a IEC 600947-5-1, Annesso K è possibile escludere i guasti di natura elettrica (non apertura dei contatti).

Se il numero di operazioni per dispositivo è inferiore a 6050 (B10d = 6050 per macchinario industriale) lungo tutto l'arco della vita della macchina (20 anni secondo EN ISO 13849-1) è possibile escludere anche il guasto di natura meccanica.

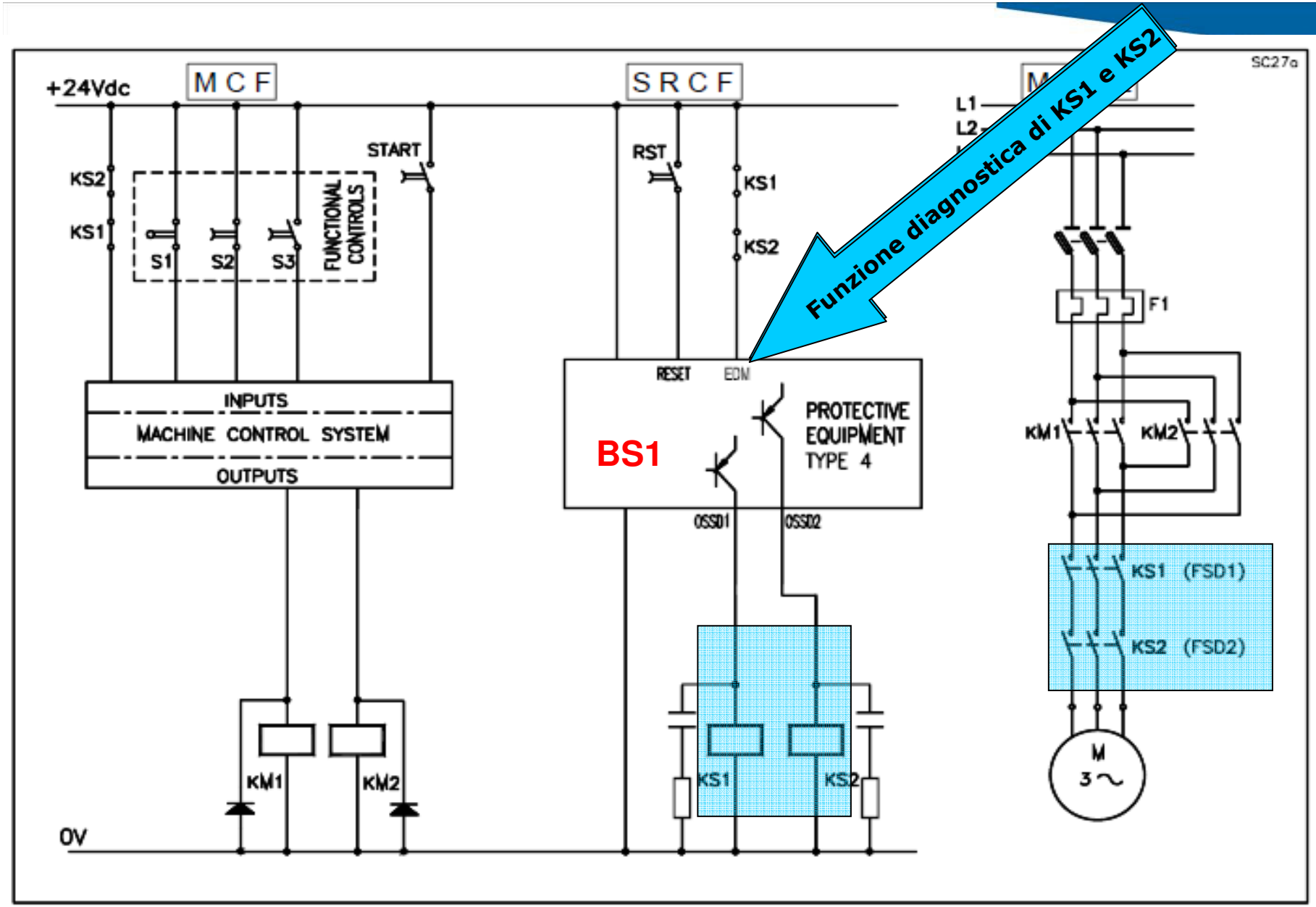
I guasti dovuti a cortocircuiti nei cavi di collegamento possono essere esclusi mediante appropriato cablaggio (separazione dei cavi, guaine di protezione, cavi schermati) e/o controllo dinamico tramite l'unità di controllo.

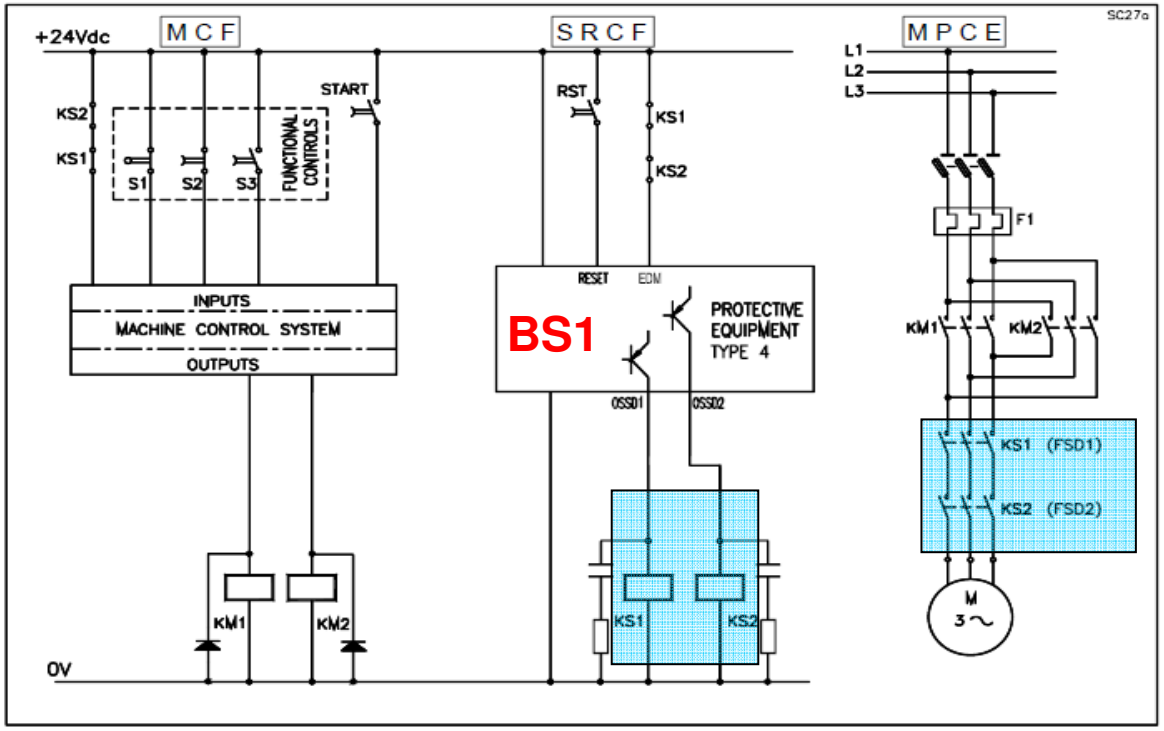
Per il calcolo del MTTFd del sottoassieme k2 / K3 bisogna considerare un numero di cicli/anno pari alla somma del numero di interventi/ anno degli E-Stop.

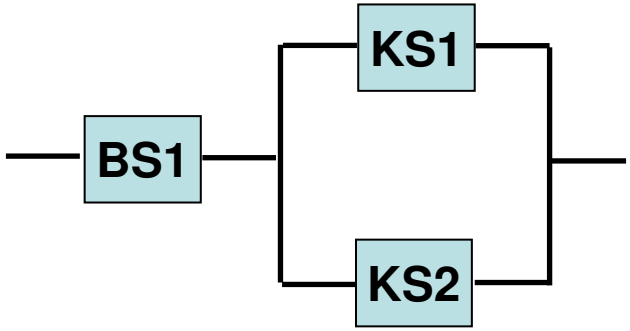
Nel caso di tre E-Stop come in figura il numero di cicli/ anno dei due contattori sarà molto basso (nell'ordine delle centinaia) per cui si può ritenere MTTFd = 100 anni.

Il DC del sottosistema K2/K3 è uguale a 99%

Risulta: MTTFd = 100 anni, DC = alto, Cat. 3 → **PLe**


SC27a
+24Vdc
MCF
SRCF
START
RST
KS2
KS1
S1
S2
S3
FUNCTIONAL CONTROLS
KS1
KS2
Funzione diagnostica di KS1 e KS2
L1
L2
F1
RESET
EDM
INPUTS
MACHINE CONTROL SYSTEM
OUTPUTS
BS1
PROTECTIVE EQUIPMENT TYPE 4
OSSD1
OSSD2
KM1
KM2
KS1 (FSD1)
KS2 (FSD2)
M
3~
KM1
KM2
KS1
KS2
0V



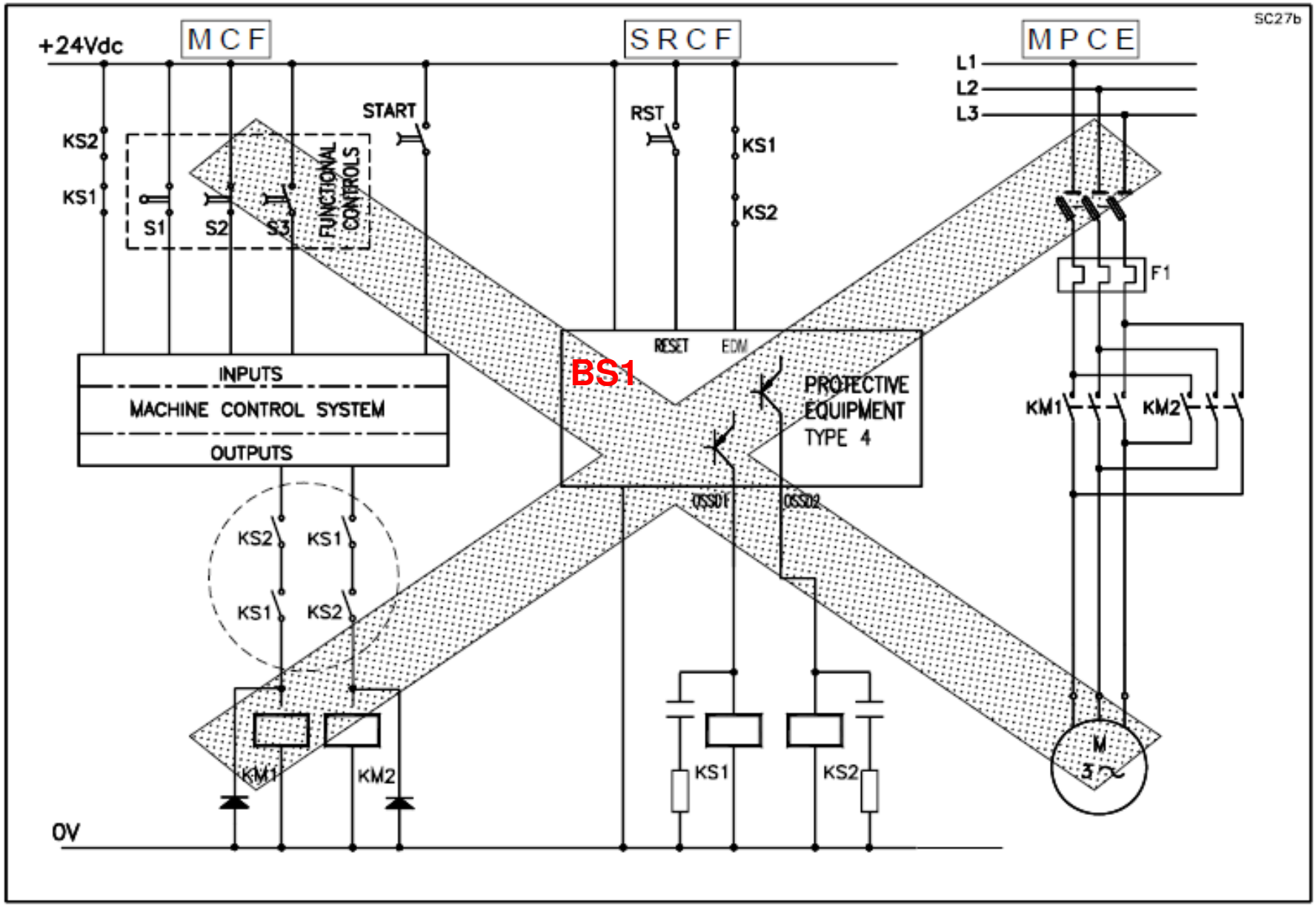


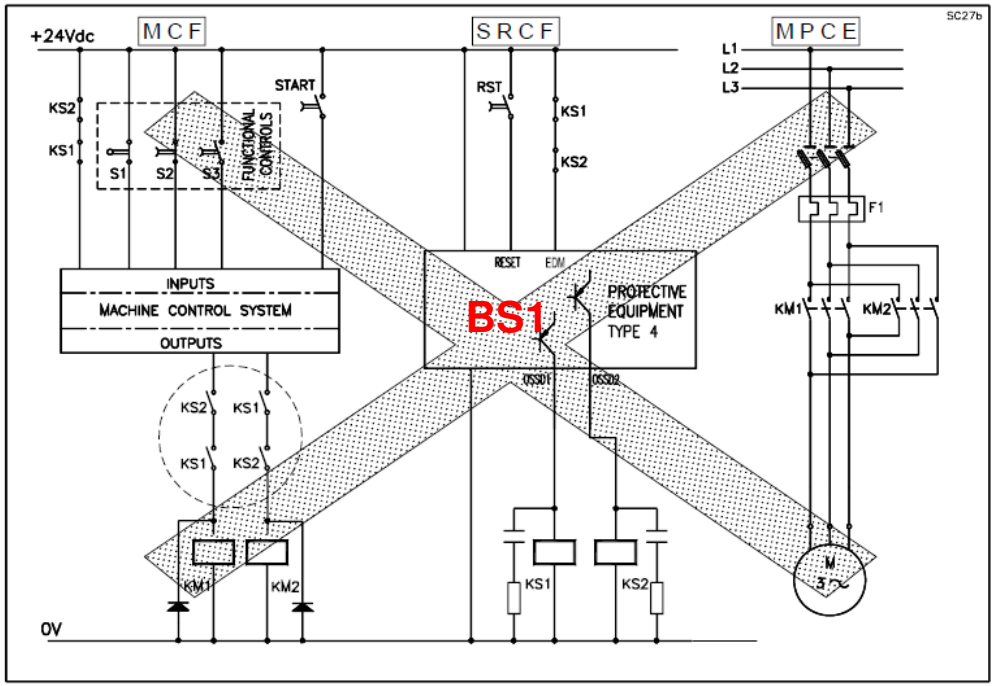
KS1 e KS2 sono contattori a contatti legati

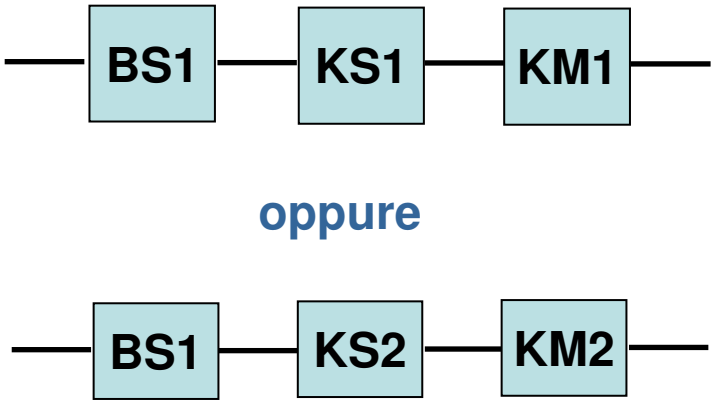
Il possibile cortocircuito fra i cavi che collegano gli OSSD a KS1 e KS2 deve essere evitato tramite appropriato layout oppure BS1 deve essere in grado di controllarlo

BS1 = AOPD Tipo 4, PLe

DC $_{KS1,KS2}$ = 99% (EDM input di BS1)


SC27b
+24Vdc
MCF
SRCF
MPCE
L1
L2
L3
START
RST
KS2
KS1
S1
S2
S3
FUNCTIONAL CONTROLS
KS1
KS2
F1
RESET
FDM
BS1
INPUTS
MACHINE CONTROL SYSTEM
OUTPUTS
PROTECTIVE EQUIPMENT TYPE 4
KM1
KM2
OSSD1
OSSD2
KS2
KS1
KS1
KS2
KM1
KM2
KS1
KS2
M
3~
0V



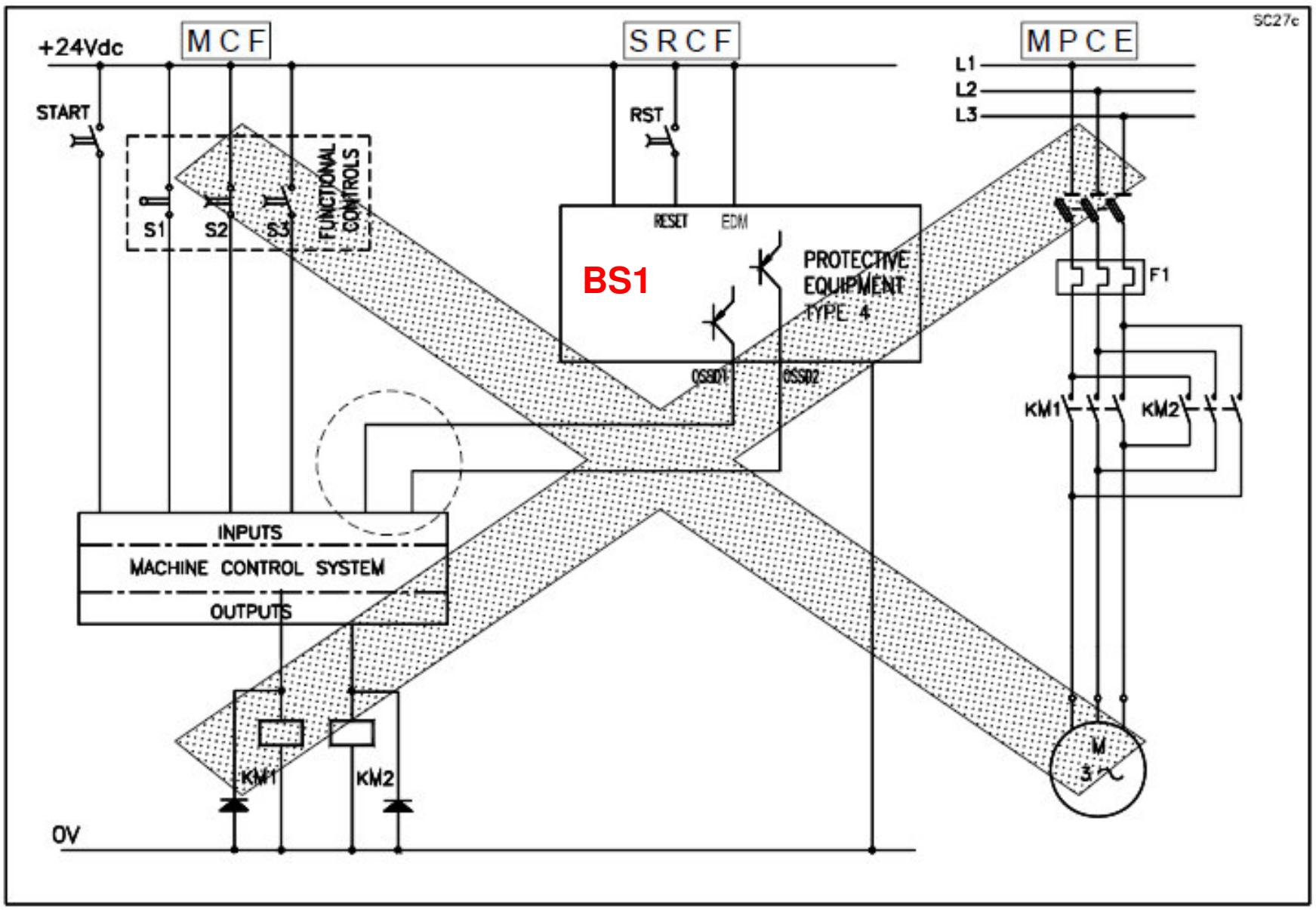


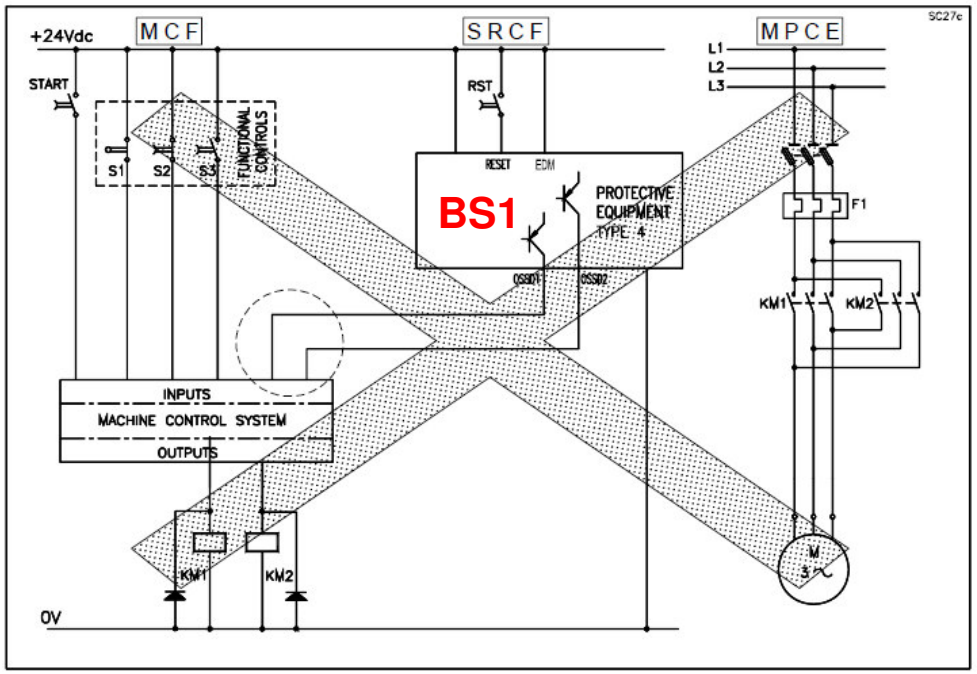
I contattori KM1 e KM2 non sono dotati di contatti legati

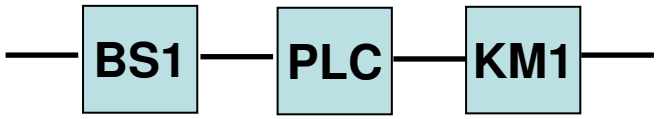
La struttura a doppio canale non viene mantenuta sulla linea di alimentazione dei motori. I guasti di KM1 (oppure KM2) non vengono rilevati.

$DC_{KS1,KS2}$ = 99% $DC_{KM1,KM2}$ = 0

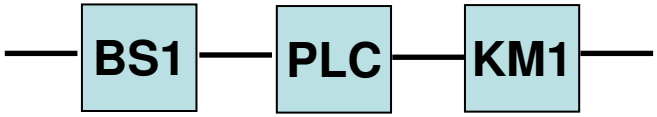
Categoria max raggiungibile = Cat.1 se $MTTFd_{canale}$ = alto , altrimenti Cat. B.


SC27c
+24Vdc
MCF
SRCF
MPCE
START
RST
L1
L2
L3
S1
S2
S3
FUNCTIONAL CONTROLS
RESET
EDM
BS1
PROTECTIVE EQUIPMENT TYPE 4
OSSD1
OSSD2
F1
KM1
KM2
INPUTS
MACHINE CONTROL SYSTEM
OUTPUTS
KM1
KM2
M
3~
0V





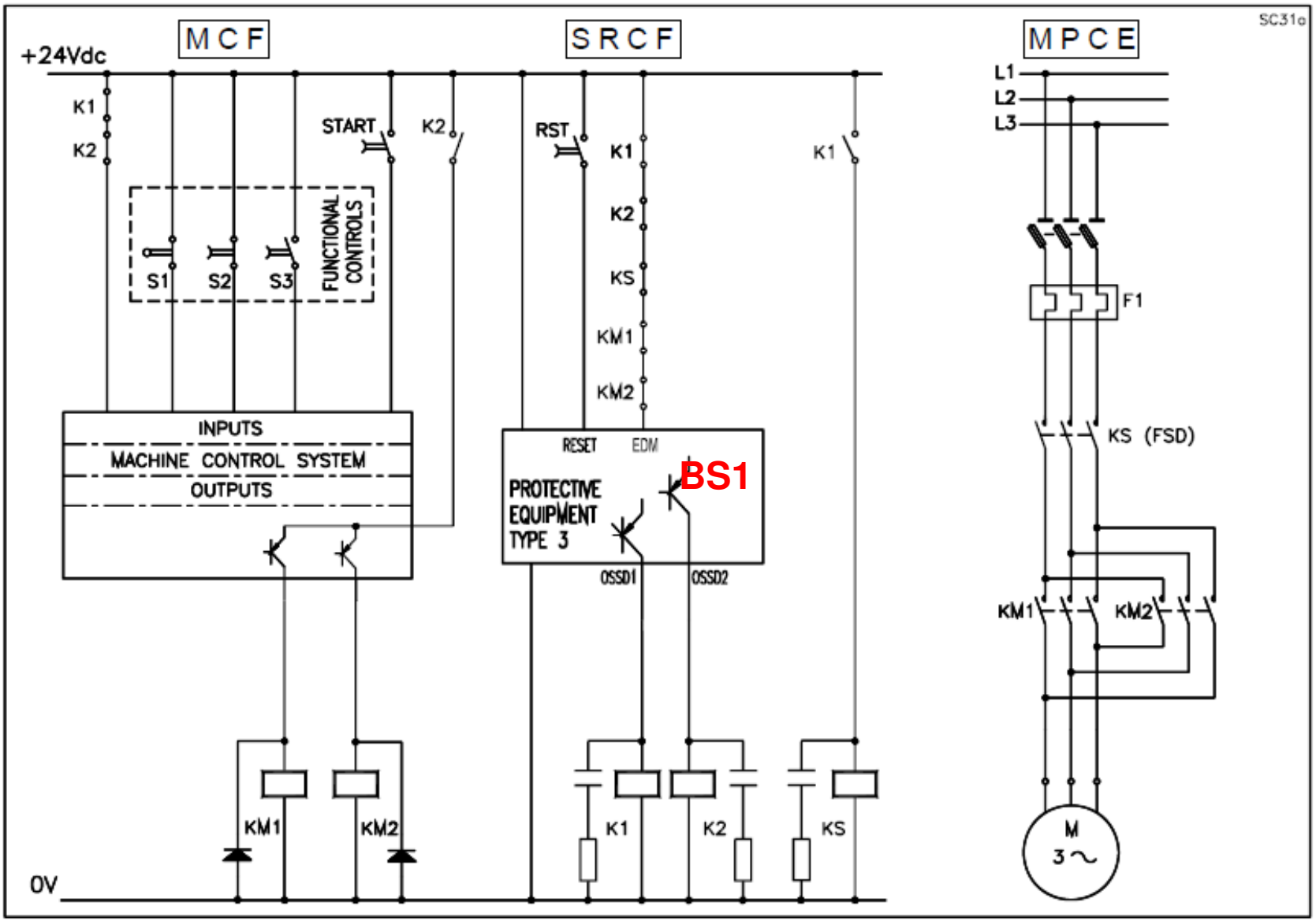
oppure

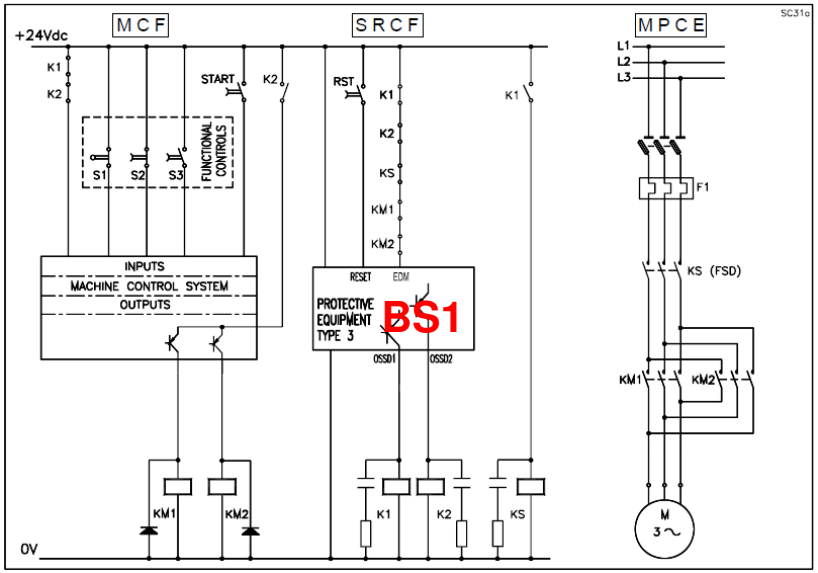


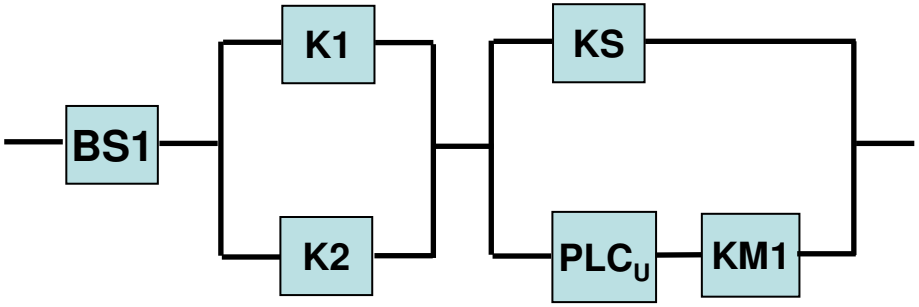
I contattori KM1 e KM2 non sono dotati di contatti legati

La struttura a doppio canale non viene mantenuta né sul PLC (perché non di sicurezza) né sulla linea di alimentazione dei motori. I guasti di KM1 (oppure KM2) non vengono rilevati.

Categoria 1 non è raggiungibile in ragione della mancanza di principi di sicurezza "ben provati" inoltre il PLC non può essere considerato un componente "ben provato".


SC31a
MCF
SRCF
MPCE
+24Vdc
K1
K2
START
K2
RST
K1
K1
S1
S2
S3
FUNCTIONAL CONTROLS
K2
KS
KM1
KM2
INPUTS
MACHINE CONTROL SYSTEM
OUTPUTS
RESET
EDM
BS1
PROTECTIVE EQUIPMENT TYPE 3
OSSD1
OSSD2
L1
L2
L3
F1
KS (FSD)
KM1
KM2
M
3~
KM1
KM2
K1
K2
KS
0V





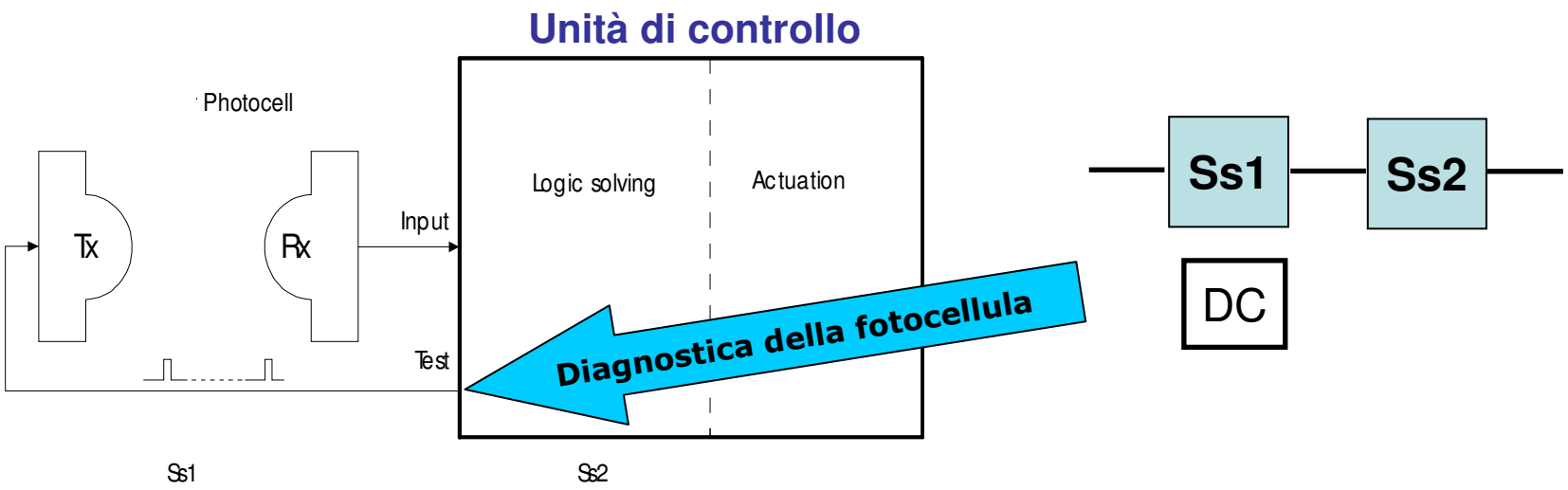
I contattori KM1 e KM2 non sono dotati di contatti legati

La struttura formata da KS, PLC_U, KM1, è ridondante ma non completamente monitorata(il modulo di uscita del PLC non è monitorato, non tutti i guasti di KM1 vengono rilevati).

Categoria max raggiungibile = Cat. 3

$DC_{K1,K2}$ = 99% DC_{KM1} = 60% DC_{PLCu} = 30% (monitorato dal processo)

MTTFd di KM1 potrebbe essere molto basso se ciclo macchina molto corto



Ss1 = Sottosistema sensore **Ss2 = Sottosistema Elaborazione logica e uscita**

SS1: MTTFd = 100 anni (dato del costruttore)

DC = 90% (Stimolo di prova ciclico mediante variazione dinamica dei segnali in ingresso)

Fotocellula conforme a EN 61496-1,2

Categoria 2

Da Tab. K1 di EN ISO 13849-1 risulta per Ss1: PFHd = 2,29 x 10^{-7} PLd

Ss2 Modulo di controllo commerciale

Condizioni di lavoro	Commutazioni	PFHd	$MTTF_d$ (anni)	$MTTF_d$ (anni) Limitato a 100	DC_{avg}	SIL	PL
Load 2A@230V_{ac}	1 ogni 30 s	2,64E-08	26,06	26,06	98,92%	3	PL d
	1 per minuto	1,55E-08	50,29	50,29	98,85%	3	PL e
	1 per ora	4,93E-09	583,26	100,00	97,24%	3	PL e
	1 per giorno	4,77E-09	701,39	100,00	96,89%	3	PL e
Load 0,5A@24V_{dc}	1 ogni 30 s	4,86E-08	13,28	13,28	98,96%	3	PL d
	1 per minuto	2,64E-08	26,06	26,06	98,92%	3	PL d
	1 per ora	5,11E-09	494,44	100,00	97,51%	3	PL e
	1 per giorno	4,78E-09	692,04	100,00	96,91%	3	PL e

Valori riferiti a carico di lavoro di 3520h/anno (220gg,16 ore/g).

$$PFHd = PFHd_{Ss1} + PFHd_{Ss2} = 2{,}29 \times 10^{-7} + 2{,}64 \times 10^{-8} = 2{,}55 \times 10^{-7} \Rightarrow$$ **PLd**

Considerazioni sui guasti sistematici dovuti alla parte ottica del sensore potrebbero limitare il PL.

PL max raggiungibile = PLc