



Safety, Detection, Control

Il muting

Cosa è il Muting

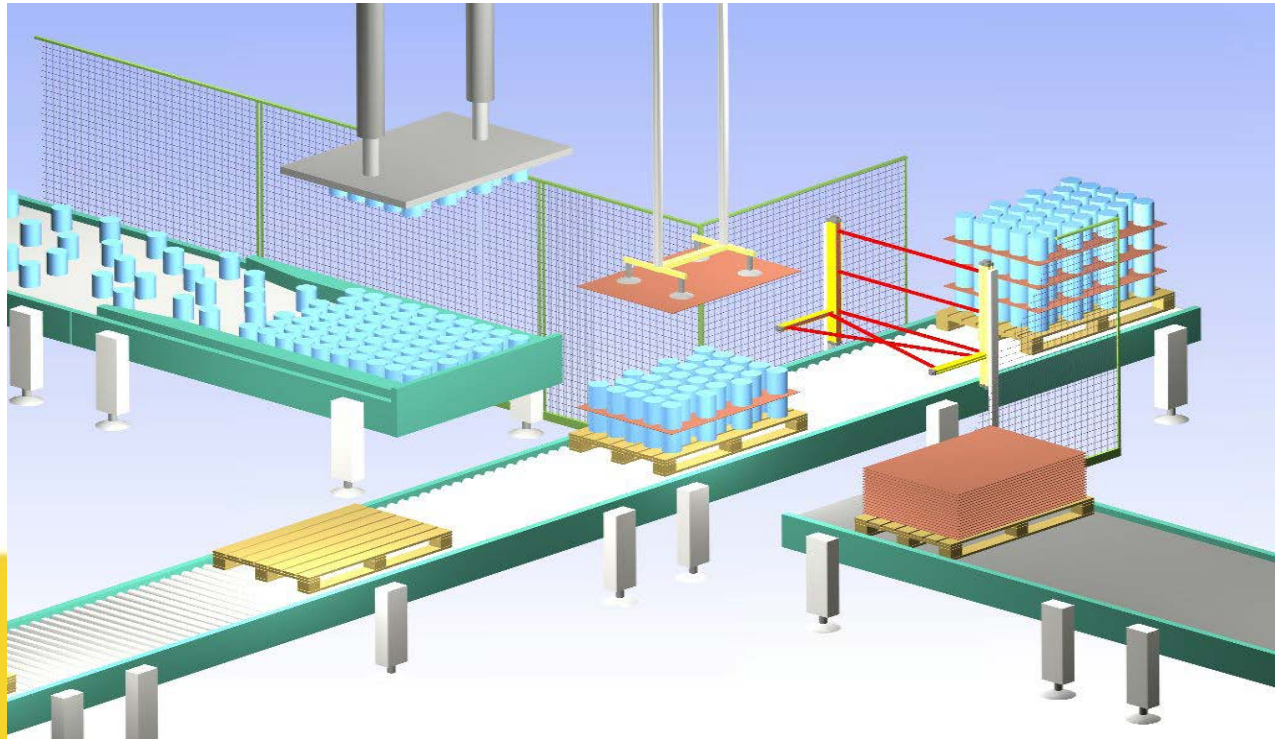
Il Muting è definito come una sospensione temporanea ed automatica di una funzione di sicurezza dei sistemi di comando di una macchina. Può essere usata per consentire l'accesso alle persone o ai materiali.

Muting per consentire l'accesso alle persone

Il Muting può essere usato per consentire l'accesso, in una determinata area, alle persone o a parti del corpo:

- durante fase non pericolosa del ciclo macchina, (ad esempio durante la corsa, non pericolosa, di apertura di una pressa)
- o
- quando la sicurezza viene mantenuta con altri mezzi, (per esempio a velocità o potenza ridotta per l'impostazione della macchina).

Muting per consentire l'accesso ai materiali



Il Muting può essere utilizzato per consentire l'accesso dei materiali solo quando la sicurezza viene mantenuta con altri mezzi, per esempio, quando la presenza di un pallet caricato su un trasportatore impedisce l'accesso alla zona pericolosa alle persone.

La IEC 62046, per la funzione di muting, specifica i seguenti requisiti:

1. The muting function shall be initiated and terminated automatically. This shall be achieved by the use of appropriately selected and placed sensors or by signals from the machine control system.

Incorrect signals, sequence, or timing of the muting sensors or signals shall not allow a mute condition.

2. The part or parts of the control system that performs the muting function shall have an appropriate safety-related performance (SIL or PL, see IEC 62061 or ISO 13849-1) and shall not reduce the safety-related performance of the protective function below that required for the application.

Esempio di Muting

Accesso consentito al materiale con l'uso di sensori fotoelettrici per la discriminazione uomo/materiale.

Si devono considerare 2 distinte funzioni di sicurezza:

SF1 = Arresto iniziato da una misura di protezione (quando una persona tenta di accedere attraverso il varco);

SF2 = Muting (quando è permesso, al pallet, di attraversare il varco).

Per quanto previsto dalla IEC 62046 il PL (o SIL) della SF2 deve essere uguale al PL (o SIL) della SF1.

Procedura per la Valutazione del PL/SIL

1) Assegnazione del PLr (o SIL) per la funzione SF1

- Per il PLr riferirsi all'allegato A della EN ISO 13849-1
- Per il SIL riferirsi all'allegato F delle EN IEC 62061

2) Calcolo del PL/SIL della catena di controllo implementata per la SF1

Valutazione del PL (EN ISO 13849-1)

La funzione di sicurezza **SF1** è composta dai seguenti SRP/CS:



Si assume che il PL (e relativo PFHd) di ciascun SRP/CS siano noti, ne consegue che:

$$PFHd_{(SF1)} = PFHd_{(SS1)} + PFHd_{(SS2)} + PFHd_{(SS3)}$$

AOPD=Active opto-electronic protective device

Valutazione del PL (EN ISO 13849-1)

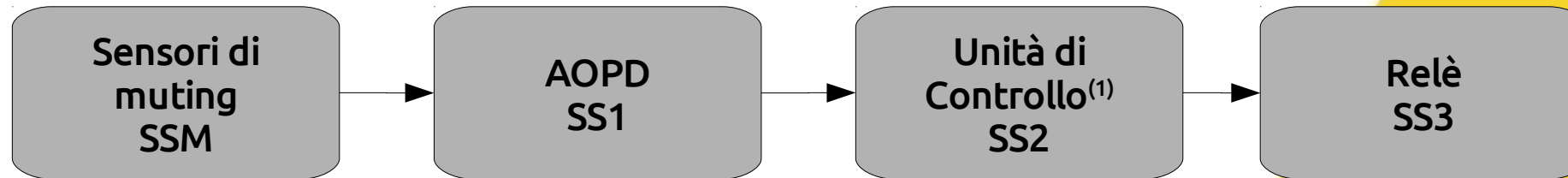
Con l'uso della Tabella 3 della EN ISO 13849-1, possiamo valutare il PL della funzione di sicurezza.

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 $< 10^{-7}$

Valutazione del PL (EN ISO 13849-1)

La funzione di sicurezza **SF2** è composta dai seguenti SRP/CS:



$$PL_{(SF1)} = PL_{(SF2)}$$

L'aggiunta di SSM non deve fare decadere il valore di $PL_{(SF2)}$ rispetto a $PL_{(SF1)}$.

⁽¹⁾Con funzione di controllo per il muting

Valutazione del PL (EN ISO 13849-1)

Valutazione di SSM

Il valore di $PL_{(SSM)}$ è altamente dipendente dal numero, dal tipo e dalla configurazione dei sensori di muting utilizzati.

Di seguito procederemo ad analizzare le tre principali configurazioni dei sensori di muting:

- 4 raggi paralleli con controllo temporale dei sensori
- 4 raggi paralleli con controllo della sequenza dei sensori
- 2 raggi incrociati

E per i seguenti tipi di sensori:

- A sbarramento (proiettore+ricevitore)
- A riflessione (catarifrangente)

Valutazione del PL (EN ISO 13849-1)

Si assume che le raccomandazioni dell'allegato D della EN IEC 62046 ed.3 sulla configurazione e sull'installazione dei sensori di muting siano completamente soddisfatte.

Nota 1:

Sensori di prossimità magnetici posizionati per rilevare pallet metallici e/o sensori meccanici usati per rilevare pallett di legno o plastici non vengono qui considerati perché non riescono a soddisfare i seguenti requisiti (clausola 5.7.3 della IEC 62046 Ed.3):

- Selezione, posizionamento e configurazione dei sensori di muting per distinguere le persone dal materiale a cui è permesso attraversare la zona di rilevamento;
- Selezione e posizionamento dei sensori di muting per rilevare il carico che deve essere trasportato ma, non il pallett o l'unità di trasporto per evitare che le persone possano entrare nella zona di pericolo salendo sopra agli stessi.

Se tali sensori sono impiegati, misure supplementari possono essere necessarie; in questo caso per il calcolo del PL anche gli effetti di tali misure supplementari associate devono essere considerati.

Valutazione del PL (EN ISO 13849-1)

NOTA 2:

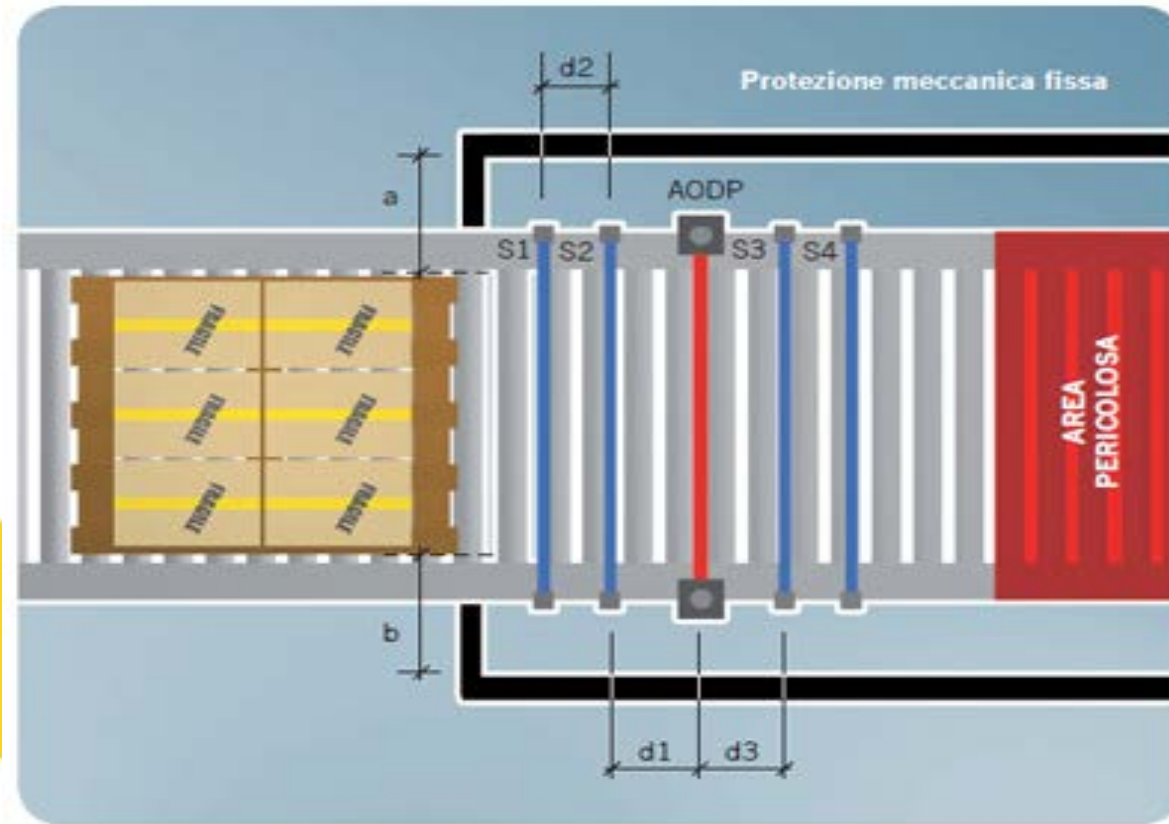
Per tutti gli esempi successivi si assume un valore MTTFd, per i sensori, di 150 anni.

NOTA 2:

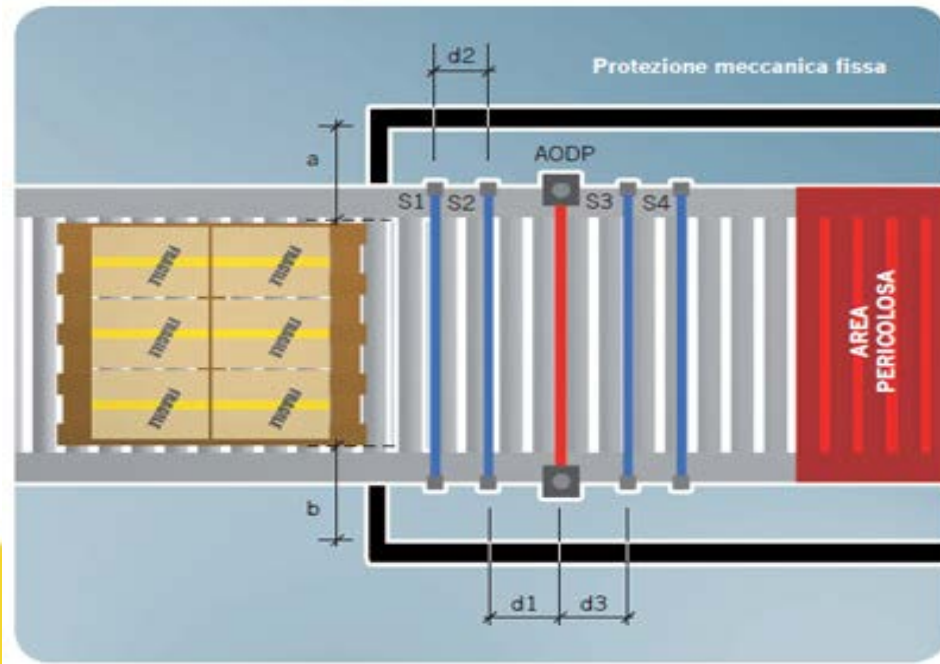
I sensori fotoelettrici sono normali sensori di automazione, senza essere di sicurezza.

Valutazione del PL (EN ISO 13849-1)

Configurazione a 4 raggi paralleli con controllo temporale dei sensori



Valutazione del PL (EN ISO 13849-1)



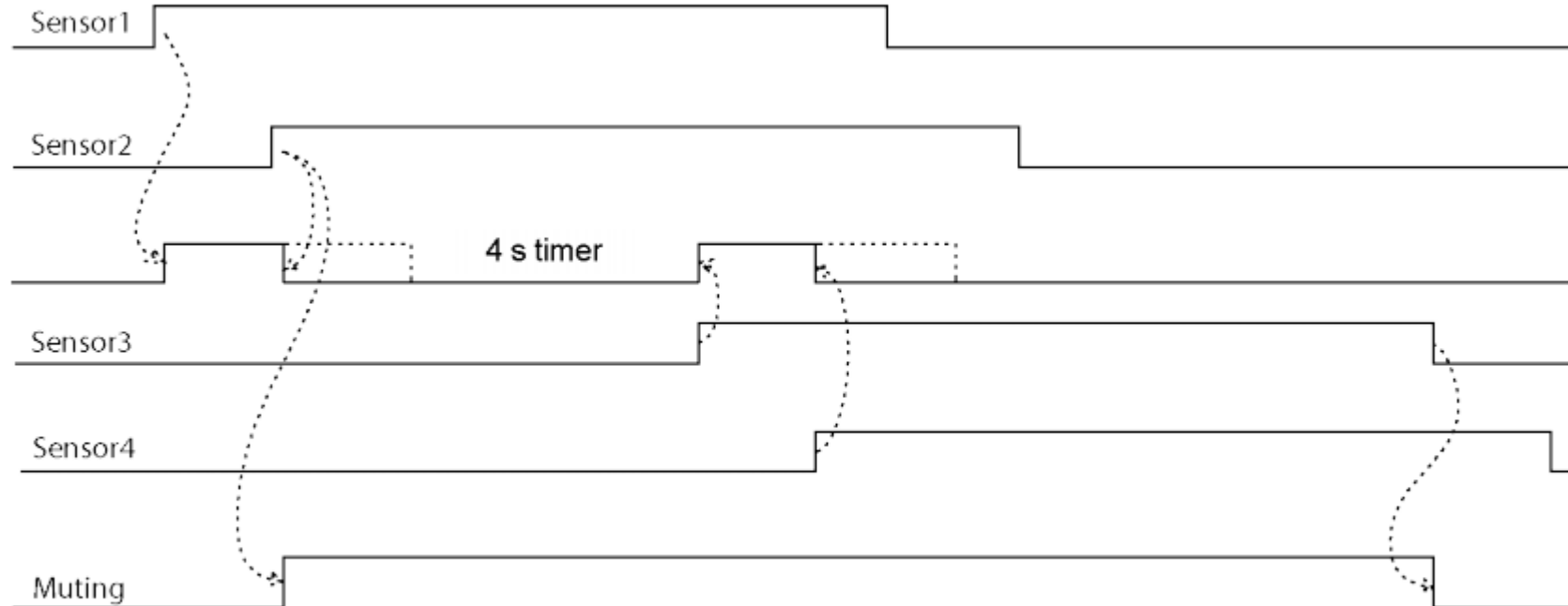
Il monitoraggio della funzione di muting si basa sulla limitazione dei tempi tra l'azionamento dei sensori S1 e S2 e tra l'azionamento dei sensori S3 e S4. Un limite massimo di 4 è stato trovato per essere il miglior compromesso per un'adeguata discriminazione uomo-pallet nelle applicazioni più usuali. Il limite di tempo 4 s deve essere monitorato.

La funzione di muting viene avviato mediante azionamento dei due sensori S1, S2 entro i termini e mantenuto dai due sensori S3, S4; questo significa che per un tempo vengono attivate tutte e quattro i sensori.

La funzione di muting termina quando viene disattivato S3 o S4.

Valutazione del PL (EN ISO 13849-1)

Diagramma temporale configurazione a 4 raggi paralleli con controllo temporale dei sensori



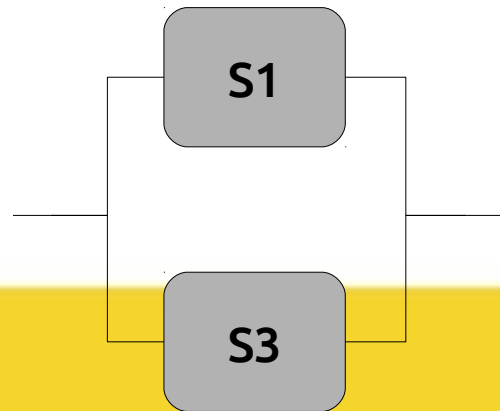
IEC

Figure D.7 – Timing diagram: four parallel beams with timing control

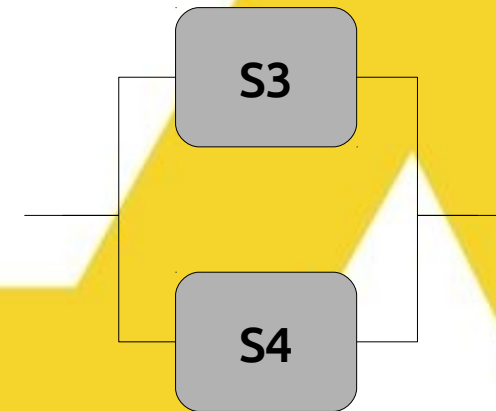
Valutazione del PL (EN ISO 13849-1)

Diagramma a blocchi configurazione a 4 raggi paralleli con controllo temporale dei sensori

Il diagramma logico a blocchi per questa configurazione, è composto da 2 distinte architetture a **doppio canale**, una per lo start e l'altra per lo stop del muting



SSstart = Sottosistema start muting

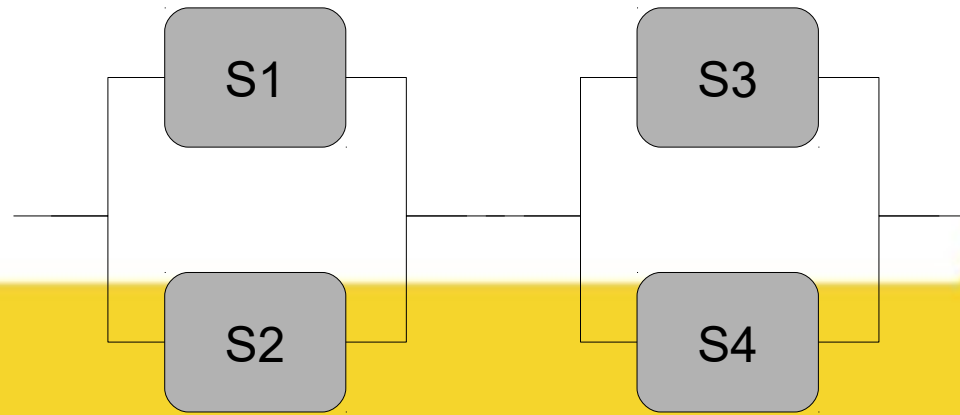


SSstop = Sottosistema stop muting

Valutazione del PL (EN ISO 13849-1)

Diagramma a blocchi configurazione a 4 raggi paralleli con controllo temporale dei sensori.

Considerando quanto detto prima, che per un breve periodo di tempo, tutti e 4 i sensori sono contemporaneamente occupati, il diagramma logico a blocchi diventa il seguente:



SSM = Sottosistema muting

Valutazione del PL (EN ISO 13849-1)

Analisi dei guasti configurazione a 4 raggi paralleli con controllo temporale dei sensori.

Tutti i singoli guasti sono rilevati immediatamente (ad esempio, entro quattro secondi) o al successivo ciclo di muting. Un accumulo di fino a tre errori non rilevati (ad esempio tre su quattro sensori con l'uscita bloccata a uno) non comporta la perdita della funzione di sicurezza.

La DC fornita dal controllore di muting ,per i relativi sensori con questa configurazione, è del 99% (temporale più controllo logico).

Tutto ciò soddisfa i requisiti della categoria 4.

Valutazione del PL (EN ISO 13849-1)

Calcolo PL configurazione a 4 raggi paralleli con controllo temporale dei sensori.

Per **SSstart**:

MTTFd (canale) = 150 anni (alto) DCavg = 99% (alto)

Dalla tabella K.1 della ISO 13849-1 si ottiene $\text{PFHd}(\text{SS1}) = 1,61 \times 10^{-8}$ e PLe

Per **SSstop**:

Se i sensori S3 e S4 hanno le stesse caratteristiche di S1 e S2 allora hanno anche lo stesso $\text{PFHd}(\text{SS2}) = 1,61 \times 10^{-8}$

Per l'intero sottosistema **SSM** si ha:

$\text{PFHd}(\text{SSM}) = \text{PFHd}(\text{SSstart}) + \text{PFHd}(\text{SSstop}) = 3,22 \times 10^{-8}$

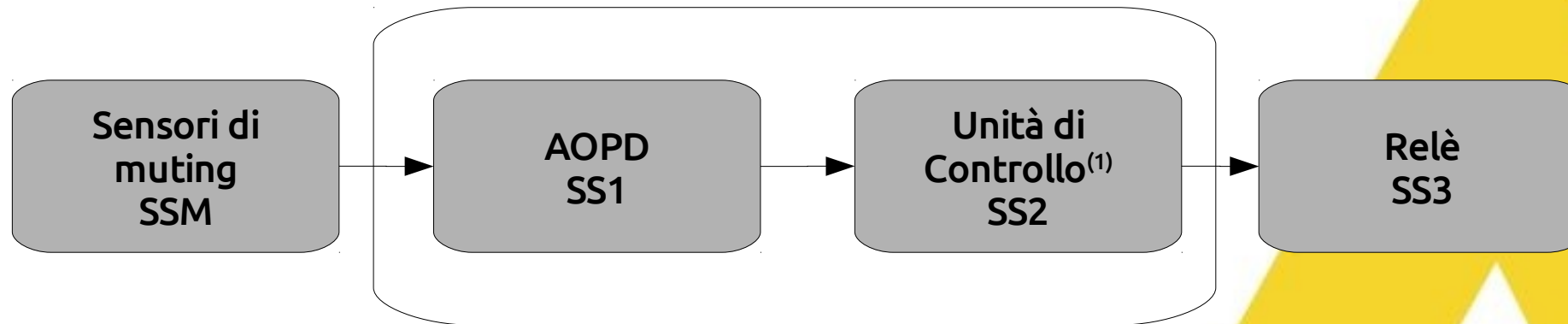
Quindi il PFHd della funzione di muting SF2 sarà :

$\text{PFHd}(\text{SF2}) = \text{PFHd}(\text{SSM}) + \text{PFHd}(\text{SS1}) + \text{PFHd}(\text{SS2}) + \text{PFHd}(\text{SS3}).$

N.B. Si è considerata la tabella K1 dell'emendamento 1, in quanto attualmente la tabella K1 considera un MTTFd di max.100 anni.

Valutazione del PL (EN ISO 13849-1)

Se il dispositivo AOPD incorpora il controllore del muting:

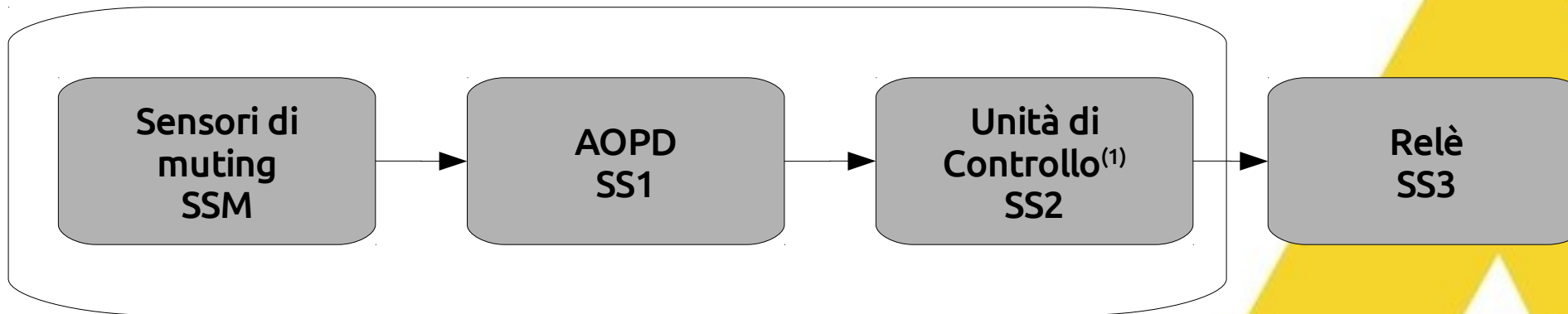


$$PFHd_{(SF2)} = PFHd_{(SSM)} + PFHd_{(SS1/SS2)} + PFHd_{(SS3)}^*$$

⁽¹⁾Con funzione di controllo per il muting

Valutazione del PL (EN ISO 13849-1)

Se il dispositivo AOPD incorpora il controllore ed i sensori di muting (come, ad es. la serie Janus della REER):

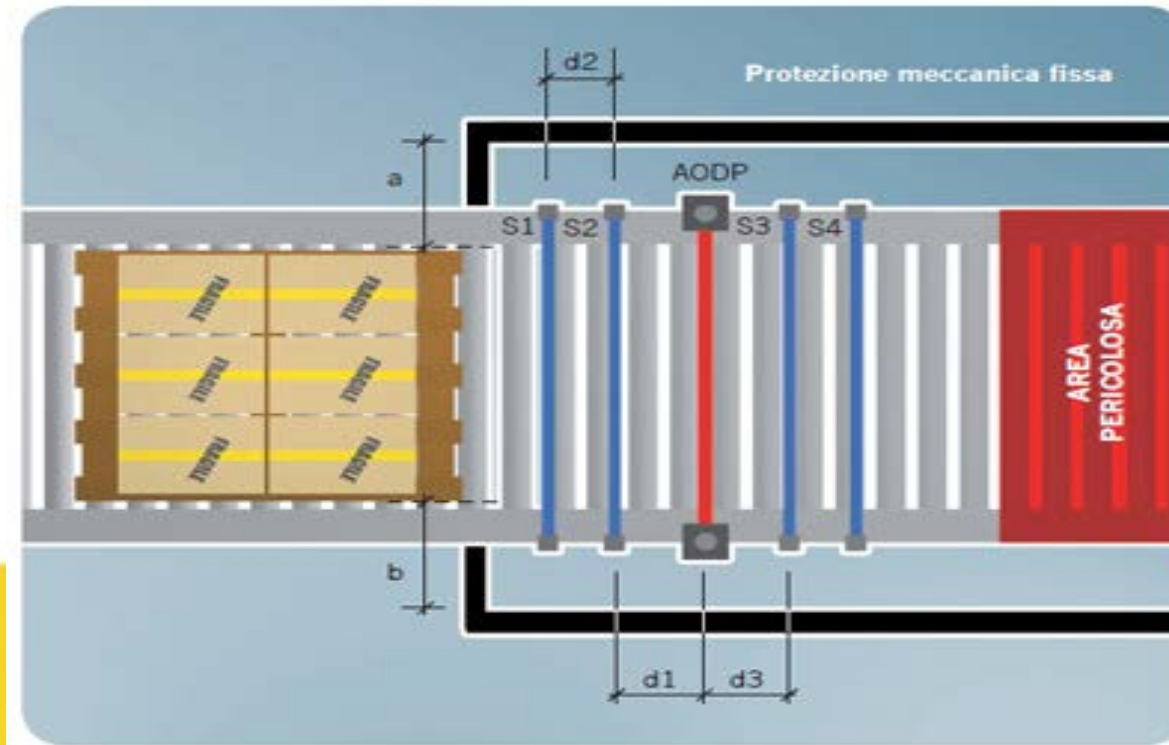


$$PFHd_{(SF2)} = PFHd_{(AOPD)} + PFHd_{(SS3)}$$

⁽¹⁾Con funzione di controllo per il muting

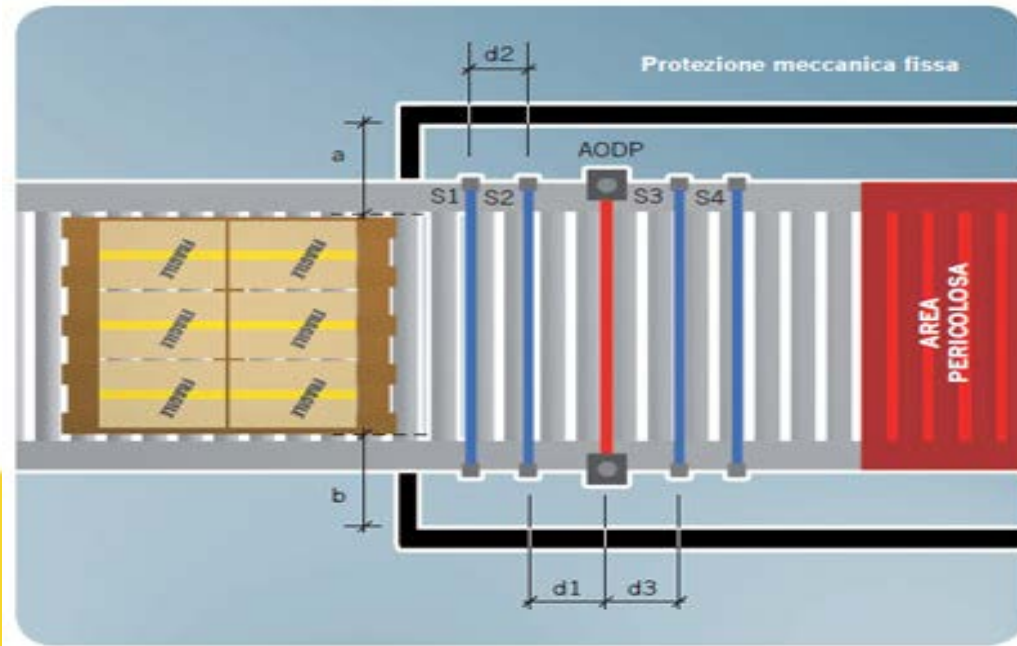
Valutazione del PL (EN ISO 13849-1)

Configurazione a 4 raggi paralleli con controllo sequenziale dei sensori



Valutazione del PL (EN ISO 13849-1)

Configurazione a 4 raggi paralleli con controllo sequenziale dei sensori



Il posizionamento dei sensori è lo stesso delle quattro fasci usato con controllo di temporizzazione.

L'avvio della funzione di muting dipende dal monitoraggio della corretta sequenza di attivazione dei sensori di muting.

Valutazione del PL (EN ISO 13849-1)

Diagramma temporale configurazione a 4 raggi paralleli con controllo sequenziale dei sensori



Figure D.9 – Timing diagram: four beams and sequence control

Valutazione del PL (EN ISO 13849-1)

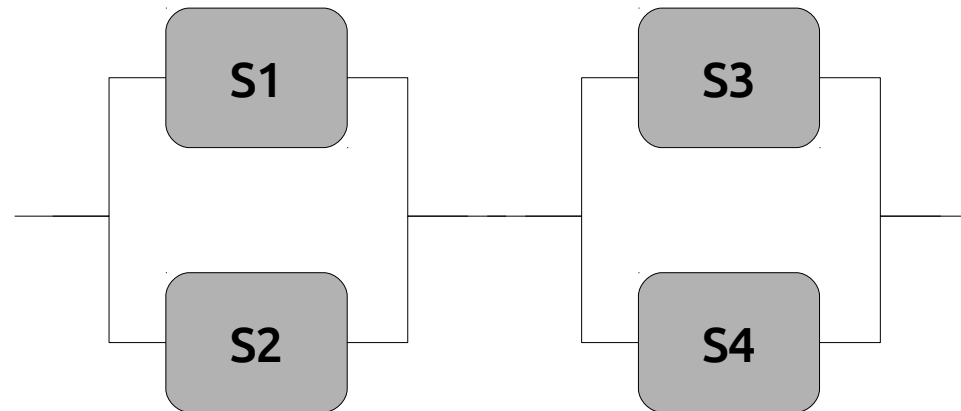
Tabella di verità configurazione a 4 raggi paralleli con controllo sequenziale dei sensori

S1	S2	Input	S3	S4	Muting
0	0	1	0	0	0
1	0	1	0	0	0
1	1	1	0	0	1
1	1	X	0	0	1
1	1	X	1	0	1
1	1	X	1	1	1
0	1	X	1	1	1
0	0	0	1	1	1
0	0	1	1	1	1
0	0	1	0	1	0
0	0	1	0	0	0

Muting
attivo

Valutazione del PL (EN ISO 13849-1)

Diagramma a blocchi configurazione a 4 raggi paralleli con controllo sequenziale dei sensori.



SSM = Sottosistema muting

Esempio architettura a due canali per inizio muting e architettura a due canali per l'arresto muting con controllo della sequenza logica dei quattro sensori in modo che solo una sequenza predefinita attiverà e disattiverà la funzione di muting.

Valutazione del PL (EN ISO 13849-1)

Analisi dei guasti configurazione a 4 raggi paralleli con controllo sequenziale dei sensori.

Tutti i singoli guasti sono rilevati immediatamente (ad esempio, sequenza scorretta) o al successivo ciclo di muting. Un accumulo di fino a tre errori non rilevati (ad esempio tre su quattro sensori con l'uscita bloccata a uno) non comporta la perdita della funzione di sicurezza.

La DC fornite dal controllore di muting ,per i relativi sensori con questa configurazione, è del 99% (temporale più controllo logico).

Tutto ciò soddisfa i requisiti della categoria 4.

Valutazione del PL (EN ISO 13849-1)

Calcolo PL configurazione a 4 raggi paralleli con controllo sequenziale dei sensori.

Valgono le stesse considerazioni della configurazione a 4 raggi paralleli con controllo temporale dei sensori.

Configurazione a 2 raggi incrociati

Valutazione del PL (EN ISO 13849-1)

Configurazione a 2 raggi incrociati

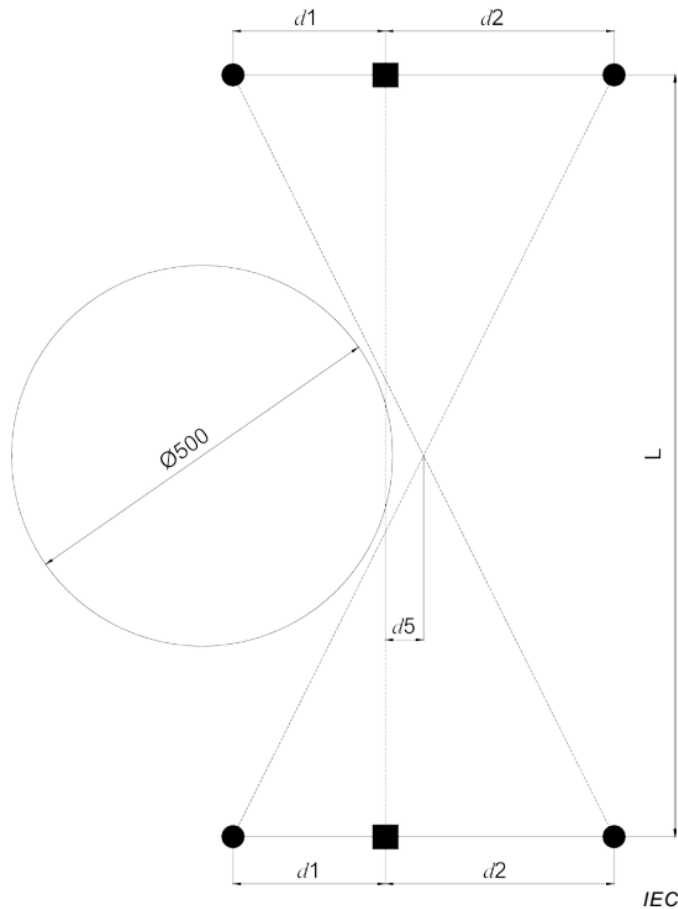
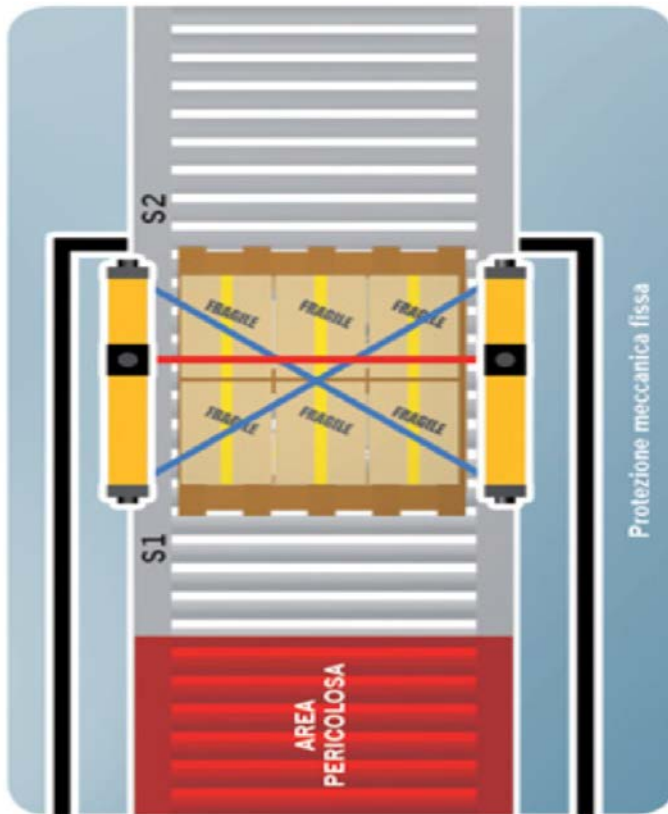


Figure D.19 – Positioning of the muting sensors

Con questa configurazione e con le distanze previste dalla IEC 62046, un oggetto di prova con $\varnothing 500$ mm simulante una persona, viene rilevato da uno dei due sensori di muting e poi dall'ESPE prima di essere rilevato dal secondo sensore di muting, quindi la funzione non viene avviata perché la sequenza dell'attivazione non è corretta.

Valutazione del PL (EN ISO 13849-1)

Configurazione a 2 raggi incrociati



La funzione di muting deve avere inizio **solo** quando i fasci dei due sensori di muting sono attivati entro un termine che è stato selezionato in base all'applicazione, ma non superiore a 4 s. Se è necessario un limite di tempo maggiore di 4 s, la discriminazione uomo / pallet non è garantita, pertanto, deve essere utilizzata una configurazione diversa, ad esempio 4 sensori.

La funzione di muting deve avere termine non appena uno dei due fasci dei sensori di muting non è più attivato.

Valutazione del PL (EN ISO 13849-1)

Diagramma temporale configurazione a 2 raggi incrociati

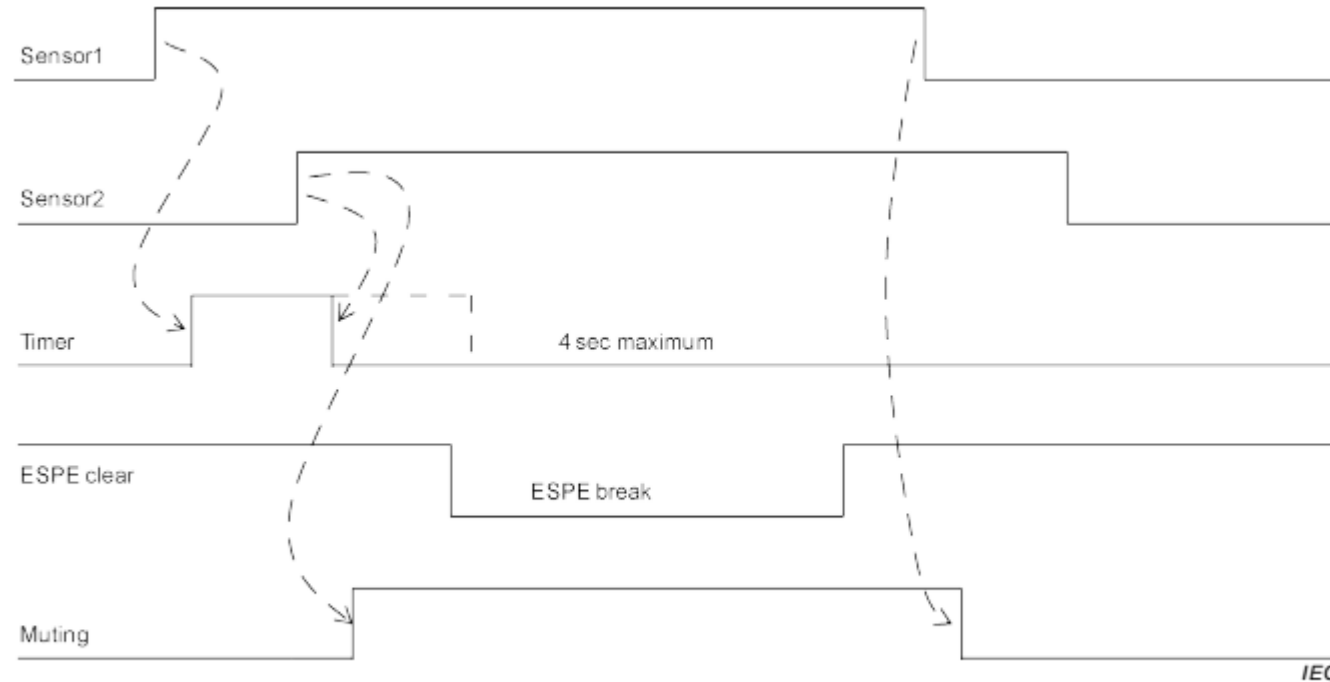
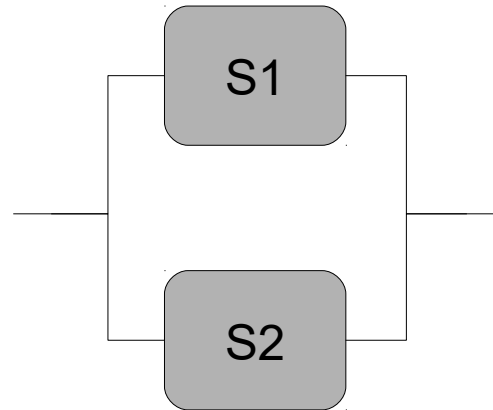


Figure D.21 – Timing diagram for two crossed beams (normal operation)

Valutazione del PL (EN ISO 13849-1)

Diagramma a blocchi configurazione a configurazione a 2 raggi incrociati.



SSM = Sottosistema muting

Esempio architettura a due canali. Stesso sottosistema per avvio/arresto muting.

Valutazione del PL (EN ISO 13849-1)

Analisi dei guasti configurazione a configurazione a 2 raggi incrociati.

Un singolo guasto non comporta la perdita della funzione di sicurezza.

La maggior parte dei guasti singoli vengono rilevati dal controllo temporale dei 4 sec.

Un accumulo di guasti non rilevati può portare alla perdita della funzione di sicurezza.

La DC fornita ai sensori da parte del controllore di muting, con questa configurazione, è del 60% (monitoraggio temporale). Questo soddisfa i requisiti della categoria 3.

Si consideri il caso in cui il pallet, dopo aver superato l'apertura, si arresta per molto tempo davanti S1 e S2.

Mentre i sensori sono azionati dal pallet, se un guasto si verifica in S1 (es. uscita guasta a uno) e successivamente anche S2 si guasta nello stesso modo, la funzione di muting non può terminare, quando il pallet si allontana .

Il varco d'accesso rimarrà in uno stato di muting permanente e questi guasti non saranno rilevati fintanto che il dispositivo è privato dell'alimentazione e acceso nuovamente. Durante tutto questo tempo, una persona può passare attraverso il passaggio senza essere rilevato.

Valutazione del PL (EN ISO 13849-1)

Calcolo PL configurazione a configurazione a 2 raggi incrociati.

MTTFd (canale) = 150 anni (alto), limitato a 100 poiché categoria 3.

DCavg = 60% (basso)

Dalla tabella K.1 della ISO 13849-1 si ottiene $PFHd(SSM) = 1,01 \times 10^{-7}$ e PLd

Quindi il PFHd della funzione di muting SF2 sarà :

$PFHd(SF2) = PFHd(SSM) + PFHd(SS1) + PFHd(SS2) + PFHd(SS3).$

O nel caso di AOPD con controllore muting integrato

$PFHd(SF2) = PFHd(SSM) + PFHd(SS1/SS2) + PFHd(SS3).$

Il muting timeout

Il tempo di muting (Muting timeout) come mezzo per evitare che l'accumulo di guasti non rilevati conduca ad un funzione di muting attiva in permanenza.

Il muting timeout

Abbiamo visto che, per la configurazione a 2 fasci incrociati, quando i sensori non sono attivati (ad esempio pallet non all'interno della zona di muting) sono controllati dal controllore di muting e i loro possibili guasti pericolosi vengono rilevati in un periodo di tempo che può variare da pochi millisecondi fino a 4 secondi a seconda delle configurazioni.

Quando i sensori sono azionati da un pallet e rimangono azionati per lungo tempo a causa di un fermo nella zona muting, gli eventuali guasti non possono essere monitorate basandosi sul tempo di muting di 4 sec., quindi eventuali guasti multipli pericolosi non rilevati (ad esempio, uscite rimaste a 1) possono accadere.

Per evitare questo accumulo di guasti pericolosi non rilevati occorre selezionare un tempo massimo per la durata del muting, al termine del quale, il muting è automaticamente disattivato e l'AOPD torna a proteggere il varco, indipendentemente dalla posizione del pallet.

Il muting timeout

Allo scadere del muting-timeout il pallet, se è già nella zona muting, verrà rilevato dall'AOPD che, a sua volta, disattiva le uscite di sicurezza così come movimenti del trasportatore.

Liberando la zona di muting (a mano o con il comando di override), se i sensori funzionano correttamente, è possibile avviare un nuovo ciclo di muting;

Se i sensori sono ancora attivati a causa di guasti, non sarà più possibile avviare un nuovo ciclo di muting.

Il ripristino del sistema è possibile solo dopo la sostituzione dei due sensori difettosi.

Una DC max. = 90% può essere ottenuta con l'implementazione della funzione di muting timeout.

Il muting timeout

Qual è il massimo muting-timeout necessario in funzione della affidabilità dei sensori per rendere trascurabile la probabilità del verificarsi di guasti multipli non rilevati?

Si assume trascurabile la probabilità di un loro accumulo se essa è di un ordine di grandezza inferiore al PFHd minimo richiesto per tale funzione di muting.

Es per un PLr = e, si veda tabella 3 della norma ISO 13849-1 che il PFHd minimo è 1×10^{-8} , quindi la probabilità di guasto di entrambi i sensori deve essere inferiore a 10^{-9}

Supponendo che tutti i guasti sono equiprobabili e che S1 e S2 hanno la stessa affidabilità, la probabilità che entrambi i sensori si guastino in un tempo t è:

$$Q = [1 - R(t)]^2 = [1 - e^{-t/m}]^2$$

Dove t è espresso in ore e m è il MTTFd, espresso in ore, di ciascun sensore.

Il muting timeout

Per $MTTFd = 150$ anni, cioè $MTTFd$ dei sensori S1 e S2 degli esempi precedenti, e un muting timeout di 40 ore otteniamo:

$$Q = [1 - e^{-40 / (24 \times 365 \times 150)}]^2 = [1 - e^{-40 / (1314000)}]^2 = 9,26 \times 10^{-10}$$

In altre parole, stanti questi dati, la probabilità di accumulo di 2 guasti è trascurabile.

Per questi sensori 40 ore dovrebbero essere il massimo consentito muting-timeout.

Nel nostro esempio, se ora mettiamo $DC = 90\%$ e Cat.3 otteniamo per SSM:

$$PFHd (SSM) = 4,29 \times 10^{-8}.$$

Il muting timeout

Ci sono guasti aggiuntivi che, in alcune circostanze, possono portare ad un accumulo di guasti non rilevati.

Questi sono per esempio:

- Disallineamento contemporaneo dei due sensori a causa di danni meccanici,
- Pezzi di materiale caduti dal pallet e rimasti di fronte al punto di incrocio dei due sensori, ecc.

Questi guasti non possono essere valutati dal punto di vista quantitativo, perché non sono influenzati dalla affidabilità dei sensori.

Il muting timeout

Considerando che il tempo necessario ad un pallet per attraversare la zona di muting è di solito meno di 15 secondi, una persona ha tutto il tempo per attraversarla e raggiungere la zona pericolosa mentre la barriera è disattivata se, a causa di questo tipo di guasti, il muting non viene arrestato dai sensori ma solo dal muting-timeout, ad esempio, di 40 ore.

Un possibile modo per occuparsi di loro è limitando il tempo di muting per il tempo che ha effettivamente impiega il pallet ad attraversare la zona di muting + 4 sec.

Ad esempio selezionando un muting-timeout di $15 + 4 = 20$ secondi.

Se il muting-timeout è limitato al tempo che impiega effettivamente il pallet per attraversare il muting, di una DC = 99% può essere considerata.

Il muting timeout

Se non è possibile limitare il muting-timeout al tempo che impiega effettivamente il pallet ad attraversare la zona muting a causa, ad esempio, delle diverse dimensioni dei pallet e quindi della variabilità della lunghezza del ciclo di muting, il monitoraggio dei segnali del sistema di trasporto può essere aggiunto per determinare quando un pallet è nella zona muting.

La funzione di muting viene "attivata" solo quando il pallet si sta avvicinando alla zona di muting e disabilitata quando la ha lasciata.

Questo monitoraggio, per essere efficace come un miglioramento di DC, deve soddisfare le prescrizioni per le funzioni di diagnostica, come specificato in

IEC 62061 par. 6.8. in modo che anche i suoi guasti (per esempio uscite "in corto" in stato ON) vengano rilevati in modo dinamico.

Il muting timeout

Se si adotta un segnale muting enable / disable monitorato, la copertura diagnostica di S1 e S2 può essere considerata $DC = 99\%$.

Con una MTTFd di S1 e S2 pari ad alto e una $DC = 99\%$, possiamo considerare che i requisiti della categoria 4 siano raggiunti e conseguentemente anche con la configurazione a due fasci è possibile raggiungere $PL = e$.

Nel nostro esempio, con una $DC = 99\%$, un $MTTFd = 150$ anni e un Cat.4 otteniamo per sottosistema SSM

$$PFHd (SSM) = 2,47 \times 10^{-8}$$

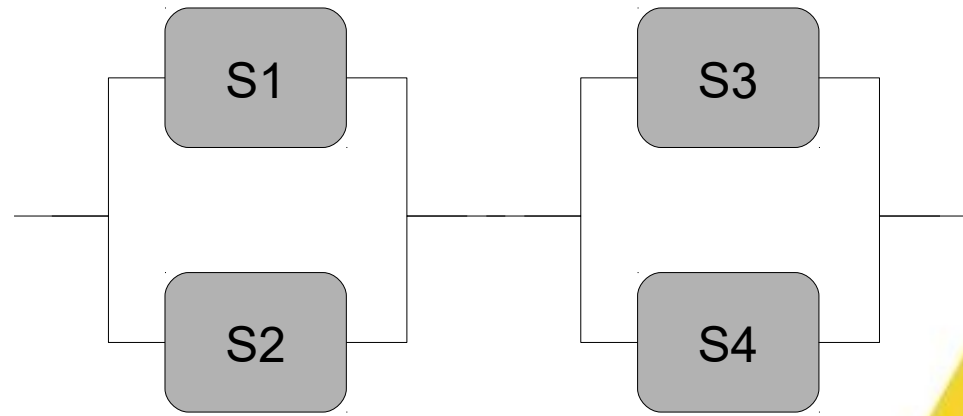
Il muting timeout

Per la configurazione a due fasci incrociati

- la discriminazione uomo / pallet viene verificata da un adeguato posizionamento dei sensori insieme all'uso del tempo di 4 secondi per impegnare entrambi i sensori;
- l'affidabilità dei sensori è controllato dal timer a 4 sec. quando la zona di muting è vuota e la funzione di muting-timeout, quando il pallet ostruisce la zona di muting. Se il muting-timeout è impostato per il tempo necessario al pallet per transitare attraverso la zona di muting, anche i guasti imputabili a causa di circostanze ignote sono rilevati.
- l'affidabilità dei sensori e i guasti aggiuntivi dovuti a circostanze sconosciute possono essere controllati anche dal segnale di muting disable/enable
- Un muting-timeout impostato al tempo impiegato dal pallet per transitare attraverso la zona muting e il segnale di muting enable / disable sono anche efficaci contro la manipolazione del sistema.

Valutazione del SIL (EN IEC 62061)

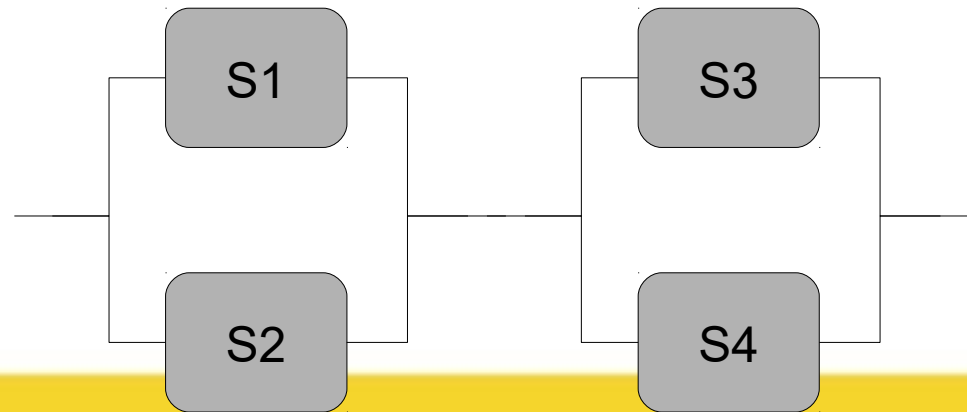
Configurazione a 4 raggi paralleli con controllo temporale dei sensori.



SSM = Sottosistema muting

Valutazione del SIL (EN IEC 62061)

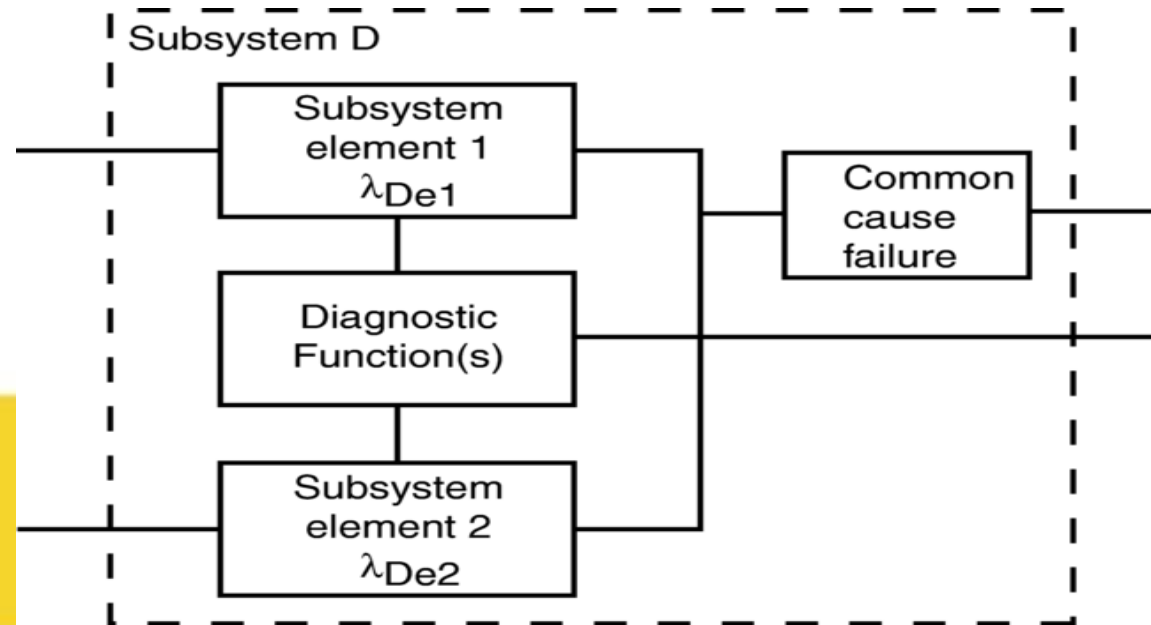
Poiché i sottosistemi S1 / S2 e S3 / S4 condividono la stessa struttura, possono essere raggruppati come descritto in IEC / TR 62061-1. SSM può quindi essere semplificata come segue:



SSM = Sottosistema semplificato muting

Valutazione del SIL (EN IEC 62061)

Questa architettura corrisponde al sottosistema D della IEC 62061.



Valutazione del SIL (EN IEC 62061)

Gli elementi del sottosistema S1, S2, S3, S4 sono identico modello, quindi si applica la formula D.2.

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_{De}$$

Dove:

λ_{DssD} = Probabilità di guasto pericoloso del sottosistema

λ_{De} = Probabilità di guasto pericoloso degli elementi

T_2 = intervallo di test diagnostico

T_1 = intervallo di test di prova o durata se inferiore

β = La suscettibilità ai guasti di causa comune;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$;

Dove λ_{DD} è il tasso di guasto pericoloso rilevabile e λ_{DU} è il tasso di guasto pericoloso non rilevabile.

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

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

Valutazione del SIL (EN IEC 62061)

Se si assume che ogni sensore ha un $MTTF_d = 150$ anni, e che la ripartizione dei guasti sia il 50% pericoloso e il 50% sicuro, diventa:

$$\lambda_d (S1) = \lambda_d (S2) = \lambda_d (S3) = \lambda_d (S4) = 1 / MTTF_d = 7,6 \times 10^{-7}$$

$$\lambda_s (S1) = \lambda_s (S2) = \lambda_s (S3) = \lambda_s (S4) = 7,6 \times 10^{-7}$$

$$DC = 0,99$$

$$T1 = 20 \text{ anni}$$

$$T2 = ?$$

$$\beta = 0,02$$

$$\lambda_{De} = \lambda_d(S1) + \lambda_d(S3) = 1,52 \times 10^{-6}$$

Valutazione del SIL (EN IEC 62061)

Per poter proseguire con il calcolo abbiamo bisogno di ricavare un valore per l'intervallo del test diagnostico T2.

Abbiamo già visto che quando i sensori non occupati (ad esempio pallet non all'interno della zona di muting) l'intervallo di test diagnostico può variare da pochi millisecondi ad alcuni secondi a seconda del controllore di muting.

Quando i sensori vengono occupati i loro guasti non possono essere più monitorati; possono essere monitorati nuovamente quando il pallet si è allontanato.

Quindi possiamo dire che l'intervallo di test diagnostico dipende dalla lunghezza, velocità e pause del pallet all'interno dell'area muting quindi risulta fortemente dipendente dal processo.

Ma, se si decide di utilizzare una funzione di timeout per il muting, T2 non dipende più dal processo, il caso peggiore sarà uguale alla lunghezza del timeout.

Valutazione del SIL (EN IEC 62061)

Con questa ipotesi si può calcolare la formula D.2.

Assumiamo per T2 due valori tipici: 30 secondi e 10 ore.

Se $T2 = 30 \text{ s}$ $\lambda_{DSSD} = 3,429 \times 10^{-8}$

Se $T2 = 10 \text{ ore}$ $\lambda_{DSSD} = 3,431 \times 10^{-8}$

Notare che la lunghezza del "muting-timeout" non modifica significativamente il PFHd di SSM.

La ragione è che il modello del sottosistema "due canali con diagnostica" già includono la probabilità che due guasti possono avvenire quasi contemporaneamente.

Valutazione del SIL (EN IEC 62061)

$$SFF = \frac{\sum \lambda_{DD} + \sum \lambda_S}{\sum \lambda_D + \sum \lambda_S}$$

SFF = 99,5% e sapendo che l'architettura implementata ha HFT(tolleranza ai guasti hardware) = 1 risulta:

PFHd = $3,4 \times 10^{-8}$ e SIL 3

Se paragoniamo questo risultato con quello calcolato utilizzando ISO 13849-1 (PFHd = $3,22 \times 10^{-8}$) vediamo che i due metodi danno quasi gli stessi numeri.

Osservazioni conclusive

Da un puro punto di vista dell'affidabilità, la DC fornita dal controllore del muting per i sensori di detta funzione, è del 99% per le configurazioni a quattro fasci e il 60% per le configurazioni a 2 fasci.

Per la configurazione a due fasci la DC può essere aumentata fino al 99% un corretto muting timeout o se un segnale di abilitazione / disabilitazione del muting è implementato.

Possono esserci guasti che potrebbero portare ad un accumulo degli stessi diversi da quelli dovuti alla affidabilità dei sensori.

Deve essere controllato l'eventuale effetto pericoloso dei suddetti guasti

La manipolazione dei sensori è un problema di sicurezza molto importante, quindi, considerare sempre un metodo per evitarla.

Ad esempio mantenendo la funzione di muting attiva solo per il tempo strettamente necessario.



GRAZIE PER L'ATTENZIONE

