REER

Your future's safe!

Guida alla sicurezza

norme per la sicurezza sul lavoro

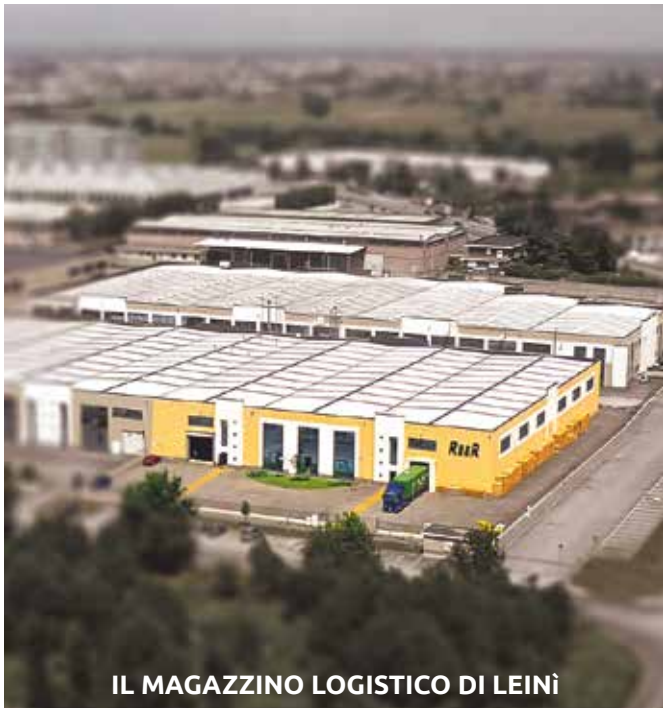
Dal 1959 il vostro partner tecnologico

Fondata nel 1959 per la distribuzione di componenti per l'industria, l'illuminazione e l'automazione domestica, a metà degli anni '70 ReeR realizza i primi sensori di sicurezza mentre a pochi anni dopo risalgono le prime barriere fotoelettriche.

Oggi ReeR è il leader italiano e uno dei maggiori costruttori al mondo di sensori optoelettronici per la sicurezza industriale.

La forte attività di export che accompagna lo sviluppo della Divisione Sicurezza è la testimonianza di una competenza sempre più globale. La rete di distributori qualificati, presente in più di 60 paesi, garantisce un accurato servizio di supporto al cliente.

LA SEDE CENTRALE DI TORINO



IL MAGAZZINO LOGISTICO DI LEINÌ

Know how

Conoscenza tecnologa e know how applicativo sono alla base dello spirito di ReeR Divisione Sicurezza.

Il 15% del personale è impiegato nella ricerca e sviluppo con competenze in ambito hardware, software e firmware.

Siamo protagonisti nel processo normativo e partecipiamo a numerosi Comitati Normativi nazionali e internazionali sulla Sicurezza delle Macchine. In tal modo ReeR è sempre all'avanguardia riguardo alla conformità dei propri prodotti.

Sicurezza e Automazione

La sicurezza nell'ambiente di lavoro è irrinunciabile; negli ambienti fortemente automatizzati diventa ulteriormente determinante.

L'esperienza maturata in collaborazione con i leader mondiali nel mercato delle macchine utensili, dell'industria automobilistica, degli impianti di confezionamento e di pallettizzazione, consente a ReeR di offrire un'ampia gamma di dispositivi di sicurezza quali barriere fotoelettriche, controllori programmabili, fotocellule, laser scanner e interfacce in grado di soddisfare ogni necessità applicativa.

ReeR è da sempre all'avanguardia anche nelle barriere optoelettroniche per automazione, misura e controllo.

Le parole chiave

Qualità

Il Sistema Qualità di ReeR è stato certificato in base alla UNI EN ISO 9001: 2008 da TUV SUD

- Insourcing di tutte le fasi principali della lavorazione
- Controllo del processo produttivo, qualità, rispetto dei tempi di consegna e competitività
- Il monitoraggio durante l'intera fase produttiva attraverso il sistemo informatico aziendale garantisce:
  - Controllo della part list
  - Tracciabilità

Ambiente

L'energia elettrica utilizzata da ReeR proviene interamente da fonti rinnovabili

RoHS è l'acronimo di Restriction of Hazardous Substances (limitazione delle sostanze pericolose). La direttiva RoHS, 2002/95/CE limita l'uso di materiali pericolosi specifici nei prodotti elettrici ed elettronici

Salute e sicurezza sul lavoro

Per ridurre i rischi sul posto di lavoro, ReeR ha messo in atto un sistema di gestione per la salute e la sicurezza dell'ambiente lavorativo ISO 45001

Processo produttivo innovativo

Controllo del processo produttivo attraverso i criteri della Lean Manufacturing

- Miglioramento continuo
- Produzione snella
- Minimizzazione sprechi
- Miglioramento tempi di consegna
- Gestione materiale ad alta rotazione a scorta

Tipologie di prodotto

Sensori di sicurezza

- Barriere fotoelettriche Tipo 4 e Tipo 2
- Fotocellule
- Switch magnetici e RFID
- Sensori induttivi di prossimità
- Encoder incrementali

Controllori di sicurezza configurabili e interfacce di sicurezza

- Ingressi per barriere di Tipo 4 e Tipo 2
- Ingressi per barriere con funzione di muting integrata
- Ingressi per segnali analogici
- Ingressi per ripari interbloccati
- Ingressi per comando a due mani
- Controllo in sicurezza della velocità SIL 3, PL e
- Controllo di arresto di emergenza

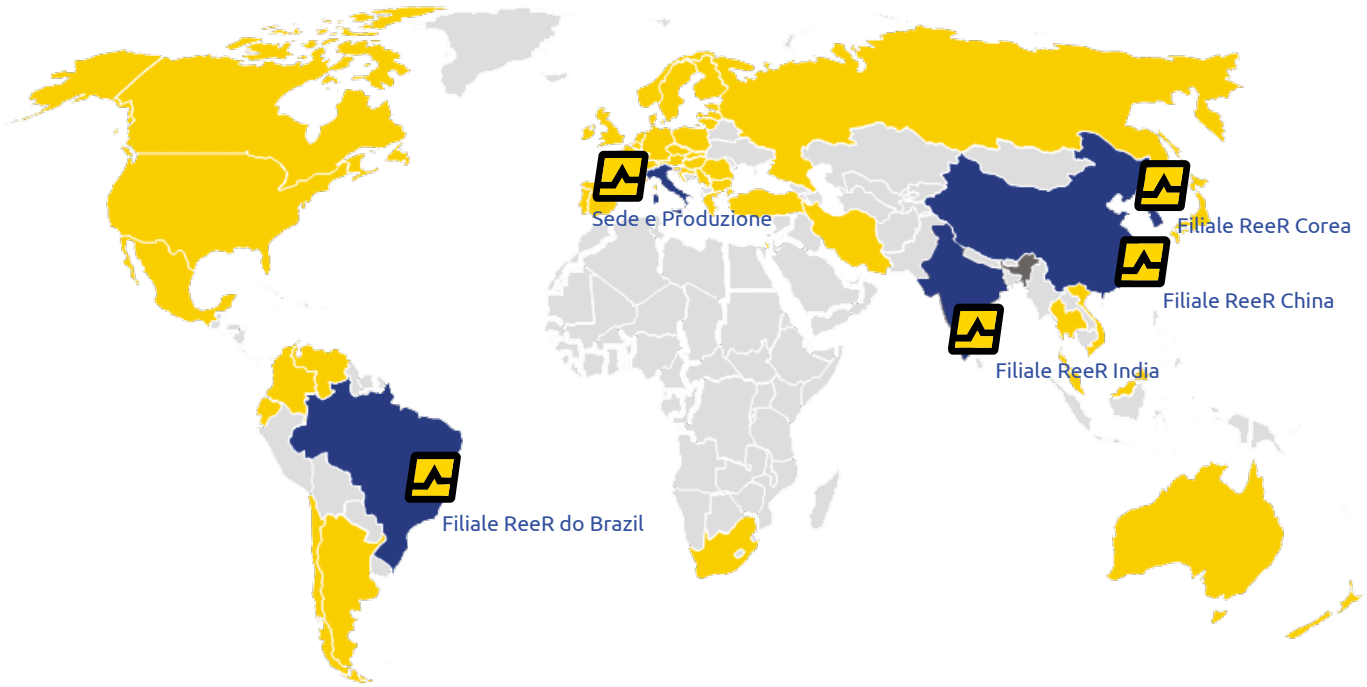
Laser scanner

Dispositivi di misura, automazione e controllo

Accessori

Rete vendita

Rete di vendita diretta in Italia, Brasile, Cina, India e Corea del Sud; 65 distributori nel mondo.



SOMMARIO

SOMMARIO

SOMMARIO

Premessa

Questa guida alla sicurezza si riferisce al complesso di norme che regolano la sicurezza delle macchine. In particolare sono prese in considerazione le importanti famiglie di norme che fanno capo alle:

- ISO 13849 "Sicurezza del macchinario"
- IEC 61508 "Sicurezza funzionale di impianti elettrici, elettronici, programmabili legati alla sicurezza". Quest'ultima norma influisce sulla sicurezza macchine attraverso la IEC 62061 "Sicurezza del macchinario. Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici e programmabili correlati alla sicurezza"
- IEC 61496 "Sicurezza del macchinario: dispositivi elettro-sensibili di protezione".

Importanti concetti statistici facenti capo al concetto di probabilità di guasto pericoloso, vengono in tal modo incorporati nei sistemi di controllo di sicurezza delle macchine e nei dispositivi di protezione e danno luogo a nuove classificazioni: parliamo dei PL (Performance Level, in ambito ISO) e dei SIL (Safety Integrity Level, in ambito IEC). PL e SIL vanno ad affiancarsi e per molti versi a sostituirsi all'ormai familiare concetto di categoria descritto nella "vecchia" EN 954-1.

La seconda edizione della specifica tecnica IEC 62046 "Applicazione dei dispositivi di protezione per il rilevamento della persona", rappresenta un'utile guida per i costruttori che vogliono utilizzare dispositivi di protezione elettrosensibili per la realizzazione dei sistemi di controllo di sicurezza delle macchine.

Direttive europee

Le Direttive Europee si propongono di armonizzare le legislazioni nazionali degli Stati membri in modo da avere regole comuni su aspetti tecnici, fiscali, economici, sanitari ecc. ed agevolare la libera circolazione dei beni, dei servizi e delle persone nell'ambito dell'Unione Europea, nel rispetto di regole comuni riconosciute da tutti gli Stati che ne fanno parte.

Una direttiva è un atto legislativo che stabilisce un obiettivo che tutti i paesi dell'UE devono raggiungere e proprio per questo è prevista l'obbligatorietà del recepimento senza modifica; ciascun paese può però decidere le modalità di recepimento. In particolare, per quanto riguarda la sicurezza del lavoro, la legislazione distingue fra due tipi di provvedimenti:

- Direttive sociali
- Direttive di prodotto

Direttive sociali

Le Direttive sociali sono indirizzate al datore di lavoro e hanno come obiettivo il miglioramento della sicurezza negli ambienti di lavoro. La Direttiva generale 89/391/CEE, concernente l'attuazione di misure volte a promuovere il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro e la Direttiva particolare ad essa correlata 2009/104/EC sull'uso delle attrezzature di lavoro, sono Direttive sociali. Altre direttive sociali di interesse sono:

- 2019/1832/UE "Attrezzature di protezione individuale"
- 90/269 CEE "Movimentazione manuale di carichi"
- 90/270 CEE "Attrezzature munite di videoterminale"

In Italia sono state recepite con il Decreto Legislativo 81/08 "Testo Unico Sicurezza".

Direttive di prodotto

Le Direttive di prodotto stabiliscono:

- I Requisiti Essenziali di Sicurezza (R.E.S.S.) cui i prodotti devono rispondere per poter liberamente circolare nel mercato europeo
- Criteri di attestazione della conformità

Le Direttive fondamentali ai fini della sicurezza delle attrezzature di lavoro sono:

- 2006/42/CE "Direttiva Macchine"
- 2014/35/UE "Direttiva Bassa Tensione"
- 2014/30/UE "Direttiva Compatibilità Elettromagnetica"
- 2014/34/UE "Direttiva ATEX"

L'osservanza dei requisiti tecnici di sicurezza indicati nelle direttive è obbligatoria.

Direttiva macchine

La 2006/42/CE "Direttiva Macchine" è destinata ai costruttori di macchine e componenti di sicurezza ed ha come obiettivi:

- La definizione dei requisiti di sicurezza e tutela della salute per il miglioramento del grado di protezione dei lavoratori addetti a macchine pericolose
- La progettazione, la realizzazione e l'immissione sul mercato dell'Unione Europea di macchine e componenti di sicurezza che rispettino i requisiti minimi di sicurezza stabiliti dalla Direttiva stessa
- La libera circolazione negli Stati membri di macchine e componenti di sicurezza conformi alla Direttiva

La Direttiva Macchine:

- Si applica a macchine e componenti di sicurezza nuovi che vengono venduti, prestati o affittati, ed a macchine usate in caso di vendita, affitto o prestito
- Stabilisce requisiti essenziali di sicurezza relativi alla progettazione e costruzione di macchine e componenti di sicurezza e definisce le procedure per la loro certificazione
- È obbligatoria dal 1 gennaio 1995 per le macchine e dal 1 gennaio 1997 per i componenti di sicurezza
- Dalle date sopra indicate, nell'Unione Europea possono essere commercializzati o messi in servizio solo prodotti conformi alla Direttiva

Procedure per la certificazione

La Direttiva Macchine:

- Prevede procedure rigorose per i componenti di sicurezza e per le macchine ad alto rischio (elencate nell'allegato 4 della direttiva stessa)
- Prevede procedure semplificate per macchine a medio e basso rischio (non comprese nell'allegato 4 della direttiva stessa)
- Prevede che il costruttore rediga per ogni prodotto un fascicolo tecnico attestante i principi di sicurezza adottati per la progettazione, realizzazione, trasporto, uso e manutenzione della macchina o del componente di sicurezza

Dichiarazione di conformità

Per certificare la conformità del prodotto alla Direttiva il costruttore deve:

- Apporre il marchio CE sul prodotto
- Allegare una dichiarazione di conformità CE attestante il rispetto della Direttiva

Certificazioni

I certificati CE di tipo hanno una validità di 5 anni (annesso IX par. 9.3); dopodiché occorrerà una nuova verifica per il mantenimento della certificazione.

Direttiva bassa tensione

La 2014/35/UE "Direttiva Bassa Tensione" ha come obiettivo quello di garantire che i materiali elettrici vengano progettati e costruiti in modo da assicurare la protezione delle persone contro i rischi di folgorazione derivanti dal loro uso o dall'influsso di agenti esterni sui materiali elettrici stessi. La Direttiva si applica a tutto il materiale elettrico destinato ad un utilizzo con tensione nominale fra:

- 50V e 1000V in corrente alternata
- 75V e 1500V in corrente continua

Direttiva compatibilità elettromagnetica

La 2014/30/UE "Direttiva Compatibilità Elettromagnetica" ha come obiettivo che i dispositivi elettrici vengano progettati e costruiti in modo che:

- il livello di emissione elettromagnetica sia limitato e tale da permettere ad altre apparecchiature elettriche di funzionare secondo il loro scopo
- il livello di immunità intrinseca ai disturbi esterni consenta loro di funzionare secondo lo scopo previsto

La Direttiva si applica a tutti i dispositivi elettrici ed elettronici in grado di provocare disturbi elettromagnetici o il cui funzionamento può essere influenzato da interferenze esterne.

Direttiva ATEX

La 2014/34/EU "Direttiva Atex "si applica a tutti gli apparecchi destinati ad essere utilizzati in zone a rischio esplosione.

La Direttiva Atex 2014/34/EU stabilisce i requisiti minimi di sicurezza che devono avere le costruzioni elettriche se impiegate in luoghi classificati pericolosi sotto l'aspetto del rischio di esplosione per presenza di gas o di polveri.

La Direttiva divide le apparecchiature in gruppi e categorie.

Il fabbricante deve decidere, in base all'utilizzo, il gruppo e la categoria di appartenenza.

- Gruppo 1: apparecchi destinati a lavori in sotterraneo nelle miniere e nei loro impianti di superficie
- Gruppo 2: apparecchi destinati ad essere utilizzati in ambienti in cui è probabile che si manifestino atmosfere esplosive

Questi gruppi sono quindi suddivisi in categorie a seconda del livello di protezione da rischio di innesco dell'atmosfera potenzialmente esplosiva.

I prodotti che appartengono al gruppo 2 sono suddivisi in tre categorie:

- Categoria 1: ambienti in cui si rileva, sempre, spesso o per lunghi periodi, un'atmosfera esplosiva dovuta a miscele di aria e gas, vapori, nebbie o miscele di aira e polveri
- Categoria 2: ambienti in cui vi è la probabilità che si manifestino atmosfere esplosive dovute a gas, vapori, nebbie o miscele di aria e polveri
- Categoria 3: ambienti in cui vi sono scarse probabilità che si manifestino, e comunque solo per breve tempo, atmosfere esplosive dovute a gas, vapori, nebbie o miscele di aria e polveri

Organismi accreditati

Gli Organismi Accreditati hanno, per ogni Stato membro, un ruolo ispettivo di controllo e di verifica del rispetto e dell'applicazione delle Direttive Europee.

Ogni Stato è responsabile della nomina e del controllo dei propri Organismi.

Essi devono avere la competenza e le risorse necessarie per espletare attività di ispezione, analisi, assistenza tecnica, misurazione ecc.

In Italia l'Organismo autorizzato a svolgere attività di accreditamento è: Accredia. Accredia mantiene un database con l'elenco di tutti gli organismi italiani accreditati per le varie direttive.

Organismi notificati

Gli Organismi Notificati sono autorizzati ad esaminare e certificare macchine e componenti di sicurezza in accordo con le Direttive ad essi applicabili.

Ogni stato membro dell'Unione Europea è tenuto a:

- Designare gli Organismi notificati indicandone le competenze
- Comunicare alla Commissione Europea e agli altri stati membri l'elenco degli Organismi notificati

La Commissione Europea pubblica nella Gazzetta Ufficiale della Comunità Europea (GUCE) una lista di tutti gli Organismi notificati allegando l'elenco dei servizi, delle macchine e/o componenti di sicurezza per cui essi sono autorizzati ad operare.

Gli Stati membri dell'Unione Europea devono verificare che tali Organismi rispettino determinati criteri etici e tecnici.

Norme Armonizzate

- Sono norme tecniche che definiscono i mezzi e le vie per soddisfare i R.E.S. richiesti dalle direttive
- Sono prodotte dai vari comitati tecnici sotto il mandato della Commissione dell'Unione Europea
- Vengono approvate ed adottate
  - dal CEN (Comitato di Normalizzazione Europea)
  - o dal CENELEC (Comitato di Normalizzazione Elettrotecnica Europea)
- Sono quindi tradotte e pubblicate nella Gazzetta Ufficiale della Comunità Europea (GUCE) e nella Gazzetta Ufficiale di ogni Paese aderente

L'osservanza di una Norma armonizzata conferisce ai prodotti o ai servizi presunzione di conformità alle Direttive. Nella maggior parte dei casi, l'uso di norme armonizzate è facoltativo. È anche possibile scegliere un'altra soluzione tecnica purché sia garantita per il prodotto o servizio l'osservanza dei R.E.S. delle Direttive applicabili.

Fasi per la realizzazione di una Norma

1. Elaborazione di un progetto di Norma (NP, New work item proposal) che sarà esaminato dai vari Comitati nazionali interessati, per commenti, proposte e successiva approvazione
2. Formazione di un gruppo di lavoro (WG, Working Group) costituito da esperti della materia da trattare appartenenti agli Stati membri (esperti di industrie del settore, esperti di laboratori di prova, rappresentanti di organizzazioni dei lavoratori, rappresentanti dei consumatori)
3. Preparazione di una bozza WD (Working Draft) e successiva elaborazione del testo tramite step successivi:
   - In IEC: CD (Committee Draft), CDV (Committee Draft for Voting), FDIS (Final Draft International Standard)
   - In ISO: CD (Committee Draft), DIS (Draft International Standard), FDIS (Final Draft International Standard).
4. Al raggiungimento del consenso (espresso tramite voto positivo a maggioranza del documento FDIS) si procede alla stesura definitiva del testo di Norma EN, alla pubblicazione ufficiale e al recepimento a livello di ogni Stato Membro.

Periodo di validità di una norma tecnica: Cinque anni a meno che non ci sia la necessità di rivederne prima i contenuti.

Struttura di una norma tecnica di prodotto

Per facilitarne l'uso e la lettura la stragrande maggioranza delle norme tecniche di prodotto hanno la seguente struttura:

- Prefazione
- Indice
- Introduzione
- Campo di applicazione
- Riferimenti Normativi
- Termini e Definizioni (simboli e abbreviazioni)
- Requisiti di sicurezza (misure per la riduzione del rischio)
- Prove (metodi di prova tramite test o analisi per la verifica dei requisiti di sicurezza)
- Dati di targa per l'identificazione
- Informazioni per l'uso in sicurezza
- Annessi normativi opzionali (forniscono disposizioni aggiuntive oltre quelle contenute nel corpo della Norma)
- Annessi informativi opzionali (forniscono informazioni aggiuntive destinate a migliorare la comprensione e l'uso del documento)
- Annesso ZA (normativo): riferimenti normativi fra le Pubblicazioni Internazionali e le corrispondenti Pubblicazioni Europee (in questo annesso sono elencati documenti internazionali o europei che sono indispensabili per l'applicazione della norma)
- Annesso ZZ (informativo): corrispondenza fra i paragrafi, sotto-paragrafi della Norma e i R.E.S. delle direttive applicabili. Una volta che la norma viene citata nella Gazzetta ufficiale dell'Unione Europea, ai sensi di una determinata Direttiva, il rispetto delle clausole normative che sono riportate nella Tabella dell'annesso ZZ conferisce, entro i limiti del campo di applicazione della norma, una presunzione di conformità ai corrispondenti requisiti della Direttiva

Le Norme Europee legate alla sicurezza si dividono in 3 gruppi:

NORME DI TIPO A - Specificano i principi generali di progettazione applicabili a tutti i tipi di macchine:

Es. EN ISO 12100 Sicurezza del macchinario - Principi generali di progettazione - Valutazione del rischio e riduzione del rischio

NORME DI TIPO B - Si dividono in due categorie:

NORME DI TIPO B1: riguardano un aspetto specifico della sicurezza

Es.	EN ISO 13855	Posizionamento dei dispositivi elettro-sensibili di sicurezza in riferimento alla velocità di avvicinamento delle parti del corpo umano
	EN ISO 13857	Distanze di sicurezza per la protezione degli arti superiori e inferiori
	EN 60204-1	Sicurezza dell'impianto elettrico a bordo macchina ecc
	EN ISO 13849 - 1,2	Parti dei sistemi di comando relativi alla sicurezza

NORME DI TIPO B2: riguardano i dispositivi di sicurezza

Es.	EN 61496-1	Dispositivi elettro-sensibili di protezione - principi generali e prove
	EN 61496-2	Dispositivi elettro-sensibili di protezione - particolari requisiti per dispositivi che utilizzano elementi optoelettronici attivi (barriere fotoelettriche)
	EN 61496-3	Dispositivi elettro-sensibili di protezione - particolari requisiti per dispositivi fotoelettrici attivi di protezione che rispondono alla riflessione diffusa (laser scanner)
	EN ISO 13850	Dispositivi di arresto di emergenza
	EN ISO 14119	Dispositivi di interblocco associati ai ripari - Principi di progettazione e di scelta

NORME DI TIPO C - Riguardano specifici tipi di macchine.

Es.	EN ISO 16092-1	Presse - Requisiti generali
	ISO 16092-2	Presse meccaniche
	EN ISO 16092-3	Presse idrauliche
	EN 415	Macchine per imballaggio
	EN 415-4	Palettizzatori e depalettizzatori
	EN ISO 10218	Robot industriali

Una norma di tipo C è prioritaria rispetto alle norme di tipo A e B.

La norma di tipo C identifica i pericoli significativi generalmente associati alla categoria di macchina in questione e fornisce le misure protettive per affrontarli. Tuttavia, l'applicazione delle norme armonizzate non esonera completamente il produttore della macchina dall'obbligo di effettuare una valutazione del rischio. Il produttore deve infatti garantire che la norma armonizzata sia adeguata alla particolare macchina e copra tutti i rischi che presenta.

Se la macchina in questione presenta pericoli che non sono coperti da una norma di tipo C, è necessaria una valutazione completa del rischio per tali pericoli e devono essere prese adeguate misure di protezione per affrontarli. In questo caso possono essere di aiuto le norme di tipo A e B.

Le norme e gli enti di certificazione in nord America

L'Ente incaricato di sorvegliare le condizioni di sicurezza sul posto di lavoro è negli Stati Uniti la Occupational Health and Safety Administration (OSHA). Inoltre, i singoli stati dell'Unione possono avere propri organismi di sorveglianza e promulgare normative più rigorose di quelle stabilite dall'OSHA. L'OSHA verifica l'applicazione delle leggi e dei regolamenti che sono in vigore a livello federale e, a sua volta, pubblica degli standard riguardanti l'utilizzo e le caratteristiche dei dispositivi di sicurezza e/o delle macchine utensili.

Un esempio importante di tale attività è lo standard OSHA 1910.217 – Mechanical Power Presses - riguardante le presse meccaniche.

L' American National Standard Institute (ANSI) pubblica norme riguardanti la sicurezza delle macchine utensili o particolari aspetti della loro costruzione o del loro funzionamento. Per la preparazione di tali standard, l'ANSI si serve spesso del contributo di associazioni volontarie quali la Robotic Industry Association (RIA) o la Association for Manufacturing Technology (AMT).

Esempi di importanti norme ANSI:
Gli standard B11, quali:

B11.1 Mechanical Power Presses (presse meccaniche)
B11.2 Hydraulic and Pneumatic Power Presses (presse idrauliche e pneumatiche)

B11.3 Power Press Brakes (presse piegatrici)
B11.4 Shears (cesoie)
B11.19 Performance Criteria for the Design, Construction, Care and Operation of Safeguarding. When referenced by other B11 Machine Tool Safety Standards (criteri di progettazione, costruzione, manutenzione e funzionamento dei dispositivi di protezione menzionati in standard B11 riguardanti le macchine utensili).

Altre norme ANSI:

B20.1 Conveyors and related equipment (nastri trasportatori)
ANSI/RIA R15.06 Safety requirements for industrial robots (requisiti di sicurezza dei robot industriali).

In Nord America, diversamente da quanto avviene in Europa, la dichiarazione di conformità alle norme vigenti non viene accettata come autorizzazione per la vendita e l'installazione di apparecchi elettrici. Prima che una installazione possa essere operativa occorre sempre un controllo sul dispositivo o sull'impianto da parte delle autorità competenti (AHJ-Authorities Having Jurisdicion). Se però il dispositivo è già certificato (Listed) da parte di un laboratorio riconosciuto (NRTL – Nationally Recognized Testing Laboratory), allora l'autorità competente è autorizzata a non verificare ulteriormente il prodotto. Il marchio di un NRTL assume in questo caso la valenza di conformità del prodotto agli standard di sicurezza.

In Nord America quindi la certificazione, anche se non obbligatoria, rende molto più agevole e sicura la vendita perché rivenditori, ispettori, utilizzatori, autorità locali accettano all'unanimità i prodotti marcati da un NRTL. Vale la pena ricordare ancora che quando una installazione è certificata esistono agevolazioni dal punto di vista assicurativo e maggiori garanzie nel senso che i sindacati potrebbero rifiutarsi di far lavorare i loro iscritti su macchine pericolose non certificate.

L'ente preposto al riconoscimento di un NRTL è l' OSHA.

Gli NRTL devono ottenere l'accreditamento per tutte le sedi nazionali ed estere per tutti i prodotti per i quali sono autorizzati a rilasciare certificazioni. Per ottenere l'accreditamento occorre, fra l'altro, dimostrare completa indipendenza da utenti, fornitori o rivenditori dei prodotti certificati. Un NRTL può sviluppare e far approvare sue norme oppure usare norme prodotte da altri NRTL. Ogni NRTL possiede un marchio univoco.

Fra gli NRTL autorizzati a rilasciare certificazioni per apparecchi e impianti elettrici uno dei più importanti è l' Underwriters Laboratories Inc. (UL).

Il Marchio di Certificazione UL Listed indica che il prodotto è stato sottoposto a test e a valutazioni secondo le norme di sicurezza statunitensi. Il marchio UL Listed generico certifica quindi la conformità ai requisiti antincendio e di sicurezza elettrica.

L'UL certifica anche componenti quali le barriere di sicurezza in base ai propri standard UL 61496-1 e UL 61496-2 che derivano dagli standard internazionali IEC 61496-1,2. Inoltre, i sistemi che incorporano software di sicurezza possono essere certificati secondo la norma specifica ANSI/UL 1998. Per le barriere fotoelettriche di sicurezza (ESPE) è prevista un'apposita marcatura che sancisce la rispondenza alla specifica norma di prodotto e alla ANSI/1998. Le barriere di sicurezza Reer rispondono a tutti questi requisiti e riportano questa marcatura.

L'UL può anche certificare la conformità con gli standard canadesi, per conto del CSA (conferendo l'apposito marchio C-UL oppure il marchio C-UL-US per prodotti diretti sia al mercato canadese che a quello statunitense).

La Canadian Standard Association (CSA) è il principale organismo di standardizzazione canadese, che funge anche da ente di certificazione per quanto riguarda la conformità dei componenti di sicurezza alle norme canadesi.

Come Nationally Recognised Test Laboratory (NRTL) americano, il CSA può testare la conformità di tutti i prodotti sotto la giurisdizione dell'OSHA e conferire il marchio CSA NRTL/C, equivalente al C-US UL; tale marchio si applica per esempio alle barriere di sicurezza.

ISO 12100:2012 - Sicurezza del macchinario - Principi generali per la progettazione - Valutazione e riduzione del rischio

Le macchine e gli impianti, per la loro funzionalità, rappresentano potenziali rischi per i lavoratori. Se una macchina può presentare dei pericoli, è necessaria una valutazione del rischio e, se pertinente, deve essere intrapresa una riduzione del rischio per portarlo ad un livello accettabile.

La ISO 12100 fornisce una metodologia per la progettazione di macchine che sicure per l'utilizzo previsto.

Dà disposizioni:

- Per l'identificazione dei pericoli
- Per la stima e la valutazione dei rischi associati alla macchina
- Su come eliminare i pericoli o fornire una sufficiente riduzione dei rischi

ISO 12100 è uno standard di tipo A.

Per gli Stati Uniti informazioni equivalenti sono fornite in ANSI 12100.

Strategia per la valutazione e la riduzione del rischio

La valutazione del rischio è un metodo completo per consentire, in modo sistematico, l'analisi e la valutazione dei rischi. Deve essere eseguito in fase di progettazione, costruzione e messa in servizio del macchinario e ogni volta che vengono apportate modifiche. Può essere utilizzato anche per la valutazione di macchinari esistenti se, ad esempio, si sono verificati incidenti o malfunzionamenti.

Per attuare la valutazione e la riduzione del rischio devono essere intraprese le seguenti azioni

1. Analisi del rischio: per determinare i limiti della macchina, che includono l'uso previsto e qualsiasi uso improprio ragionevolmente prevedibile. Inoltre per identificare i pericoli e le situazioni pericolose associate alle attività della persona (tutte le salvaguardie dovrebbero essere ignorate mentre viene eseguita l'identificazione del pericolo).
2. Valutazione del rischio: per valutare il rischio di ogni pericolo e situazione pericolosa identificate e prendere decisioni sulla necessità di ridurre il rischio.
3. Riduzione del rischio: Se il pericolo non può essere eliminato, ridurre il rischio associato implementando misure di protezione.

Il processo è iterativo e possono essere necessarie diverse applicazioni successive.

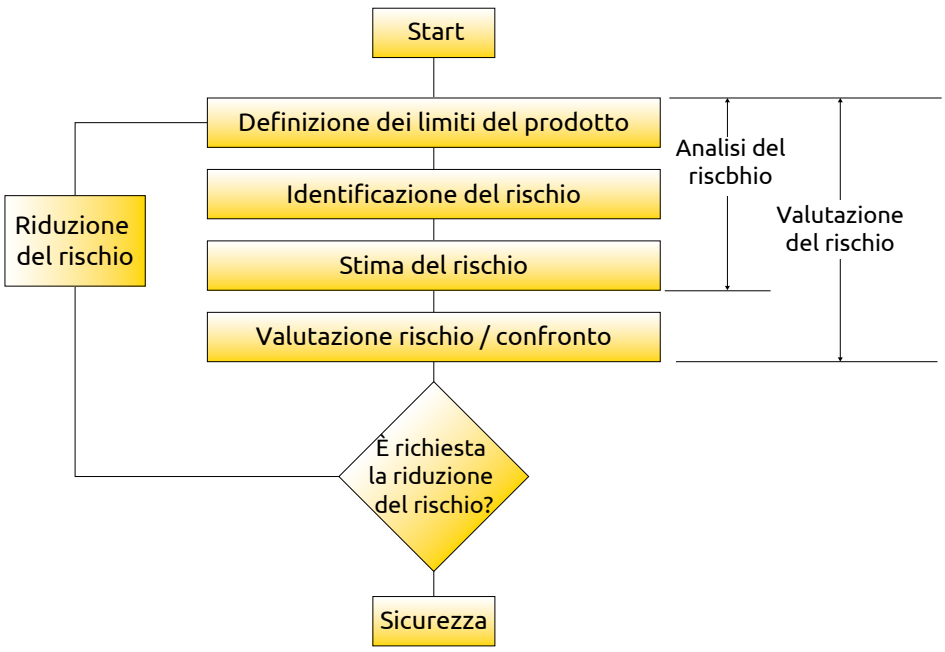


Fig. 1. Strategia per la valutazione e la riduzione del rischio

L'obiettivo da raggiungere è ridurre il rischio a un livello accettabile (tollerabile) considerando che la riduzione del rischio ottenuta: deve essere efficace in tutte le fasi del ciclo di vita della macchina e non deve pregiudicare le funzioni e l'usabilità della stessa.

Quando vengono apportate modifiche al processo o alla macchina oppure se vengono aggiunte delle nuove misure di protezione, tutte le fasi della valutazione del rischio devono essere ripetute per verificare se:

- Sono state apportate modifiche ai limiti operativi della macchina
- Sono stati introdotti nuovi pericoli o situazioni pericolose
- Il livello di rischio di eventuali situazioni pericolose esistenti è stato aumentato
- Le misure di protezione aggiunte sono efficaci nel ridurre il rischio
- La riduzione del rischio prevista è stata raggiunta

Il raggiungimento della necessaria riduzione del rischio è solo uno delle informazioni per la decisione di interrompere il processo iterativo di riduzione del rischio. Questa decisione dovrebbe comportare considerazioni aggiuntive come regolamenti, leggi nazionali e organizzazione del lavoro.

1 - Analisi del rischio

Determinazione del limite della macchina

Il primo passo dell'analisi del rischio consiste nel fornire una chiara descrizione delle capacità meccaniche, fisiche e funzionali della macchina. Determinare i limiti di spazio della macchina, significa determinare la gamma di movimenti, i requisiti di spazio per le persone che interagiscono con la macchina (anche durante la manutenzione) il tipo di interazione umana, i limiti ambientali di funzionamento (temperature minime e massime, ambiente asciutto o bagnato e intemperie, tolleranza alla polvere, ecc.), diverse modalità di funzionamento, interfaccia di alimentazione.

Identificazione dei pericoli

Dopo aver determinato i limiti della macchina, il passaggio essenziale in qualsiasi valutazione del rischio della macchina è l'identificazione sistematica dei pericoli ragionevolmente prevedibili che possono insorgere durante l'intero ciclo di vita (trasporto, installazione, messa in servizio, uso, disabilitazione, smontaggio). Solo se tutti i pericoli sono identificati correttamente, è possibile intervenire per ridurre i rischi associati. Pericoli non identificati possono causare lesioni. È quindi importante garantire che l'identificazione dei pericoli sia sistematica e completa.

Per realizzare l'identificazione del pericolo, è necessario identificare:

- Le operazioni che devono essere eseguite dal macchinario
- I compiti che devono essere eseguiti dalle persone che interagiscono con la macchina, considerando comportamenti non intenzionali o un uso improprio ragionevolmente prevedibile della macchina
- Le caratteristiche dei materiali da lavorare
- L'ambiente in cui la macchina può essere utilizzata

Pericoli generati dall'interazione uomo-macchina	Pericoli genenrati dalla macchina
Impostazioni	Pericoli elettrici
Verifiche	Pericoli meccanici
Programmazione	Pericoli legati alla temperatura
Caricamento e scaricamento manuale	Pericoli generati dal rumore
Canbio degli attrezzi	Pericoli generati dalle vibrazioni
Partenza e arresto dellla macchina	Pericoli generati dalle radiazioni
Ripartenza dopo un arresto imprevisto	Pericoli generati dal materiale
Pulizia e manutenzione	Pericoli relativi all'ambiente
Manutenzione preventiva e riparazioni	Pericoli realtivi all'emissione di sostanze

2 - Valutazione del rischio

Una volta identificati i pericoli e le situazioni pericolose, è necessario effettuare una stima dei rischi associati a ciascun pericolo e a ciascuna situazione pericolosa. Convertire l'impatto del rischio in termini numerici è un compito difficile perché non esiste una scala di rischio universale. La ISO 12100 ha deciso di definire il rischio come una combinazione della gravità del danno e della probabilità di accadimento di tale danno.

Il rischio può quindi essere misurato creando una scala basata sul prodotto di conseguenza (in termini di danno alle persone) e probabilità di accadimento (probabilità che un evento causi lesioni).

Rischio = Conseguenza del danno x probabilità di accadimento

Tipicamente, per migliorare l'accuratezza della stima della probabilità di accadimento del danno, vengono aggiunti parametri come la frequenza e la durata dell'esposizione al pericolo, la probabilità che si verifichi un evento pericoloso e le possibilità tecniche e umane di evitare o limitare il danno.

RISCHIO relativo al pericolo considerato — è una funzione di — GRAVITÀ DEL DANNO che può derivare dal pericolo considerato — e — PROBABILITÀ CHE SI VERIFICHI IL DANNO
- Esposizione delle persone al pericolo
- verificarsi di un evento pericoloso
- possibilità di evitare o limitare il danno

La formula diventa:

Rischio = Conseguenza del danno x (tempo di esposizione + possibilità di accadimento + possibilità di evitare o limitare il danno)

È stata sviluppata una varietà di strumenti che aiutano il progettista in questo processo di valutazione del rischio, tra cui tabelle, grafici di rischio, metodi numerici.

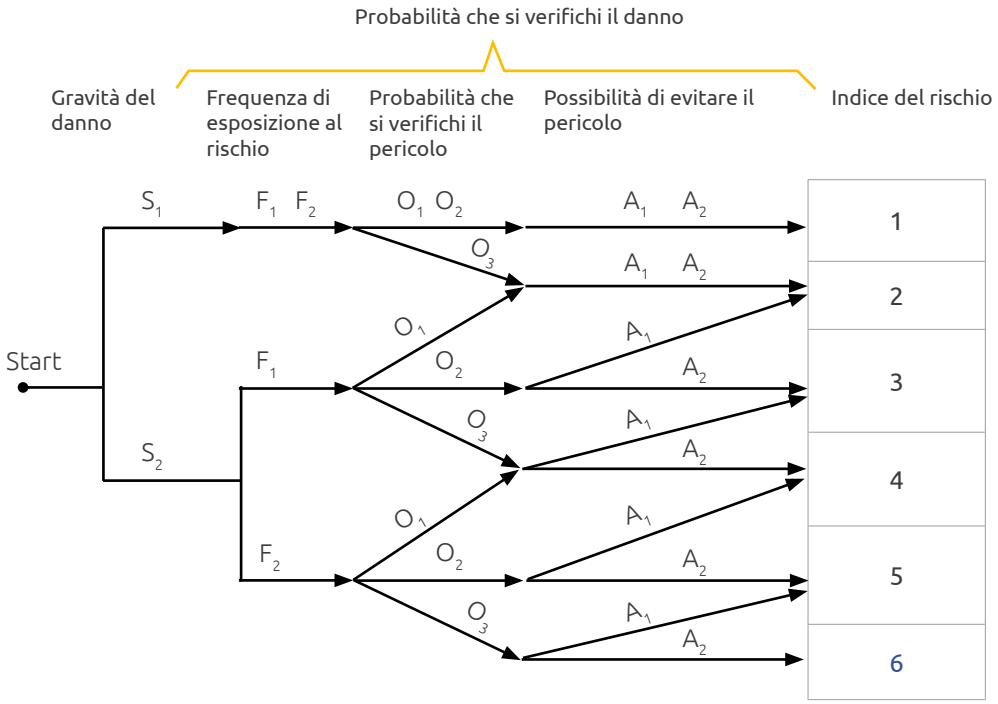
Esempio di grafico del rischio

S: gravità della lesione
S1: reversibile
S2: irreversibile o morto

F: frequenza o tempo di esposizione al pericolo
F1: raro / corto
F2: continuo prolungato

O: probabilità di accadimento del pericolo
O1: molto basso
O2: basso
O3: alto

A: rischio evitabile o limitazione del danno
A1: possibile
A2: impossibile



Esempio matrice del rischio

Conseguenze	Gravità	Class Cl (Fr+P+Av)				
	G	3-4	5-7	8-10	11-13	14-15
Morte, perdita di un occhio o di un braccio	4					
Permanente: perdita di dita	3					
Reversibile: intervento medico	2					
Reversibile: pronto soccorso	1					

rischio inaccettabile
rischio moderato
rischio tollerabile

Frequenza di esposizione al rischio, Fr	
≥ 1 per ora	5
< 1 per ora ≥ 1 per giorno	5
< 1 per giorno ≥ 1 per 2 settimane	4
< 1 per 2 settimane ≥ 1 per 1 anno	3
< 1 per anno	2

Probabilità evento pericoloso, P	
Molto alta	5
Probabile	4
Possibile	3
Scarsa	2
Trascurabile	1

Probabilità di evitare o limitare il danno, Av	
Impossibile	5
Possibile	3
Probabile	1

Fig. 2. Esempio matrice del rischio

La scelta del metodo da utilizzare per la stima del rischio è in gran parte legata al tipo di macchinario e alla natura dei pericoli. È inoltre necessario tenere conto delle capacità, dell'esperienza e delle preferenze del professionista che realizza la valutazione.

Il rispetto delle regole per la stima del rischio è più importante che cercare di raggiungere l'accuratezza assoluta dei risultati.

3 - Principi di riduzione del rischio

Dopo che la valutazione del rischio è stata definita, deve essere effettuata un'analisi per determinare se eventuali situazioni pericolose che richiedono un'ulteriore riduzione del rischio. Implementare la riduzione del rischio significa ridurrlo ad un livello “accettabile” di rischio residuo per le persone.

Sicurezza non significa zero rischi

Il rischio zero possibile solo quando il pericolo è COMPLETA-MENTE rimosso

Sicurezza significa libertà da rischi inaccettabili

In generale, i costruttori concordano sul fatto che una strategia di riduzione del rischio dovrebbe utilizzare un approccio gerarchico denominato metodo in tre fasi.

Il metodo in tre fasi deve essere applicato nella seguente sequenza:

- Fase 1 integrazione dei concetti di sicurezza in fase di progettazione
- Fase 2 aggiungere misure di protezione contro i rischi che non possono essere rimossi dalla progettazione
- Fase 3 informare e mettere in guardia sui rischi residui

Fase 1: integrazione dei concetti di sicurezza in fase di progettazione

La progettazione intrinsecamente sicura è il primo e più importante passo nel processo di riduzione del rischio. È probabile che le misure di protezione, che sono parte integrante della progettazione della macchina, rimangano efficaci mentre l'esperienza ha dimostrato che anche una protezione ben progettata può fallire o può essere violata. Inoltre è possibile che le informazioni per l'uso non vengano seguite correttamente.

Si ottengono misure di progettazione intrinsecamente sicure:

a. Attraverso un'adeguata scelta delle caratteristiche di progettazione meccanica, ad esempio, evitando spigoli vivi, angoli e parti sporgenti, evitando punti di schiacciamento, punti di taglio e punti di aggrovigliamento
b. Progettando macchine in modo da avere una stabilità sufficiente nelle condizioni d'uso specificate. I fattori da considerare includono
   - La geometria della base e la distribuzione del peso, compreso il carico
   - Le forze dinamiche dovute ai movimenti di parti della macchina o di elementi trattenuti dalla macchina che possono determinare un momento ribaltante
   - Vibrazioni, oscillazioni
c. Riducendo l'interazione tra le persone esposte e la macchina. Questo obiettivo può essere raggiunto limitando il tempo di esposizione al pericolo, ad esempio mediante:
   - Stazioni di carico e scarico automatiche
   - Lavori di installazione e manutenzione dall'esterno delle zone pericolose
   - Utilizzo di componenti affidabili per ridurre i lavori di manutenzione
   - Concetto operativo chiaro e inequivocabile (ad es. marcatura precisa dei comandi)
   - Utilizzo della procedura di Lock-Out/Tag-Out
d. Limitando l'esposizione all'alimentazione elettrica (contatto diretto e indiretto) Un'alimentazione stabile è particolarmente importante nelle applicazioni legate alla sicurezza. Gli alimentatori devono resistere a brevi interruzioni di corrente. Per ogni collegamento di alimentazione deve essere previsto un dispositivo di isolamento dell'alimentazione. Per gli alimentatori a 24 V CC, utilizzare un circuito di Classe 2 che offre protezione contro l'innesco di incendi e scosse elettriche. Un'altra opzione per fornire protezione contro le scosse elettriche consiste nell'utilizzare una bassissima tensione di sicurezza (SELV, PELV).
e. Utilizzando involucri idonei per la protezione dei componenti elettrici. Le custodie per apparecchiature elettriche devono soddisfare i requisiti per le classificazioni delle custodie. Due sistemi di classificazione ampiamente accettati sono i tipi/numero NEMA e il codice di classificazione IP.

   Le classificazioni delle custodie descrivono la protezione contro l'ingresso di acqua e corpi estranei (polvere). Inoltre, descrivono la protezione contro il contatto diretto con parti in tensione.

   NEMA (National Electric Manufacturers' Association) è comunemente specificato nelle installazioni negli Stati Uniti IP (International Protection), deriva dalla IEC ed è tipicamente utilizzato in Europa.

   Tipicamente, gli armadi di controllo dovrebbero essere NEMA 13 o IP 54.
f. Selezionando componenti immuni ai disturbi previsti. La macchina ed i componenti utilizzati devono essere scelti in modo da essere immuni ai disturbi elettromagnetici previsti. Requisiti più elevati si applicano ai componenti di sicurezza. Le seguenti linee guida di progettazione aiuteranno a prevenire i problemi EMC:
   - Collegamento equipotenziale continuo mediante connessioni conduttive tra parti di macchinari e sistemi
   - Separazione fisica dall'unità di alimentazione (alimentazione/sistemi attuatori/inverter)
   - Lo schermo non deve essere utilizzato per trasportare correnti di collegamento equipotenziale
   - Collegare l'eventuale messa a terra/messa a terra funzionale (FE) fornita
   - Utilizzo di cavi twistati per la trasmissione dei dati (bus di campo)
g. Impedendo l'avvio imprevisto. L'allacciamento alla rete elettrica o l'accensione di un'alimentazione esterna non devono comportare l'avviamento delle parti funzionanti di una macchina.

   Deve essere impedito un riavvio spontaneo di una macchina dopo un'interruzione dell'alimentazione (ad esempio, mediante l'uso di un relè, un contattore o una valvola automantenuti).

   Ogni macchina deve essere dotata di un comando per l'arresto della macchina durante il normale funzionamento.

Un comando di arresto della macchina deve avere una priorità maggiore rispetto ai comandi di messa in funzione della macchina.

Deve essere disponibile almeno una funzione di arresto di categoria 0.

Categoria di arresto 0: arresto incontrollato togliendo immediatamente alimentazione agli attuatori della macchina (elementi di azionamento)

Categoria di arresto 1: arresto controllato con alimentazione disponibile agli attuatori della macchina per raggiungere l'arresto, quindi l'alimentazione viene rimossa quando viene raggiunto l'arresto

Categoria di arresto 2: arresto controllato con alimentazione lasciata disponibile per l'attuatore della macchina

Fase 2 - Riduzione del rischio mediante misure di protezione

Se i pericoli non possono essere rimossi o i rischi non possono essere adeguatamente ridotti mediante misure di progettazione intrinsecamente sicure, devono essere applicate misure di protezione aggiuntive, disposte in modo da ridurre la probabilità che si verifichi l'evento pericoloso eliminando le cause probabili o imporre una limitazione esposizione ai pericoli o per aumentare la possibilità di evitare il danno o almeno riducendone l'intensità.

Le misure di protezione possono essere passive, attive, complementari.

Misure protettive passive

Sono indipendenti dal sistema di controllo della macchina e non necessitano di essere attivati per svolgere la loro funzione di riduzione del rischio, sono efficaci in modo continuo. Vengono utilizzati quando non è richiesto l'accesso alla zona pericolosa durante il normale funzionamento.

Esempi di misure di protezione passiva sono le protezioni permanenti t (saldate al corpo macchina) e le recinzioni amovibili che possono essere rimosse solo a macchina ferma con apposito attrezzo non facilmente a disposizione degli operatori. Forniscono protezione riducendo la durata dell'esposizione al pericolo.

Misure protettive attive

Le misure di protezione attive vengono attivate in risposta a una modifica definita di una proprietà misurabile di un ingresso (ad es. un sensore o un interruttore). Hanno lo scopo di ridurre il rischio generato dai seguenti eventi:

a. Interazione umana con la macchina
   È possibile che una persona, coinvolta in un determinato processo della macchina, con il suo comportamento si esponga a pericolosi movimenti della macchina.

   Esempi di misure di protezione attiva idonee a ridurre i rischi generati dall'interazione umana con la macchina sono gli ESPE, le pedane di sicurezza, i dispositivi di abilitazione, i dispositivi di comando a uomo presente, i ripari di interblocco.
   Forniscono protezione riducendo la probabilità di accadimento del danno.

   Sono destinati a lavorare immediatamente su uno specifico evento di avvio. Il loro ruolo è garantire che persone o parti del corpo umano non vengano ferite dalle parti pericolose della macchina.

   La "domanda" di protezione è generata dalla persona con la sua interazione (operazioni) con il processo macchina.

b. Guasti del sistema di controllo dell'automazione della macchina (MCS)
   È possibile che un guasto di un componente del sistema di controllo dell'automazione della macchina coinvolto in un determinato processo della macchina possa generare situazioni pericolose come aumento di superfici calde, fiamme, vibrazioni eccessive, esplosioni ecc.

   Esempi di misure di protezione attiva idonee a ridurre il rischio dovuto a guasti ai componenti del sistema di controllo dell'automazione della macchina sono i limitatori di coppia, i limitatori di pressione o temperatura, i limitatori di velocità eccessiva, i dispositivi di monitoraggio dell'emissione di radiazioni o gas, i rivelatori di incendio e di fumo.
   Forniscono protezione riducendo la probabilità di accadimento del danno.

   Sono impiegati come mezzo di prevenzione e sono destinati a funzionare prima che si verifichi uno specifico evento di avvio. Il loro ruolo è quello di garantire che l'incidente non avvenga, o almeno di rallentarne lo sviluppo o di limitare a un livello accettabile la deviazione del processo.

   La “domanda” viene generata a causa di un guasto del sistema di automazione della macchina.

c. Uso improprio della macchina.
È possibile che un uso intenso della macchina dovuto alla pressione del tempo o ad elevate sollecitazioni dovute a carichi eccessivi o alla lavorazione di materiale non idoneo possa portare la macchina a lavorare al di fuori dei suoi limiti di progettazione che a sua volta possono generare guasti meccanici della macchina stessa o danneggiamento della merce da lavorare e, in una seconda fase, può generare rischi per le persone.

Esempi di misure di protezione attiva idonee a ridurre il rischio dovuto ad un uso improprio sono limitatori di coppia, limitatori di pressione, limitatori di sovravelocità, sensori estensimetrici, sensori di sovraccarico di corrente. Forniscono protezione riducendo la probabilità di accadimento del danno.

La “domanda” è generata dal sovraccarico della macchina a causa del suo uso improprio.

NOTA: Laddove una misura di protezione sia implementata attraverso il sistema di controllo relativo alla sicurezza della macchina, è consigliabile utilizzare i metodi descritti nella ISO EN ISO 13849-1 o EN IEC 62061 per la stima del rischio perché forniscono automaticamente la corrispondenza tra i PL / SIL richiesto e rischio stimato.

Misure protettive complementari

Per ottenere un'ulteriore riduzione del rischio, può essere necessario utilizzare misure di protezione complementari in considerazione dell'uso previsto e dell'uso improprio ragionevolmente prevedibile della macchina.

Le misure di protezione complementari il cui principale effetto è quello di evitare o limitare i danni sono l'arresto di emergenza, le misure per consentire un accesso sicuro ai macchinari, le misure per la fuga e il salvataggio delle persone intrappolate.

NOTA: l'arresto di emergenza non è considerato una protezione primaria perché non impedisce o rileva l'accesso a una zona pericolosa. Il livello di sicurezza deve essere definito in base alla valutazione del rischio della macchina.

Protezioni complementari il cui effetto principale è quello di ridurre la durata dell'esposizione al pericolo sono dispositivi idonei all'isolamento energetico come valvole di intercettazione e interruttori di isolamento, dispositivi idonei alla dissipazione dell'energia come valvole limitatrici di pressione, blocchi meccanici per impedire movimenti.

Fase 3 - Riduzione del rischio mediante misure amministrative

Per garantire che le misure di protezione passive, attive e complementari implementate rimangano efficaci durante tutto il ciclo di vita della macchina sono necessarie ulteriori azioni basate su procedure e organizzazione.

a. Procedure per la manutenzione.
La mancanza di manutenzione (scarsa lubrificazione e perdita di liquido di raffreddamento) può portare a guasti o errori meccanici. Per ridurre questo tipo di rischi, è necessario sviluppare e implementare istruzioni dettagliate per la manutenzione.

b. Provvedimenti amministrativi - Procedure organizzative del lavoro.
Dovrebbero essere operative almeno le seguenti misure organizzative:
   - Ruoli e responsabilità ben definiti dei lavoratori, dei supervisori e della direzione
   - Un piano per la formazione periodica dei lavoratori
   - Disponibilità di strumenti idonei per la manutenzione e le verifiche
   - Un piano di ispezioni periodiche per verificare l'integrità delle protezioni
   - Un piano per la fuga e per le procedure di emergenza
   - Mezzi per tenere traccia delle verifiche periodiche

c. Informazioni per l'uso. Le informazioni per l'uso sono parte integrante della progettazione di una macchina
   - Informa l'utente sull'uso previsto della macchina
   - Deve contenere tutte le indicazioni necessarie per garantire un uso sicuro e corretto della macchina
   - Informa e avverte l'utente del rischio residuo
   - Indica, se del caso, la necessità di dispositivi di protezione individuale

Segnali visivi, come luci lampeggianti e segnali acustici come le sirene, possono essere utilizzati per avvertire di un evento pericoloso imminente come l'avvio della macchina o la velocità eccessiva.

Tali segnali devono essere emessi prima del verificarsi dell'evento pericoloso ed essere differenziati da tutti gli altri segnali utilizzati.

Laddove le informazioni per l'uso siano conservate in formato elettronico (CD, DVD, nastro, disco rigido, ecc.), le informazioni su questioni relative alla sicurezza che richiedono un'azione immediata devono sempre essere supportate da una copia cartacea prontamente disponibile.

Funzione di sicurezza come misura di protezione “attiva”.

Le misure di protezione attiva vengono generalmente implementate selezionando e combinando in modo appropriato componenti hardware (come sensori, interruttori, unità logiche, relè, ecc.) per costruire un sistema di controllo relativo alla sicurezza.

Si dice che un sistema di controllo che esegue una misura di protezione attiva svolga una funzione di sicurezza e il sistema di controllo stesso è chiamato Safety Related Control System. In macchine complesse può accadere che più movimenti pericolosi possano potenzialmente ferire l'operatore. Per ogni pericolo per il quale è necessaria una misura di protezione attiva, deve essere implementata una funzione di sicurezza corrispondente.

Può quindi accadere che lo stesso sistema di controllo relativo alla sicurezza debba gestire più funzioni di sicurezza.

Quando una funzione di sicurezza è attivata, la macchina viene portata in uno stato di sicurezza in tempo prima che si possa verificare una situazione pericolosa per le persone.

Elenco delle tipiche funzioni di sicurezza atte a ridurre il rischio originato dalle interazioni uomo-macchina.

Funzioni di sicurezza	Esempi di applicazioni
Funzione di arresto, relativa alla sicurezza, avviata da una protezione	Arrestare un motore in risposta all'intervento di un dispositivo di protezione
Funzione di Reset manuale	Azione destinata a ristabilire la salvaguardia dopo la sua attuazione. Riconoscimento che il rischio non è più presente
Funzione di Start/restart	L'inizio di un movimento pericoloso può avvenire solo quando una situazione pericolosa non esiste più
Funzione di Muting	Sospensione temporanea automatica di una funzione di sicurezza
Funzione Hold-to-run	I movimenti pericolosi della macchina possono essere controllati da una posizione all'interno della zona di pericolo, ad es. la modalità a impulsi durante l'impostazione
Prevenzione di avviamenti imprevisti	Mantenere una macchina ferma mentre le persone sono presenti nelle zone pericolose
Selezione della modalità operativa	Attivazione delle funzioni di sicurezza tramite un selettore della modalità di funzionamento
Movimento sicuro, posizione sicura	Sovravelocità, controllo extracorsa

Elenco delle tipiche funzioni di sicurezza idonee a ridurre i rischi originati da guasti dell'MCS

Controllo o limitazione di	
Velocità	Temperatura
Coppia	Posizione
Alimentazione	Tempo di arresto
Pressione	Distanza di arresto

Struttura di una funzione di sicurezza

Una funzione di sicurezza in genere inizia con il rilevamento e la valutazione di un "evento di avvio" e termina con un'uscita che provoca un'azione su un "attuatore macchina"

Realizzazione di una funzione di sicurezza

Una funzione di sicurezza è solitamente costituita da una combinazione in serie di tre sottofunzioni che svolgono rispettivamente i compiti di rilevamento, valutazione e azione.

Ciascuna sottofunzione può essere implementata da:

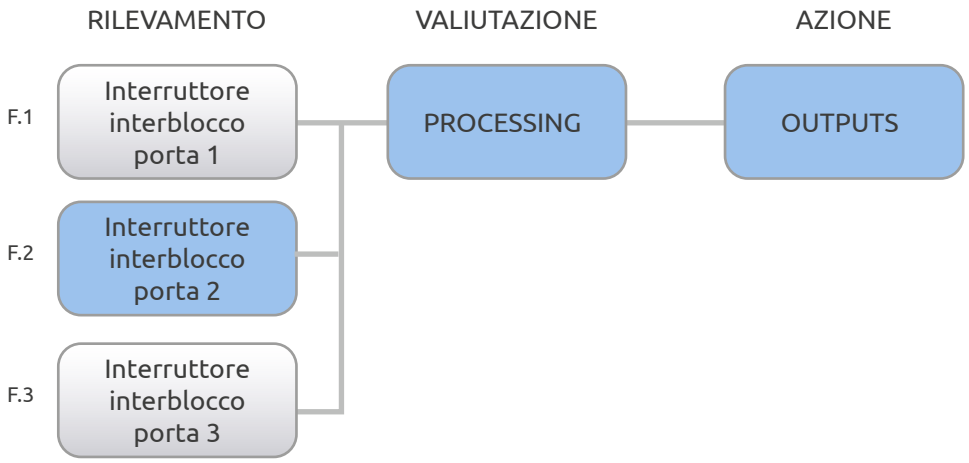
- Utilizzo di sottosistemi precedentemente convalidati
- Progettazione di nuovi sottosistemi
- Una combinazione di entrambe le alternative

Qualsiasi delle tecnologie disponibili (elettrica, idraulica, pneumatica, meccanica) può essere utilizzata singolarmente o in combinazione.

Esempio:

Un movimento pericoloso è protetto da una recinzione munita di cinque ripari. L'apertura di una delle cinque porte interrompe il movimento pericoloso.

Si possono considerare quattro funzioni di sicurezza separate, una per ogni porta, se si presume che venga aperta una sola porta alla volta.



Per esempio. Per la funzione di sicurezza F. 2, riferita alla porta n°2, nel computo della funzione di sicurezza vengono considerati solo i blocchi evidenziati in azzurro.

Integrazione di un sistema di controllo relativo alla sicurezza nel sistema di controllo della macchina

Per l'integrazione di un sistema di controllo relativo alla sicurezza nel sistema di controllo della macchina (MCS) devono essere applicati i seguenti principi:

- Il sistema di controllo relativo alla sicurezza è separato e indipendente dall'MCS
- Il sistema di controllo relativo alla sicurezza è destinato esclusivamente alla protezione diretta o indiretta delle persone; non partecipa attivamente al processo della macchina e si attiva solo al verificarsi di una situazione di pericolo

- L'affidabilità dell'MCS non assume alcun ruolo per l'esecuzione della funzione di sicurezza. È l'affidabilità del sistema di controllo relativo alla sicurezza a destare preoccupazione; maggiore è la probabilità che una persona sia esposta al rischio, maggiore dovrebbe essere la disponibilità del sistema di controllo relativo alla sicurezza
- Quando si verifica un guasto pericoloso nel sistema di controllo relativo alla sicurezza, la macchina viene portata in uno stato sicuro. Il riavvio del processo della macchina è accettato solo dopo la riparazione e il ripristino del sistema di controllo relativo alla sicurezza
- È anche possibile che un sistema di controllo relativo alla sicurezza esegua funzioni di sicurezza e funzioni di comando della macchina (ad esempio una barriera fotoelettrica di sicurezza o un dispositivo di controllo a due mani possono essere utilizzati sia per la protezione che per il riavvio del ciclo).

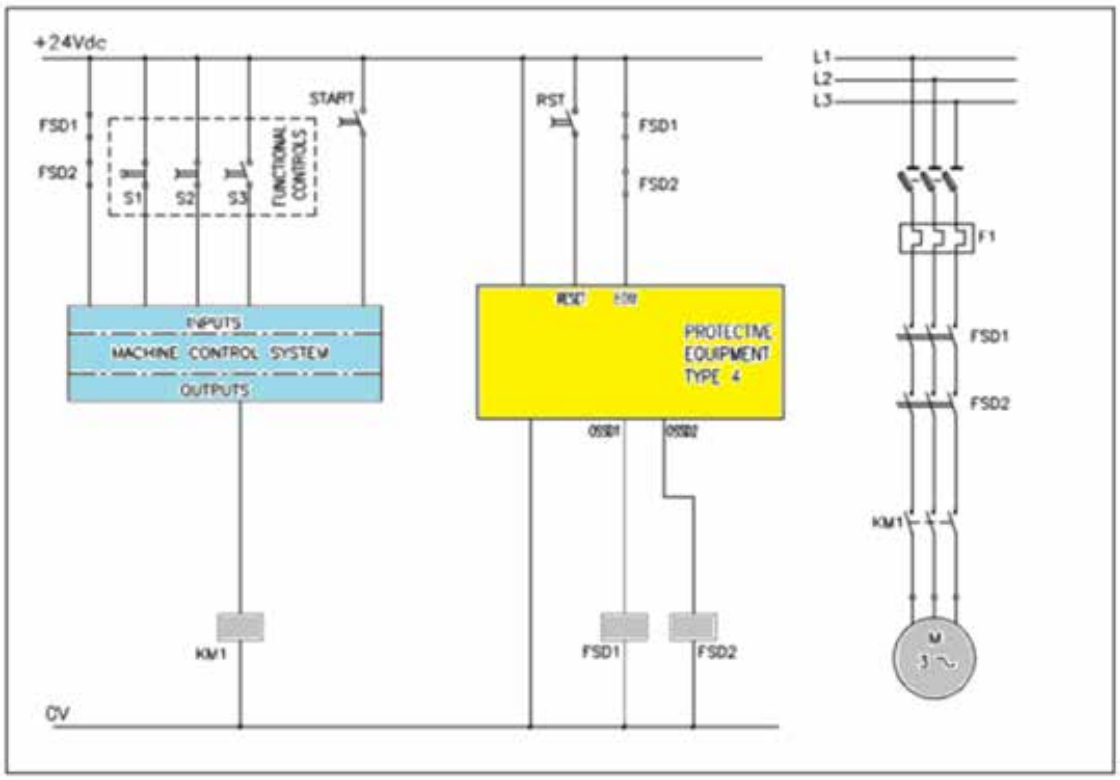
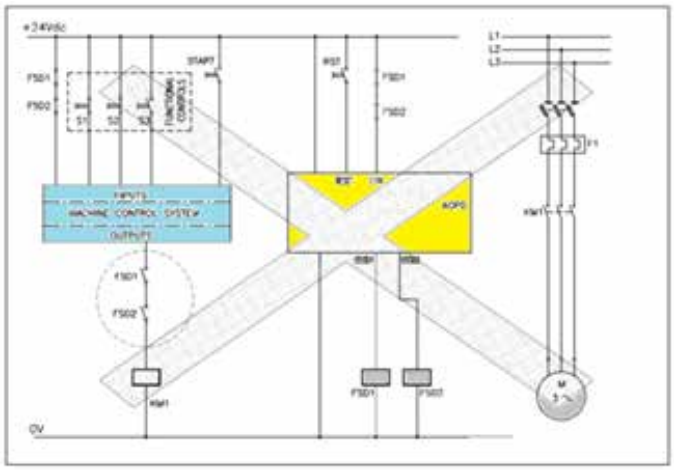
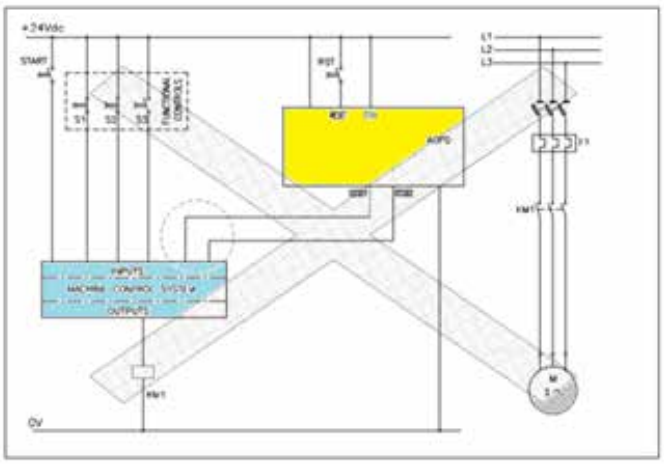


Fig. 3. Esempio di integrazione di un sistema di controllo relativo alla sicurezza con un PLC



La mancata apertura (ad es. per contatti saldati) di KM1 impedisce l'arresto del motore.



Se le uscite dell'SRP/CS sono collegate agli ingressi di un PLC standard (non di sicurezza), i guasti hw e sw all'interno del PLC o il guasto del KM1 possono impedire l'arresto del motore.

Fig. 4. Esempi di errata integrazione

Le norme sulla sicurezza funzionale

Quando la sicurezza è subordinata al buon funzionamento del sistema di controllo della macchina, questo deve essere concepito in modo che la probabilità di suoi errori funzionali sia sufficientemente bassa. Se questo non è possibile, gli eventuali errori non devono portare alla perdita della funzione di sicurezza. Per soddisfare questi requisiti è consigliabile utilizzare le norme armonizzate create con il mandato della Commissione Europea (presunzione di conformità). Infatti, l'uso delle norme armonizzate permette di evitare perdite di tempo e costi supplementari nel caso occorra dimostrare la conformità del sistema di controllo di sicurezza ai requisiti essenziali della Direttiva Macchine.

Nel seguito sono esposti i principi fondamentali delle norme ISO 13849-1 e la IEC 62061- che sono le più usate nella progettazione delle funzioni di sicurezza dei sistemi di controllo delle macchine.

Entro i limiti dello scopo e del campo di applicazione queste due norme forniscono presunzione di conformità con i requisiti essenziali elencati nel paragrafo 1.2.1 dell'allegato I della direttiva 2006/46/CE.

I contenuti qui illustrati si riferiscono alle edizioni in vigore EN 13849-1: 2015 e EN 62061:2005 + AMD1: 2012+ AMD2: 2015

NOTA: Sono in avanzata fase di elaborazione le nuove edizioni che probabilmente vedranno la luce nel 2021

ISO 13849-1,2 Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza – Principi generali per la progettazione

Le EN ISO 13849-1,2 sono utilizzate nell'ambito della riduzione sistematica dei rischi descritta nella ISO 12100 per la parte che riguarda il progetto del sistema di controllo di sicurezza della macchina.

La norma ISO 13849-1 serve appunto come guida per progettare le parti del sistema di comando che servono per realizzare le funzioni di sicurezza. Si può usare per tutti i tipi di macchinari indipendentemente dal tipo di tecnologia utilizzata (elettrica, idraulica, pneumatica, ecc.) Queste parti possono essere costituite da hardware e/o software e possono essere separate dal sistema di comando della macchina o farne parte integrante.

La ISO 13849-1 è applicabile solo nel caso che la funzione di protezione sia richiesta con frequenza superiore a una volta all'anno (funzionamento in High demand mode) oppure sia richiesta costantemente (Continuous mode of operation) perchè le tabelle e le formule contenute nella norma sono relative a questi due tipi di funzionamento.

Esempi di prodotti che sono comunemente integrati in un sistema di controllo di sicurezza sono: relè, elettrovalvole, interruttori di posizione, PLC, moduli di sicurezza configurabili, controlli motore, dispositivi di comando a due mani, apparecchiature sensibili alla pressione, barriere fotoelettriche, laser scanner.

Le parti del sistema di controllo della macchina legate alla sicurezza sono indicate con l'acronimo SRP/CS (Safety Related Parts of Control System).

Oltre all'implementazione le funzioni di sicurezza, un SRP/CS può anche implementare funzioni operative, ma solo le parti legate alla sicurezza rientrano nell'ambito di applicazione della norma.

Per valutare il livello di prestazione di sicurezza di un SRP/CS, si usa il termine **PL** (*Performance Level*) che sta a indicare la capacità di un SRP/CS di garantire una riduzione dei rischi adeguata entro predefinite condizioni di funzionamento.

Il livello di prestazione è misurato con una scala a 5 livelli, da PLa a PLe; ad ogni livello è associato un intervallo di valori di probabilità media di guasto pericoloso (PFH_D).

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

Fig. 5. La Tabella della norma: Performance levels (PL)

Valutazione del rischio e assegnazione del Performance Level richiesto - PLr

Per ogni funzione di sicurezza individuata, il progettista deve decidere quale dovrà essere il contributo alla riduzione del rischio che essa deve fornire.

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

Il Parametro che viene usato per indicare il contributo alla riduzione del rischio richiesto per quella funzione di sicurezza è il **PLr** (*Performance Level Required*).

Il parametro PL invece, rappresenta il Livello di prestazione raggiunto dall'hardware che implementa quella funzione di sicurezza. Va da sé che il PL deve almeno essere uguale o superiore al PLr.

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.

Lo strumento usato nella ISO 13849-1 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 PL r. Se vengono individuate più funzioni di sicurezza, per ognuna di esse occorre definire il PLr.

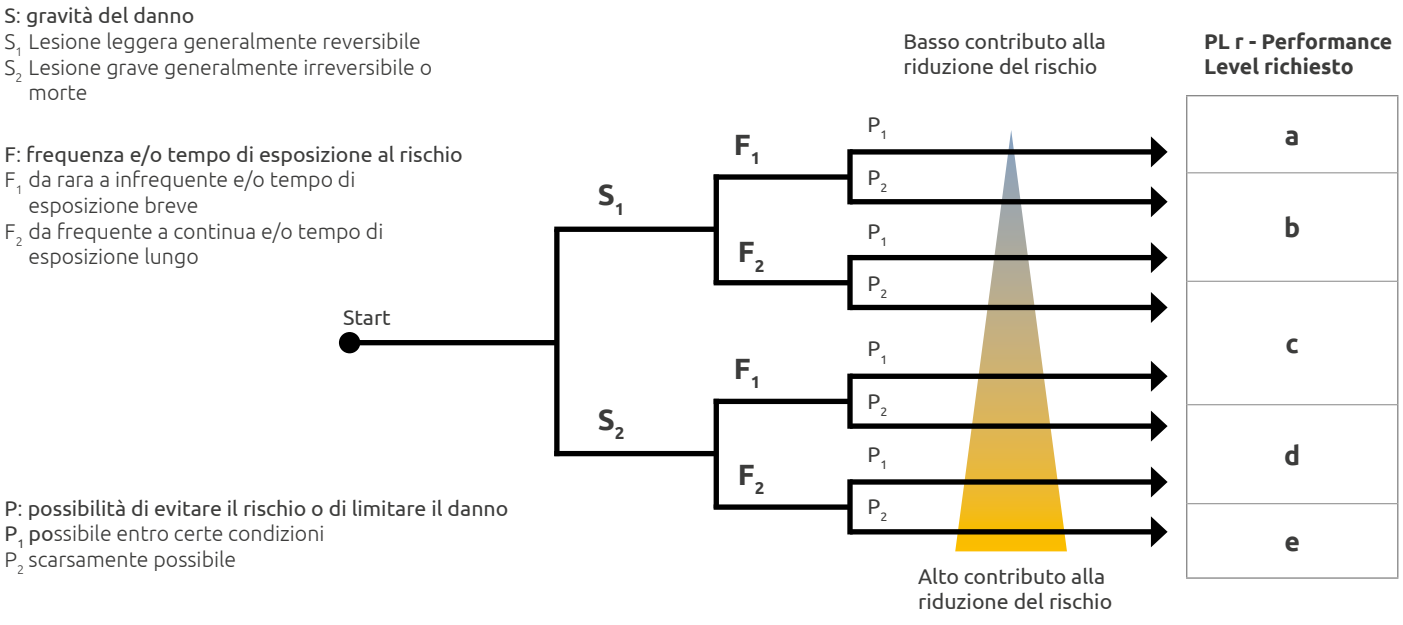


Fig. 6. Grafico delle decisioni per determinare il valore di PL r

PL r(e) fornisce il più alto contributo alla riduzione del rischio, PL r(a) il più basso.

Considerazioni sul parametro S

È necessario fare una valutazione sul tipo di lesioni che potrebbero derivare da un malfunzionamento della funzione di sicurezza. La EN 13849-1 propone solo due possibilità:

- S1 = lesione leggera
- S2 = lesione grave

Sono considerate lesioni leggere le graffi, sbucciature, lividi, lacerazioni senza complicanze. Sono considerate lesioni gravi le amputazioni, le perdite di funzionalità di un arto, la perdita di un occhio, morte.

Considerazioni sul parametro F

La distinzione fra F1 e F2 può essere formulata come segue:

Si sceglie F2 se la frequenza di esposizione al pericolo è maggiore di una volta ogni 15 minuti. Si sceglie F1 se la frequenza di esposizione al pericolo non è maggiore di una volta ogni 15 minuti e il tempo di esposizione accumulato non supera 1/20 del tempo operativo complessivo.

Considerazioni sulla probabilità di accadimento dell'evento pericoloso

La probabilità del verificarsi di un evento pericoloso dipende sia dal comportamento umano sia da guasti tecnici, dovrebbe essere basata su fattori come:

- Dati di affidabilità del sistema di controllo
- La storia degli incidenti su macchine analoghe (con lo stesso rischio, stesso processo, stessa azione dell'operatore e stessa tecnologia che causa il pericolo).

La probabilità di occorrenza è sempre valutata uguale a 1 perché nella maggior parte dei casi la probabilità corretta non è nota o è difficile da stimare.

Se la probabilità del verificarsi di un evento pericoloso può essere giudicata bassa, il PLr può essere ridotto un livello.

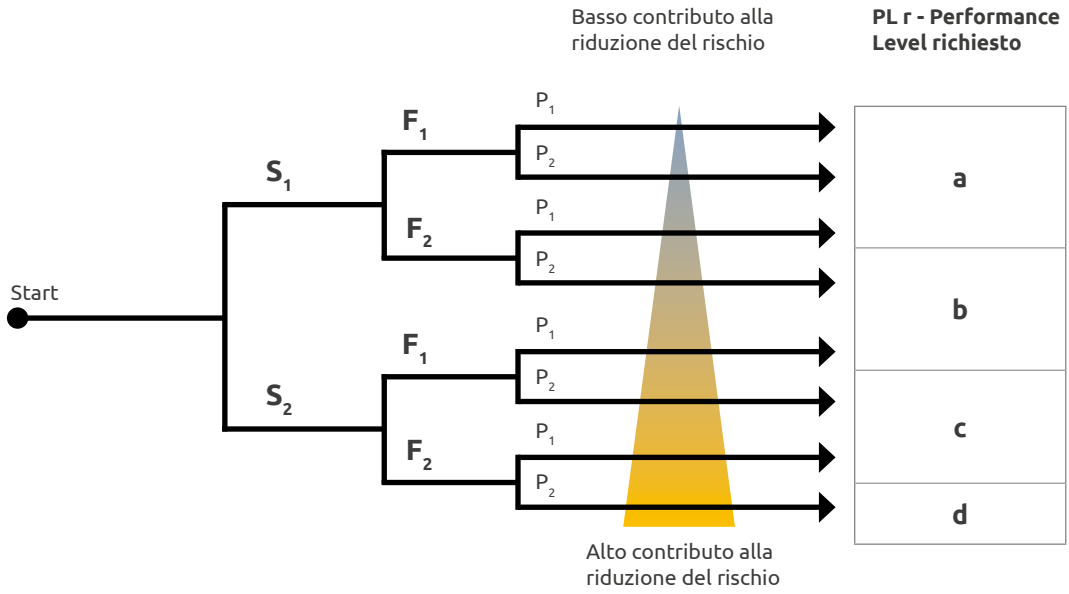


Fig. 7. Grafico delle decisioni per determinare il valore di PLr se la probabilità (P) del verificarsi di un evento pericoloso può essere giudicata bassa

Sovrapposizioni dei pericoli

È possibile che una stessa persona possa essere sottoposta all'interazione simultanea di più pericoli dovuti per esempio alla presenza di più movimenti pericolosi della macchina che potrebbero potenzialmente crearle un danno.

Se la valutazione della probabilità di guasto fosse fatta prendendo in considerazione tutti i componenti coinvolti nell'insieme delle operazioni, si arriverebbe ben presto a valori di PFH_D molto alti (anche se si usassero componenti con valori di $MTTF_D$ molto alti) con conseguente impossibilità di raggiungere il PL richiesto.

Le cose si complicano ancora di più nel caso che i singoli rischi richiedano PLr diversi.

Per superare questi problemi è consentito separare i rischi, se questo è possibile, e assegnare ad ognuno di essi una funzione di sicurezza separata.

Questa possibilità deve essere analizzata dal progettista durante il processo di valutazione del rischio. Prima si identifica la zona pericolosa, poi si identificano tutti i movimenti pericolosi delle varie parti della macchina che insistono sulla stessa zona pericolosa, quindi si considerano le operazioni da svolgere e quali sono le parti del corpo a rischio.

Se dall'analisi si evince che è possibile separare i vari movimenti pericolosi allora ad ogni movimento pericoloso si assegna una funzione di sicurezza separata e si calcola il relativo PL.

Esempio 1

In una cella di produzione che coinvolge più robot su operazioni diverse la funzione di arresto a seguito dell'intrusione della barriera, può essere valutata singolarmente per ciascun robot.

Per l'esempio della cella di lavorazione illustrata, si possono individuare le seguenti funzioni di sicurezza:

SF1: L'interruzione della barriera di sicurezza comporta l'arresto di tutti gli azionamenti del robot 1

SF2: L'interruzione della barriera di sicurezza comporta l'arresto di tutti gli azionamenti del robot 2

SF3: L'interruzione della barriera di sicurezza comporta l'arresto di tutti gli azionamenti del robot 3

Fig. 8. Cella di produzione che coinvolge più robot su operazioni diverse

La stessa considerazione vale per esempio per una tavola rotante dotata di più dispositivi di serraggio; la valutazione del rischio può essere fatta separatamente per ogni pinza.

Esempio 2

In un robot di saldatura l'operatore è esposto contemporaneamente al rischio di schiacciatura dovuto al movimento della testa del robot e al rischio di bruciatura dovuto all'utensile montato sulla testa, in questo caso testa del robot e utensile vanno contemporaneamente presi in considerazione nella valutazione della funzione di sicurezza.

Esempio 3

Un robot in modalità di apprendimento può essere mantenuto attivo ed alimentato anche quando la porta di ingresso della cella è aperta solo se viene usato un dispositivo di abilitazione locale ad azione mantenuta ed il robot sia in modalità di funziionamento a velocità ridotta di sicurezza.

Nel calcolo del PFH_D vanno perciò inserite le probabilità di guasto di tutti e tre i dispositivi perché il guasto pericoloso anche di uno solo di essi porta immediatamente a una condizione di pericolo.

Individuazione della funzione di sicurezza e specifica di progettazione

Per decidere quali funzioni di sicurezza siano necessarie bisogna tener conto dell'uso previsto della macchina (incluso l'uso scorretto ragionevolmente prevedibile). Per ogni funzione di sicurezza deve essere redatto un documentato nel quale sono dettagliate almeno le seguenti specifiche:

- Risultato della valutazione dei rischi per ogni pericolo (Valore di PLr)
- Comportamento che si intende ottenere o impedire con la funzione di sicurezza (es. all'apertura del riparo la macchina esegue uno stop Cat.0)
- Uso previsto della macchina e uso scorretto ragionevolmente prevedibile
- Funzionamento in condizioni di emergenza
- Tempo di risposta della funzione di sicurezza
- Modalità di ripristino dopo un'azione di protezione (funzionamento automatico oppure manuale)
- Modalità di intervento (relative a una zona o parte della macchina)
- Necessità di sospensione della funzione di sicurezza (muting, banking)
- Modalità di by-pass della funzione di sicurezza per riparazione, messa a punto, pulizia, ricerca guasti ecc.
- Eventuale descrizione delle interconnessioni tra diverse funzioni di sicurezza
- Frequenza di intervento della funzione di sicurezza
- Priorità delle funzioni che, se attive contemporaneamente possono causare conflitti di funzionamento

Per aiutare il progettista, la norma elenca le principali funzioni di sicurezza che in genere sono implementate in un SRP/CS e per alcune di esse fornisce i principali requisiti di sicurezza:

- Funzione di arresto legata alla sicurezza avviata da una misura di salvaguardia
- Funzione di ripristino manuale
- Funzione di avviamento/riavviamento
- Funzione di comando locale
- Funzione di inibizione (Muting)
- Funzione di comando ad azione mantenuta
- Funzione dispositivo di abilitazione
- Prevenzione dell'avviamento inatteso
- Fuga e salvataggio di persone intrappolate
- Funzione di isolamento e dissipazione di energia
- Modalità di comando e selezione di modalità
- Funzione di arresto d'emergenza

Funzione di arresto di sicurezza

La funzione di arresto avviata dall'attuazione di un dispositivo di protezione deve portare la macchina in uno stato sicuro nel minor tempo possibile.

La funzione di arresto deve avere la priorità su una fermata per motivi operativi.

Quando un gruppo di macchine lavora insieme in modo coordinato, si deve aver cura di segnalare al controllo di supervisione e/o alle altre macchine l'esistenza di tale arresto di sicurezza.

Dopo l'attuazione di un comando di arresto da parte di un dispositivo di protezione, la condizione di arresto deve essere mantenuta fino al sussistere di condizioni sicure per il riavvio.

Funzione di ripristino manuale

Il Reset ripristina il mezzo di protezione e annulla il comando di arresto sicuro. Se stabilito dalla valutazione del rischio, tale annullamento deve essere confermato mediante un'azione manuale, separata e deliberata (ripristino manuale). La funzione di ripristino manuale deve:

- Essere autorizzata attraverso un dispositivo separato, compreso nella SRP/CS e azionato manualmente
- Essere abilitata solo se tutti i mezzi di protezione sono operativi
- Non avviare essa stessa un movimento o una situazione pericolosa
- Avvenire mediante un'azione deliberata
- Abilitare il sistema di comando affinché accetti il comando di avvio
- Essere abilitata solo dopo aver disinserito l'attuatore dalla sua posizione di ON

Funzione di Muting

La funzione di Muting non deve esporre le persone a situazioni pericolose. Durante il Muting, le condizioni di sicurezza devono essere garantite con altri mezzi. Al termine del Muting, tutte le funzioni di sicurezza della SRP/CS devono essere ripristinate automaticamente. Il PL delle parti del SRP/CS che realizzano la funzione di Muting devono essere tali da non diminuire il livello di sicurezza della funzione di sicurezza alla quale è associato il Muting.

Parametri legati alla sicurezza

Quando lo scostamento di parametri quali posizione, velocità, temperatura o pressione, oltre i limiti impostati può causare problemi di sicurezza, il sistema di comando deve attuare misure appropriate (per esempio attuazione dell'arresto, segnale di avvertimento, allarme).

Fluttuazioni, perdita e ripristino di fonti di alimentazione

Quando si verificano fluttuazioni nei livelli di alimentazione al di fuori dell'intervallo operativo di progettazione, inclusa la perdita dell'alimentazione, la SRP/CS deve continuare a fornire o inviare segnali d'uscita che consentano alle altre parti del sistema macchina di mantenere uno stato sicuro.

E – Stop

L'E-Stop è definito "misura di protezione complementare" (non è una funzione di sicurezza).

Viene usato per ridurre il rischio dovuto a guasti o incidenti non ragionevolmente prevedibili a parti della macchina, inclusi guasti ai dispositivi di protezione. Poiché deve essere disponibile in caso di avaria degli altri dispositivi protezione, anche ad essa conviene applicare la EN ISO 13849-1.

Deve essere disponibile e operativo in ogni momento e deve bypassare tutte le altre funzioni e modi operativi della macchina (senza compromettere eventuali strutture progettate per il rilascio di persone intrappolate). Qualsiasi comando di avviamento (volontario, non intenzionale, o imprevisto) non deve avere efficacia su quelle parti della macchina fermate dal comando di E-stop fino a quando il dispositivo non venga ripristinato manualmente.

Il PLr della funzione E-Stop dovrebbe essere uguale a quello della funzione di sicurezza con PLr più alto coinvolta nella realizzazione del SRP/CS.

Funzione di controllo locale

Quando una macchina è controllata localmente, ad es. mediante un dispositivo di controllo portatile occorre che:

- Il selettore del dispositivo di controllo locale deve essere situato al di fuori della zona di pericolo
- Il controllo locale deve essere attivo solo nella parte della zona pericolosa individuata dall'analisi di rischio
- Il passaggio da controllo locale a controllo principale non deve creare una situazione pericolosa

Tempo di risposta

Quando, a seguito della valutazione di rischio, si ritiene che il tempo di risposta dell'SRP / CS possa essere determinante ai fini della sicurezza, esso dovrà essere sommato al tempo di risposta degli altri dispositivi che compongono il sistema di controllo di sicurezza in modo da formare il tempo complessivo di risposta della macchina.

Il tempo di risposta complessivo richiesto per l'arresto della macchina può influenzare la progettazione della parte relativa alla sicurezza, ad es. potrebbe essere necessario aggiungere un sistema di frenatura.

Realizzazione di una Funzione di sicurezza tramite un SRP/CS

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

Si possono usare tutte le tecnologie disponibili, anche in combinazione; elettrica, idraulica, pneumatica, meccanica ecc.

È anche possibile che una SRP/CS implementi funzioni di sicurezza e normali funzioni di comando (per esempio una Barriera Fotoelettrica o un Controllo a due mani possono essere usati sia per protezione che per avviamento ciclo).

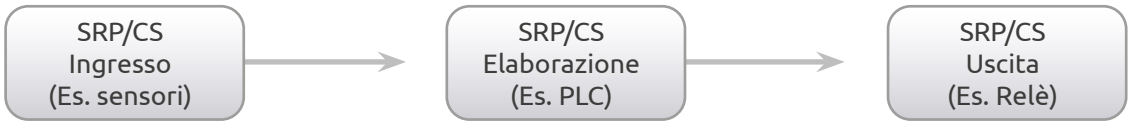


Fig. 9. Rappresentazione schematica a blocchi di una tipica funzione di sicurezza

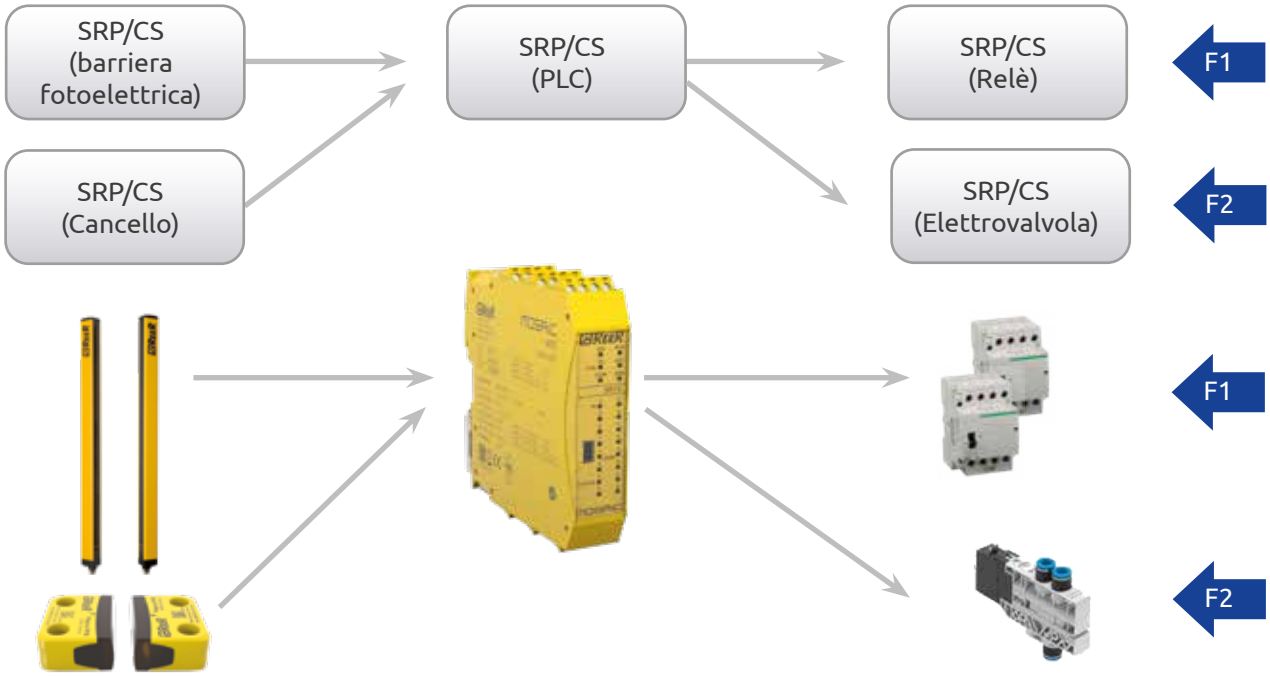


Fig. 10. Diverse funzioni di sicurezza possono condividere una o più SRP/CS

Il progettista deve decidere il contributo alla riduzione del rischio che è necessario sia fornito da ciascuna funzione di sicurezza.

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

Fase di progettazione di SRP/CS – Aspetti organizzativi

Prima di realizzare un SRP/CS, al fine di ridurre il più possibile l'introduzione di guasti sistematici durante la fase di progettazione oppure a seguito di successive modifiche, è necessario dotarsi di una organizzazione gestionale che segua procedure strutturate che coprano l'intero ciclo di vita del SRP/CS. Ogni attività di progettazione dovrebbe essere adeguatamente specificata, documentata e verificata.

PL e del PFH_D dei SRP/CS

Il PL dipende da numerosi fattori, inclusi la struttura hardware e software, la capacità di rilevare per tempo eventuali guasti interni che potrebbero limitarne le prestazioni di sicurezza, l'affidabilità dei componenti, la capacità di limitare i guasti da causa comune, la qualità del processo di progettazione, le sollecitazioni operative, le condizioni ambientali e il ciclo operativo della macchina.

Si devono considerare tutti i casi di uso previsto e uso scorretto ragionevolmente prevedibile.

Il seguente prospetto riassume gli aspetti quantificabili, assegnando ad essi un valore complessivo di probabilità di guasto, e gli aspetti qualitativi che devono essere soddisfatti al fine di ottenere un PL.

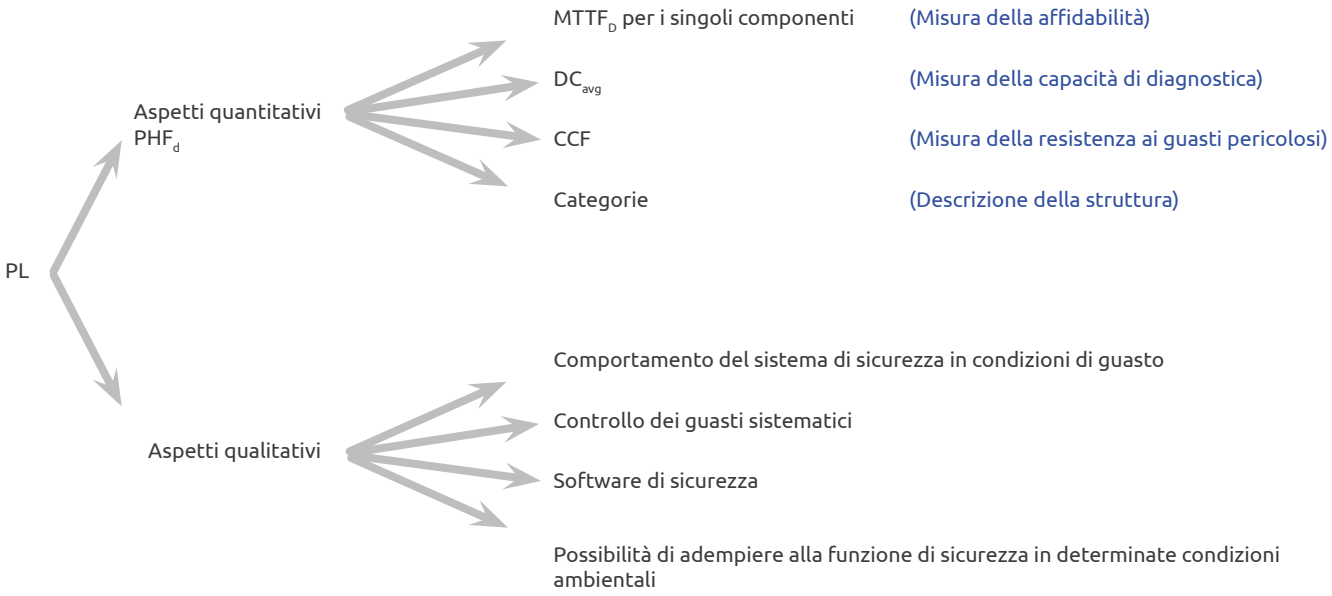


Fig. 11. Aspetti qualitativi e quantitativi da rispettare per progettare un sistema di controllo di sicurezza

IMPORTANTE!

Il valore della Probabilità media di guasto pericoloso/ora è solo uno dei parametri che contribuiscono all'assegnazione del PL. Per poter rivendicare un valore di 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 13849-1 e di aver rispettato i requisiti di sviluppo sia per il software applicativo che per quello incorporato.*

Calcolo del PFHD

Il metodo usato per valutare la parte del PL legata agli aspetti quantitativi è quello di calcolare la probabilità che all'SRP/CS possa capitare un guasto pericoloso in un determinato periodo di tempo, in particolare in un'ora, tenendo conto dell'affidabilità dei suoi componenti.

Quanto maggiore è il contributo alla riduzione del rischio fornito dal SRP/CS tanto più bassa deve essere la sua Probabilità di guasto pericoloso/ora (PFH_D).
È considerato pericoloso un guasto che, se non rilevato, inibisce la funzione di protezione del sistema.

Esistono diversi metodi per effettuare una stima della Probabilità media di guasto pericoloso/ora di un sistema o di un sottosistema. Questi metodi richiedono l'uso di complesse formule matematiche proprie della teoria della affidabilità dei sistemi e 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 - oppure guasto non pericoloso)
- la percentuale di guasti pericolosi rilevati dalle tecniche automatiche di autodiagnosi implementate rispetto al totale dei guasti pericolosi
- La percentuale di guasti pericolosi non rilevati dalle tecniche automatiche di autodiagnosi implementate rispetto al totale dei guasti pericolosi

L'ISO 13849-1 semplifica questo processo sostituendo le formule matematiche con tabelle pre-calcolate per diverse combinazioni di Categorie, di valori di massima di $MTTF_D$ e di DC_{avg} che vengono determinati anch'essi tramite tabelle.

Il processo di progettazione di un SRP/CS può essere riassunto nei seguenti passi:

1. Scelta della struttura del sistema (Categoria)
2. Calcolo di $MTTF_D$
3. Scelta delle tecniche di autodiagnosi e calcolo di DC_{avg}
4. Verifica di CCF per le architetture ridondanti
5. Calcolo di PL tramite la Tabella 5 o la Tabella K.1
6. Verifica del PL (se il PL calcolato è inferiore al PL r occorre ritornare al passo 1)
7. Validazione

Categorie e loro relazione con il $MTTF_D$, la DC_{avg} e con le CCF

Per aiutare il progettista nel calcolo del PL di una SRP/CS, la EN/ISO 13849 utilizza una metodologia basata su 5 particolari strutture denominate **Categorie** che costituiscono l'ossatura su cui si basano tutti gli aspetti quantificabili che concorrono alla formazione del PL.

Le Categorie descrivono un SRP/CS in relazione alla:

- Disposizione strutturale delle sue parti
- Sua tolleranza ai guasti
- Suo comportamento in condizioni di guasto
- Affidabilità dei suoi componenti

Ciò vuol dire che la prestazione di sicurezza viene raggiunta non solo tramite particolari architetture hardware (che la norma definisce: designated architecture), ma anche attraverso un uso attento di componenti affidabili e, se necessario, di adeguate tecniche di monitoraggio.

La scelta di una categoria dipende principalmente da:

- Riduzione del rischio che deve essere fornita dal SRP/CS
- Livello di prestazione richiesto (PL r)
- Tecnologia usata
- Rischio derivante dal guasto della SRP/CS
- Possibilità di evitare guasti in quella SRP/CS (guasti sistematici)
- Probabilità che si verifichino guasti in quella SRP/CS
- Tempo medio di guasto pericoloso ($MTTF_D$)
- Copertura diagnostica (DC)
- Guasti per causa comune (CCF) nel caso delle categorie 2, 3 e 4

Vale la pena precisare che le *designated architectures* raffigurate in ciascuna Categoria servono per dare una rappresentazione logica della struttura del sistema, la realizzazione tecnica e lo schema circuitale funzionale possono anche apparire completamente diversi.

Le *designated architectures* possono anche servire per descrivere una parte o una sotto-parte di un sistema di controllo che risponde a determinati segnali di input e genera segnali di output di sicurezza; pertanto il blocco "input" può rappresentare, ad esempio, una barriera fotoelettrica (AOPD) oppure contatti di interruttori. Il blocco "output" può rappresentare, ad esempio, una uscita di sicurezza (OSSD), una combinazione di contatti di relè.

Per le categorie 3 e 4 la rappresentazione a doppio canale non sta a significare che tutte le parti devono necessariamente essere fisicamente ridondanti ma che esistono mezzi ridondanti per garantire che un singolo guasto non può portare alla perdita della funzione di sicurezza.

Esistono sicuramente più modi per realizzare architetture in grado di soddisfare i requisiti stabiliti dalle Categorie, ma se si fa rientrare la struttura del sistema di controllo in una (o più) delle 5 Categorie, allora per il calcolo del livello di prestazione di sicurezza (PL) è possibile usare le procedure semplificate descritte nella norma.

Se un'architettura devia da quelle delle Categorie allora il suo PL non può essere calcolato con il metodo semplificato della norma, ma deve essere giustificato con mezzi analitici, ad esempio tramite modellazione di Markov, al fine di mostrare che tramite tale architettura è possibile raggiunge il livello di prestazione richiesto (PL r). Markov infatti offre una notevole capacità di gestire molte delle caratteristiche tecniche che sono implementate nei moderni dispositivi di sicurezza, per esempio è possibile modellare eventi periodici come i test automatici di diagnostica dei guasti.

Panoramica dei principali requisiti di sicurezza e delle principali caratteristiche funzionali delle 5 Categorie

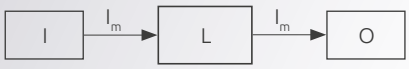
Le categorie rispecchiano quello che già avviene nel modo del macchinario industriale, infatti la maggior parte dei controlli implementati possono essere ricondotti a un numero molto limitato di tipologie di controlli di sicurezza. Vale a dire:

- Sistemi a canale singolo non testati che si basano sulla affidabilità dei componenti (si cerca di evitare il guasto)
- Sistemi a canale singolo dotati di test (si cerca di rilevare il guasto)
- Sistemi a canale doppio con auto-diagnosi (si cerca di controllare il guasto)
- Sistemi a canale doppio con auto-diagnosi di alta qualità (si controllano anche guasti multipli)

NOTA: Le linee e le frecce nelle figure seguenti rappresentano interconnessioni logiche, funzionali e diagnostiche.

Cat. B

Tolleranza al guasto = 0

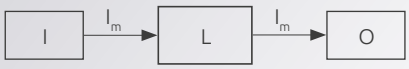


Canale singolo senza diagnostica

PL_{max} = b
DC = 0
$MTTF_D$ = da basso a medio
Uso di principi di sicurezza di base (i componenti devono resistere alle sollecitazioni di impiego)

Cat. 1

Tolleranza al guasto = 0



Canale singolo senza diagnostica

PL_{max} = c
DC = 0
$MTTF_D$ = alto
Uso di principi di sicurezza di base e "ben provati" e uso di componenti "ben provati"; no componenti complessi (PLC, Asic)

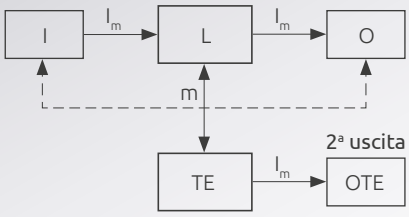
Un "componente ben provato" è un componente che è stato:

- ampiamente utilizzato in passato con risultati positivi in applicazioni simili
- realizzato e verificato utilizzando principi che ne dimostrano l'idoneità, l'affidabilità e la robustezza per applicazioni legate alla sicurezza.

La qualificazione di un componente come ben provato dipende dalla sua applicazione. Esempio, un interruttore di posizione con contatti ad apertura positiva può essere ben provato per una macchina utensile ed allo stesso tempo inappropriato per l'applicazione nell'industria alimentare.

Cat. 2

Tolleranza al guasto = 0



Canale singolo con diagnostica

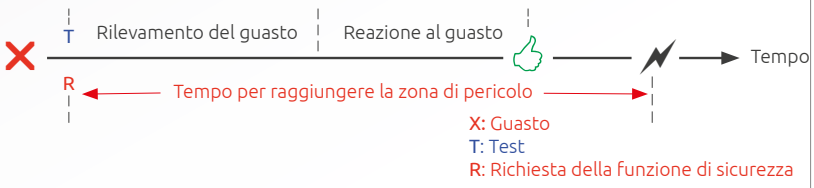
PL_{max} = d
DC = da basso a medio
$MTTF_D$ = da basso a medio (considerare solo i componenti appartenenti al canale funzionale)
$MTTF_D$ del TE deve essere maggiore di 0,5 x $MTTF_D$ canale
Se così non fosse occorre declassare l' $MTTF_D$ canale
Uso di principi di sicurezza di base
Uso di principi di sicurezza "ben provati"

Il test stesso non deve creare una situazione di pericolo (es. causare un aumento del tempo di risposta).

La funzione di sicurezza deve essere testata almeno all'avviamento e prima che possa verificarsi una condizione di pericolo (avviamento di un nuovo ciclo). La frequenza del Test del canale funzionale doveva essere almeno 100 volte più alta della cadenza di richiesta della funzione di sicurezza.

Per rapporti superiori a 25 e inferiori a 100 è possibile usare i valori PFH_D (riportati nella tabella K .1 per la Cat. 2) moltiplicati per un fattore 1,1.

Il test può anche essere eseguito all'istante della richiesta della funzione di sicurezza, purché il tempo complessivo per rilevare il guasto e per portare la macchina in una condizione sicura (di solito la macchina viene fermata) sia più breve del tempo che impiega una persona a raggiungere il punto pericoloso.

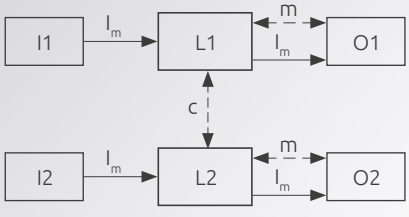


Per PLr = a e fino al PLr = c, quando, al rilevamento del guasto, non sia possibile dare inizio a uno stato sicuro (per esempio a causa della saldatura del contatto nel dispositivo di uscita), può essere sufficiente che l'uscita OTE fornisca solo un segnale di avvertimento.

Per PLr = d, l'uscita OTE deve dare inizio a uno stato sicuro che viene mantenuto fino a quando il guasto viene cancellato.

Cat. 3

Tolleranza al guasto = 1

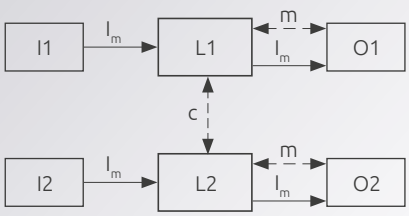


Canale doppio con diagnostica

PL_{max} = e
DC = da basso a medio
$MTTF_D$ = da basso a medio
Uso di principi di sicurezza di base
Uso di principi di sicurezza "ben provati"
Un singolo guasto non porta alla perdita della funzione di sicurezza. Quando ragionevolmente realizzabile, il singolo guasto deve essere rilevato durante o prima della successiva richiesta della funzione di sicurezza.
Non tutti i guasti possono essere rilevati.
L'accumulo di guasti non rilevati porta alla perdita della funzione di sicurezza

Cat. 4

Tolleranza al guasto = 1



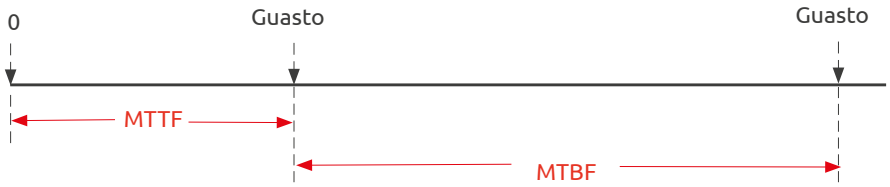
Canale doppio con diagnostica

PL_{max} = e
DC = alto
$MTTF_D$ = alto
Uso di principi di sicurezza di base
Uso di principi di sicurezza "ben provati"
Un singolo guasto non porta alla perdita della funzione di sicurezza.
I guasti devono essere rilevati in tempo prima della perdita della funzione di sicurezza. Per esempio immediatamente al loro verificarsi, oppure all'accensione o alla fine del ciclo operativo della macchina. Se questo rilevamento non è possibile, la combinazione di due guasti non deve portare alla perdita della funzione di sicurezza.

Calcolo di $MTTF_D$

L'affidabilità vera di un componente non è mai nota esattamente, però la statistica e il calcolo delle probabilità ci offrono lo strumento per stimarla.

La probabilità di un componente di non guastarsi durante il suo funzionamento è misurata dal suo tasso di guasto λ (numero 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) oppure MTTF (mean time to failure) nel caso ci si riferisca al primo guasto dopo l'avviamento iniziale.



Se poi interessa conoscere solo la durata media di funzionamento prima che capiti un guasto potenzialmente pericoloso, si usa l'acronimo $MTTF_D$ (mean time to dangerous failure). Ai fini del calcolo del PFH_D interessa conoscere solo l'$MTTF_D$, cioè quella parte del tasso di guasto relativa ai guasti che possano causare un funzionamento pericoloso del sistema.

Per aiutare il progettista nel capire quali sono i guasti da considerare, la EN ISO 13849-2 (Annessi da A a D) fornisce, per ogni tecnologia, una lista di guasti e le condizioni entro le quali è possibile assumere a priori che alcuni guasti non si possano presentare (faults exclusion).

La lista non è esaustiva e, se necessario, possono essere aggiunti guasti ulteriori in funzione della particolare applicazione.

In pratica, sulla base dei guasti indicati nella EN ISO 13849-2 e dei guasti possibili, derivati dal progetto in esame, conviene costruire per ogni SRP/CS una lista dei componenti usati e per ognuno di essi stabilire i guasti da considerare. Si deve determinare quindi l'incidenza dei guasti pericolosi rispetto a tutti i guasti possibili di quel componente e vedere se alcuni di questi guasti possono essere esclusi a priori.

Per semplicità di calcolo la norma consente di valutare, per ogni componente, come pericolosi il 50% dei guasti possibili (worst case), quindi:

$$MTTF_D = 2 \times MTTF$$

Inoltre, sempre nell'ottica della semplificazione, si è adottato il seguente criterio:

- Qualora un "primo guasto" ne causi direttamente altri, la probabilità è la stessa di quella del primo guasto; ne consegue che il primo guasto e tutti quelli da esso derivati devono essere considerati come un singolo guasto
- Qualora in alcune circostanze due guasti possano avere la stessa causa comune, devono essere considerati come un guasto singolo (CCF)
- Il verificarsi simultaneo di due o più guasti dovuti a cause diverse è altamente improbabile (prodotto di due probabilità già estremamente basse) e pertanto non viene considerato. Ciò vuol dire che è accettabile che il verificarsi simultaneo di guasti multipli indipendenti possa generare un pericolo
- Ogni SRP/CS deve essere ragionevolmente affidabile in modo che la probabilità di "primo guasto" sia bassa; non sono perciò presi in considerazione valori di $MTTF_D$ inferiori a 3 anni

Dove reperire i dati di affidabilità dei componenti?

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

a. Impiego dei dati del fabbricante
b. Impiego dei dati contenuti nella tabella C.1 per i componenti meccanici, idraulici, pneumatici, elettrici, di più comune impiego e per i quali il meccanismo di guasto è prevalentemente legato all'usura dei materiali
c. Impiego dei dati contenuti nelle tabelle da C.2 a C.7 per componenti elettronici
d. Scelta di dieci anni

L'uso dei dati contenuti nella tabella C.1 è consentito solo se si dimostra di aver seguito le pratiche di buona tecnica, vale a dire:

- I componenti sono stati progettati e fabbricati secondo principi di sicurezza di base e ben provati in conformità alla ISO13849-2 o alla norma pertinente. (Confermato nella scheda tecnica del componente)
- Il fabbricante del componente specifica l'applicazione appropriata e le condizioni operative per l'utilizzatore
- Il fabbricante del SRP/CS, utilizzatore del componente, dichiara di averlo impiegato avendo applicato principi di sicurezza di base ben provati secondo la ISO 13849-2

$MTTF_D$ di componenti soggetti a usura

Per tutti i componenti elettromeccanici e pneumatici soggetti a usura (es. relè, elettro-valvole, interruttori) 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 B_{10} (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 B_{10} per cui si hanno guasti pericolosi nell'applicazione considerata viene indicata con B_{10D}.

In assenza di informazioni dettagliate la EN ISO 13849-1 consiglia di considerare come pericolosi il 50% dei guasti, quindi:

$$B_{10D} = 2 \times B_{10}$$

Conoscendo il B_{10D} e il numero medio di operazioni in un anno (Nop) si ricava il valore di $MTTF_D$ nel seguente modo:

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times N_{op}}$$

Dove:

$$N_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{Cycle}}$$

Con le seguenti ipotesi sulle applicazioni dei componenti:
h_{op} è le media delle operazioni al giorno espressa in ore
d_{op} è la media delle operazioni all'anno espresse in giorni
Tcycle è il tempo medio di funzionamento tra l'inizio dei due cicli successivi del componente. (Ad esempio commutazione di una valvola) in secondi per ciclo

La vita utile del componente deve poi essere limitata a T_{10D} (tempo entro il quale il 10% dei componenti in esame subisce un guasto pericoloso).

$$T_{10D} = \frac{B_{10D}}{N_{op}}$$

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

Esempio Relè:

B_{10} = 3.000.000 cicli

Carico di lavoro

d_{op} = 220 gg/anno
h_{op} = 16 h/giorno (due turni)
t_{ciclo} = 15 s (ciclo macchina)

$$N_{op} = \frac{220 \times 16 \times 3600}{15} \approx 0{,}84 \times 10^6$$

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times N_{op}} = \frac{2 \times 3 \times 10^6}{0{,}1 \times 0{,}84 \times 10^6} \approx 71 \text{ anni}$$

$$T_{10D} = \frac{B_{10D}}{N_{op}} = \frac{2 \times 3 \times 10^6}{0{,}84 \times 10^6} \approx 7{,}1 \text{ anni}$$

La vita utile del relè è di poco superiore a 7 anni. Il relè deve essere sostituito al settimo anno di funzionamento.

Calcolo del $MTTF_D$ del SRP/CS

La relazione che lega l'affidabilità dei componenti, il loro numero in un canale ed il $MTTF_D$ totale del canale è la seguente:

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}}$$

Dove con $MTTF_{Di}$ si è indicato il valore di $MTTF_D$ di ogni singolo componente

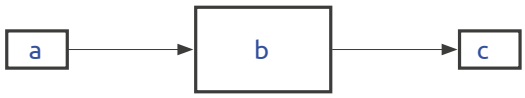
La formula è valida anche per più SRP/CS collegati in serie per formare un canale in cui il guasto di un componente provoca il guasto dell'intero canale.

Gli $MTTF_D$ di un canale maggiore di 100 anni non sono accettabili in quanto i PFHd dell'SRP/CS non devono dipendere solo dall'affidabilità dei componenti. Un'eccezione è la Categoria 4 dove il limite è esteso fino a 2500 anni.

Singoli componenti del canale si possono avere valori di $MTTF_D$ superiori ai 100 anni.

Esempio: canale formato da tre componenti a, b e c

a) $MTTF_D = 228$
b) $MTTF_D = 45662$
c) $MTTF_D = 14269$



$$\frac{1}{MTTF_D} = \frac{1}{228} + \frac{1}{45662} + \frac{1}{14269} \approx 4{,}38 \times 10^{-3} + 2{,}19 \times 10^{-5} + 7 \times 10^{-5} \approx 4{,}5 \times 10^{-3}$$

$$MTTF_D = \frac{1}{4{,}5 \times 10^{-3}} \approx 223 \text{ anni}$$ Va limitato a 100 anni fino a PL d

Nel caso di sistemi doppi canale (Cat. 3 e Cat. 4) un solo canale necessita del calcolo dell'$MTTF_d$ ma se l' $MTTF_D$ totale ha valori diversi per i due canali (non omogenei) si hanno a disposizione due possibilità:

a. Si considera il valore più basso dei due (worst case)
b. Si usa la seguente formula che agli effetti del calcolo ri-omogenizza i due canali. Si sostituisce cioè il sistema a doppio canale con uno equivalente avente $MTTF_D$ identici per entrambi I canali

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

$MTTF_{DC}1$ e $MTTF_{DC2}$ sono i valori dei due canali.

Completato il calcolo, si sceglie la classe di $MTTF_D$ tramite la seguente tabella:

Indicazione di $MTTF_D$	Valori espressi in anni
Basso	$3 \le MTTF_D < 10$
Medio	$10 \le MTTF_D < 30$
Alto	$30 \le MTTF_D < 100$

Guasti che si possono escludere a priori

La possibilità di escludere guasti è legata al compromesso tra i requisiti di sicurezza che impongono di prendere in considerazione tutti i guasti pericolosi e la possibilità teorica che un determinato tipo di guasto pericoloso possa verificarsi.

L'esclusione dei guasti è basata su:

- La scarsa probabilità tecnica che alcuni guasti possano verificarsi
- L'esperienza tecnica generalmente accettata su un certo tipo di componente, indipendentemente dall'applicazione considerata
- I requisiti tecnici relativi all'applicazione e al rischio in esame

Poiché un'esclusione di guasti può portare a un PL molto alto, nella documentazione tecnica deve essere fornita una giustificazione dettagliata.

Per componenti nuovi o che non sono nella lista, si deve effettuare un'analisi FMEA (vedere IEC 60812) per stabilire i guasti che devono essere considerati per tali componenti e quelli che possono essere esclusi.

Se per un componente è possibile escludere guasti pericolosi, il suo contributo al $MTTF_D$ è nullo.

Per componenti elettromeccanici, l'analisi sulla possibile esclusione dei guasti deve essere condotta separatamente per la parte meccanica e per la parte elettrica, prendendo in considerazione le condizioni ambientali e possibili influenze esterne.

Scelta delle tecniche di auto-diagnosi e calcolo di DC_{avg}

Se si suppone:

- Che un guasto può sempre capitare (altrimenti non ci sarebbe motivo di definire l'MTTF)
- Che i meccanismi per il rilevamento dei guasti non sono tutti parimenti efficienti e immediati (dipende dal tipo di guasto, per alcuni guasti può occorrere più tempo) e che non è possibile pensare di poter rilevare tutti i guasti
- Che tuttavia adottando opportuni accorgimenti circuitali è possibile rilevare la maggior parte dei guasti pericolosi

Allora si può definire un parametro DC che indica quanto il sistema sia efficiente nel rilevare un proprio eventuale malfunzionamento in tempo (in tempo = prima che possa capitare un secondo guasto pericoloso).

Regola generale per il calcolo del valore di DC

Il parametro DC è espresso come rapporto fra il tasso di guasto dei guasti pericolosi rilevati dalle misure di autodiagnosi implementati , λdd , e il tasso di guasto di tutti i guasti pericolosi possibili λd (rilevati e non rilevati).

$$DC = \frac{\sum \lambda dd}{\sum \lambda d}$$

Dalla conoscenza di λ_d e dalla conoscenza della percentuale di copertura guasti fornita dalle misure diagnostiche impiegate è possibile ricavare λ_{dd} (rilevabili) e λdu (non rilevabili) e quindi calcolare il valore DC dell'intero sottosistema.

Metodo semplificato per il calcolo del valore di DC

Il progettista, se decide di avvalersi di tecniche diagnostiche per aumentare la copertura guasti, può scegliere le tecniche che ritiene più adatte fra quelle elencate in Tabella E.1 della norma. La Tabella E:1 fornisce una lista di 34 diverse tecniche di diagnosi suddivisa in tre famiglie (per circuiti di ingresso, per la logica di elaborazione dei segnali, per i circuiti di uscita).

Per ogni tecnica è assegnato un punteggio percentuale variabile fra 0% e 99%.

- 0% = nessun guasto pericoloso viene rilevato
- 60% = bassa percentuale di rilevamento di guasti pericolosi
- 90% = media percentuale di rilevamento di guasti pericolosi
- 99% = alta percentuale di rilevamento di guasti pericolosi

Può capitare che per le singole parti siano state usate tecniche di diagnosi con livelli DC diversi. In questo caso la norma fornisce una formula che consente di calcolare il DC totale dell'intero sistema (DC_{avg})

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

Dove con $MTTF_{Di}$ e DC_N sono indicati rispettivamente I valori di $MTTF_D$ e DC relativi ai singoli componenti del sottosistema.

Nota: in questa formula, $MTTF_D$, non deve essere tagliato a 100 anni o 2500 per la sola categoria 4.

Si può vedere che se una parte ha valori di DC e di $MTTF_D$ bassi ha molto peso e porta ad un valore di DC_{avg} basso.

Un componente non testato hanno DC = 0 e contribuiscono solo per il denominatore.

Completato il calcolo, si sceglie la classe di DC_{avg} tramite la tabella a fianco:

Relativamente alle tabelle precedenti, per le misure diagnostiche per le quali è indicato un intervallo di valori, il valore corretto della DC può essere determinato considerando tra tutti i guasti pericolosi quali sono quelli rilevati da quella particolare misura. In caso di dubbio conviene basarsi su una stima derivata da una FMEA.

Definizione DC_{avg}	Definizione DC_{avg}
Nessuna	DC < 60%
Basso	60% ≤ DC < 90%
Medio	90% ≤ DC < 99%
Alto	99% ≤ DC

Verifica di CCF per le architetture ridondanti

I CCF (Common Cause Failures) sono guasti dovuti a un'unica causa che possono interessare più componenti contemporaneamente.

CCF si possono verificare simultaneamente su più componenti a causa di uno shock, oppure a causa di un aumento di stress del sistema (ad es. per aumento improvviso di temperatura, umidità, vibrazioni) o per errori di progetto.

È importante valutare se possono verificarsi guasti per causa comune. Questi guasti infatti possono vanificare gli effetti di ridondanza. Se per effetto di CCF due o più canali distinti, in un sistema a più canali, si trovano contemporaneamente nello stato di errore, l'intero sistema di comando potrebbe perdere l'effetto di protezione.

Per la Categoria 2, per la Categoria 3 e per la Categoria 4 occorre quindi implementare strategie di difesa in modo da ridurre la probabilità di avere CCF. Ciò significa ridurre il fattore di accoppiamento fra i canali, scegliere componenti robusti , aumentare l'affidabilità intrinseca del sistema e garantire che l'ambiente operativo rientri nei vincoli di progettazione

La ISO 13849-1 presenta, nella Tabella F.1, una lista di 10 misure. Se applicate, è ipotizzabile che il valore della frazione residua dei guasti di modo comune sia minore o uguale al 2%.

Le misure sono raggruppate nelle seguenti categorie:

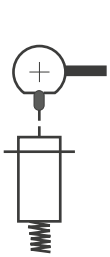
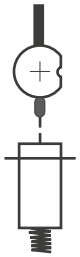
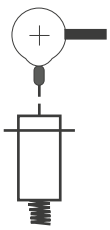
Progettazione fisica	Separazione / segregazione
	Diversità / ridondanza
	Complessità / design / applicazione / maturità / esperienza
Analisi	Valutazione / analisi e feedback dei dati
Problemi umani	Competenza / formazione / cultura della sicurezza dei progettisti
Problemi ambientali	EMC / Controllo ambientale / inquinamento di sistemi fluidici

A ogni misura contenuta nella lista è assegnato un punteggio. La somma totale vale 100. Deve essere raggiunto un punteggio di 65 o superiore. Con un punteggio di 65 è ipotizzabile che la frazione residua di guasti per causa comune sia inferiore o uguale al 2%. Se, invece, il punteggio totale è inferiore a 65, devono essere presi ulteriori provvedimenti.

I crediti più elevati sono assegnati alle misure contro le influenze ambientali (25 punti) e all'uso di differenti tecnologie/ progetti o principi fisici per i due canali (20 punti).

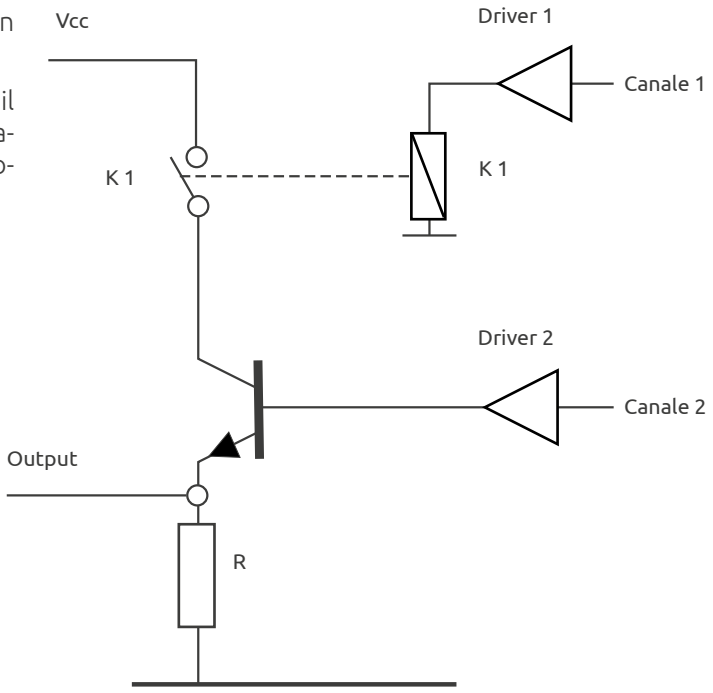
Esempio di diversità:

Due interruttori di posizione usati in modo combinato, uno ad azionamento meccanico diretto e uno a azionamento meccanico indiretto come illustrato nella tabella seguente:

Azionamento Meccanico	Protezione chiusa	Protezione aperta	Modo di funzionamento	Esempio di comportamento in caso di guasto
Diretto			Lo stantuffo (attuatore) è tenuto premuto da una camma finché la protezione non è chiusa. Quando la protezione è chiusa, l'uscita cambia di stato come risultato dell'azione della molla di richiamo.	L'uscita rimarrà nello stato sicuro quando la protezione non è chiusa anche se la molla si rompe.
Indiretto			Lo stantuffo (attuatore) è tenuto premuto da una camma finché la protezione è chiusa. Quando la protezione è aperta, l'uscita cambia di stato come risultato dell'azione della molla di richiamo.	Se la molla si rompe l'uscita può trovarsi in uno stato non sicuro anche se la protezione non è chiusa.

Oppure uno ad azionamento meccanico e uno tipo non meccanico come nell'esempio a fianco.

Ogni misura della lista deve essere valutata. Si assegna il punteggio riportato solo se la misura è stata completamente applicata; in caso di adozione solo parziale il valore ad essa associato è zero.



Metodo semplificato per la stima della parte quantificabile del PL

Dopo aver definito la Categoria e aver verificato che siano state rispettate le condizioni di CCF (per architetture ridondanti), avendo calcolato i valori di $MTTF_D$, e di DC_{avg}, il PL e il PFH_D si possono ricavare direttamente dalla tabella K.1 della norma.

I valori della tabella K.1 sono stati ricavati applicando il Metodo di Markov alle designated architectures delle 5 Categorie. Per tale motivo se si usa il metodo semplificato qui descritto non è possibile derogare dalle Categorie.

I valori della tabella K.1 sono stati calcolati assumendo che:

- Il mission time = 20 anni
- Il tasso di guasto dei componenti costante per tutto il mission time
- Per la categoria 2: La frequenza di Test è almeno 100 volte superiore alla frequenza della domanda della funzione di sicurezza e l'$MTTF_D$ del canale di test è maggiore della metà del $MTTF_D$ del canale funzionale

Nella colonna di sinistra si identifica il valore di $MTTF_D$ calcolato e, dopo aver identificato la colonna corrispondente alla Categoria implementtata e al DC_{avg} calcolato, in corrispondenza si legge il PL e il valore di PFH_D

	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)													
$MTTF_d$ di ogni canale anni	Cat. B DC_{avg} = nessuna	PL	Cat. 1 DC_{avg} = nessuna	PL	Cat. 2 DC_{avg} = bassa	PL	Cat. 2 DC_{avg} = media	PL	Cat. 3 DC_{avg} = bassa	PL	Cat. 3 DC_{avg} = media	PL	Cat. 4 DC_{avg} = alta	PL
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		
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				
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d						
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c								
62			$1{,}84 \times 10^{-6}$	c										
68														

Se interessa solo il valore di PL allora si può usare il grafico di figura 5 della norma.

La combinazione di Categoria e DC_{avg} identifica una delle sette colonne; il valore di $MTTF_D$ calcolato determina quale parte della colonna considerare. Sulla sinistra del grafico si legge poi direttamente il valore di PL corrispondente.

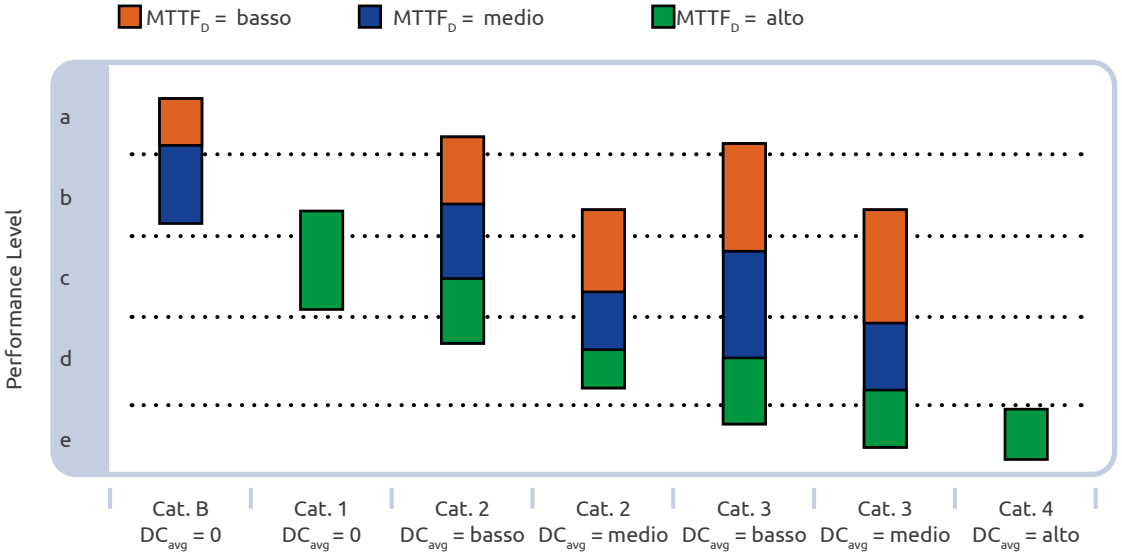


Fig. 12. Figura "5" di ISO 13849-1

Può capitare che la parte di colonna scelta comprenda due o tre possibili valori di PL (es. nel caso di Cat. 3, D_{Cavg} = medio e $MTTF_D$ = low, sono possibili i seguenti tre valori: PLb, PLc, PLd); in questi casi, per poter ricavare il valore di PL corretto si usa la tabella K.1. Il grafico di Fig. 5 può anche essere usato per fare delle ipotesi di lavoro; può per esempio essere usato per decidere quale Categoria usare in base al PL r necessario. Ad esempio, per un PL r pari a "c" sono possibili le seguenti cinque alternative:

1. Categoria 3 con $MTTF_D$ = basso e DC_{avg} media
2. Categoria 3 con $MTTF_D$ = medio e DC_{avg} bassa
3. Categoria 2 con $MTTF_D$ = medio e DC_{avg} media
4. Categoria 2 con $MTTF_D$ = alto e DC_{avg} bassa
5. Categoria 1 con $MTTF_D$ = alto

Stima del PL sulla base dell'informazione della Categoria

Questo metodo è applicabile solo alla parte di uscita di una SRP/CS.

Se per componenti meccanici, idraulici o pneumatici (o componenti che comprendono tecnologie miste ad esempio freno meccanico a comando pneumatico) non sono disponibili dati di affidabilità specifici per una data applicazione, il fabbricante della macchina può valutare gli aspetti quantificabili del PL senza conoscere il valore di $MTTF_D$ o B10D.

In questo caso, il PL è implementato dall'architettura, dalla diagnostica e dalle misure contro il CCF. La tabella seguente mostra la relazione fra il PL e il PFH_D conseguibile e le Categorie.

	PFH_D (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	$2*10^{-5}$	*	0	0	0	0
PL b	$5*10^{-6}$	*	0	0	0	0
PL c	$1,7*10^{-6}$	-	*2	*1	0	0
PL d	$2,9*10^{-7}$	-	-	-	*1	0
PL e	$4,7*10^{-8}$	-	-	-	-	*1

* La categoria applicata è raccomandata
0 La categoria applicata è opzionale
\- La categoria non è consentita
*1 Si devono utilizzare componenti collaudati o ben provati (confermati dal fabbricante dei componenti per essere idonei per tale applicazione particolare) e ben provati principi di sicurezza.
*2 Si devono utilizzare componenti e principi di sicurezza ben provati. Per i componenti legati alla sicurezza che non sono sorvegliati dal processo, il valore $T10_D$ può essere determinato sulla base di dati di collaudo del fabbricante della macchina.

PLa e il PLb possono essere raggiunti facendo ricorso alla Categoria B; PLc può essere raggiunto facendo ricorso alla Categoria 1 o alla Categoria 2; PLd può essere raggiunto facendo ricorso alla Categoria 3; PLe può essere ottenuto facendo ricorso alla Categoria 4.

Inoltre:

- Se si fa ricorso alla Categoria 1 per ottenere un PLc, è indispensabile:
  - Determinare il valore del $T10_D$ dei componenti coinvolti nella sicurezza. Tale valore può essere determinato sulla base di dati "proven in use" forniti dal costruttore della macchina
- Per la Categoria 2, devono:
  - Essere utilizzati principi di sicurezza ben provati e componenti ben provati dichiarati idonei dal fabbricante del componente per la particolare applicazione
  - $MTTF_D$ del canale di prova deve essere almeno di 10 anni
  - DC_{avg} deve essere bassa o media
  - Devono essere messe in atto misure per il controllo di CCF
- Se si fa ricorso alla Categoria 3, devono:
  - Essere utilizzati componenti ben provati e principi di sicurezza ben provati
  - DC_{avg} deve essere bassa o media
  - Devono essere messe in atto misure per il controllo di CCF
- Se si fa ricorso alla Categoria 4, devono:
  - Essere utilizzati componenti ben provati e principi di sicurezza ben provati
  - DC_{avg} deve essere alta
  - Devono essere messe in atto misure per il controllo di CCF

Poiché non si può usare la formula E.1 della norma per il calcolo del DC_{avg} a causa della indisponibilità dei valori $MTTF_D$, il DC_{avg} va calcolato semplicemente come media aritmetica dei singoli valori di DC dei componenti della parte di uscita del SRP/CS.

La dimostrazione che il componente sia "proven-in-use" si basa sull'analisi dei guasti del componente in un lungo periodo di tempo usato nella specifica configurazione e per quella particolare applicazione. Deve esistere una evidenza documentata che la probabilità di guasti sistematici pericolosi di quel componente, in quella specifica applicazione, sia sufficientemente bassa per il valore di PL richiesto.

Il concetto di componente "proven in use" deriva dalla norma IEC 61508.

Combinazione di più SRP/CS

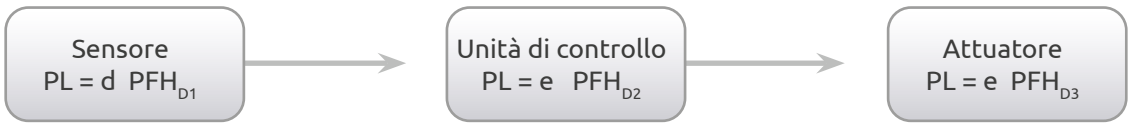
Fin qui si è visto come calcolare il PL e il PFH_D delle singole SRP/CS.

Resta ora da calcolare il PFH_D e il PL della funzione di sicurezza formata dalla combinazione serie di più sottositemi che possono anche essere realizzati con architetture differenti (es. barriera di sicurezza, logica di controllo, uscita di potenza). I sosttositemi vanno letti a partire dal punto dove entrano i segnali relativi alla sicurezza e terminano all'uscita degli elementi di controllo degli attuatori.

La norma propone metodi; uno dettagliato se per i singoli sottositemi oltre al PL si conosce anche il PFH_D e uno semplificato se si ha a disposizione solo il PL.

Metodo dettagliato

Se è noto il PFH_D delli singoli sottositemi, IL PFH_D totale è pari alla somma dei valori di PFH_D dei singoli sottositemi.



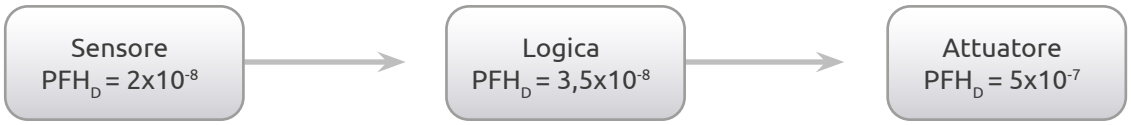
$$PFH_D = PFH_{D1} + PFH_{D2} + PFH_{D3}$$

Noto il PFH_D della combinazione, per risalire al PL complessivo della funzione di sicurezza si usa la tabella seguente.

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

Fig. 13. La Tabella della norma: Performance leves (PL)

Esempio numerico:

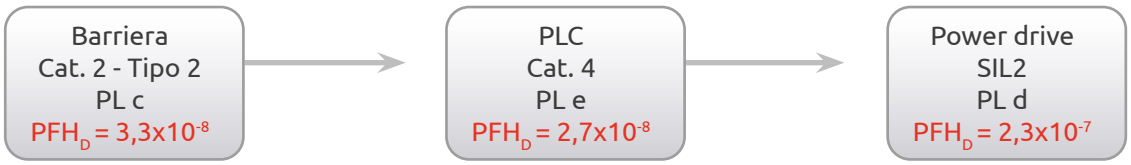


$$PFH_{D(SRP/CS)} = 2x10^{-8} + 3,5x10^{-8} + 5x10^{-7} = 5,55 \times 10^{-7}$$

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

Il PL totale non può essere maggiore del PL più basso di tutti i sottosistemi che compongono la funzione di sicurezza

Esempio di limitazione:



La funzione di sicurezza è formata da una Barriera Fotoelettrica di Tipo 2, PLc, da un'unità di controllo PLe e da un azionamento PLd

Sommando i valori di PFH_D risulta:

$$PFH_D = 3,3x10^{-8} + 2,7x10^{-8} + 2,3x10^{-7} = 5,33 \times 10^{-7}$$

Portando questo risultato nella tabella, ne segue che il PL risultante dovrebbe essere PLd

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

Ricordando tuttavia i vincoli dovuti a guasti sistematici ai quali sono sottoposte le Barriere Fotoelettriche di Tipo 2:

TIPO ESPE	PL	SIL
2	a, b, c	1
3	a, b, c, d	1, 2
4	a, b, c, d, e	1, 2, 3

Fig. 14. PL massimo che può raggiungere una funzione di sicurezza che impiega Barriere fotoelettriche di sicurezza

Risulta che il massimo PL raggiungibile dalla funzione di sicurezza diventa PLc

Metodo semplificato

Se è noto solo il PL delle singoli sottositemi si può avere una stima del PL della combinazione usando la tabella seguente nel seguente modo:

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

Fig. 15. Tabella per il calcolo del PL totale

1. Si individua la parte col PL più basso "PL (low)" prima colonna
2. Si individuano il numero di parti che hanno il PL più basso "n (low)" seconda colonna
3. In corrispondenza si ricava il PL totale (terza colonna)

Il PL ricavato tramite questa approssimazione si riferisce a valori di PFH_D che si trovano a metà del range del corrispondente PL

Nell' esempio indicato:

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

PL low = c
N Low = 1
PL Complessivo = c
$PFH_D = 2 \times 10^{-6}$

Interconnessioni fra sottositemi

Bisogna inoltre fare particolare attenzione alle interfacce tra i sottosistemi:

Tutte le connessioni (ad es. conduttori o bus di comunicazione dati) devono essere già considerati nel PL di uno dei sottosistemi interessati o gli errori dovuti alle connessioni devono essere esclusi o trascurabili.

I sottosistemi di sicurezza disposti in serie devono essere compatibili alle loro interfacce.

In altre parole, ogni stato di uscita di un sottosistema deve essere adatto per l'avvio dello stato sicuro del sottosistema a valle.

IEC 62061 Sicurezza del macchinario – Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per il controllo delle macchine

La IEC 62061 è derivata dalla IEC 61508 "Sicurezza funzionale dei sistemi elettrici/elettronici/elettronici programmabili relativi alla sicurezza".

La IEC 61508 è la norma internazionale di riferimento per la sicurezza funzionale dei sistemi elettrici elettronici ed elettronici programmabili.
È divisa in sette parti. Le prime tre parti stabiliscono i requisiti di sicurezza sia per l'hardware che per il software mentre le rimanenti parti sono informative, di supporto per la corretta applicazione delle prime tre.

La IEC 62061 conserva le caratteristiche della IEC 61508, ne semplifica i requisiti di sicurezza (sia per l'hardware che per il software) adattandoli alle esigenze del macchinario industriale.

Sono presi in considerazione requisiti di sicurezza solo per il funzionamento "high demand mode" (richiesta della funzione di sicurezza maggiore di una volta per anno).

La norma si basa su due concetti fondamentali:

- Gestione della sicurezza funzionale
- Livello di integrità della sicurezza

Gestione della sicurezza funzionale

Vengono precisati tutti quegli aspetti del processo di progettazione che sono necessari per raggiungere la sicurezza funzionale richiesta, che vanno quindi dall'assegnazione delle prescrizioni di sicurezza, alla documentazione, alla gestione del progetto fino alla validazione dello stesso.

Per ogni progetto dovrà essere redatto, documentato e aggiornato, per quanto necessario, un Piano della sicurezza funzionale.

Il piano della sicurezza funzionale dovrà individuare le persone, i reparti e le risorse responsabili delle attività di progettazione e costruzione del sistema di sicurezza.

Livello di integrità della sicurezza (Safety Integrity Level: SIL)

Vengono fornite una metodologia e delle prescrizioni per:

- Specificare i requisiti funzionali per ogni funzione di sicurezza da realizzare
- Assegnare il Livello di Integrità della Sicurezza (SIL) per ogni funzione di sicurezza individuata
- Consentire la progettazione di un sistema di controllo di sicurezza (SRECS) idoneo alla funzione di sicurezza da realizzare
- Validare lo SRECS

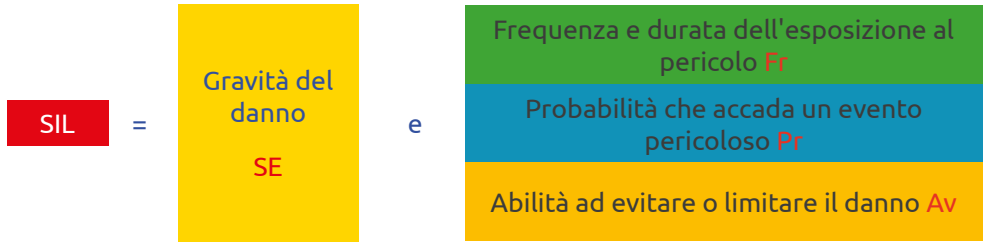
Attribuzione del SIL

Per l'assegnazione del SIL si può usare il metodo descritto nell'allegato A (la norma consente tuttavia di avvalersi anche delle tecniche descritte nella IEC 61508-5). Per ogni pericolo individuato occorre valutare:

- Il grado di severità (Se) del possibile danno
- Probabilità del verificarsi di tale danno

La probabilità che accada un evento pericoloso è funzione di:

- la frequenza e la durata (Fr) di esposizione al pericolo
- La probabilità di evento pericoloso (Pr)
- L'abilità di evitare o limitare il danno (Av)



Ne deriva che per ogni pericolo individuato devono essere valutati i parametri Se, Fr, Pr, Av:

- Grado di gravità (Se) del danno
- Frequenza e tempo (Fr) di esposizione al pericolo
- Probabilità che accada 'evento pericoloso (Pr) associato a ciascuna modalità di funzionamento della macchina
- Possibilità di evitare il pericolo (Av). Maggiore è la difficolta per evitare il pericolo, più il valore di AV è elevato

Gravità (Se)

La gravità viene decisa in base alle conseguenze di un infortunio.

Consequenza	Gravità (Se)
Irreversibile: more, perdita di un occhio o di un arto	4
Irreversibile: rottura di arto(i), perdita di dito(a)	3
Reversibile: lesioni che richiedono l'attenzione di un medico	2
Reversibile: lesioni che richiedono un primo soccorso	1

Fig. 16. Tabella A1 - Classificazione della Gravità (Se)

Frequenza e durata dell'esposizione al rischio (Fr)

- L'intervallo medio tra l'esposizione al rischio e la frequenza media di accesso alla zona pericolosa, viene stimata considerando i seguenti aspetti:
  - Tutte le modalità di utilizzo (normale funzionamento, manutenzione)
  - La natura dell'accesso (per l'alimentazione manuale di materiali, impostazioni)
  - Tempo trascorso nella zona pericolosa
  - Frequenza di accesso

Classificazione della frequenza e durata dell'esposizione al rischio (Fr)

Frequenza di esposizione	Durata dell'esposizione ≥ 10 min	Durata dell'esposizione < 10 min
≥ 1 per ora	5	5
Da < 1 per ora a ≥ 1 per giorno	5	4
Da < 1 per giorno a ≥ 1 per 2 settimana	4	3
Da < 1 per 2 settimana a ≥ 1 per anno	3	2
< 1 per anno	2	1

Fig. 17. Tabella A2 - Frequeenza e durata di esposizione al rischio (Fr)

Probabilità che accada un evento pericoloso (Pr)

Questo parametro può essere stimato tenendo conto del comportamento umano (stress, abilità, complessità della macchina) rispetto all'interazione con le parti della macchina da cui potrebbe derivare il pericolo.

Per considerare il caso peggiore si dovrebbe considerare una probabilità molto alta.

Per poter utilizzare della probabilità di accadimento dell'evento inferiori, sono richiesti elevati livello di competenze degli operatori e una conoscenza approfondita dell'applicazione.

Probabilità dell'evento	Probabilità (Pr)
Molto alta	5
Probabile	4
Possibile	3
Rara	2
Trascurabile	1

Fig. 18. Tabella A3 - Classificazione della probabilità che accada un evento pericoloso (Pr)

Probabilità di evitare o limitare il danno (Av)

Tiene conto:

- Velocità improvvisa, rapida o lenta del verificarsi di un evento pericoloso
- Possibilità di sottrarsi al pericolo spostandosi
- La natura del componente pericoloso
- Possibilità di riconoscere il pericolo

Probabilità di evitare o limitare il danno (Av)	
Impossibile	5
Rara	3
Probabile	1

Fig. 19. Tabella A4 - classificazione della probabilità di evitare o limitare il danno (Av)

Attenzione: l'opzione "probabile" va scelta solo se il pericolo è chiaramente riconoscibile e se il tempo per intervenire o per abbandonare l'area pericolosa è sufficiente.

La somma dei punteggi per gli attributi di frequenza, probabilità che accada l'evento pericoloso e la possibilità di evitarlo fornisce la classe di probabilità (Cl) del pericolo:

$$Cl = Fr + Pr + Av$$

La tabella seguente, che è un estratto del form di figura A.3 della norma IEC 62061, permette di ricavare in modo semplice il SIL da assegnare alla funzione di sicurezza.

Tabella A.6 - Matrice per l'attribuzione del SIL

Conseguenze	Severità	Classe Cl				
		4	5-7	8-10	11-13	14-15
Morte, perdita di un occhio o di un braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente: perdita di dita	3		OM	SIL 1	SIL 2	SIL 3
Reversibile: intervento medico	2			OM	SIL 1	SIL 2
Reversibile: pronto soccorso	1				OM	SIL 1

Fig. 20. Tabella 3 della IEC 62061

Attribuzione dei requisiti di sicurezza specifici (SRS) e dei requisiti funzionali di sicurezza

La specificazione dei requisiti di sicurezza (SRS) deve includere almeno le seguenti caratteristiche della macchina:

- Tempo di ciclo
  - prestazioni del tempo di risposta
  - condizioni ambientali
  - frequenza di commutazione e duty cycle di eventuali dispositivi elettromeccanici utilizzati.
- Interazioni uomo-macchina
- Comportamento della macchina in condizioni di lavoro normali
- Reazione richiesta della funzione di sicurezza

La specificazione dei requisiti funzionali deve descrivere i dettagli di ciascuna funzione di sicurezza, in particolare:

- Descrizione della funzione di sicurezza
- Condizioni di ripristino e condizioni di riavvio della macchina dopo l'attivazione della funzione di sicurezza
- Tempo di risposta della funzione di sicurezza
- Interfacce della funzione di sicurezza con le altre parti del sistema di controllo della macchina
- Modalità di funzionamento della macchina in cui la funzione di sicurezza deve essere attiva o disattivata

Processo di progettazione di un SCS (sistema di controllo relativo alla sicurezza)

Ogni funzione di sicurezza deve essere descritta in termini di:

- Requisiti operativi (modalità di funzionamento, tempo di ciclo, condizioni ambientali, tempo di risposta, tipo di interfaccia con altri componenti o sottosistemi, livello EMC, ecc.)
- Requisiti di sicurezza (SIL).

Ciascuna funzione di sicurezza deve essere suddivisa in sottofunzioni, ad es. sottofunzione per segnali di ingresso, sottofunzione per elaborazione dati logici, sottofunzione per segnali di uscita.

Un sottosistema è quindi associato a ciascuna sottofunzione.

I sottosistemi possono essere costituiti da componenti di qualsiasi tecnologia, elettrici, elettronici, pneumatici, idraulici, interconnessi tra loro. I singoli componenti sono chiamati elementi di sottosistema.

La realizzazione tecnica di un SCS assumerà quindi una struttura tipica come quella mostrata in figura (esempio di controllo accessi attuato tramite barriera fotoelettrica).

Fig. 21. Struttura tipica di un SCS

Un SCS può implementare più funzioni di sicurezza. Ciascuna funzione di sicurezza può essere composta da più sottosistemi. Un sottosistema può condividere più sottofunzioni.

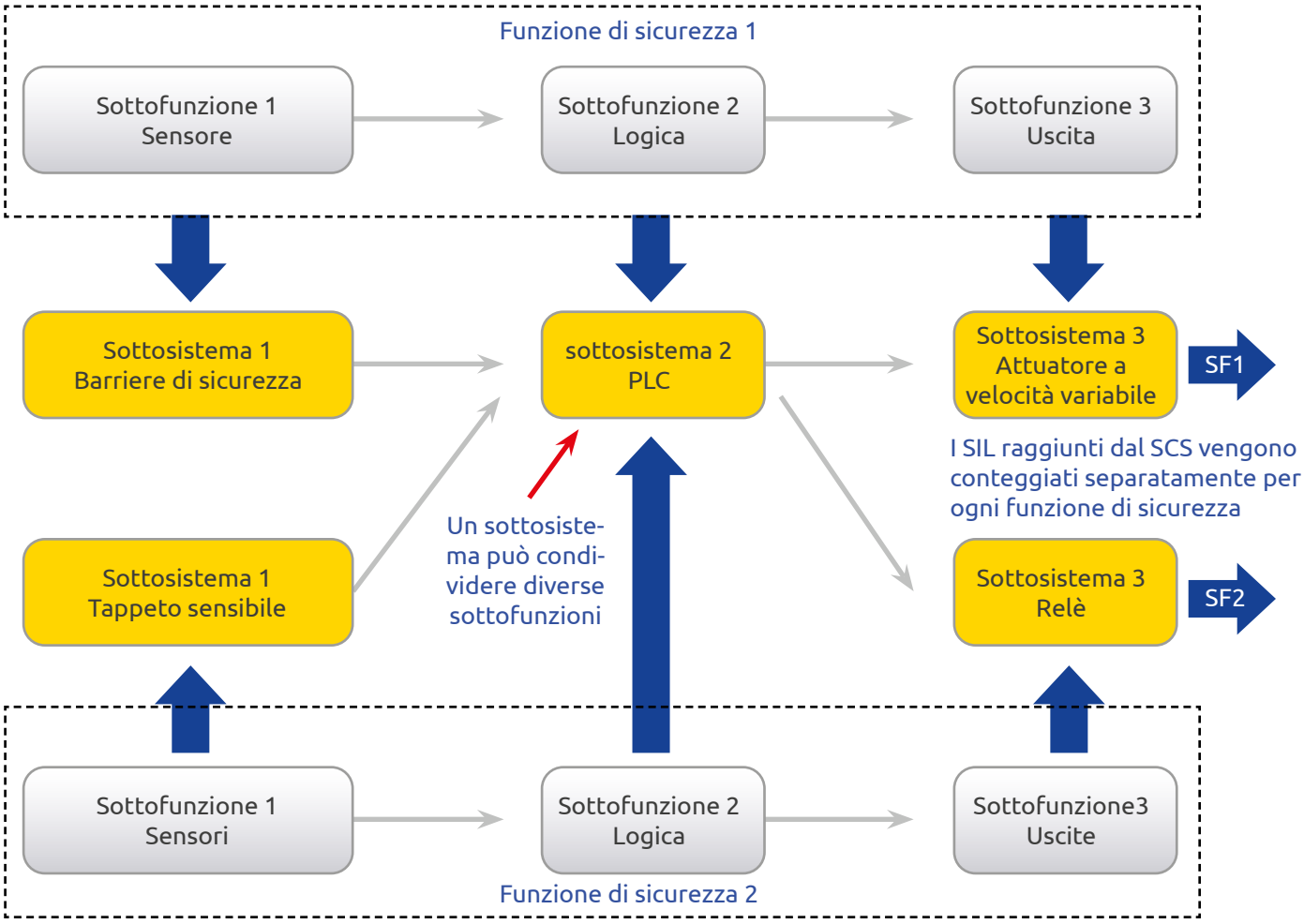


Fig. 22. Fig. 3 Struttura generale di un SCS

Se un sottosistema condivide funzioni di sicurezza con diversi livelli di integrità della sicurezza, il suo hardware e software devono essere trattati come se richiedessero il livello di integrità della sicurezza più alto.

Se un sottosistema implementa sia funzioni di sicurezza che altre funzioni, tutto il suo hardware e software deve essere trattato come relativo alla sicurezza a meno che le funzioni di sicurezza e le altre funzioni non siano sufficientemente indipendenti.

Se la comunicazione di dati digitali viene utilizzata come parte di un SCS, devono essere soddisfatti i requisiti pertinenti alla sicurezza funzionale dei bus di campo (IEC 61784-3) in conformità con l'obiettivo SIL della funzione di sicurezza.

Utilizzo di un sottosistema pre-progettato

È possibile combinare sottosistemi progettati con questa norma con sottosistemi progettati con altre norme di sicurezza. La tabella 4 della IEC 62061 fornisce una corrispondenza con i valori SIL o PL di sottosistemi progettati con altre norme.

IEC 62061	IEC 62061	IEC 61508	ISO 13849
PFH	SIL	almeno ...	almeno ...
$< 10^{-5}$	SIL1	SIL 1	PL b,c
$< 10^{-6}$	SIL 2	SIL 2	PL d
$< 10^{-7}$	SIL 3	SIL 3	PL e

Fig. 23. Tabella S4 - SIL e PFH richiesti per i sottosistemi pre-progettati

La colonna IEC 61508 include standard basati su SIL che soddisfano gli stessi vincoli architetturali, come IEC 61800-5-2 e IEC 60947-5-3.

Non è possibile individuare una perfetta corrispondenza bi-univoca tra PL e SIL; tuttavia è possibile confrontare la parte probabilistica di PL e SIL perché utilizzano lo stesso concetto per definire il grado di resistenza ai guasti, ovvero il PFH. Dato che il calcolo e i metodi utilizzati non sono gli stessi per entrambi gli standard sarà possibile confrontare i range ma non i valori esatti del calcolp.

Inoltre, vengono imposte alcune restrizioni:

- PL b non corrisponde a SIL1 nel caso di una struttura di Categoria B.
- Non si può presumere corrispondenza tra IEC 62061 e IEC 61511 (tutte le parti) o ISO 26262

PFH come parametro per misurare l'integrità della sicurezza hardware dell'SCS

Il parametro utilizzato per definire le prestazioni di sicurezza del SIL (Safety Integrity Level) è la probabilità di guasto pericoloso/ora (PFH_d). Più alto è il SIL, meno è probabile che SCS non esegua la funzione di sicurezza richiesta.

Il SIL deve essere definito per ciascuna funzione relativa alla sicurezza risultante dall'analisi dei rischi.

La tabella 3 della norma fornisce una corrispondenza tra SIL e PFH.

Limiti del SIL e valori di PFH

SIL	Valori PFH
1	< 10-5
2	$< 10^{-6}$
3	$< 10^{-7}$

Fig. 24. Tabella 3 - Limiti del SIL e valori PFH

Determinazione del PFH del SCS

Il PFH di un SCS è la somma dei singoli valori del PFH di tutti i sottosistemi che partecipano alla realizzazione del SCS e include la probabilità di errori di trasmissione pericolosi (PTE) per qualsiasi comunicazione di dati digitali.

PFH scs = PFH sottosistema 1 + ... + PFH sottosistema n +PTE

I sottosistemi di cablaggio hardware fanno parte dell'integrità sistematica e possibili guasti pericolosi nel cablaggio possono essere rilevati dalla diagnostica in linea.

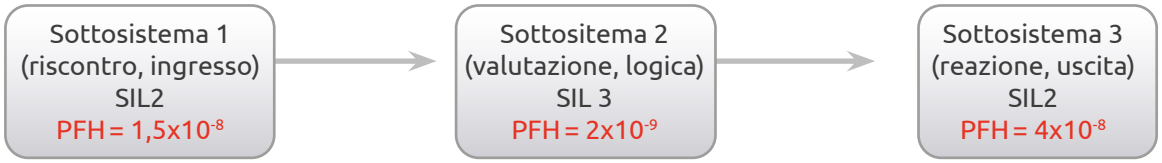
Determinazione del SIL del SCS

Dopo aver derivato il PFH dell'SCS, il SIL risultante è ricavato dalla Tabella 3. Ne deriva che il SIL massimo è limitato dalla somma dei valori PFH di tutti i sottosistemi.

I valori PFH non sono soggetti a restrizioni (ad esempio, un produttore può rivendicare per un dispositivo SIL 2 un PFH inferiore a 10^{-7} ma il SIL dell'SCS può essere solo uguale o inferiore al SIL più basso di uno qualsiasi dei sottosistemi che costituiscono SCS.

Esempio:

$$PFH_{CS} = 1{,}5x10^{-8} + 2x10^{-9} + 4x10^{-8} = 5{,}7 \times 10^{-8}$$



Limiti del SIL e valori di PFH

SIL	Valori PFH
1	< 10-5
2	< 10-6
3	< 10-7

Ne deriva che il SIL di questo SCS, nonostante il valore PFH complessivo sia adatto per un SIL 3, è limitato a SIL 2, essendo SIL 2 il SIL inferiore dei tre sottosistemi.

Inoltre, l'integrità di sicurezza dell'SCS è limitata anche dalle capacità sistematiche (ad esempio influenze ambientali, EMC e principio di rilevamento).

Requisiti per l'integrità sistematica della sicurezza

Il valore di PFH è solo uno dei parametri che contribuiscono all'assegnazione del SIL.

Per richiedere un SIL è inoltre necessario dimostrare che tutti i requisiti relativi a:

- Per evitare i guasti hardware sistematici
- Il controllo dei guasti sistematici
- L'utilizzo di componenti robusti e affidabili (conformi alle norme di prodotto, ove disponibili)
- Le condizioni ambientali in cui dovrà operare il sistema di sicurezza.

Sono stati presi in considerazione e rispettati e, qualora fosse necessario scrivere del codice software, aver adottato tutti gli aspetti organizzativi e progettuali rilevanti per il SIL obiettivo.

Misure di sicurezza rispetto ai fenomeni elettromagnetici

L'SCS non deve essere influenzato da interferenze elettromagnetiche al punto da disturbare o rendere inefficace la funzione di sicurezza in un modo che potrebbe comportare un rischio inaccettabile.

È pertanto obbligatoria una prestazione adeguata rispetto ai disturbi elettromagnetici.

Se disponibili, devono essere utilizzati solo dispositivi o apparecchiature elettriche e/o elettroniche che soddisfano i requisiti della relativa norma di prodotto in materia di immunità ai fenomeni elettromagnetici. Esempi di tali standard di prodotto sono IEC 61326-3-1, IEC 61800-5-2, IEC 61496-1, IEC 60947-5-3 (stadio CD).

Se non esiste una norma di prodotto dedicata alle influenze elettromagnetiche sugli aspetti di sicurezza funzionale, dovrebbe essere applicata la norma generica IEC 61000-6-7:2014. Deve essere effettuata un'analisi completa della sicurezza relativa agli effetti dei disturbi elettromagnetici sull'SCS per ricavare i limiti di immunità richiesti per il SIL necessario.

Per i sottosistemi pre-progettati secondo questo standard, i disturbi elettromagnetici prevedibili nell'ambiente reale dell'apparecchiatura dovrebbero essere considerate nell'SRS. I requisiti di immunità dovrebbero essere basati sulla norma generica IEC 61000-6-7:2014 se per il sottosistema non esiste una famiglia di prodotti dedicata o una norma di prodotto pertinente che affronti le influenze elettromagnetiche sulla sicurezza funzionale. Per i sottosistemi pre-progettati progettati secondo PL a o PL b di ISO 13849-1 seguire lo standard EMI applicabile è IEC 61000-6-2:2014.

Per l'integrazione di SCS nell'equipaggiamento elettrico della macchina devono essere applicate le misure EMI secondo l'allegato H della IEC 60204-1. In particolare:

- Evitare grandi circuiti conduttivi, non installare diversi sistemi di cablaggio elettrico in percorsi comuni (ad es. cavi di alimentazione, comunicazione, controllo e segnale)
- Utilizzare il filtro RF e la protezione da sovratensione e transitoria per i segnali di ingresso/uscita relativi alla sicurezza
- Se applicabile, cavi schermati e con messa a terra per motori o filtro sinusoidale tra motore e inverter o misure equivalenti.

Software applicativo relativo alla sicurezza

Quando si sviluppa un software applicativo, è preferibile separare il SW che esegue funzioni di base della macchina non di sicurezza dalle funzioni relative alla sicurezza. Laddove il software esegua sia funzioni non di sicurezza che funzioni di sicurezza, tutto il software deve essere trattato come relativo alla sicurezza.

I processi di gestione della configurazione ei processi di gestione delle modifiche devono essere definiti e documentati.

La gestione della configurazione del software deve consentire un'identificazione univoca e precisa della versione del software.

Le modifiche al SW devono essere soggette a un'analisi d'impatto che identifichi tutte le parti software interessate e le necessarie attività di riprogettazione, revisione e test per confermare che i requisiti di sicurezza del software pertinenti siano ancora soddisfatti.

Lo Standard descrive due diversi livelli di software applicativo: SW livello 1 e SW livello 2. Il SW livello 3 non è trattato in questo Standard.

SW Livello 1

Si tratta di un software applicativo che utilizza un linguaggio a variabilità limitata (LVL) dovuto all'utilizzo di moduli hardware e software pre-progettati. Esempio di sistemi che utilizzano LVL: PLC di sicurezza con LVL o relè programmabile di sicurezza.

I seguenti linguaggi sono LVL: diagramma ladder, diagramma a blocchi funzione e diagramma funzionale sequenziale.

La clausola 8.3 della norma fornisce requisiti dettagliati riguardanti il ciclo di vita della sicurezza del SW, la progettazione del SW, la progettazione del modulo, la codifica, il collaudo, la gestione delle modifiche e la documentazione.

La specifica dei requisiti di sicurezza del software deve essere sviluppata per ciascun sottosistema in base alla specifica e all'architettura SCS, documentata e gestita durante l'intero ciclo di vita dell'SCS.

È possibile utilizzare un modello del ciclo di vita della sicurezza SW come il modello V semplificato.

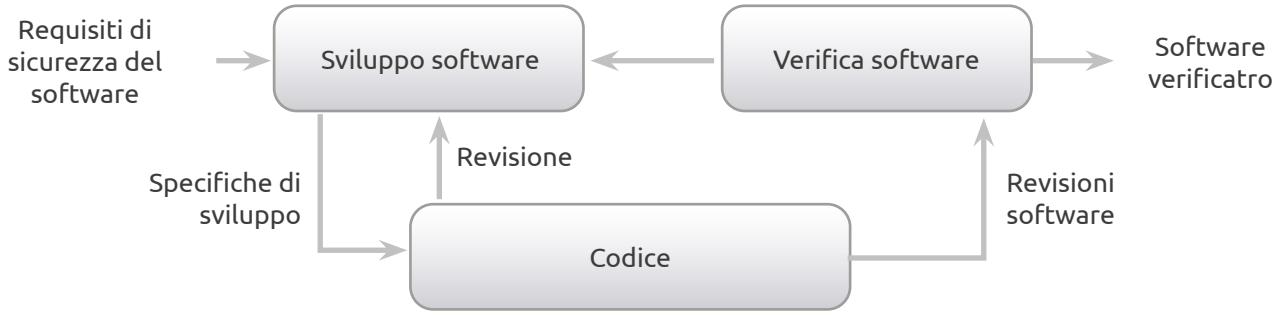


Fig. 25. Modello V per SW Livello 1

Il lato sinistro rappresenta i requisiti, ovvero le cose da raggiungere. Il lato destro dettaglia la verifica del software.

L'uscita di ciascuna fase deve essere verificata rispetto ai requisiti dell'ingresso della stessa fase.

Si raccomanda di utilizzare, ove possibile, moduli software approvati pre-progettati ma, se i moduli della libreria forniti dal produttore non sono soddisfacenti, la progettazione di moduli software personalizzati può anche essere sviluppata secondo questo modello V semplificato.

Ciascun modulo che non è stato valutato in precedenza deve essere testato rispetto ai casi di prova. Il test del software deve includere la simulazione del guasto e la relativa reazione al guasto a seconda dell'integrità di sicurezza richiesta.

SW livello 2

Viene introdotto il livello software 2 per supportare Full Variability Language (FVL). Esempio di sistemi che utilizzano FVL: PLC di sicurezza con FVL conforme a questa norma.

I seguenti linguaggi sono FVL: Ada, C, Pascal, Instruction List, linguaggi assembler, C++, Java e SQL.

Il SIL massimo raggiungibile per il livello SW 2 è SIL 2.

Il livello SW 2 è di maggiore complessità rispetto al livello SW 1 a causa dell'uso di linguaggi di programmazione completamente variabili. Pertanto, deve essere utilizzato un modello V più dettagliato.

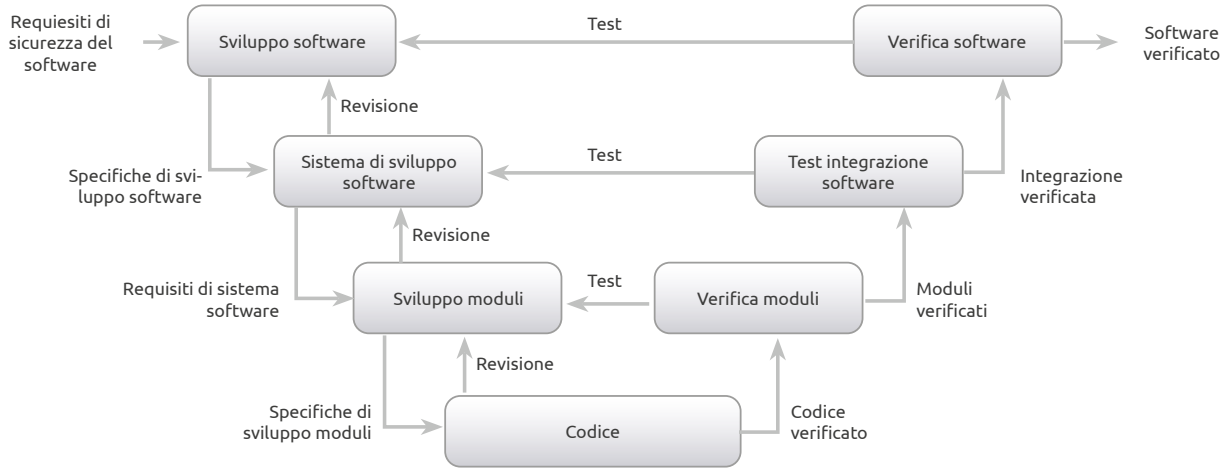


Fig. 26. Modello V del ciclo di vita della sicurezza del software per il livello 2 del software

Il lato sinistro rappresenta i requisiti, cioè le cose da raggiungere. Il lato destro dettaglia le verifiche del software.

La clausola 8.4 della norma fornisce requisiti dettagliati riguardanti il ciclo di vita della sicurezza del SW, la progettazione del SW, la progettazione del modulo, la codifica, il collaudo, la gestione delle modifiche e la documentazione.

La progettazione deve includere l'auto-monitoraggio del flusso di controllo e del flusso di dati appropriato al SIL del SCS.

Gli input della specifica di progettazione del software devono essere correlati in modo diretto agli output desiderati e viceversa.

La progettazione del sistema SW deve seguire un approccio modulare con una dimensione del modulo limitata, un'interfaccia completamente definita e un punto di ingresso/uscita in subroutine e funzioni. Ciascun modulo deve avere una singola funzione chiaramente compresa. La dimensione massima del modulo deve essere limitata a una funzione di sicurezza completa.

Laddove i moduli della libreria software sviluppati in precedenza debbano essere utilizzati come parte della progettazione, deve essere dimostrata la loro idoneità a soddisfare le specifiche dei requisiti di sicurezza del SW.

I casi di test di integrazione del SW devono essere eseguiti e documentati.

Il test del software includerà anche la simulazione del guasto e la relativa reazione al guasto. Si applicano le prove funzionali come misura di base. Dive possibile Il codice dovrebbe essere testato mediante simulazione.

Il test del software comprende due tipi di attività: devono essere eseguite sia l'analisi statica che l'analisi dinamica.

SW livello 3

Per applicazioni SW conforme a SIL 3 deve essere applicata la IEC 61508-3.

È richiesto un alto livello di competenza per progettare secondo il livello 3 del SW. I fattori che rendono l'uso della norma IEC 61508-3 per il livello 3 del SW più appropriato rispetto all'uso del SW 2 sono:

- Elevato grado di complessità della funzione di sicurezza
- Un gran numero di funzioni di sicurezza
- Grande dimensione del progetto.

Progettazione e sviluppo di sottosistemi

Fase uno - Scelta dell'architettura (struttura).

La norma propone quattro architetture predefinite e per ognuna di esse prevede una formula semplificata per il calcolo del PFH.

Le quattro architetture si differenziano per la tolleranza ai guasti hardware (HFT) e per la presenza (o assenza) della diagnostica.

Le quattro architetture corrispondono alle configurazioni più diffuse utilizzate nel campo della sicurezza dei macchinari.

Una tolleranza ai guasti hardware di N significa che il sottosistema tollera fino a N guasti prima di perdere le sue prestazioni di sicurezza. N +1 guasti possono causare la perdita della funzione di sicurezza.

Quando si definisce la tolleranza ai guasti di un'architettura non viene dato credito a misure aggiuntive in grado di controllare gli effetti dei guasti, come la diagnostica.

Per l'architettura B e D i due canali sono sufficientemente indipendenti; ovvero sono progettati in modo tale che un singolo canale sia in grado di svolgere la funzione indipendentemente dall'altro. Lo stesso vale per l'architettura C per il canale funzionale rispetto al canale diagnostico.

Architettura del sottosistema A:
HFT = 0 - Singolo canale senza funzione diagnostica

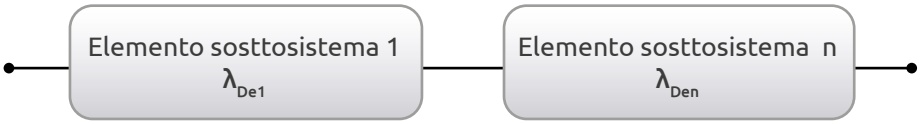


Fig. 27. Architettura di base del sottosistema A

Qualsiasi guasto pericoloso di un elemento del sottosistema provoca la perdita della funzione di sicurezza.

$$(1) \quad PFH = \lambda_{De1} + ... + \lambda_{Den}$$

λ_{Dei} è il tasso di guasto pericoloso di un elemento del singolo canale.

Confronto con EN ISO 13849-1:

Cat. B (PLmax = b) e Cat. 1 (PLmax = c)

Architettura del sottosistema B
HFT = 1 - Doppio canale senza funzione diagnostica

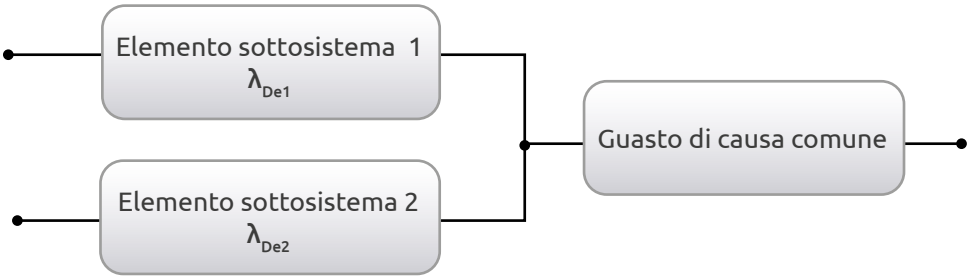


Fig. 28. Architettura di base del sottosistema B

Un singolo guasto di qualsiasi elemento del sottosistema non provoca la perdita della funzione di sicurezza

$$(2) \quad PFH = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

- λ_{De1} è il tasso di guasto pericoloso di un elemento del primo canale funzionale.
- λ_{De2} è il tasso di guasto pericoloso di un elemento del secondo canale funzionale.
- T_1 è la vita utile o l'intervallo del test di prova, qualunque sia il minore. In ogni caso non superiore a 20 anni
- β è la suscettibilità ai guasti per causa comune.

Nessuna corrispondenza con le categorie della EN ISO 13849-1

Architettura del sottosistema C:
HFT = 0 Canale singolo con funzione diagnostica

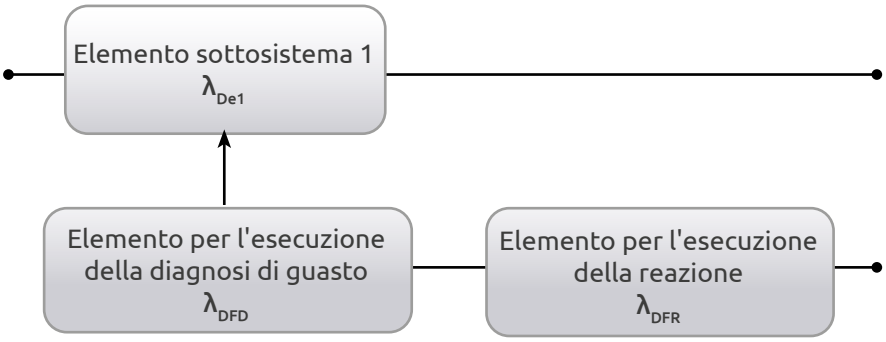


Fig. 29. Architettura di base del sottosistema C

Qualsiasi guasto pericoloso non rilevato di un elemento del sottosistema del canale funzionale comporta la perdita della funzione di sicurezza. Quando la funzione diagnostica rileva un guasto pericoloso di un elemento del sottosistema del canale funzionale, la funzione diagnostica stessa avvia una reazione all'errore.

$$(3) \quad PFH = \sum_{i=1}^{n} \lambda_{Dei} - DC \times \left(\sum_{i=1}^{n} \lambda_{Dei} - \lambda_{CC} \right) \times \left\{ 1 - \frac{1}{2} \left[\sum_{i=1}^{n} \lambda_{D\,FHj} - \lambda_{CC} \right] \times T_1 \right\}$$

Con

$$(4) \quad \lambda_{CC} = \beta \times min \left(\sum_{i=1}^{n} \lambda_{Dei} \; , \; \sum_{i=1}^{n} \lambda_{D\,FHj} \right)$$

e

$$(5) \quad DC = \frac{\sum_{i=1}^{n} (DC_i \times \lambda_{Dei})}{\sum_{i=1}^{n} \lambda_{Dei}}$$

dove:

T_1 è la vita utile o l'intervallo del test di prova, qualunque sia il minore. In ogni caso non superiore a 20 anni

λ_{Dei} è il tasso di guasto pericoloso dell'elemento ei all'interno del singolo canale funzionale.

n è il numero di elementi del singolo canale funzionale.

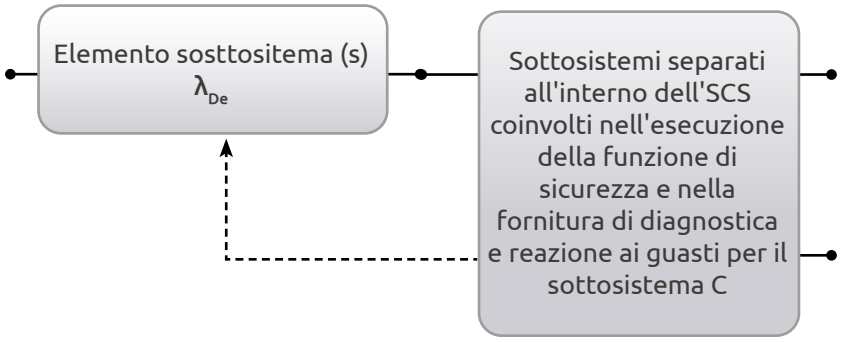
$\lambda_{DFHj} = \lambda_{DFDj} + \lambda_{DFRj}$ è il tasso di guasto degli elementi numero j all'interno del singolo canale che realizza la funzione di gestione dei guasti.

m è il numero di elementi del singolo canale che realizza le funzioni di gestione degli errori

DCi è la copertura diagnostica per l'elemento ei del singolo canale funzionale.

β è la suscettibilità ai guasti per causa comune del canale funzionale e del canale diagnostico

Se la funzione diagnostica viene eseguita da un sottosistema separato all'interno dell'SCS



Quindi:

$$\lambda_{D\,FH\,j} = 0$$

β < 2% a causa della separazione dei due sottosistemi. Quiindi le equazioni si semplificano a:

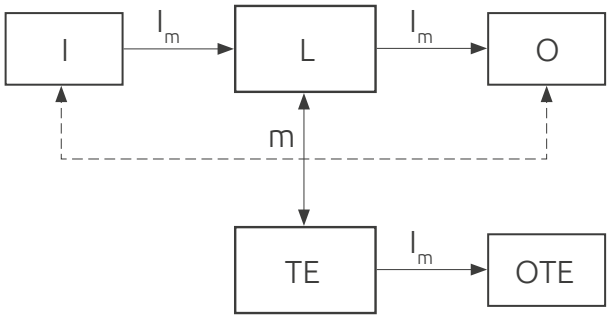
$$(6) \quad PFH = (1 - DC_1) \times \lambda_{De1} + \ldots + (1 - DC_n) \times \lambda_{Den}$$

Il tasso di test delle funzioni diagnostiche deve essere almeno 100 volte superiore al tasso di richiesta della funzione di sicurezza e il tempo necessario per la reazione al guasto deve essere breve per portare il sistema in uno stato sicuro prima che si verifichi un evento pericoloso.

In alternativa, il test può essere eseguito periodicamente. In questo caso la somma dell'intervallo di test, più il tempo necessario per rilevare il guasto più il tempo necessario per portare il sistema in uno stato sicuro è inferiore al tempo di sicurezza del processo.

Il test può anche essere eseguito immediatamente alla richiesta della funzione di sicurezza. In questo caso il tempo necessario per rilevare un guasto e portare il sistema in uno stato sicuro deve essere inferiore al tempo di sicurezza del processo.

Confronto con EN ISO 13849-1



Cat. 2 (PLmax = d)

Architettura del sottosistema D
HFT = 1 Doppio canale con funzione diagnostica

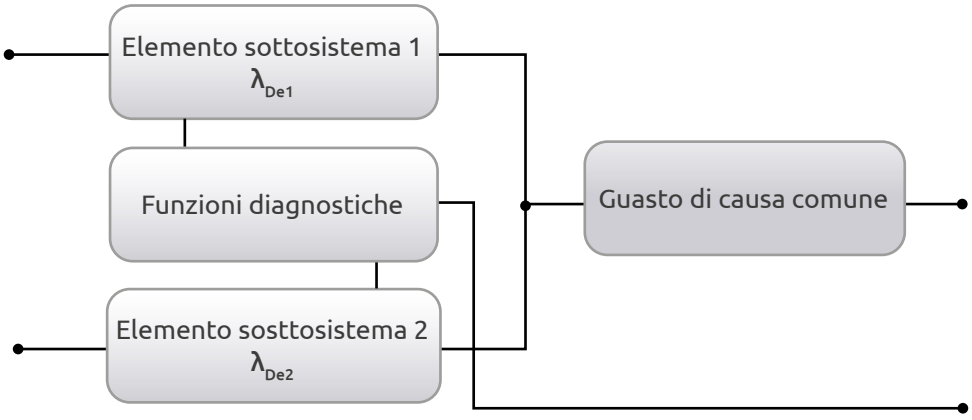


Fig. 30. Architettura del sottosistema D

Per gli elementi del sottosistema con le stesse caratteristiche:

$$(7)\quad PFH = (1-\beta)^2 \times [DC \times T_2 + (1-DC) \times T_1] \times \lambda_{De2} + \beta \times \lambda_{De}$$

Per elementi di sottosistemi con caratteristiche differenti

$$(8)\quad PFH = (1-\beta)^2 \times [\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2-DC_1-DC_2) \times T_2/2 + \beta \times (\lambda_{De1} \times \lambda_{De2})/2$$

Dove:

T_2 è l'intervallo del test diagnostico.

T_1 è la vita utile o l'intervallo del test di prova, qualunque sia il minore. In ogni caso non superiore a 20 anni

β è la suscettibilità ai guasti per causa comune.

λ_{De1} è il tasso di guasto pericoloso dell'elemento 1 del sottosistema.

λ_{De2} è il tasso di guasto pericoloso dell'elemento 2 del sottosistema.

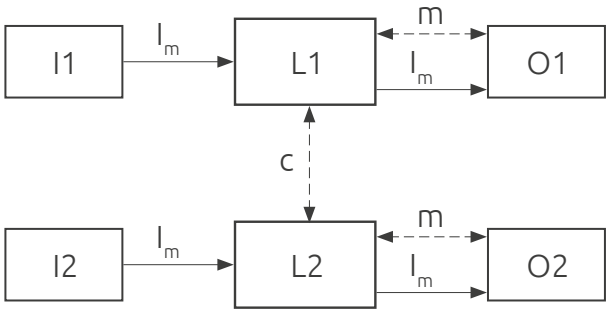
DC_1 è la copertura diagnostica per l'elemento 1 del sottosistema.

DC_2 è la copertura diagnostica per l'elemento 2 del sottosistema.

Un singolo guasto pericoloso di qualsiasi elemento del sottosistema non provoca la perdita della funzione di sicurezza. Se la funzione diagnostica rileva un guasto di un elemento del sottosistema, la funzione diagnostica stessa avvia una reazione all'errore.

La funzione diagnostica viene eseguita continuamente e la somma dell'intervallo del test diagnostico e del tempo necessario per eseguire la reazione al guasto specificata, al fine di portare il sistema in uno stato sicuro, deve essere inferiore al tempo di sicurezza del processo.

Confronto con EN ISO 13849-1



Cat. 3 (PL_{max} = d)
Cat. 4 (PL = e)

Fase due - Determinazione dei parametri λ, λ_d, λ_s, λ_{dd}, λ_{du}

Considerazioni generali

Ai fini della determinazione dei tassi di guasto degli elementi del sottosistema, devono essere presi in considerazione i seguenti criteri di guasto:

- Se, a causa di un guasto, altri componenti si rompono, il primo guasto insieme a tutti i guasti successivi sarà considerato come un guasto unico
- Due o più guasti separati aventi una causa comune devono essere considerati come un unico guasto
- Il verificarsi simultaneo di due o più guasti, aventi cause separate, è considerato altamente improbabile e pertanto non deve essere considerato
- Alcuni guasti possono essere esclusi, a condizione che la probabilità che si verifichino sia molto bassa in relazione ai requisiti di integrità della sicurezza del sottosistema

Una base per la considerazione dei guasti è fornita nella ISO 13849-2 (allegati da A a D).

Per l'elenco dei componenti/elementi inclusi negli Allegati da A a D, sono forniti:

- Le cause da considerare
- Le esclusioni di guasti consentite, considerando gli aspetti ambientali e applicativi e le condizioni in cui è consentita l'esclusione di guasti

Componenti elettrici/elettronici

Determinazione di λ

In generale, per questa tipologia di componenti il costruttore non fornisce dati di affidabilità perché dipendono fortemente dall'utilizzo del componente e dalle caratteristiche dell'ambiente.

I dati di affidabilità possono essere trovati nella serie di standard SN 29500 o in MIL-HDBK 217F o OREDA 2015 o anche nel manuale di affidabilità EXIDA.

I tassi di guasto sono espressi in FIT (Failure in time)

1 FIT = 1 x 10-9 ore

I valori di FIT sono dati alle condizioni operative di riferimento (tensione, corrente, dissipazione ecc..) e alla temperatura ambiente di 40°C. Il valore indicato è λref in FIT.

Esempio: per un resistore a fil di metallo è λ_{ref} = 0,2 FIT

Se le condizioni operative effettive sono diverse da quelle di riferimento, è necessario apportare correzioni utilizzando formule che sono previste nello stesso documento per ciascuna famiglia di componenti.

Determinazione di λ_d e λ_s

Dopo aver determinato λ per ciascun elemento del sottosistema (es. derivato da uno dei database citati), si dovrebbero considerare le diverse modalità di guasto dell'elemento del sottosistema. In genere si presume che non tutte le modalità di guasto portino a un guasto pericoloso. Per determinare i guasti da considerare per ciascun elemento e per decidere se si tratta di guasti sicuri o guasti pericolosi, dovrebbe essere eseguita una tecnica di analisi, come l'analisi della modalità di guasto e degli effetti (FMEA) o l'analisi dell'albero dei guasti (FTA).

Per effettuare questa analisi tecnica, sono necessarie le seguenti informazioni:

- Gli schemi hardware del sottosistema che descrivono ogni componente e le interconnessioni tra i componenti
- Per ogni componente le modalità di guasto e le relative percentuali della probabilità di guasto totale

Per aiutare il progettista, sono disponibili diverse fonti di settore riconosciute dove trovare un elenco di modalità di guasto insieme al rapporto modalità di guasto.

Esempio di modalità di guasto tipiche e rapporto di guasto (%) di alcuni componenti elettronici

Component		Shorts	Opens	Drift
Bipolar transistors		80	20	—
Field effect transistors		80	10	10
Diodes	general purpose	80	20	—
	Zener	70	20	
		20	60	20
Optocoupler		10	50	40
Resistors, fixed (film)		—	60	40
Capacitors	foil	15	80	5
	ceramic	70	10	20
	Al	30	30	40
Coils		20	80	—

Fig. 31. Modalità di guasto e rapporto di guasto

Il processo dovrebbe essere il seguente:

Classificazione di ogni modalità di errore in base al fatto che questo porta a:

- Un guasto sicuro (l'errore non ha alcuna influenza o l'errore porta a uno stato sicuro senza una misura diagnostica
- Un guasto pericoloso (porta senza diagnosi a un malfunzionamento pericoloso)
- Non vengono presi in considerazione i componenti che non fanno parte di una funzione di sicurezza o di una misura diagnostica e che non hanno alcuna influenza sulla funzione di sicurezza.

Facendo questa analisi, non considerare gli effetti delle tecniche diagnostiche implementate! Gli effetti della diagnostica sono considerati separatamente; si veda la clausola: calcolo della DC.

Dalla stima di λ di ciascun componente e dalla categorizzazione dei guasti (sicuro, pericoloso) calcolare la probabilità di guasto sicuro (λS) e la probabilità di guasto pericoloso (λD).

Esempio, giusto per descrivere come applicare il metodo:

Prendiamo per facilità di calcolo il caso di due componenti, un condensatore ceramico e un resistore a film metallico che fanno parte dei componenti di un canale funzionale.

Per il condensatore otteniamo da SN 29500 un tasso di guasto di 2 FIT ($\lambda = 2 \times 10^{-9}$). Dall'analisi del circuito emerge che un cortocircuito del condensatore o una deriva porta a un guasto pericoloso, mentre un circuito aperto porta a un guasto sicuro.

Per il resistore otteniamo da SN 29500 un tasso di guasto di 0,2 FIT ($\lambda = 0{,}2 \times 10^{-9}$). Dall'analisi del circuito emerge che un circuito aperto della resistenza o una deriva porta ad un guasto pericoloso, un corto circuito porta ad un guasto sicuro, ma questo tipo di guasto è escluso, per via della tecnologia. (vedi ISO 13849-2).

Per il condensatore:

$\lambda_{Scap} = 2 \times 10^{-9} \times 0{,}1 = 2 \times 10^{-10}$
$\lambda_{Dcap} = 2 \times 10^{-9} \times (0{,}7 + 0{,}2) = 1{,}8 \times 10^{-9}$

Per il resistore:

$\lambda_{Dres} = 0{,}2 \times 10^{-9} \times (0{,}6 + 0{,}4) = 0{,}2 \times 10^{-9}$

Ovviamente gli stessi calcoli devono essere effettuati per tutte le componenti del canale.

Si ricavano quindi i valori complessivi di λ_S e λ_D per il canale sommando i valori di λ_S e λ_D di ogni componente.

Limitatamente ai componenti del nostro esempio:

$\lambda_{Schannnel} = 2 \times 10^{-10}$
$\lambda_{Dchannel} = 1{,}8 \times 10^{-9} + 0{,}2 \times 10^{-9} = 2 \times 10^{-9}$

Metodo alternativo:

Se non sono disponibili informazioni specifiche sulle modalità di guasto, il 50 % dei guasti può essere stimato come pericoloso, in questo caso λ_S e λ_D sono approssimati a:

Per il condensatore:

$\lambda_{Scap} = 2 \times 10^{-9} \times 0{,}5 = 1 \times 10^{-9}$
$\lambda_{Dcap} = 2 \times 10^{-9} \times (0{,}5) = 1 \times 10^{-9}$

Per il resistore:

La tecnologia utilizzata esclude il guasto di corto circuito; se non sono disponibili informazioni aggiuntive, tutti gli altri guasti sono da considerarsi pericolosi:

$\lambda_{Dres} = 0{,}2 \times 10^{-9}$

Determinazione di λ_d per componenti elettromeccanici

Per i componenti elettromeccanici, pneumatici e meccanici soggetti ad usura (es. relè ed elettrovalvole) la percentuale di guasti aumenta con il numero di cicli elaborati.

Per questo motivo, la loro affidabilità è solitamente correlata al numero di cicli eseguiti e non al tempo per il quale hanno lavorato.

Il parametro fornito dal costruttore è il B_{10} o il B_{10d} espresso in numero di operazioni; questo è il numero di operazioni dopo le quali si verificano guasti nel 10% dei componenti verificati (test di resistenza sotto carico specificato).

Se non sono disponibili i dati del produttore, per un elenco di componenti idraulici, pneumatici ed elettromeccanici, è possibile utilizzare anche i valori B_{10d} o $MTTF_d$ riportati nella Tabella C.1 della norma. L'uso di questi valori è consentito solo alle seguenti condizioni:

Per la progettazione del componente sono stati utilizzati principi di sicurezza basilari e ben collaudati secondo ISO 13849-2 (confermati nella scheda tecnica del componente)

Il produttore del componente specifica che il componente può essere utilizzato per applicazioni relative alla sicurezza

Il progettista del sottosistema conferma che il componente viene utilizzato rispettando i principi di sicurezza di base e ben collaudati secondo ISO 13849-2.

I componenti idraulici elencati in Tabella C.1 sono caratterizzati con MTTFd. Per la conversione di MTTFd in un valore λd può essere utilizzata la seguente equazione di base:

$$(9)\quad \lambda_d = \frac{1}{MTTF_D \times 8760\ h/a}$$

Nota: $MTTF_d$ è espresso in anni; un anno è circa 8760 nostri

Per la conversione di $B_{10d\,i}$n un valore λ_d si può utilizzare la seguente equazione:

$$(10)\quad \lambda_d = (0.1 \times C) / B_{10d}$$

dove:
C = nop / 8760 (numero medio di operazioni all'ora)

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{T_{cycle}}$$ numero di operazioni annuali

h_{op} = operazione media, in ore al giorno
d_{op} = operazione media, in giorni all'anno
t_{cycle} = tempo tra l'inizio di due cicli successivi in secondi per ciclo.
8760 = numero di ore in un anno

Il tempo di funzionamento del componente deve quindi essere limitato a T_{10d} che è il tempo medio entro il quale il 10% dei componenti subisce un guasto pericoloso.

$$(11) \quad T_{10d} = 0,1 / \lambda_d$$

Se è disponibile solo B_{10} (il numero di operazioni dopo le quali il 10% dei componenti in prova subisce un guasto), B_{10d} può essere derivato conoscendo il rapporto dei guasti pericolosi (RDF)

$$(12) \quad B_{10d} = B_{10} / RDF$$

Se non sono disponibili altre informazioni, l'RDF è stimato a 0,5 (50 % di guasto pericoloso).

Esempio:

Per un relè a basso carico, il produttore specifica un B_{10} = 10 M cicli se utilizzato a basso carico (20% del carico nominale).

Il relè viene utilizzato su una macchina azionata come segue:

220 giorni/anno; 16 h/giorno (due turni); ciclo macchina: 1 min (60 cicli/h)

Dalle formule di cui sopra deriva:

Numero medio di operazioni annuali nop = 211200

Operazione media per ora C = 24,11 /h

Non vengono fornite informazioni riguardo a B10d, pertanto si assume B10d = 2 x B10

quindi: $\lambda_d = 0,1 * 24,11 / 20*10^6 = 1,2*10^{-7}$/h

Un'analisi più precisa può essere effettuata recuperando da un database di affidabilità l'elenco delle modalità di guasto e dei rapporti di modalità di guasto del relè e analizzando, per l'applicazione data, quali sono i guasti pericolosi:

Esempio:

Componenti	Modalità di guasto	Rapporti tipici della modalità di guasto %	
Relè	Tutti i contatti rimangono in posizione eccitata quando la bobina è diseccitata	25	D
	Tutti i contatti rimangono in posizione diseccitata quando la bobina è eccitata	25	S
	Il contatto non si aprirà	10	D
	Il contatto non si chiude	10	S
	Cortocircuito simultaneo tra tre contatti di un contatto in scambio	10	D
	Chiusura simultanea del contatto normalmente aperto e normalmente chiuso	10	D
	Cortocircuito tra due coppie di contatti e/o tra contatto e terminale della bobina	10	D

Rapporto guasti pericolosi (RDF) = 65%

Dall'equazione: B_{10d} = 10M / 0,65 = 15,38M operazioni

Allora $\lambda d = \lambda_d = 0,1 * 24,11 / 15,38*10^6 = 1,57*10^{-7}$/h

Fase 3 - Determinazione della Copertura Diagnostica (DC) e dei parametri λ_{dd} e λ_{du}

Supponendo che

- Un guasto può sempre accadere (altrimenti non ci sarebbe motivo di definire λ)
- Non è possibile rilevare tutti i guasti perché i meccanismi per la rilevazione dei guasti non sono tutti ugualmente efficaci ed immediati (per alcuni guasti potrebbe richiedere più tempo)
- Tuttavia, adottando misure diagnostiche appropriate, è possibile rilevare la maggior parte dei guasti pericolosi

È possibile definire un parametro DC che fornisce una stima dell'efficienza della misura diagnostica implementata.

La DC è definita come il rapporto tra il tasso dei guasti pericolosi rilevati (λ_{dd}) rispetto a tutti i guasti pericolosi rilevati e non rilevati (λ_d).

$$(13) \quad DC = \lambda_{dd} / \lambda_d$$

Chiamando λ_{du} la frazione di guasti pericolosi che rimangono inosservati ne deriva che:

$$(14) \quad \lambda_d = \lambda_{dd} + \lambda_{du}$$

e:

$$(15) \quad \lambda_{dd} = \lambda_d \times DC$$

$$(16) \quad \lambda_{du} = \lambda_d \times (1 - DC)$$

La norma IEC 62061 fornisce un elenco di diverse tecniche diagnostiche nell'allegato D e per ciascuna di esse viene assegnato un parametro DC che rappresenta la frazione di guasti pericolosi che possono essere rilevati dall'applicazione di tale tecnica diagnostica.

La gamma CC va da 0% a 99%
DC = 0% indica che non è stato rilevato alcun guasto pericoloso
DC = 99% rappresenta una frazione molto elevata di guasti pericolosi rilevati

Il progettista deve selezionare per ogni elemento del sottosistema, la tecnica diagnostica più adatta alla sua applicazione (per i segnali di ingresso, per la logica di elaborazione, per le uscite) e nel contempo garantire il livello di CC necessario.

Esempio: se la misura diagnostica attuata per il controllo dei guasti pericolosi del relè dell'esempio precedente è attuata monitorando il funzionamento del relè tramite un contatto NC collegato meccanicamente, dalla tabella D.1 segue DC = 99%:

Quindi:

$\lambda_{dd} = 1{,}2 \times 10^{-7} \times 0{,}99 = 1{,}188 \times 10^{-7}$
$\lambda_{du} = 1{,}2 \times 10^{-7} \times 0{,}01 = 1{,}2 \times 10^{-9}$

Realizzazione di funzioni diagnostiche

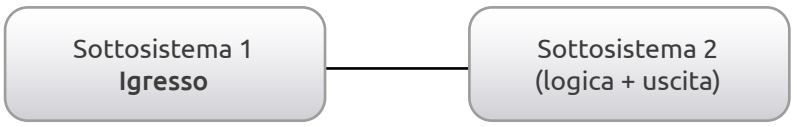
$$(17) \quad DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d}$$

Dove:

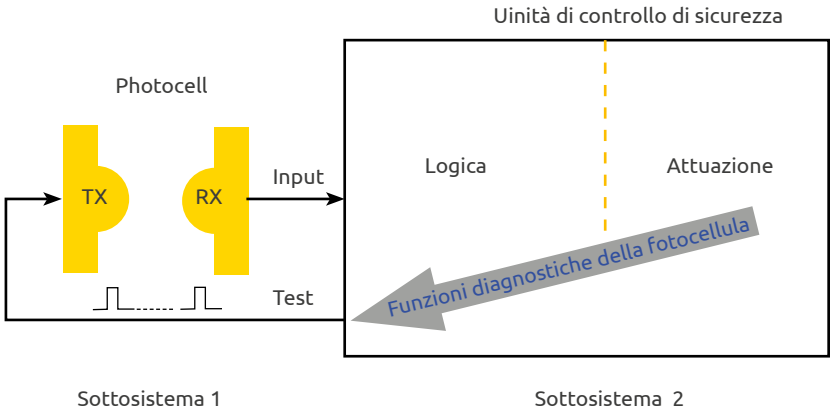
$\sum \lambda_{dd}$ è la somma del tasso di guasti pericolosi rilevati di tutti gli elementi del sottosistema e

$\sum \lambda_d$ è la somma del tasso di guasti pericolosi di tutti gli elementi del sottosistema

Le funzioni diagnostiche sono considerate come funzioni separate che possono avere anche una struttura diversa rispetto al SCS e possono essere svolte da:



a. Lo stesso sottosistema che richiede la diagnostica
b. Sottosistemi del SCS che non eseguono l'SCF



c. Altri sottosistemi del SCS

Esempio di funzione diagnostica di tipo c)

L'SCS è composto da due sottosistemi:

Il sottosistema 1 è una fotocelluna con MTBF = 10 anni (emettitore + ricevitore)
Il sottosistema 2 è un'unità di controllo di sicurezza AU SX classificata SIL 2 con un PFH = 5 x 10^{-9}

Misura diagnostica selezionata: monitoraggio online con verifica del tempo di risposta della fotocellula

Dalla tabella D.1: stimolo di prova ciclico mediante variazione dinamica dei segnali di ingresso DC = 90%.

Sottosistema 1:
Ai fini del calcolo, MTBF può essere assunto pari a MTTF,

Il rapporto dei guasti pericolosi è quindi stimato pari a 0,5
$MTTF_d = 2 \times MTTF$
$\lambda_d = 5{,}7 \times 10^{-6}$
HFT = 0 (architettura C)
$\beta \leq 2\%$

Poiché la funzione diagnostica viene eseguita dal sottosistema separato 2 all'interno dell'SCS, è possibile applicare la formula per la stima della PFH:

PFH (sottosistema 1) = (1-DC) x 5,7 x 10^{-6} = 5,7 x 10^{-7}

Il PFH complessivo dell'SCS è:

PFH (SCS) = 5,7 x 10^{-7} + 5 x 10^{-9} = 5,75 x 10^{-7}

Fase 4- Stima della frazione di guasto sicuro

Dopo aver derivato per ogni sottosistema il PFH è importante assicurarsi che il SIL associato sia compatibile con i limiti imposti dall'architettura. Il livello di integrità della sicurezza più alto che può essere rivendicato per il sottosistema è limitato dalle frazioni di guasto sicuro (SFF) come specificato nella tabella seguente

Safe failure fraction (SFF)	Tolleranza ai guasti hardware		
	0	1	2
SFF < 60%	Non permesso	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 3
SFF ≥ 99%	SIL 3	SIL 3	SIL 3

La frazione di guasto sicuro del sottosistema (SFF) è, per definizione, la frazione del tasso di guasto complessivo che non si traduce in un guasto pericoloso.

È quindi il rapporto tra la somma dei guasti sicuri complessivi e guasti pericolosi rilevati dalle tecniche diagnostiche implementate e la somma di tutti i guasti possibili (sicuro, pericoloso rilevato e pericoloso non rilevato).

$$(18) \quad SFF = (\Sigma\lambda_s + \Sigma\lambda_{dd}) / \Sigma\lambda_s + \Sigma\lambda_d$$

Per il calcolo devono essere presi in considerazione tutti i componenti, compresi quelli elettrici, elettronici, elettromeccanici, meccanici ecc., necessari per consentire al sottosistema di elaborare la funzione di sicurezza.

Metodologia per la stima della suscettibilità ai guasti per causa comune

In caso di strutture ridondanti, la metodologia utilizzata per il calcolo del PFH presuppone una sufficiente indipendenza operativa dei due canali.

Tuttavia, se i canali non sono completamente indipendenti, i guasti di causa comune dovuti a un singolo evento o condizione possono causare un malfunzionamento critico contemporaneamente su entrambi i canali in un'architettura a doppio canale.

Esempi di guasti dovuti a cause comuni, tali guasti di causa comune sono:

- Sovratensioni (una sovratensione abbastanza forte da causare più guasti catastrofici. un canale probabilmente distruggerà anche l'altro nello stesso tempo)
- Impurità del fluido (le valvole di entrambi i canali non si aprono)
- Sovratemperatura (a causa di un guasto delle ventole di raffreddamento).

Stima dell'effetto di CCF

La probabilità di guasto per causa comune introduce il problema di stimare i tassi di guasto simultaneo per più componenti oltre ai loro tassi di guasto individuali.

La IEC 62061 risolve questo problema utilizzando il metodo di punteggio proposto nell'allegato E.

La tabella E.1 del presente allegato riporta un elenco di misure ea ciascuna misura viene assegnato un valore associato che rappresenta il contributo di ciascuna misura alla riduzione dei guasti per causa comune.

Tutti i fattori che incidono sulla progettazione del sottosistema devono essere sommati per fornire un punteggio complessivo.

Per ogni misura elencata può essere rivendicato solo il punteggio pieno o nulla.

Se una misura è soddisfatta solo in parte, il punteggio secondo questa misura è zero.

Laddove si possa dimostrare che mezzi equivalenti per evitare CCF possono essere raggiunti attraverso l'uso di misure di progettazione specifiche (ad esempio l'uso di dispositivi optoisolati anziché cavi schermati), allora il punteggio pertinente può essere rivendicato in quanto ciò può essere considerato fornire lo stesso contributo per evitare CCF.

Se è possibile ottenere mezzi equivalenti per evitare il CCF attraverso l'uso di misure di progettazione specifiche (ad esempio l'uso di dispositivi opto-isolati anziché cavi schermati), è possibile rivendicare il punteggio pertinente.

Il punteggio complessivo viene utilizzato per determinare il fattore di guasto per causa comune β dalla tabella F.2 come valore percentuale.

Punteggio complessivo	fattore (β) per i guasti di causa comune
≤ 35	10% (0,1)
36 to 65	5% (0,05)
66 to 85	2% (0,02)
86 t0 100	1% (0,01)

Questo fattore β sarà utilizzato nelle formule per il calcolo del PFH di un sottosistema.

EN ISO 14119 Sicurezza del macchinario - Dispositivi di interblocco associati ai ripari mobili. Principi per la progettazione e scelta dei dispositivi

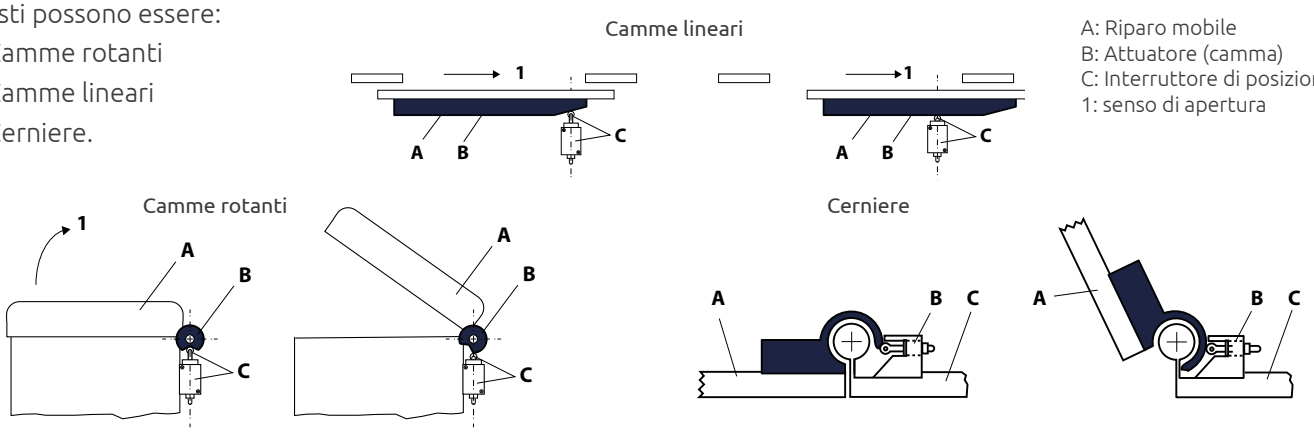
Suddivisione dei dispositivi di interblocco

Si definisce un dispositivo interbloccato, un interblocco meccanico, elettrico o di altra natura, il cui scopo è impedire il funzionamento delle operazioni pericolose delle macchine, in specifiche condizioni (generalmente fino a quando i ripari non sono chiusi).

Dispositivi di Tipo 1 - Non codificati

Questi possono essere:

- Camme rotanti
- Camme lineari
- Cerniere.

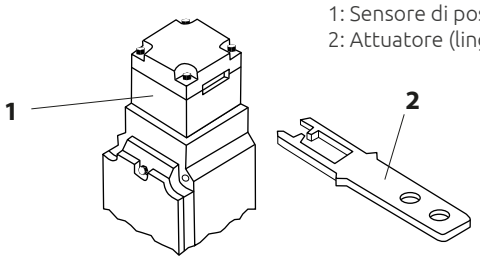


A: Riparo mobile
B: Attuatore (camma)
C: Interruttore di posizione
1: senso di apertura

Dispositivi di Tipo 2 - Codificati

Per attuatore codificato, secondo la ISO 14119:2013, § 3.13 si intende un dispositivo progettato per attivare un determinato sensore ad esempio per mezzo della forma. Esistono tre livelli di codifica:

- Attuatore con livello di codifica basso: attuatore in cui sono disponibili solo da 1 a 9 variazioni della codifica
- Attuatore con livello di codifica medio: attuatore in cui sono disponibili da 10 a 1000 variazioni della codifica
- Attuatore con livello di codifica alto: attuatore in cui sono disponibili più di 1000 variazioni della codifica

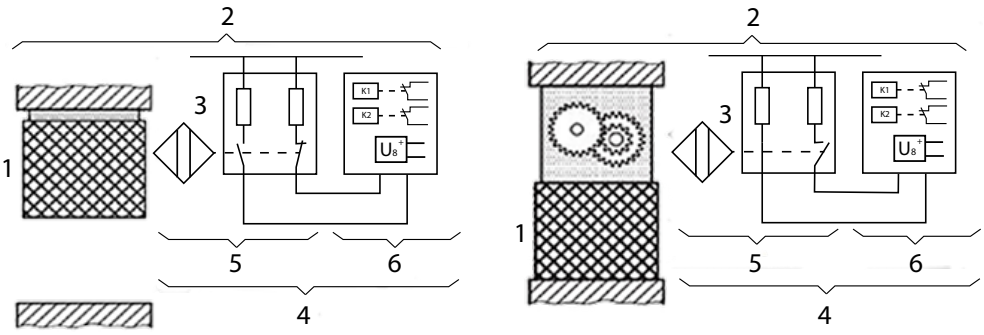


1: Sensore di posizione
2: Attuatore (linguetta o chiave)

Dispositivi di Tipo 3 - Non codificati

Questi possono essere:

- Induttivi - Azionati dal metallo del riparo
- Magnetici - Azionati da un magnete non codificato
- Capacitivi - Ultrasuoni o ottici



Riparo mobile chiuso

Riparo mobile aperto

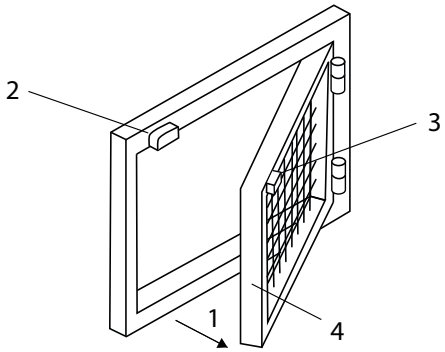
1: Riparo mobile
2: Dispositivo di interblocco
3: Attuatore (induttivo, magnetico o capacitivo)
4:Interruttore di prossimità
5: Sistema di attuazione
6: Sistema di uscita

Dispositivi di Tipo 4 - Codificati

Questi possono essere:

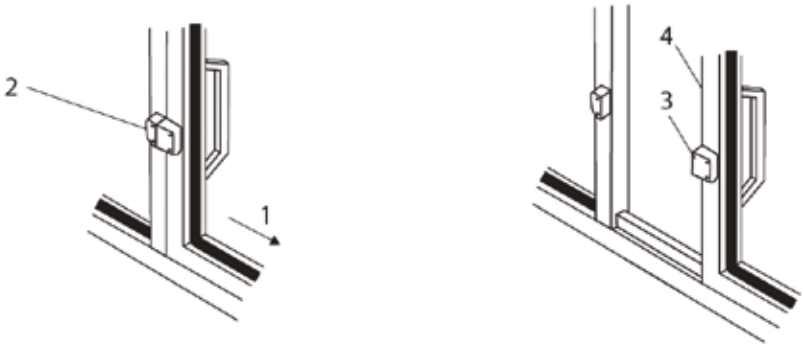
- Magnetici - Azionati da un magnete codificato
- RFID
- Ottici - Azionati da un ottica codificata

Sensore RFDI



1: Senso di apertura
2: Dispositivo di interblocco di tipo 4
3: RFID codificato
4: Riparo mobile

Dispositivi di interblocco di tipo 4 con magnete codificato

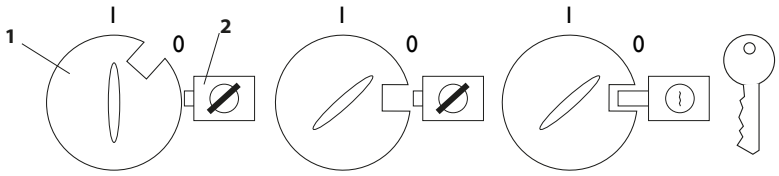


1: Senso di apertura
2: Dispositivo di interblocco di tipo 4
3: Magnete attuatore codificato
4: Riparo mobile

Dispositivi di Tipo 5 - Codificati

Ad esempio i dispositivi di Interblocco a chiave bloccata

1: Interruttore
2: Serratura



La distanza dei ripari

Come per le fotocellule di sicurezza, si deve tenere in considerazione, il tempo di arresto del movimento pericoloso in relazione alla velocità di avvicinamento. Per i valori tipici, fare riferimento alla ISO 13855:2010.

La serie di più contatti elettromeccanici

Si applica ai soli circuiti ridondanti con contatti elettromeccanici normalmente chiusi (N.C.) in serie o normalmente aperti (N.A.) in parallelo.

Fino ad ora, per una serie logica di contatti N.C., si è considerato un DC=60%, permettendo di ottenere un PL d (non un PL e). La mascheratura dei guasti, potrebbe portare ad una copertura diagnostica inferiore e quindi nulla.

Basandosi su DC = λ_{dd} / λ_{d} (rapporto tra i guasti pericolosi rilevati e quelli totali) può facilmente portare ad un DC<60%.

Dispositivi di interblocco che si basano sulla “esclusione di guasto”

La norma specifica che il massimo livello di sicurezza raggiungibile dai dispositivi di interblocco basati sulla “esclusione di guasto”, generalmente, è PL d. Infatti per questi dispositivi esiste la possibilità che un singolo guasto meccanico determini la perdita della funzione di sicurezza.

Ad esempio un guasto meccanico relativo alla chiave (attuatore) o a qualche parte del dispositivo meccanico di blocco può far trasmettere ai contatti elettrici in uscita una falsa informazione.

In alcune circostanze è comunque possibile raggiungere il livello di sicurezza PL e. Si tratta dei casi di “esclusione dei guasti per il blocco della protezione”.

Il livello di sicurezza raggiunto in questi casi non è necessariamente limitato dell’esclusione dei guasti per rottura del dispositivo di bloccaggio meccanico.

Devono però essere verificati specifici requisiti: la forza di ritenuta specificata (FZh) del dispositivo di blocco della protezione deve essere sufficiente per resistere alle forze statiche previste sul bullone di bloccaggio, inotre è necessario prevenire qualsiasi effetto sul dispositivo di blocco delle protezione determinato dalle forze dinamiche dovute al movimento del riparo.

Funzione di interblocco e funzione di bloccaggio

La norma pone l’accento sul fatto che la funzione di interblocco e quella di bloccaggio sono 2 funzioni di sicurezza separate con Pl r che possono anche essere diversi (PL r Bloccaggio < PL r interblocco)

Misure per evitare l’elusione del dispositivo di interblocco

I ripari e i dispositivi di protezione delle macchine non devono essere facilmente elusi o resi inefficaci (Direttiva Macchine 2006/42/EC). Sono richiesti provvedimenti per minimizzare la manomissione.

Elusione secondo la ISO 14119:2013, § 3.7 e § 3.8

Per elusione si intende un’azione che rende inoperativo un dispositivo di interblocco o lo scavalca con il risultato che la macchina è utilizzata in un modo differente da quello previsto dal fabbricante o senza le misure di sicurezza necessarie. Per elusione in un modo ragionevolmente prevedibile si intende un’elusione effettuata manualmente o mediante l’utilizzo di attrezzi facilmente disponibili.

Occorre implementare un modo operativo idoneo a ridurre le motiviazioni che possono portare all’elusione. Se non possibile allora possono essere adottate delle misure per ridurre l’elusione dei dispositivi di interblocco;

- Impedire l’accesso agli elementi che costituiscono il dispositivo di interblocco: posizione difficilmente raggiungibile, ostacoli fisici, montaggio in zone nascoste)
- Impedire la sostituzione degli attuatori utilizzando dispositivi di interblocco codificati
- Impedire lo smontaggio o lo spostamento dei dispositivi di interblocco (saldature, incollaggio, rivettatura, ecc..)
- Monitoraggio dello stato del dispositivo di interblocco
- Aggiunta di un ulteriore dispositivo di interblocco con un differente principio di attuazione. In questo caso si potrà verificare la plausibilità dello stato di entrambi i dispositivi

La tabella 3 della norma ISO 14119:2013 specifica le misure aggiuntive anti-manomissione che devono essere adottate a seconda dei dispositivi di interblocco utilizzati.

Misure anti-manomissione nel caso di sensori magnetici a basso livello di codifica (MAGNUS)

Obbligatorio:

- Montaggio in luoghi non raggiungibli, oppure montaggio in zone incassate e non visibili della macchina, oppure monitoraggio dello stato
- Fissaggio dell’attuatore in modo che sia difficile rimuoverlo

Raccomandazioni:

- Un secondo sensore magnetico
- Controllo di plausibilità di entrambi i sensori

Controllo della velocità in sicurezza

I sistemi di controllo della velocità di sicurezza che usano sensori (encoder, proximity) per la misura della velocità, devono essere in grado di rilevare possibili guasti pericolosi dei sensori stessi.

Combinazioni tra sensori e controllori di sicurezza

Encoder di sicurezza certificati Sin/Cos SIL3 +  Moduli Mosaic per il controllo in sicurezza della velocità MV1 o MV2 = SIL 3 PL e Cat. 4

L'Encoder è un sensore di sicurezza con classificazione SIL. I moduli Mosaic (MV1 o MV2) controllano:

- Le informazioni fornite dal sensore (sin/cos)
- Eventuali guasti sui cavi di collegamento

È possibile applicare l'esclusione del guasto meccanico (allentamento o perdita di accoppiamento meccanico con il motore). Il sistema di accoppiamento deve essere progettato, costruito e validato com specificato nella tabella B 8 della norma EN 61800-5-2:2016.

Nota: Nel caso il livello di sicurezza dell'encoder fosse SIL 2, il risultato della combinazione (encoder + moduli MV del sistema Mosiac) diventerebbe SIL 2 - Pl d.

Encoder non di sicurezza TTL o HTL o Sin/Cos +  1 Proximity +  Moduli Mosaic per il controllo in sicurezza della velocità MV1 o MV2 = Up to SIL 3 PL e Cat. 3

I due sensori non di sicurezza (encoder e proximity) formano un sistema doppio canale. I moduli Mosaic (MV1 o MV2) controllano:

- Le informazioni fornite dai due sensori (ad esempio le differenze tra i due valori misurati)
- Eventuali guasti sui cavi di collegamento

Il sistema doppio canale ha una copertura diagnostica pari al 90% (DC_{avg} = 90% medio)

Il sistema di accoppiamento meccanico del encoder con il motore deve essere progettato, costruito e validato com specificato nella tabella B 8 della norma EN 61800-5-2:2016. Utilizzando opportune soluzioni meccaniche, devono inoltre essere esclusi guasti meccanici sull'accoppiamento della ruota fonica utilizzata dal proximity.

La soluzione con sistema doppio canale permette di raggiungere la Cat. 3.
I due canali non sono omogenei perche i due sensori utilizzano diverse tecnologie. Questo permette di ridurre i guasti di causa comune aumentano il punteggio relativo al CCF (Common Cause Failure).

Per il calcolo del PL, è necessario conoscere i valori di $MTTF_d$ di entrambi i sensori.

2 Proximity +  Modulo Mosaic per il controllo in sicurezza della velocità MV0 = **Up to SIL 3 - PL e - Cat. 3**

I due proximity non di sicurezza formano un sistema doppio canale.

- I due proximity devono essere installati in modo da generare segnali interlacciati.
- Il modulo Mosaic (MV0) verifica che i due sensori misurino la stessa velocità. Il guasto di uno dei due canali (elettrico o meccanico) provoca una diversità nei valori misurati rilevata dal controllore che genera un segnale di allarme.
- Utilizzando opportune soluzioni meccaniche, devono essere esclusi guasti meccanici sull'accoppiamento della ruota fonica utilizzata dai proximity.

Se si verificano le condizioni elencate, la copertura diagnostica è pari al 90% (DC_{avg} = 90% medio).

Anche in quato caso abbiamo un sistema doppio canale che permette di raggiungere la Cat. 3
I due canali sono omogenei (sensori di uguale tecnologia). Questo può aumentare la possibilità di guasti di causa comune rispetto alla soluzione Encoder + Proximity, rendendo più difficile il raggiungimento del punteggio minimo (65) del fattore CCF (Common Cause Failure).

Per il calcolo del PL, è necessario conoscere i valori di $MTTF_d$ di entrambi i sensori.

2 Encoder non di sicurezza TTL o HTL o Sin/Cos +  Moduli Mosaic per il controllo in sicurezza della velocità MV1 o MV2 = **Up to SIL 3 PL e Cat. 3**

I due encoder non di sicurezza formano un sistema doppio canale.

- I moduli Mosaic (MV1 o MV2) verificano che i due sensori misurino la stessa velocità. Il guasto di uno dei due canali (elettrico o meccanico) provoca una diversità nei valori misurati rilevata dal controllore che genera un segnale di allarme.
- È possibile applicare l'esclusione del guasto meccanico (allentamento o perdita di accoppiamento meccanico con il motore). Il sistema di accoppiamento deve essere progettato, costruito e validato com specificato nella tabella B 8 della norma EN 61800-5-2:2016.

La soluzione con sistema doppio canale permette di raggiungere la Cat. 3 con una copertura diagnostica è pari al 90% (DC_{avg} = 90% medio).

I due canali sono omogenei (sensori di uguale tecnologia). Questo può aumentare la possibilità di guasti di causa comune rendendo più difficile il raggiungimento del punteggio minimo (65) del fattore CCF (Common Cause Failure).

Per il calcolo del PL, è necessario conoscere i valori di $MTTF_d$ di entrambi i sensori.

Encoder non di sicurezza TTL o HTL o Sin/Cos +  Moduli Mosaic per il controllo in sicurezza della velocità MV1 = **Cat. B PL b**

L'utilizzo di un singolo sensore (singolo canale) non permette al modulo Mosaic MV1 di eseguire dei controlli di palusibilità sulle informazioni ricevute.

Un guasto meccanico o elettrico sul canale non può quindi essere rilevato. Il controllore Mosaic è in grado di rilvare solo eventuali problemi di collegamento dei cavi.

Non è possibile una copertura diagnistica, quindi $DC_{avg} = 0$

Questa soluzione permette di raggiungere la Cat. B, mentre il limite massimo raggiungibile di livello di sicurezza è PL b.

Utilizzando opportune soluzioni meccaniche, possono essere esclusi guasti meccanici sull'accoppiamento tra l'encoder ed il motore.

Per il calcolo del PL, è necessario conoscere il valorl di $MTTF_d$ dell'encoder.

Questa soluzione potrebbe raggiungere il livello di sicurezza **SIL 1 - PL c - Cat. 1** solo se l'encoder utilizzato può considerarsi un componente "ben provato" per applicazioni di sicurezza (EN ISO 13849-1 tab. 10) e il suo $MTTF_d$ è più alto di 30 anni. Sebbene teoricamente possibile, questa soluzione non è consigliata per le seguente ragioni:

- La ISO EN 13849-1 (§ 6.2.4) fornisce le seguenti definizioni:
  Un "componente ben provato" è un componente che è stato:
  ampiamente utilizzato in passato con risultati positivi in applicazioni simili
  realizzato e verificato utilizzando principi che ne dimostrano l'idoneità, l'affidabilità e la robustezza per applicazioni legate alla sicurezza. La qualificazione di un componente come ben provato dipende dalla sua applicazione. Esempio, un interruttore di posizione con contatti ad apertura positiva può essere ben provato per una macchina utensile ed allo stesso tempo inappropriato per l'applicazione nell'industria alimentare.
- Componenti elettronici complessi (per esempio: PLC, microprocessori, circuiti integrati relativi ad applicazioni specifiche) non possono essere considerati componenti ben provati
- Gli encoder non fanno parte dell'elenco dei componenti ben provati della tabella D3 della ISO EN 13849-2
- Un encoder può essere dichiarato un componente ben provato per applicazioni di sicurezza solo se l'utilizzatore dell'encoder può dimostrare e documentare il suo corretto comportamento e l'elevata affidabilità in tutte le condizioni ambientali che possono essere assunte per l'intera vita del dispositivo, per un sufficiente numero di parti e per un tempo adeguatamente lungo

1 Proximity +  Moduli Mosaic per il controllo in sicurezza della velocità MV0 = Cat. B - PL b

Il proximity deve avere due uscite antivalenti.

L'utilizzo di un singolo sensore (singolo canale) non permette al modulo Mosaic MV0 di eseguire dei controlli di palusibilità sulle informazioni ricevute.

Un guasto meccanico o elettrico sul canale non può quindi essere rilevato. Il controllore Mosaic è in grado di rilvare solo eventuali problemi di collegamento dei cavi.

Non è possibile una copertura diagnistica, quindi $DC_{avg} = 0$

Questa soluzione permette di raggiungere la Cat. B, mentre il limite massimo raggiungibile di livello di sicurezza è PL b.

Utilizzando opportune soluzioni meccaniche, possono essere esclusi guasti meccanici sull'accoppiamento tra l'encoder ed il motore.

Per il calcolo del PL, è necessario conoscere il valorl di $MTTF_d$ dell'encoder.

Attenzione: Quando si utilizzano ruote foniche, potrebbe verificarsi un problema a causa dell'isteresi del sensore. Se la ruota fonica si ferma in una posizione in cui la zona rilevata dal sensore si trova al limite (destro o sinistro) della zona rilevabile (es. a destra o a sinistra del dente della ruota), il sistema può eseguire erroneamente il conteggio di questa zona.

Questa soluzione potrebbe raggiungere il livello di sicurezza **SIL 1 - PL c - Cat. 1** solo se il prozimity utilizzato può considerarsi un componente "ben provato" per applicazioni di sicurezza (EN ISO 13849-1 tab. 10) e il suo $MTTF_d$ è più alto di 30 anni. Sebbene teoricamente possibile, questa soluzione non è consigliata per le stesse ragioni indicate al punto precedente. Quanto indicato per l'encoder è valido anche per il proximity.

Elenchiamo i principi generali di sicurezza validi per tutte le combinazioni illustrate.

I sensori devono essere fissati, installati e cablati secondo le istruzioni del produttore. Rispettare i principi di sicurezza meccanica ed elettrica di base (solo per le parti non fornite dal produttore del sensore). In particolare su:

- Meccanico:
  - Corretto dimensionamento e sagomatura
  - Selezione, combinazione, disposizioni, assemblaggio e installazione corretti dei componenti / sistema
  - Fissaggio corretto
- Elettrico:
  - Selezione, combinazione, disposizioni, assemblaggio e installazione corretti dei componenti / sistema
  - Corretto incollaggio protettivo
  - Resistente alle condizioni ambientali
  - Fissaggio sicuro dei dispositivi di ingresso
  - Protezione del circuito di controllo Orientamento in modalità guasto

Principi di sicurezza aggiuntivi per combinazioni di livelli di sicurezza SIL1 - PL c, SIL2 - PL d, SIL 3 - PL e

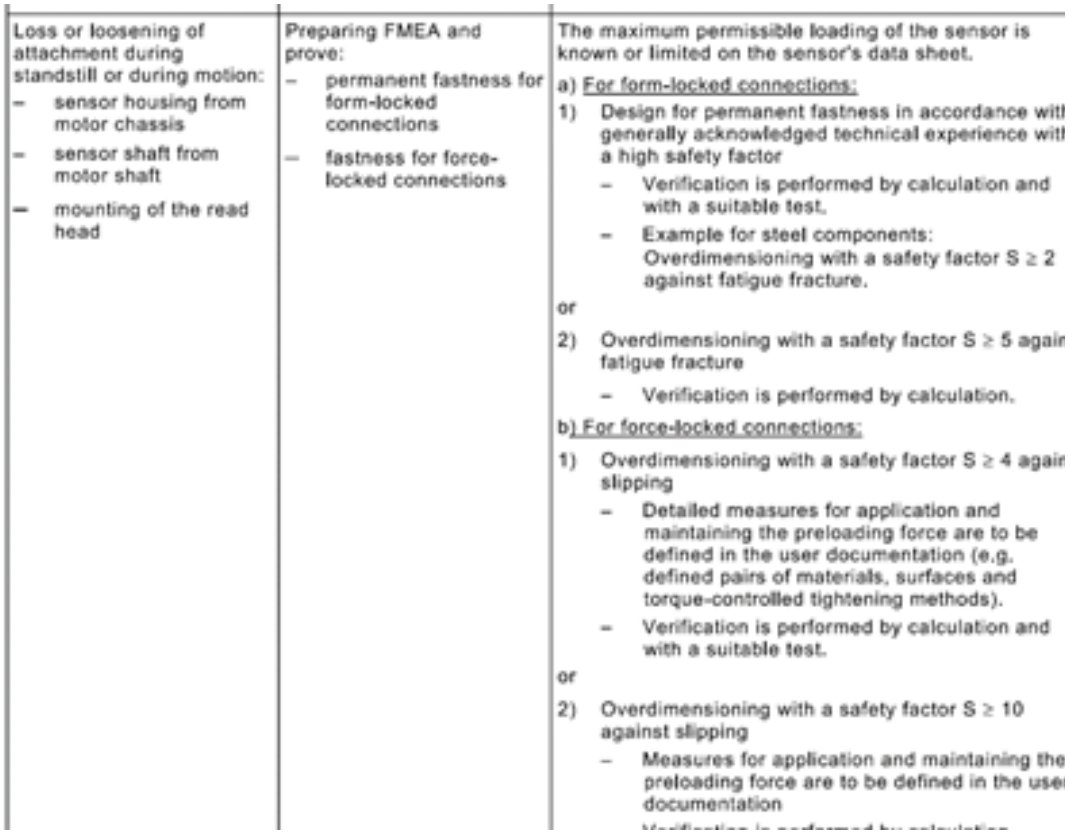
Rispettare i principi di sicurezza meccanica ed elettrica ben collaudati (solo per le parti non fornite dal produttore del sensore). In particolare su:

- Meccanico:
  - Fattore di sovradimensionamento / sicurezza
  - Posizione sicura
  - Accurata selezione, combinazione, disposizione, assemblaggio e installazione di componenti / sistemi relativi all'applicazione
  - Accurata selezione del fissaggio in relazione all'applicazione
  - Gamma limitata di forza e parametri simili
  - Gamma limitata di velocità e parametri simili.
- Elettrico:
  - Prevenzione dei guasti nei cavi
  - Limitazione dei parametri elettrici
  - Nessun stato indefinito

- Orientamento della modalità di guasto
- Modalità di guasto orientata
- Riduzione al minimo della possibilità di guasti.

La tabella D.8 della norma IEC EN 61800-5-2 (2016)ci fornisce l'elenco dei guasti pericolosi considerati per questi sensori e delle possibili esclusioni di guasto.

- Maggiore sarà la quantità di guasti rilevati dal controllore, più alta sarà la copertura diagnostica e quindi migliore il livello di sicurezza raggiungibile per la funzione considerata.
- La possibilità di applicare l'esclusione dei guasti elimina la necessità di controllarli e aumenta la prestazione di sicurezza raggiungibile.
- Al fine di confermare l'esclusione del guasto per tutta la vita del dispositivo, possono essere applicate ulteriori misure atte a garantire che le condizioni ambientali di utilizzo (Vibrazioni, urti, temperatura) non superino quelle stabilite che hanno portato alla decisione di escludere il guasto.



Loss or loosening of attachment during standstill or during motion: – sensor housing from motor chassis – sensor shaft from motor shaft – mounting of the read head	Preparing FMEA and prove: – permanent fastness for form-locked connections – fastness for force-locked connections	The maximum permissible loading of the sensor is known or limited on the sensor's data sheet. a) For form-locked connections: 1) Design for permanent fastness in accordance witl generally acknowledged technical experience witl a high safety factor – Verification is performed by calculation and with a suitable test. – Example for steel components: Overdimensioning with a safety factor S ≥ 2 against fatigue fracture. or 2) Overdimensioning with a safety factor S ≥ 5 agair fatigue fracture – Verification is performed by calculation. b) For force-locked connections: 1) Overdimensioning with a safety factor S ≥ 4 agair slipping – Detailed measures for application and maintaining the preloading force are to be defined in the user documentation (e.g. defined pairs of materials, surfaces and torque-controlled tightening methods). – Verification is performed by calculation and with a suitable test. or 2) Overdimensioning with a safety factor S ≥ 10 against slipping – Measures for application and maintaining the preloading force are to be defined in the use documentation

Fig. 32. - Estratto della Tabella D.8 della normativa EN 618005-2: 2016

Moduli di sicurezza analogici Mosaic (MA2 - MA4) e sensori analogici

Molto spesso nelle macchine e negli impianti industriali, sono presenti processi che richiedo funzioni di sicurezza in grado di raggiungere i livelli PL o SIL. Ad esempio, la norma EN528 per i trasloelevatori, richiede un controllo di peso con un performance level PL r=d. Per rispondere a questa esigenza, nella gamma Mosaic sono stati aggiunti i moduli MA2 e MA4 in grado di effettuare una valutazione in sicurezza di grandezze analogiche.

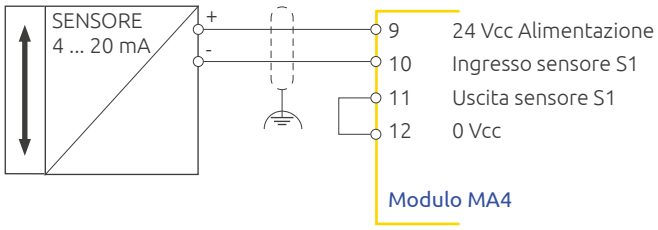
I moduli MA2 e MA4 sono certificati secondo la Direttiva macchine 2006/42/CE. Sono anche conformi anche agli standard delle serie EN IEC 61508, quindi possono essere utilizzati anche negli impianti di processo, per sistemi SIS e funzioni SIF.

I moduli MA2 e MA4 possono gestire 2 o 4 canali di ingresso analogici. Questi ingressi possono essere usati singolarmente oppure in coppia.

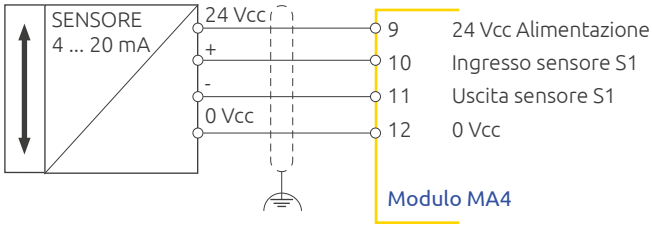
- Quando gli ingressi vengono utilizzati singolarmente, a seconda dei sensori collegati, il sistema può raggiungere un livello di sicurezza fino a SIL 1 o SIL 2 e PL d.
- Quando gli ingressi sono utilizzati in coppia, a seconda dei sensori collegati, il sistema può raggiungere un livello di sicurezza pari a SIL 3 / PLe.

Ogni ingresso analogico è completamente isolato fino a 500 VDC. MA2 e MA4 possono essere configurati per essere connessi a 1 o 2 sensori con uscita in corrente (0÷20mA, 4÷20mA) o sensori con uscita in tensione (0÷10V). Sono inoltre possibili diverse configurazioni di collegamento.

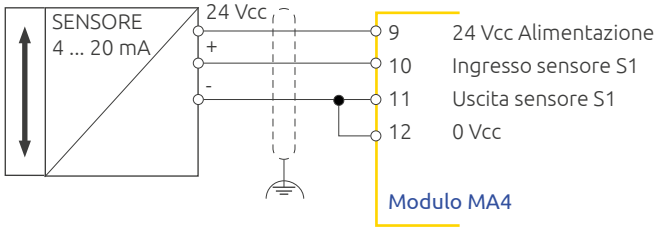
Sensore con uscita in corrente 2 fili



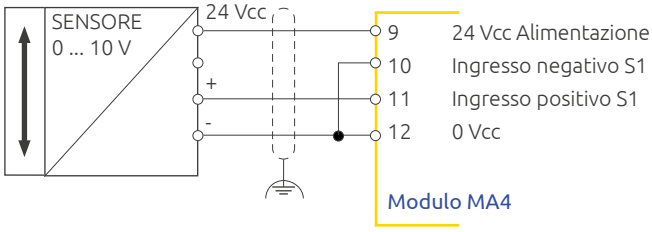
Sensore con uscita in corrente 4 fili



Sensore con uscita in corrente 3 fili



Sensore con uscita in tensione 3 fili



Sensori con uscite in tensione 0-5V. Questi sensori possono essere collegati a moduli configurati per ingresso in tensione selezionando nel Software MSD un valore di fondo scala due volte superiore. Esempio: se il fondo scala è 100 kg a 5V, occorre selezionare 200 kg . In questo caso, 1 bit di risoluzione andrà perso sui 16 disponibili.

Esistono inoltre sensori in grado di misurare valori sia positivi che negativi. I moduli analogici Mosaic possono accettare dai sensori anche valori negativi (ad esempio un flusso può andare nelle due direzioni, la pressione può anche essere vuoto, ecc.).

In questo caso il segnale di output potrà avere, per esempio:

- Un fondo scala minimo che si riferisce a un valore negativo (4 mA)
- Un fondo scala massimo che si riferisce a un valore positivo (20 mA)
- Il valore zero sarà posizionato al centro della scala (12 mA)

Moduli MA2, MA4 utilizzati con sensori analogici di sicurezza

In commercio sono disponibili sensori analogici già certificati SIL (Tipicamente secondo IEC 61508). Questa Norma è utilizzata principalmente nel mondo dell'industria di processo e meno conosciuta nel mondo delle macchine e dell'automazione industriale dove vengono utilizzate le EN ISO 13849-1/2 e EN 62061. Per esempio:

- Sensori di temperatura
- Sensori di flusso
- Sensori di pressione
- Sensori di LEL (Lower explosive limit) per zone Atex
- Sensori di peso
- Sensori fiamma
- Trasduttori di grandezze fisiche in segnali di corrente da 4 a 20 mA sempre con certificazioni SIL.

L'utilizzo di questi sensori già classificati SIL facilita il calcolo dell'integrità di sicurezza complessiva della funzione di sicurezza. per calcolare il livello di sicurezza raggiungibile, anche se necessario.

Semplificando il più possibile, analizziamo questi esempi:

Livello di sicurezza secondo la IEC 61508

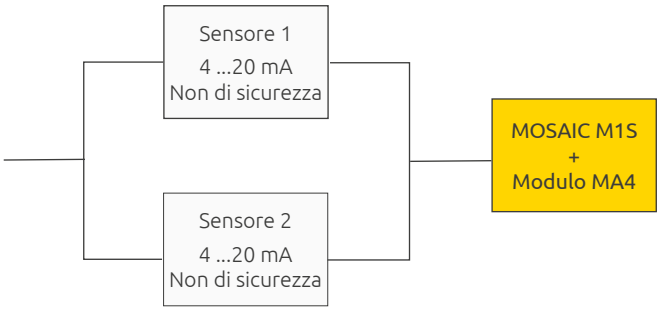
Sensore	MA2, MA4	Livello di sicurezza applicazione
1 sensore SIL 3	SIL3	SIL 3
2 sensori SIL 2 in parallelo	SIL3	SIL 3
2 sensori SIL 1 in parallelo	SIL3	SIL 2
1 sensore SIL 2	SIL3	SIL 2
1 sensore SIL 1	SIL3	SIL 1

Moduli MA2, MA4 utilizzati con sensori analogici non di sicurezza

Esistono sensori analogici non di sicurezza. Utilizzando i moduli analogici Mosaic MA2 e MA4 questi sensori possono essere utilizzati anche per funzioni di sicurezza secondo la EN ISO 13849. Prendiamo in considerazione la EN ISO 13849-1 in quanto è la norma che viene più frequentemente utilizzata nell'ambito delle macchine.

Le caratteristiche dei moduli MA2 MA4 permettono di connettere 2 sensori di misura, di metterli in relazione tra loro realizzando la ridondanza ed il cross monitoring per incrementare il livello di sicurezza totale ottenibile dal sistema. In questo modo è possibile ottenere la verifica della misurazione ed ottenere un livello di sicurezza superiore a quello ottenibile usando un solo sensore.

Possono essere utilizzati sensori di automazione, ovvero senza livello di sicurezza PL/SIL dichiarato dal costruttore e raggiungere comunque un livello di sicurezza anche molto elevato, fino a SIL 3 / PLe, naturalmente soddisfacendo tutte le condizioni richieste dalle normative. A fianco una rappresentazione logica del sistema.



Di seguito verrà presentato un esempio dove saranno analizzati gli aspetti più importanti delle valutazioni da eseguire e verranno messe in evidenza le procedure che devono essere messe in atto per assicurare che, con il sistema Mosaic, venga raggiunto il livello di sicurezza richiesto.

Nell'esempio sono rappresentati: Sensori non di sicurezza (senza PL/SIL dichiarato dal costruttore) 4-20 mA e Mosaic M1S con modulo MA4.

Analizzeremo quindi quale è il PL raggiungibile e a quali condizioni.

Questa architettura rappresenta una coppia di sensori analogici che misurano la stessa grandezza fisica.

Occorre verificare che:

- La Funzione di sicurezza SF (Safety Function), generi un segnale di arresto (qui non rappresentato) al superamento di un certo valore di soglia
- Il comportamento in caso di guasto sia stato ben identificato. Con i sistemi di sicurezza che misurano grandezze analogiche, la valutazione del comportamento in caso di guasto è più complessa. Il comportamento va valutato molto bene e la decisione è spesso non univoca. In generale si può dire che, in caso di guasto di un componente, il sistema si deve comportare come se il segnale che ne proviene avesse superato la soglia oltre la quale la macchina deve essere arrestata (guasto orientato verso la sicurezza).
- Il software relativo alla sicurezza sia stato realizzato secondo EN ISO13849-1 §4.6
- Siano verificati ed esclusi i guasti sistematici (EN ISO13849-1 Allegato G)
- Sia verificata la capacità di eseguire la funzione di sicurezza alle condizioni ambientali previste

L'architettura con 2 sensori indica una categoria 3 o 4 per la presenza della ridondanza. Verificheremo quali condizioni si devono rispettare per ottenere la Categoria 4 o la Categoria 3.

Bisogna far riferimento alla tabella 10 della ISO 13849-1, che si occupa di fare una prima classificazione:

Categoria	Riassunto delle caratteristiche	Comportamento del sistema	Principi usati per ottenere la sicurezza	$MTTF_D$ di ogni canale	Copertura diagnostica (DC_{avg})	Guasti di modo comune (CCF)
B	Progettazione secondo i principi di base della sicurezza	Un guasto può portare alla perdita della condizione di sicurezza	Selezione dei componenti	Basso	Nessuno	-
1	Come B + uso di componenti e principi ben provati	Come B ma meno probabile	Come B	Alto	Nessuno	-
2	Come B + Test delle funzioni di sicurezza ad intervalli "adeguati"	Un guasto può portare alla perdita della condizione sicura tra un test e l'altro. Il test riconosce la perdita della funzione di sicurezza.	Architettura	Basso	Basso - Medio	Valutare
3	Come B + un singolo guasto non deve portare alla perdita della condizione sicura e se possibile, il singolo guasto deve essere identificato	Un guasto non può portare alla perdita della condizione sicura. Alcuni guasti devono essere identificati. L'accumulazione di guasti può portare alla perdita della condizione sicura.	Architettura	Basso	Basso - Medio	Valutare
4	Come B + un singolo guasto non deve portare alla perdita della condizione sicura. Il singolo guasto deve essere identificato prima della necessità di intervento e comunque l'accumulo di guasti non deve portare alla perdita della condizione sicura	Un guasto non può portare alla perdita della condizione sicura. L'identificazione dei guasti (alta DC_{avg}) accumulati riduce la probabilità di perdita della condizione sicura	Architettura	Alto	Alto e include l'accumulo dei guasti	Valutare

Seguendo le istruzioni della tabella occorre:

- Conformità alle norme pertinenti per la resistenza alle influenze previste (Verificare il datasheet del costruttore dei sensori).
- Utilizzo di principi di sicurezza di base.
- Utilizzo di principi di sicurezza ben provati.
- Singola tolleranza al guasto e rilevamento dei guasti ragionevolmente prevedibili

Valore di $MTTF_D$

Determiniamo la durata media di funzionamento, espressa in anni, prima che capiti un guasto casuale potenzialmente pericoloso o "Mean Time to dangerous Failures" ($MTTF_D$).

Normalmente Il costruttore dei sensori analogici non fornisce dati di "*Performance Level*" (PL) / "*Probability of dangerous Failure per Hour*" (PFH_D) né di "*Mean Time to dangerous Failures*" ($MTTF_D$) ma solo il valore di "*Mean time between failure*" (MTBF) che, in questo esempio, assumiamo 54 anni (dato reale ricavato da un costruttore). Se anche questo valore non fosse disponibile è possibile ricavare dei valori standard dalla nomra EN ISO13849-1 Allegato C. In questo caso è possibile fare le seguenti assunzioni:

$$MTTF = MTBF + MTTR \text{ (Mean Time To Restoration)}$$

"*Mean time to restoration*" (MTTR) o tempo medio di riparazione, è l'intervallo di tempo durante il quale una apparecchiatura è in uno stato di indisponibilità a causa di un guasto. L'MTTR comprende il tempo per la diagnosi, quello per l'arrivo del tecnico di manutenzione, l'arrivo del componente da sostituire e la riparazione vera e propria. Per le apparecchiature elettroniche MTTR può essere considerato trascurabile (non si ripara, si sostituisce).

$$MTTF \approx MTBF$$

Quando non è noto il tasso di guasti pericolosi, EN13849-1, permette di assumere che essi siano il 50% di tutti i guasti, quindi:

$$MTTF_D = 2 \times MTBF$$

$$MTTF_D = 2 \times 54 = 108 \text{ anni}$$

Questa valutazione si riferisce al singolo sensore.

Considerazioni sulla Copertura Diagnostica

Determiniamo ora il valore della Copertura Diagnostica "*Diagnostic Coverage*" (DC).

La Copertura Diagnostica specifica quanto il sistema è efficiente nel determinare i propri malfunzionamenti in tempo reale cioè prima che si verifichi un altro guasto.

Ci baseremo sulla tabella E1 (illustrata a fianco) della norma ISO 13849, che fornisce un elenco di 34 differenti tecniche di diagnosi che possono essere usate per aumentare la capacità di rilevamento guasti di un circuito.

Le tecniche sono suddivise in tre famiglie (circuiti di ingresso, logica di elaborazione del segnale e circuiti di uscita). Per ogni tecnica viene assegnato un punteggio percentuale compreso tra 0% e 99%.

MosaicMA4eMA2eseguonoilcrossmonitoring [A] come richiesto da tabella, quindi il sistema raggiunge il 99% di DC.

Questo non è ancora sufficiente perché il sistema raggiunga la Categoria 4.

Misure	DC
Dispositivo di ingresso	
Stimolo di prova ciclico mediante variazione dinamica dei segnali in ingresso	90%
Controllo di plausibilità, per esempio utilizzo di contatti collegati meccanicamente normalmente aperti e normalmente chiusi	99%
Sorveglianza incrociata degli ingressi senza prova dinamica	Da 0% a 99%, in funzione della frequenza con cui l'applicazione varia il segnale
Sorveglianza incrociata dei segnali in ingresso con prova dinamica se i cortocircuiti non sono rilevabili (per I/O multipli)	90%
Sorveglianza incrociata dei segnali in ingresso e dei risultati intermedi all'interno della logica (L), sorveglianza software temporale e logica del flusso di programma e rilevamento delle avarie statiche e dei cortocircuiti (per I/O multipli)	99%
Sorveglianza indiretta (per esempio sorveglianza mediante pressostato, sorveglianza della posizione elettrica degli attuatori)	Da 90% a 99%, in funzione dell'applicazione
Sorveglianza diretta (per esempio sorveglianza della posizione elettrica delle valvole di comando, sorveglianza dei dispositivi elettromeccanici mediante elementi di contatto collegati meccanicamente)	99%
Rilevamento avarie mediante il processo	Da 0% a 99%, in funzione dell'applicazione; questa misura da sola non è sufficiente per il livello di prestazione richiesto "e"!
Sorveglianza di alcune caratteristiche del sensore (tempo di risposta, intervallo dei segnali analogici, per esempio resistenza elettrica, capacità)	60%

A

Guasti accumulati

Per la Categoria 4 la tabella 10 della ISO 13849-1 (vedere pagina precedente) richiede che il DC sia Alto (99%) e include l'accumulo dei guasti, cioè che possano accadere più guasti, uno dopo l'altro, senza che questo degradi la funzione di sicurezza.

Occorre rilevare il singolo guasto nel momento in cui avviene o prima della successiva richiesta della funzione di sicurezza. Nel caso questo non sia possibile, un accumulo di guasti non rilevati non deve portare alla perdita della funzione di sicurezza.

Per rispettare questa richiesta anche la scelta dei sensori o di come utilizzarli ha importanza.

1. Un sensore con uscita 0-10 V ha il valore minimo a 0 Vcc che non è distinguibile da un corto circuito a 0 Vcc. Inoltre entrambi i sensori potrebbero avere questo tipo di guasto provocando di conseguenza con un accumulo di guasti.
2. I sensori con uscita in corrente 0-20 mA seguono la stessa logica ma con un guasto pericoloso rappresentato da un circuito aperto (ad esempio un cavo scollegato).

In applicazioni di sicurezza, obbligatoriamente se vogliamo raggiungere una Categoria 4, questi sensori devono essere evitati oppure va programmata una soglia per cui al di sotto di un certo valore, per esempio 0,5 Vcc o 2 mA, il sistema reagisce come ad un guasto. Con il sistema Mosaic, ad esempio, è possibile configurare i parametri di funzionamento tramite il software MSD per incrementare la DC. Possono infatti essere implementati dei controlli intermedi come:

a. Errore di misura tra i 2 sensori.
b. Controllo temporale di fuori soglia.

Rimane un importante aspetto riguardante la copertura diagnostica e l'accumulo dei guasti. Il caso in cui il valore in uscita dei sensori non cambi per un periodo di tempo.

Ipotizziamo che i sensori, per esempio di temperatura, misurino per lungo tempo lo stesso valore, trasmettendo sempre lo stesso valore di corrente, per esempio 5 mA. Uno dei possibili guasti che potrebbero verificarsi è quello in cui, entrambi i sensori, in sequenza, si rompano trasmettendo sempre lo stesso valore di corrente. Un guasto del genere non potrebbe essere rilevato dal sistema di sicurezza.

Per essere certi di rilevare anche questo tipo di *guasti accumulati*, occorre effettuare dei test dinamici, ad esempio facendo variare la temperatura nella parte di macchina a cui sono collegati i sensori, con una frequenza predeterminata (ad esempio 4 volte all'ora). Questo tipo di test è obbligatorio per la categoria 4.

Concludendo queste valutazioni sui guasti accumulati, dobbiamo puntualizzare:

1. È spesso impossibile forzare dei cambiamenti obbligati in un processo. Per quanto riguarda il nostro esempio, potrebbe essere complesso far cambiare la temperatura ad una parte della macchina.
2. Tutto questo è richiesto SOLO per la Categoria 4.
3. L'uso di sensori e soglie adeguatamente scelti per evitare corto circuiti o circuiti aperti non rilevati è importante anche nel computo dei CCF, descritto di seguito.

Se vogliamo ottenere una categoria 4 dobbiamo: aumentare la Copertura Diagnostica (DC) o almeno verificare che l'uso del nostro sistema di sicurezza sia il migliore possibile. sistono dei metodi per valutare quale deve essere l'intervallo di tempo tra 2 cambiamenti successivi dei valori misurati dai sensori:

- alcuni presuppongono valutazioni matematico statistiche delle caratteristiche di affidabilità dei sensori utilizzati e della loro configurazione. Esistono dei metodi di calcolo consolidati nell'uso ma complessi per analizzarli in questa guida. Comunque l'uso di strumenti matematici complessi non garantisce l'esattezza del risultato.
- altri prendono in considerazione l'applicazione pratica in modo logico e puntano ad avere un intervallo di test significativamente più basso della durata della inattività dei sensori oppure realizzare un test prima dell'uso della macchina e della necessità della funzione di sicurezza.

L'obiettivo finale è che l'accumulo di guasti, anche non rilevati, non porti mai alla perdita della funzione di sicurezza. Questa è la richiesta obbligatoria della Categoria 4, spesso è impossibile da rispettare pienamente.

Considerazioni sui guasti di causa comune "*Commmon Cause Failure*" (CCF)

Si tratta del guasto risultante da uno o più eventi che provoca il malfunzionamento contemporaneo dei canali di un sistema a due o più canali.

Fornisce una indicazione del grado di indipendenza di funzionamento dei canali di un sistema ridondante.

Utilizzando la tabella F1 (illustrata a fianco) della norma ISO 13849, viene assegnato un punteggio relativamente ad ogni misura contro i guasti di causa comune. Il massimo punteggio raggiungibile è 100.

Il calcolo e le verifiche sono comuni per tutte le categorie.

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
5	**Competenza/formazione**	
	Formazione di progettisti/responsabili della manutenzione alla comprensione di cause e conseguenze dei guasti da causa comune	5
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

a) Quando le misure tecnologiche non sono pertinenti, i punti connessi a questa colonna possono essere considerati nel calcolo completo.

1. Separazione / Segregazione

Uso di cavi schermati - Con l'uso delle uscite analogiche si usano già normalmente cavi schermati, ed è il singolo cavo ad essere schermato.

Rilevamento guasti come corto circuiti o circuiti aperti - Le caratteristiche di rilevamento dei segnali analogici in corrente (0 ... 20 mA) o in tensione (0 ... 10 V) permettono di soddisfare le misure indicate. Si può fare agevolmente escludendo i valori come 0 V o 0 mA.

Quindi è agevole ottenere i 15 punti.

2. Diversità

Uso di sensori diversi - Ad esempio con i moduli Mosaic MA2 MA4 possono essere utilizzati 2 sensori non solo con fondo scala diversi ma, addirittura, con uscite di tipo diverso (tensione o corrente).

Quindi è agevole ottenere i 20 punti.

3. Progettazione / Applicazione / Esperienza

Utilizzo di protezioni - Inserendo le protezioni opportune e necessarie (Over-Voltage e Over-Current) si possono ottenere 15 punti.

Utilizzo di componenti ben provati - I dispositivi con uscita analogica non rientrano tra i componenti ben provati (EN 13849-2 tabella D.4). Quindi 0 punti.

4. Valutazione / Analisi

Sono necessarie analisi "*failure mode and effect analysis*" (FMEA) .

Visti i tempi che richiederebbero queste analisi, per questa misura assegnamo 0 punti non svolgendo alcuna attività.

Bisogna comunque fare la considerazione che una FMEA non è necessariamente un calcolo matematico delle probabilità di rischio, ma è una analisi di tutti i tipi di guasto per valutare i loro effetti. Una valutazione di questo tipo va comunque effettuata al momento di scegliere e installare dei sensori, per cui potrebbe valere la pena di documentarla e ottenere i pochi 5 punti che questa merita.

5. Competenza / Formazione

Considerando i progettisti preparati a comprendere il generarsi dei CCF e le relative conseguenze, assegnamo 5 punti.

6. Ambiente

Il sistema deve essere immune agli effetti dell'ambiente circostante, come la sporcizia.
Inoltre il sistema deve essere immune ai disturbi EMC, in particolare ai disturbi EMC generanti CCF (Disturbi di modo comune e/o differenziale). Solo se si può dimostrare (documentare anche con test), abbiamo 25 Punti.

Tutte le altre condizioni ambientali (temperatura, umidità, vibrazioni…) debbono essere prese in considerazione. Solo se si può dimostrare l'immunità, abbiamo 10 Punti.

È necessario ottenere almeno 65 punti. Appare abbastanza evidente che le condizioni per raggiungere la Categoria 3 sono abbastanza agevoli. Più critico il raggiungimento della Categoria 4 di sistema (da non confondere con quella del modulo) a causa della difficoltà di rilevare il cumulo di guasti.

In sostanza:

1. Nel caso in cui sia dimostrabile che DC=99% e venga rilevato l'accumulo dei guasti, si rispettano i requisiti della Categoria 4.
2. Nel caso in cui sia dimostrabile che DC>90% e non venga rilevato l'accumulo dei guasti, si rispettano i requisiti della Categoria 3.

Conclusioni

Basandoci sulla tabella K1 della EN 13849-1 La funzione di sicurezza del nostro esempio, con $MTTF_D$ dei sensori di 108 anni, con DC_{avg} alto ma, per esempio, senza le condizioni richieste dalla Categoria 4 perché non riusciamo a testare i sensori a intervalli regolari, si raggiunge comunque il PL e (riquadro verde).

	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)															
$MTTF_d$ di ogni canale anni	Cat. B DC_{avg} = nessuna	PL	Cat. 1 DC_{avg} = nessuna	PL	Cat. 2 DC_{avg} = bassa	PL	Cat. 2 DC_{avg} = media	PL	Cat. 3 DC_{avg} = bassa	PL	Cat. 3 DC_{avg} = media	PL	Cat. 4 DC_{avg} = alta	PL
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

Prendendo il dato dalla tabella, il sottosistema dei sensori avrà:

$$PL=e \text{ con } PFH_D=4,29x10^{-8}$$

L'altro componente del sistema è Mosaic.

Dal report di Mosaic per una combinazione di M1S + MA4 ottengo un valore di:

$$PFH_D=2,97x10^{-8}$$

Per calcolare il PL complessivo devo sommare i PFH_D

$$PFH_D \text{ totale} = PFH_{D\_sensori} + PFH_{D\_Mosaic} = 4{,}29x10^{-8} + 2{,}97x10^{-8} = 7{,}26x10^{-8}$$

Corrisponde ancora ad un PL=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 $< 10^{-7}$
Nota Oltre alla probabilità media di guasto pericoloso per ora, anche altre misure sono necessarie per raggiungere il PL.	

Uso di sensori non di sicurezza per funzioni di sicurezza secondo EN IEC 62061

Le medesime considerazioni fatte con la 13849 si possono ripetere anche con questa norma per l'automazione di processo.

I metodi di calcolo e analisi sono però assai più complessi.

Per un approccio semplificato è possibile riferirsi a questa tabella della EN ISO 13849 che propone una relazione tra i valori finali raggiunti.

PL	SIL (IEC 61508-1, per informazioni) modalità elevata/continua di funzionamento
a	Nessuna corrispondenza
b	1
c	1
d	2
e	3

Glossario

Sigla	Definizione	Norma di Riferimento	Descrizione
β (Beta)	Common cause failure factor	IEC 62061	Fattore di indipendenza di funzionamento dei canali di un sistema a più canali. È un numero compreso fra 0,1 e 0,01 in funzione del valore di CCF raggiunto.
λ (Lambda)	Failure rate	IEC 62061	Frequenza di guasto dei guasti di tipo casuale. La frequenza del verificarsi dei guasti di tipo casuale nel tempo di un componente viene comunemente indicata col nome di "tasso di guasto" (Failure Rate) e si misura in numero di guasti per unità oraria. Il suo inverso è detto "tempo medio fra i guasti" ed è misurato in ore; è comunemente indicato con la sigla MTBF (Mean Time Between Failures). I guasti casuali sono provocati da improvvise accumulazioni di sollecitazioni oltre la resistenza massima di progetto del componente. Possono capitare ad intervalli casuali e in maniera del tutto inaspettata. La frequenza di guasto presa su tempi sufficientemente lunghi è pressochè costante. I metodi di calcolo del valore di PFH_D descritti nelle due norme si riferiscono solo alla stima dei guasti di tipo casuale. L'unità di misura comunemente usata per indicare il tasso di guasto è il FIT (Failure In Time) che corrisponde a un guasto per miliardo di ore di funzionamento (F=1 quindi significa un guasto ogni 109 ore) .
λ_s	Safe failure rate	IEC 62061	Tasso di guasto dei guasti non pericolosi. I guasti non pericolosi sono quelli che non hanno effetto sulla prestazione di sicurezza del sistema di controllo. In loro presenza il sistema di controllo continua a garantire protezione.
λ_d	Dangerous failure rate	IEC 62061	Tasso di guasto dei guasti che possono portare a funzionamenti pericolosi. I guasti pericolosi sono quelli che impediscono al sistema di controllo di continuare a fornire protezione.
λ_{dd}	Dangerous detected failure rate	IEC 62061	Tasso di guasto dei guasti pericolosi rilevabili. I guasti pericolosi rilevabili sono quelli che possono essere individuati dai sistemi automatici di autodiagnosi.
λ_{du}	Dangerous undetected failure rate	IEC 62061	Tasso di guasto dei guasti pericolosi che non è possibile rilevare. I guasti pericolosi non rilevabili sono quelli che non possono essere rilevati dai sistemi di autodiagnosi interni. Sono quelli che determinano il valore di PFH_D e, di conseguenza, il valore di SIL o PL.
Cat.	Categoria	ISO 13849-1	La Categoria è il parametro principale che va preso in considerazione per raggiungere un determinato valore di PL. Specifica il comportamento del SRP/CS in relazione alla resistenza ai guasti e al conseguente comportamento in condizioni di guasto. In funzione della disposizione strutturale delle parti vengono definite cinque categorie.
CCF	Common Cause Failure	ISO 13849-1 IEC 62061	Guasto per cause comuni. Guasto risultante da uno o più eventi che provoca il malfunzionamento contemporaneo dei canali di un sistema a due o più canali. Fornisce una indicazione del grado di indipendenza di funzionamento dei canali di un sistema ridondante. Viene valutato assegnando un punteggio. Il massimo punteggio raggiungibile è 100.
DC	Diagnostic Coverage	ISO 13849-1 IEC 62061	Riduzione della probabilità di guasti pericolosi dell'hardware derivanti dal funzionamento dei sistemi automatici di autodiagnosi. Indica quanto il sistema sia efficiente nel rilevare per tempo un proprio eventuale malfunzionamento. Viene espresso con una percentuale compresa fra il 60% e il 99%.
$MTTF_D$	Mean Time to dangerous Failures	ISO 13849-1	Durata media di funzionamento, espressa in anni, prima che capiti un guasto casuale potenzialmente pericoloso (e non guasto generico). Può essere riferita a un singolo componente, oppure a un singolo canale, oppure al sistema di sicurezza completo.

Sigla	Definizione	Norma di riferimento	Descrizione
PFH_D	Probability of dangerous Failure /Hour	IEC 62061	Probabilità media di guasto pericoloso in 1 h. Rappresenta in modo quantitativo il fattore di riduzione di rischio fornito dal sistema di controllo di sicurezza.
PL	Performance Level	ISO 13849-1	Livello di prestazione. Nella ISO 13849-1, per valutare il grado di resistenza ai guasti viene usato il concetto di "Livello di prestazione" (PL). Rappresenta la capacità da parte di un SRP/CS di svolgere una funzione di sicurezza entro prevedibili condizioni di funzionamento. Sono stabiliti 5 livelli, da PL a a PL e. PL e fornisce il più alto livello di riduzione del rischio, PL a il più basso.
PL r	Performance Level required	ISO 13849-1	Livello di prestazione richiesto. Rappresenta il contributo alla riduzione del rischio che deve fornire ogni funzione di sicurezza implementata nel SRP/CS. Il valore di PL r si determina tramite l'uso del grafico dei rischi.
SIL	Safety Integrity Level	IEC 62061	Livello di integrità della sicurezza. Livello discreto (uno dei tre possibili) che serve per descrivere la resistenza ai guasti di un sistema di controllo di sicurezza secondo la norma IEC 62061, dove il livello 3 garantisce la protezione più elevata e il livello 1 la più bassa.
SILCL	SIL CLaim	IEC 62061	Massimo SIL che può raggiungere un sottosistema in funzione della sua architettura e della sua capacità di rilevamento dei guasti.
SRP/CS	Safety Related Parts of Control Systems	ISO 13849-1	Parte del sistema di controllo della macchina che è in grado di mantenere o portare la macchina in uno stato sicuro in funzione dello stato di determinati sensori di sicurezza.
SRECS	Safety Related Electrical, electronic and programmable electronic Control System	IEC 62061	Sistema di controllo di sicurezza elettrico, elettronico, elettronico programmabile il cui guasto aumenta immediatamente il grado di rischio associato al funzionamento della macchina.
T1	Proof test interval	IEC 62061	Intervallo di test di prova. Il Proof test è una verifica di tipo esterno e manuale che serve per rilevare avarie e decadimenti nelle prestazioni dei componenti che non possono essere rilevate dai sistemi interni di autodiagnosi. L'unità di misura è il tempo (mesi oppure, più comunemente, anni).
T2	Diagnostic test interval	IEC 62061	Intervallo di test delle funzioni di autodiagnosi. Tempo che intercorre fra un test di possibili avarie interne e quello successivo. I test sono condotti in modo automatico da appositi circuiti che possono essere interni allo SRECS oppure appartenere ad altri SRECS. L'unità di misura è il tempo (da millisecondi a ore).
SFF	Safe Failure Fraction	IEC 62061	Frazione del tasso di guasto globale che non comporta un guasto pericoloso. Rappresenta la percentuale di guasti non pericolosi rispetto al numero di guasti totali del sistema di controllo di sicurezza.

SENSORI

BARRIERE FOTOELETTRICHE DI SICUREZZA

Elementi caratteristici

Le barriere fotoelettriche di sicurezza sono dispositivi elettrosensibili di protezione (ESPE) composti da uno o più raggi che emessi da un elemento Emettitore e ricevuti da un elemento Ricevitore, creano un'area immateriale controllata.

Quando il dispositivo di sicurezza scelto è una barriera fotoelettrica (AOPD Active Optoelectronic Protective Device) esso può solo essere di TIPO 2 o di TIPO 4 come stabilito dalla Norma Internazionale IEC 61496 1-2.

I due "Tipi" differiscono per la prestazione di sicurezza garantita in presenza di guasti e sono correlati con le categorie della ISO 13849-1 ma non hanno lo stesso significato perché qui per definire il grado di robustezza ai guasti (safety integrity) oltre agli aspetti legati all'architettura del sistema ed alle tipologie dei guasti dell'hardware e del software vengono presi in considerazione ulteriori parametri caratteristici delle tecnologie di rilevamento usate (sostanzialmente di tipo ottico) e che riguardano principalmente l'immunità da interferenze luminose e le caratteristiche costruttive dei sistemi ottici.

La norma armonizzata IEC EN 61496-1 Ed. 3 e le novità per le barriere di tipo 2

Con la pubblicazione della norma armonizzata IEC EN 61496-1 Ed. 3 non è più possibile usare una barriera di sicurezza di Tipo 2 per funzioni di sicurezza valutate SIL 2 / PL d. Se è richiesto un livello di sicurezza pari a SIL 2 / PL d (o più alto) e si vuole utilizzare ancora una barriera di sicurezza, occorrerà allora usare una barriera fotoelettrica di sicurezza di Tipo 4.

Questo requisito normativo deriva dal fatto che la riduzione del rischio, che può essere ottenuta tramite una barriera fotoelettrica di sicurezza, non è funzione solo del livello di prestazione relativa alla sicurezza delle sue parti elettroniche, ma è determinata anche dalle sue capacità sistematiche (per esempio: influenze ambientali, EMC, prestazione ottica e principio di rilevamento).

Le capacità sistematiche di una barriera fotoelettrica di tipo 2 potrebbero infatti non essere sufficienti per garantire una adeguata riduzione del rischio per applicazioni SIL 2 / PL d. La norma stabilisce anche che l'etichettatura delle barriere di sicurezza di Tipo 2 riporti obbligatoriamente tale limitazione a SIL 1 / PL c.

I valori di PFH_D dichiarati per la parte elettronica di comando del dispositivo non sono invece limitati, perciò nella valutazione globale della funzione di sicurezza è possibile usare il valore di PFH_D fornito dal costruttore del dispositivo anche se questo eccede il range di SIL 1 / PL c.

Altezza protetta

È l'altezza controllata dalla barriera. Se essa è posizionata orizzontalmente tale valore indica la profondità della zona protetta.

Portata

È la massima distanza operativa che può esistere tra emettitore e ricevitore. Nell'utilizzo di specchi deviatori è necessario tenere in considerazione. il fattore di assorbimento che ciascuno di essi introduce e che mediamente è del 15%.

Tempo di risposta

È il tempo che la barriera impiega ad inviare il segnale di allarme, una volta intercettata la zona protetta.

BARRIERE FOTOELETTRICHE DI SICUREZZA

Risoluzione

Per tutte le barriere fotoelettriche di sicurezza della ReeR la risoluzione è la dimensione minima che un oggetto deve avere perché questo, attraversando l'area controllata, causi sicuramente l'intervento del dispositivo ed il conseguente arresto del movimento pericoloso della macchina.

- Barriere monoraggio: la risoluzione R è uguale al diametro della lente.
- Barriere multiraggio: la risoluzione R è uguale alla somma del diametro della lente più la distanza tra due lenti adiacenti.

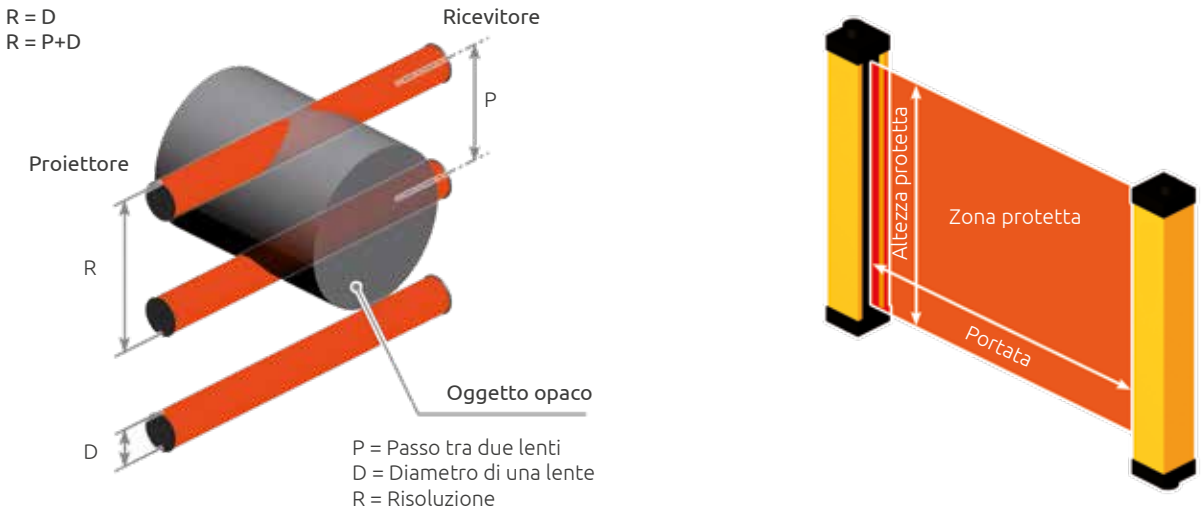


Fig. 33. Risoluzione delle barriere fotoelettroniche

Vantaggi delle barriere fotoelettriche

- Efficace protezione in caso di affaticamento, malessere o distrazione dell'operatore
- Aumento della capacità produttiva della macchina poiché la barriera non richiede lo spostamento manuale di ripari fisici o l'attesa della loro apertura
- Operazioni di carico e scarico macchina più veloci
- Riduzione dei tempi di accesso alle zone operative
- Eliminazione del rischio di manomissione in quanto qualsiasi intervento irregolare sulla barriera provoca l'arresto della macchina
- Installazione semplice e rapida con grande capacità di adattamento sulla macchina anche in caso di successiva variazione di posizionamento
- Possibilità di realizzare protezioni di grandi dimensioni, lineari o perimetrali su più lati a costi molto ridotti
- Praticità e rapidità di manutenzione della macchina poiché non devono essere rimosse protezioni fisiche come griglie, cancelli ecc.
- Miglioramento estetico ed ergonomico della macchina

La specifica tecnica IEC EN 62046 Ed. 3 - Applicazione ed integrazione dei Dispositivi Elettro-sensibili di protezione al macchinario industriale

La specifica tecnica IEC TS 62046 Ed. 3, fornisce raccomandazioni per l'installazione e l'uso dei Dispositivi Elettro-sensibili di Protezione (ESPE).

Si applica quindi principalmente a Barriere Fotoelettriche, Laser Scanner, Bordi e Tappeti sensibili.

Questo documento, che definisce lo stato dell'arte, vuole rispondere alle esigenze del costruttore e dell'utilizzatore della macchina.

La IEC TS 62046 in sostanza disciplina non tanto la costruzione di un dispositivo elettrosensibile, quanto il suo corretto posizionamento ed interfacciamento col macchinario.

L'obiettivo è quello di assicurare che, attraverso una corretta scelta e applicazione del dispositivo di protezione, i rischi di infortunio per l'operatore siano ridotti al minimo possibile.

La IEC TS 62046 tratta nel dettaglio importanti aspetti legati all'uso degli ESPE, quali i criteri di scelta, le modalità d'uso, l'integrazione con il sistema di controllo della macchina, e dà anche indicazioni relative a particolari funzioni delle barriere fotoelettriche di sicurezza quali il Muting e il Blanking.

Questa specifica tecnica fornisce raccomandazioni per l'installazione e l'uso dei Dispositivi Elettro-sensibili di Protezione (ESPE). Si applica quindi principalmente a Barriere Fotoelettriche e Laser Scanner.

Questa specifica tecnica serve per far fronte alle esigenze del costruttore e dell'utilizzatore della macchina. La IEC TS 62046 in sostanza disciplina non tanto la costruzione di un dispositivo elettro-sensibile, quanto la selezione del modello più idoneo all'applicazione, il suo corretto posizionamento ed il suo corretto interfacciamento col macchinario.

Processo di selezione

L'obiettivo del processo di selezione di un dispositivo di protezione (ESPE) è quello di assicurare che, attraverso una corretta scelta e applicazione del dispositivo (e se necessario tramite l'integrazione di altre misure di sicurezza) i rischi di infortunio per l'operatore siano ridotti al minimo accettabile.

Per poter fare una scelta corretta occorre tener conto dei seguenti fattori che possono influenzare negativamente l'efficacia della protezione:

- caratteristiche della macchina da proteggere
- caratteristiche legate all'ambiente di lavoro nel quale presumibilmente la macchina dovrà operare
- dimensioni e caratteristiche del corpo umano
- modalità d'uso dell'ESPE
- caratteristiche dell'ESPE

BARRIERE FOTOELETTRICHE DI SICUREZZA

Caratteristiche della macchina

Affinché le protezioni fotoelettriche di sicurezza siano efficaci è necessario verificare che siano adatte alla conformazione della zona per forma e dimensioni: larghezza e altezza dell'area di accesso.

Prima di decidere l'utilizzo di un ESPE è necessario tener conto che questi dispositivi non forniscono protezione se:

- la macchina proietta materiali, trucioli o parti lavorate
- emette radiazioni nocive
- parti della superficie raggiungono temperature elevate
- il livello di rumore generato è intollerabile
- è impossibile arrestare la macchina una volta avviata perché questo potrebbe introdurre ulteriori rischi oppure perché a causa del particolare tipo di funzionamento la macchina può essere fermata solo a fine ciclo.

oppure il loro uso può risultare scarsamente efficiente se:

- il tempo di arresto della macchina non è conosciuto oppure è variabile in modo aleatorio a causa di ritardi non quantificabili introdotti dal circuito di comando o a causa di sistemi frenanti sotto-dimensionati
- non è possibile arrestare la macchina in ogni punto del suo ciclo di lavoro

Caratteristiche ambientali

Occorre valutare attentamente l'ambiente nel quale si presume dovrà lavorare la macchina. Prima della scelta del dispositivo dovranno quindi essere disponibili tutte le informazioni necessarie sull'ambiente di lavoro e sulle possibili variazioni che è ragionevole aspettarsi durante l'arco di vita della macchina.

Una lista non esaustiva di condizioni ambientali che possono influenzare negativamente il funzionamento di un dispositivo di protezione opto-elettronico sono le seguenti.

- Interferenze elettromagnetiche
  - scariche elettrostatiche
  - radio frequenze (telefoni portatili)
  - fulmini
- Vibrazioni meccaniche, urti
- Interferenze luminose
  - variazione di luce ambientale
  - superfici riflettenti
  - sorgenti infrarosse pulsate (telecomandi, fotocellule)
- Inquinamento
  - acqua
  - polvere
  - sostanze chimiche corrosive
  - fumi
- Variazioni di temperatura
- Umidità
- Radiazioni

Se poi dovessero esistere particolari condizioni operative come funzionamento all'aperto (nebbia, pioggia, neve) oppure funzionamento in atmosfere potenzialmente esplosive o infiammabili (vernici, segatura), allora potrebbero essere necessari ulteriori requisiti di immunità ambientale che normalmente dovranno essere concordati con il costruttore del dispositivo stesso.

Dimensioni e caratteristiche del corpo umano

Poiché la funzione principale dell'ESPE è quella di rilevare il corpo umano o parti di esso, occorrerà tener conto della sua anatomia (dimensioni delle dita, mani, gambe), della velocità massima prevedibile del loro movimento, del modo di interagire con la macchina.

La risoluzione, cioè l'oggetto minimo rilevabile deve essere funzione della parte del corpo da proteggere (es. dita, mani, gambe, braccia). In genere questa scelta va fatta consultando il catalogo o il manuale istruzioni del produttore dell'ESPE.

Modalità d'uso del dispositivo di protezione

Gli ESPE possono assolvere principalmente alle seguenti funzioni:

- Sensore di attraversamento
- Sensore di presenza
- Sensore combinato di presenza ed attraversamento

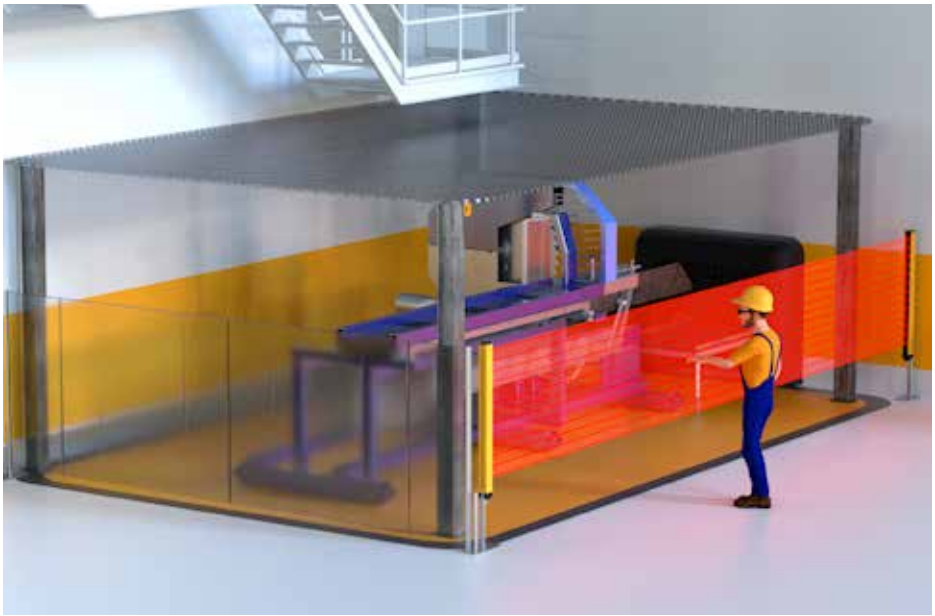
Uso dell'ESPE come sensore di attraversamento

Qualora il dispositivo di protezione venga usato come sensore di attraversamento esso dovrà essere posizionato ad una distanza sufficiente (Distanza di sicurezza) affinché la macchina possa fermarsi (o possa raggiungere uno stato sicuro) prima che qualsiasi parte del corpo raggiunga la zona pericolosa.

Per il calcolo della distanza di sicurezza si dovrà tener conto:

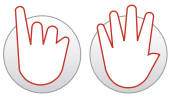
- delle capacità di rilevamento del sensore rispetto alle caratteristiche della parte del corpo umano da rilevare
- della velocità di avvicinamento
- del tempo di risposta dell'ESPE
- del tempo di arresto della macchina misurato nelle condizioni di funzionamento peggiori (massimo carico, massima velocità, eventuali fattori che possono portare ad un deterioramento delle prestazioni di frenata, basse temperature, etc.)
- di eventuali superfici riflettenti che potrebbero, in determinate condizioni, creare un percorso alternativo ai raggi ottici e conseguentemente non permettere al sensore di rilevare l'intrusione

E' importante che il vincolo della distanza di sicurezza venga mantenuto per tutte le direzioni prevedibili di avvicinamento alla zona pericolosa considerando inoltre la massima estensione di tutte le superfici mobili e dell'eventuale movimento del pezzo durante la lavorazione.



BARRIERE FOTOELETTRICHE DI SICUREZZA

Definizione tipo di rilevamento

	RILEVAMENTO	CARATTERISTICHE	VANTAGGI
	Dita o mani 	Tipo di rilevamento necessario quando l'operatore deve lavorare a breve distanza dal punto pericoloso. La risoluzione della barriera deve essere tra 14 mm e 40 mm.	Possibilità di ridurre gli ingombri limitando al massimo lo spazio tra protezione e pericolo. Riduzione tempi di carico e scarico macchina. Minore affaticamento operatore, maggiore produttività.
	Rilevamento della presenza del corpo nel controllo accessi 	Tipo di rilevamento ideale per controllo di accessi e protezioni perimetrali su uno o più lati anche su lunghe distanze. La barriera deve essere posta ad almeno 850 mm dal pericolo. Barriera normalmente composta da 2-3-4 raggi.	Costo della protezione molto ridotto grazie ad un numero di raggi limitato. Possibilità di proteggere aree di grandi dimensioni anche con l'uso di più specchi deviatori. Vedi nota in basso
	Presenza in area a rischio 	Tipo di rilevamento realizzato con posizionamento orizzontale della barriera che consente di controllare in modo continuo la presenza di un ostacolo su una determinata area. La risoluzione della barriera dipende dall'altezza del piano di rilevamento, ma in ogni caso non può superare 116 mm.	Possibilità di controllare zone non visibili dai punti di comando della macchina. Possibilità di impedire l'avviamento involontario della macchina mentre l'operatore si trova nella zona pericolosa.

Non deve essere possibile un avviamento involontario della macchina dopo che una persona, avendo attraversato l'area sensibile, venga a trovarsi – non rilevata - all'interno dell'area pericolosa. Metodi idonei per eliminare questo rischio sono:
Uso della funzione di Start/Restart - interlock con comando posizionato in modo che la zona pericolosa sia visibile e che il comando non sia raggiungibile da chi si trova all'interno della zona pericolosa. Il comando di Restart deve essere controllato in sicurezza.
Uso di un sensore di presenza uomo all'interno dell'area pericolosa.
Uso di ostacoli che impediscano alla persona di rimanere – non rilevata - fra la zona protetta dal sensore e la zona pericolosa.

Calcolo della distanza di sicurezza

L'efficacia della protezione dipende fortemente dal corretto posizionamento della barriera rispetto al pericolo.

La barriera deve essere posizionata ad una distanza maggiore o uguale alla minima distanza di sicurezza S, in modo che il raggiungimento del punto pericoloso sia possibile solo dopo l'arresto dell'azione pericolosa della macchina.

Il posizionamento deve essere tale da:

- Impedire il raggiungimento del punto pericoloso senza attraversare la zona controllata dalla barriera
- Non consentire la presenza di una persona nella zona pericolosa senza che essa sia rilevata. Per questo caso potrebbe essere necessario ricorrere a dispositivi di sicurezza aggiuntivi (es.: barriere fotoelettriche orizzontali)

La Norma ISO 13855 fornisce gli elementi per il calcolo della distanza di sicurezza.

Se la macchina considerata è soggetta ad una norma specifica di tipo C è necessario fare riferimento a tale norma.

Se la distanza S calcolata risulta eccessiva è necessario:

- ridurre il tempo totale di arresto della macchina
- migliorare la risoluzione della barriera

Fig. 34. Protezione su un lato

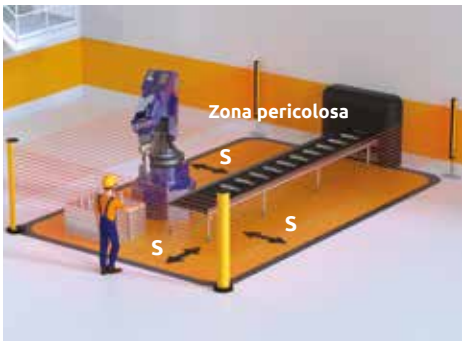


Fig. 35. Protezione su tre lati con l'utilizzo di specchi

Fig. 36. deviatori

Formula generale per il calcolo della distanza di sicurezza

$$S = K \times T + C$$

S	distanza minima di sicurezza tra la protezione ed il punto pericoloso, espressa in mm
K	velocità di avvicinamento del corpo o delle parti del corpo, espressa in mm al secondo. I valori di K possono essere: K = 2000 mm al secondo per distanze di sicurezza fino a 500 mm K = 1600 mm al secondo per distanze di sicurezza superiori a 500 mm
T	tempo totale di arresto macchina formato da: t1 tempo di risposta del dispositivo di protezione in secondi t2 tempo di reazione della macchina per l'arresto dell'azione pericolosa, in secondi
C	distanza aggiuntiva espressa in mm

BARRIERE FOTOELETTRICHE DI SICUREZZA

Direzione di avvicinamento perpendicolare al piano protetto α=90° (± 5°)

1. Punto pericoloso
2. Piano protetto
3. Piano di riferimento

a. Altezza punto pericoloso
S. Distanza di sicurezza

Fig. 37. Possibilità di raggiungere il punto pericoloso solo attraverso l'area sensibile

Barriere con risoluzione per rilevamento mani o dita. Risoluzione barriera (d): 14 - 20 - 30 - 40 mm

Calcolo distanza sicurezza:

S = K x T + C

K = 2000 o 1600
(vedere calcoli seguenti)

T = t1 + t2 Formula generale per il calcolo della distanza di sicurezza. Vedere a pagina 91

C = 8x(d-14)

S = 2000xT + 8x(d-14)

- La distanza S non deve essere inferiore a 100 mm
- Se la distanza S risultante è superiore a 500 mm è possibile ricalcolare la distanza utilizzando K=1600 ma in questo caso la distanza non deve comunque essere inferiore a 500 mm

S = 1600xT + 8x(d-14)

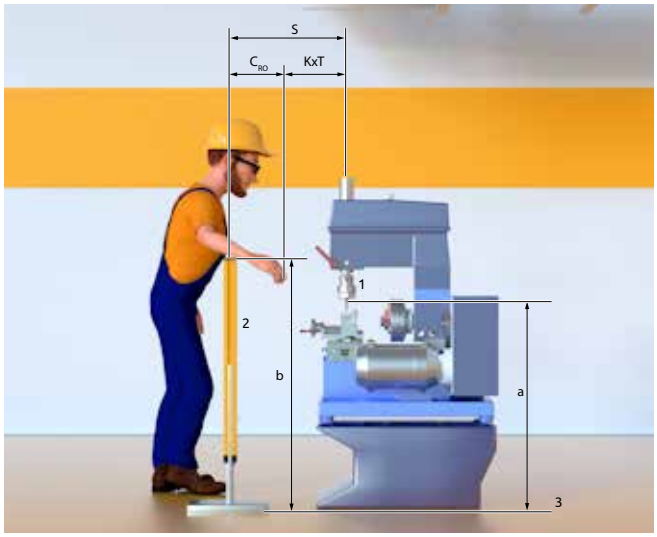
Barriere con risoluzione per rilevamento braccia o gambe. Risoluzione barriera (d): 50 - 90 mm

Calcolo distanza sicurezza:

S = K x T + C

K = 1600
T = t1 + t2
C = 850

S = 1600xT + 850



C_{R0} = Vedere tabella di seguito

1. Punto pericoloso
2. Piano protetto
3. Piano di riferimento

a. Altezza punto pericoloso
b. Altezza bordo superiore barriere
S. Distanza di sicurezza

Fig. 38. Possibilità di raggiungere il punto pericoloso sporgendosi oltre il bordo dell'area sensibile

Possibilità di raggiungere la zona pericolosa sporgendosi oltre il bordo superiore della zona sensibile di una barriera verticale.

In questo caso Il valore di C, denominato "C_{RO}", si ricava dalla Tabella 1 della ISO 13855:2010.

Calcolo distanza sicurezza:

$$S = K \times T + C_{RO}$$

K = 2000 o 1600
(vedere calcoli seguenti)

T = t1 + t2 Formula generale per il calcolo della distanza di sicurezza. Vedere a pagina 91

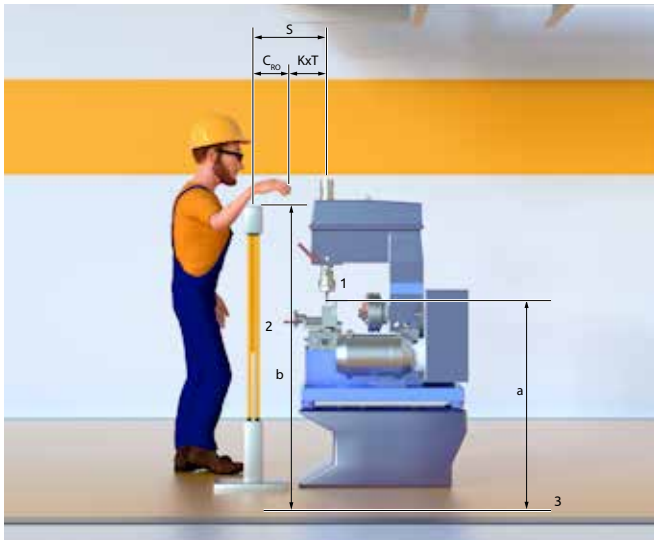
Note:

- Non è ammessa l'interpolazione
- Se le distanze a, b o C_{RO} ricadono fra due valori della tabella occorre usare il maggiore dei due
- Il valore di C_{RO} calcolato usando la Tabella 1 della ISO 13855:2010 va sempre paragonato al valore di C calcolato nel modo "tradizionale" C = 8x(d-14). Il valore da adottare sarà il maggiore dei due

Altezza della zona pericolosa "a"	Altezza "b" del bordo superiore della zona protetta dalla barriera fotoelettrica											
	900	1000	1100	1200	1300	1400	1600	1800	2000	2200	2400	2600
	Distanza aggiuntiva C_{R0}											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	800	750	450	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0

(Tabella 1 della ISO 13855:2010)

BARRIERE FOTOELETTRICHE DI SICUREZZA



1. Punto pericoloso
2. Piano protetto
3. Piano di riferimento

a. Altezza punto pericoloso
b. Altezza bordo superiore protezione
S. Distanza di sicurezza

Fig. 39. Possibilità di raggiungere il punto pericoloso appoggiandosi alla protezione meccanica e baypassare la barriera

Nel caso di protezioni combinate meccaniche ed elettro-sensibili (come in figura), dove sarebbe possibile appoggiarsi alla protezione meccanica e baypassare la barriera

Per il calcolo del parametro C si devono utilizzare le tabelle della norma ISO 13857:2007 (ex EN 294):

- Tabella 1 (per applicazioni a basso rischio) oppure
- Tabella 2 (per applicazioni ad alto rischio)

In questo catalogo le due tabelle della norma ISO 13857:2007 (ex EN 294) - Distanze di sicurezza per impedire il raggiungimento di zone pericolose con arti superiori e inferiori - non sono riportate.

1. Punto pericoloso
3. Piano di riferimento

S. Distanza di sicurezza
Hra. Altezza raggio più alto
Hrb. Altezza raggio più basso

Fig. 40. Possibilità di raggiungere il punto pericoloso solo attraverso l'area sensibile. Barriere con 2- 3 - 4 raggi

Barriere per controllo presenza in area pericolosa. Barriera con 2 - 3- 4 raggi

Calcolo distanza sicurezza:

$S = K \times T + C$

K = 1600

T = t1 + t2 Formula generale per il calcolo della distanza di sicurezza. Vedere a pagina 91

C = 850

$S = 1600xT + 850$

Note per barriere a 2 raggi

- H raggio più alto = 900 mm
- H raggio più basso = 400 mm può essere usato solo se permesso dall'analisi del rischio.

Note per barriere a 3 raggi

- H raggio più basso = 300 mm
- H raggio inter medio = 700 mm
- H raggio più alto = 1100 mm

Note per barriere a 4 raggi

- H raggio più basso = 300 mm
- H raggio intermedio 1 = 600 mm
- H raggio intermedio 2 = 900 mm
- H raggio più alto = 1200 mm

Direzione di avvicinamento parallelo al piano protetto α =0° (± 5°)

1. Punto pericoloso
2. Piano protetto
3. Piano di riferimento

a. Altezza punto pericoloso
x. Distanza tra la fine della zona di rilevamento e bordo della macchina
S. Distanza di sicurezza
H. Altezza zona sensibile

Fig. 41. Barriere orizzontali per controllo presenza in area pericolosa

Barriere orizzontali per controllo presenza in area pericolosa.

Calcolo distanza sicurezza:

S = K x T + C

K = 1600

T = t1 + t2 Formula generale per il calcolo della distanza di sicurezza. Vedere a pagina 91

C = 1200 - (0,4 x H)

S = 1600xT + (1200 - 0,4xH)

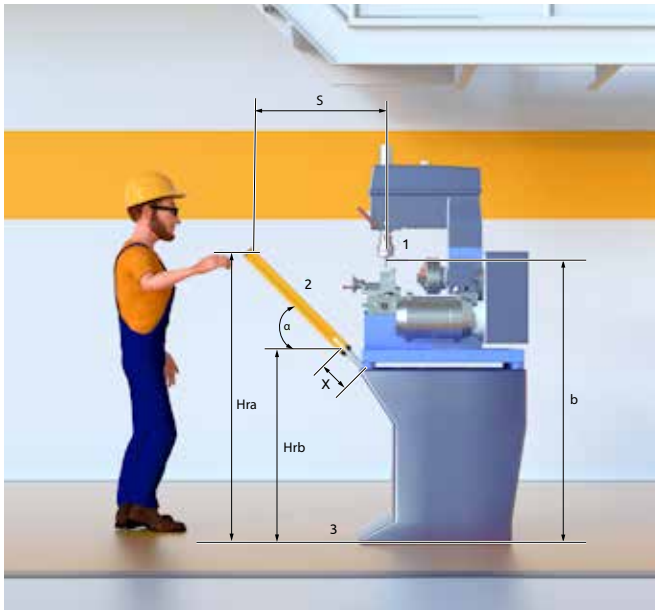
Note:

- C = 1200 - (0,4 x H) deve essere sempre uguale o maggiore di 850 mm
- L'altezza massima permessa è: H_{max} = 1000 mm
- L'altezza H è in rapporto alla risoluzione d della barriera e si calcola con la seguente formula: ***H = 15 x (d - 50)***
- Si può utilizzare questa formula in modo inverso anche per calcolare la risoluzione massima utilizzabile alle varie altezze: **d = H / 15 + 50**.
  La risoluzione massima da utilizzare è per esempio:
  con Hmax = 1000 mm d = 116 mm
  con Hmin = 0 mm d = 50 mm
- Qualora l'altezza H sia superiore a 300 mm la possibilità di accesso al di sotto dei raggi deve essere presa in considerazione durante l'analisi dei rischi

Quando si usa la barriera come sensore combinato di presenza e attraversamento, la distanza x deve essere minore o uguale alla capacità di rilevamento.

BARRIERE FOTOELETTRICHE DI SICUREZZA

Direzione di avvicinamento angolare rispetto al piano protetto 5°< α <85°



1. Punto pericoloso
2. Piano protetto
3. Piano di riferimento

a. Altezza punto pericoloso
S. Distanza di sicurezza
x. Distanza tra la fine della zona di rilevamento e bordo della macchina
Hra. Altezza raggio più alto
Hrb. Altezza raggio più basso

Fig. 42. Possibilità di raggiungere il punto pericoloso attraverso l'area sensibile

Barriere inclinate per rilevamento delle mani o braccia e controllo presenza in area pericolosa.

Con angolo α > ±30° fare riferimento ai casi "direzione di avvicinamento perpendicolare al piano protetto α=90° (± 5°)" a pagina 92.

Con angolo α < ±30° fare riferimento al caso "DIrezione di avvicinamento parallelo al piano protetto α =0° (± 5°)" a pagina 95.

Note:

- La distanza S è riferita al raggio più lontano dal punto pericoloso
- L'altezza del raggio più lontano dal punto pericoloso non deve essere superiore a 1000 mm
- Per il calcolo dell'altezza H o della risoluzione d applicare al raggio più basso le seguenti formule:
  H = 15 x (d - 50)
  d = H / 15 + 50
- Quando si usa la barriera come sensore combinato di presenza e attraversamento, la distanza x deve essere minore o uguale alla capacità di rilevamento

Nel calcolo della distanza di sicurezza occorre poi tener conto delle tolleranze d'installazione, dell'accuratezza nella misura dei tempi di risposta e del possibile degrado delle prestazioni dei sistemi frenanti.

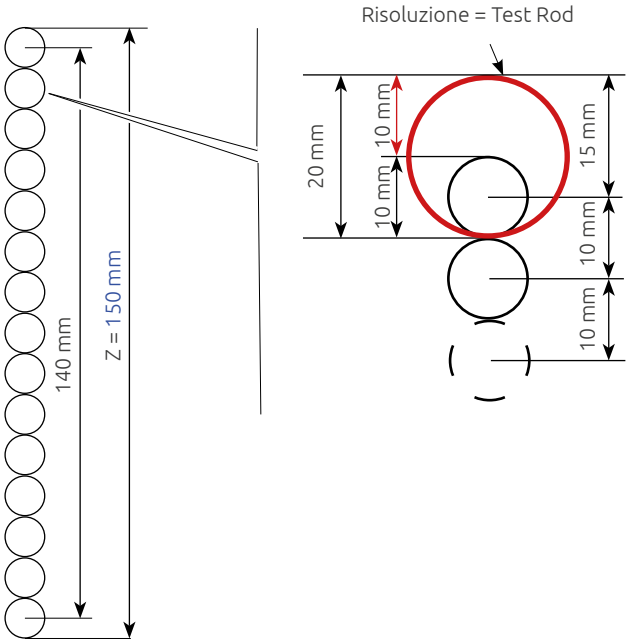
È consigliabile aumentare il valore così calcolato almeno del 10% per tener conto delle tolleranze d'installazione, dell'accuratezza nella misura dei tempi di risposta e per il possibile degrado delle prestazioni dei sistemi frenanti.

Come si vede dalle formule, il tempo totale di arresto gioca un ruolo importante nel calcolo della distanza di sicurezza; quando è prevedibile un degrado nel tempo del sistema frenante è necessario l'uso di un dispositivo di controllo del tempo di arresto (SPM). Il controllo del tempo di arresto non è necessario quando:
- Il sistema è molto affidabile e non soggetto a deterioramento
- La macchina viene arrestata solo raramente
- È implementato un efficace controllo preventivo del tempo di arresto e dei sistemi di frenata della macchina.

Criteri per la determinazione dell'altezza protetta della barriera

I calcoli di esempio, per determinare l'altezza protetta dalla barriera, sono relativi ai modelli seguenti:

- Modello: EOS 152 A
- Altezza protetta nominale: 160 mm
- Risoluzione: 20 mm
- Numero di raggi: 15
- Diametro lente: 10 mm



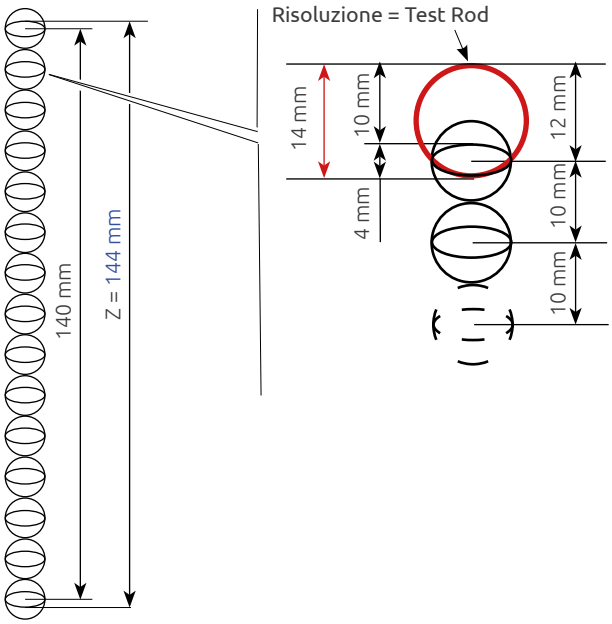
Al fine di tener conto delle dimensioni del "Test Rod" (risoluzione), è necessario aggiungere alla dimensione Z 10 mm ad ogni lato.

Altezza protetta = 150 + 10 + 10 = 170 mm.

Questo valore viene convenzionalmente arrotondato a 160 mm.

Possiamo utilizzare lo stesso valore nominale di altezza protetta (160 mm) per tutte le altre risoluzioni.

- Modello: EOS 151 A
- Altezza protetta nominale: 160 mm
- Risoluzione: 14 mm
- Numero di raggi: 15
- Dimensioni lente: 10 x 4 mm



Al fine di tener conto delle dimensioni del "Test Rod" (risoluzione), è necessario aggiungere alla dimensione Z 10 mm ad ogni lato.

Altezza protetta = 144 + 10 + 10 = 164 mm.

Questo valore viene convenzionalmente arrotondato a 160 mm.

Come si può intuire, possiamo utilizzare lo stesso valore nominale di altezza protetta (160 mm) anche per la risoluzione 14 mm.

Uso dell'ESPE come sensore di presenza

La funzione principale di un dispositivo di protezione usato come sensore di presenza è quello di mantenere la macchina in uno stato sicuro fintanto che una persona o parte di essa si trova all'interno dell'area sensibile.

La zona sensibile dovrà quindi essere configurata in modo tale da non permettere che una persona possa restare all'interno dell'area pericolosa o ad una distanza inferiore alla distanza di sicurezza senza essere rilevata.

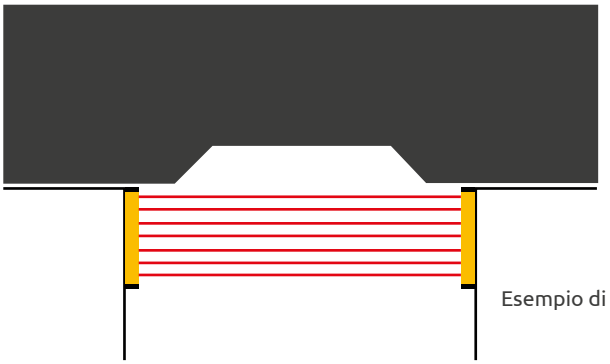
Se il dispositivo di protezione assolve solo la funzione di sensore di presenza, esso dovrà essere usato in combinazione con altre misure di sicurezza (es. riparo interbloccato o sensore di attraversamento) per assicurare che la macchina si trovi in uno stato sicuro prima che sia possibile accedervi.

Nel dimensionamento dell'area protetta, oltre al calcolo della distanza di sicurezza, occorre far si che la zona pericolosa sia raggiungibile solo attraverso l'area sensibile del sensore.

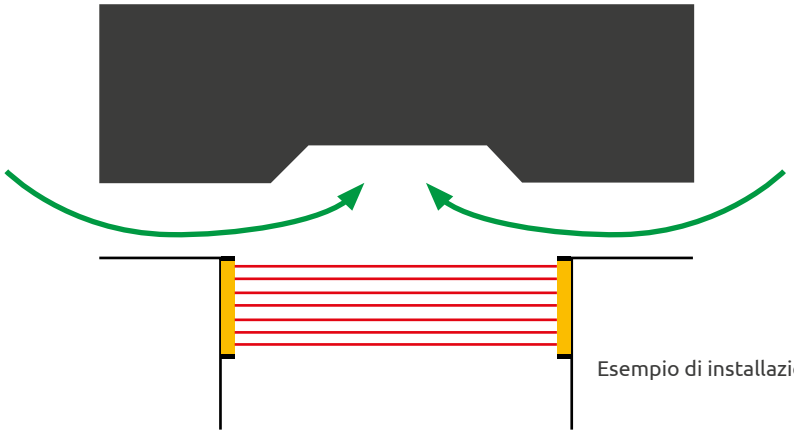
Non deve essere possibile raggiungere l'area pericolosa scavalcando oppure strisciando al di sotto dell'area sensibile o sporgendosi oltre il bordo dell'area sensibile.

BARRIERE FOTOELETTRICHE DI SICUREZZA

Per segregare le parti della macchina non protette dall'ESPE occorrono ripari solidi (interbloccati col circuito di controllo della macchina se possono essere rimossi per permettere l'accesso per manutenzione).



Esempio di installazione corretta



Esempio di installazione errata

Non deve essere possibile un avviamento involontario della macchina dopo che una persona, avendo attraversato l'area sensibile, venga a trovarsi all'interno dell'area pericolosa.

Metodi idonei per eliminare questo rischio sono:

- Uso della funzione di restart - interlock
- Uso di un sensore di presenza uomo all'interno dell'area pericolosa
- Uso di ostacoli che impediscano alla persona di rimanere fra zona protetta e zona pericolosa

Funzione di MUTING

La funzione di Muting è l'esclusione temporanea, automatica ed effettuata in condizioni di sicurezza della barriera di protezione in relazione al ciclo macchina. Esistono fondamentalmente due tipologie di applicazioni:

1. Permettere l'accesso di persone all'interno dell'area pericolosa durante la parte non pericolosa del ciclo macchina.

Esempio: Posizionamento o Rimozione del pezzo da lavorare

In relazione alla posizione dell'utensile, che è l'elemento pericoloso, una delle due barriere (quella di fronte alla zona di lavoro utensile) è attiva mentre l'altra è in Muting per consentire all'operatore di procedere alle operazioni di carico / scarico del pezzo da lavorare. La condizione di Muting delle due barriere verrà poi invertita quando l'utensile dovrà lavorare nella parte opposta della macchina.

2. Permettere il transito del materiale ed impedire l'accesso della persona.

Esempio: Uscita pallet dalla zona pericolosa

La barriera di sicurezza è dotata di sensori di Muting in grado di effettuare una efficace discriminazione tra la persona e il materiale autorizzato a transitare attraverso il varco controllato.

I requisiti essenziali riguardanti la funzione di Muting sono descritti nelle seguenti Norme:

IEC TS 62046 "Applicazione dei dispositivi di protezione per il rilevamento della persona".
EN 415-10 "Sicurezza della macchine per imballare – Palettizzatori e depalettizzatori".
IEC 61496-1 "Dispositivi elettrosensibili di protezione".

Prescrizioni generali:

- La funzione di Muting è una sospensione temporanea della funzione di sicurezza che deve essere attivata e disattivata in modo automatico
- Il Livello di sicurezza del circuito che implementa la funzione di Muting deve essere pari a quella della funzione di sicurezza che viene temporaneamente disabilitata in modo che la prestazione di protezione dell'intero sistema non venga diminuita
- L'attivazione e successiva disattivazione della funzione di Muting deve avvenire solo attraverso l'uso di due o più segnali cablati e indipendenti attivati mediante una sequenza temporale o spaziale corretta. Questo fa si che un singolo guasto non possa attivare la funzione di Muting
- Non deve essere possibile attivare la funzione di Muting quando l'ESPE ha le uscite di sicurezza disattivate
- Non deve essere possibile iniziare una funzione di Muting mediante spegnimento e successiva riaccensione del dispositivo
- Il Muting dovrà essere attivato in un appropriato punto del ciclo macchina e cioè solo quando non esistono rischi per l'operatore
- I sensori di Muting devono essere meccanicamente protetti affinché eventuali urti non ne modifichino l'allineamento

BARRIERE FOTOELETTRICHE DI SICUREZZA

MUTING: impianti di pallettizzazione e movimento materiali

Prescrizioni per il controllo dei varchi:

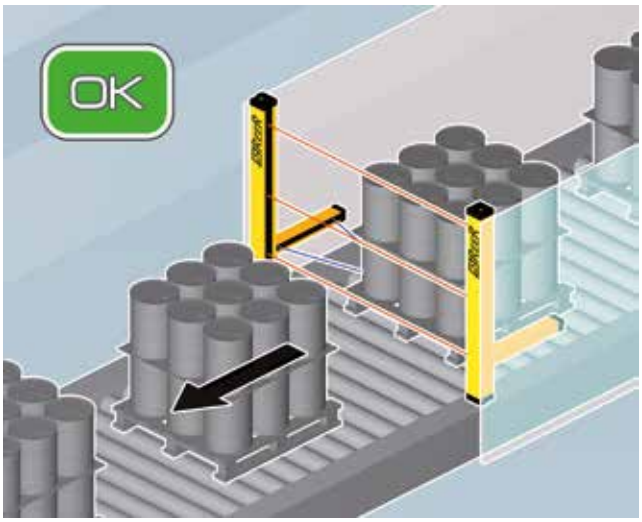
- Occorre rilevare il carico e non il pallet, altrimenti l'operatore potrebbe attraversare il varco facendosi trasportare dal pallet
- Il tempo di Muting deve essere limitato all'effettivo tempo di transito del materiale attraverso il varco
- La funzione di Muting deve essere limitata nel tempo
- Un disallineamento dei sensori che produca un effetto simile alla loro attivazione non deve permettere una condizione permanente di Muting
- La configurazione scelta ed il posizionamento dei sensori di Muting deve essere tale da permettere una sicura distinzione fra persona e materiale
- Il lay-out del varco e il posizionamento dei sensori e delle protezioni laterali deve essere tale da non permettere il transito di una persona verso la zona pericolosa durante la fase di Muting per tutto il tempo di transito del pallet attraverso il varco

È quindi necessario realizzare un sistema in sicurezza che deve essere in grado di discriminare tra:

- il materiale autorizzato
- la persona non autorizzata

→ a transitare attraverso la barriera

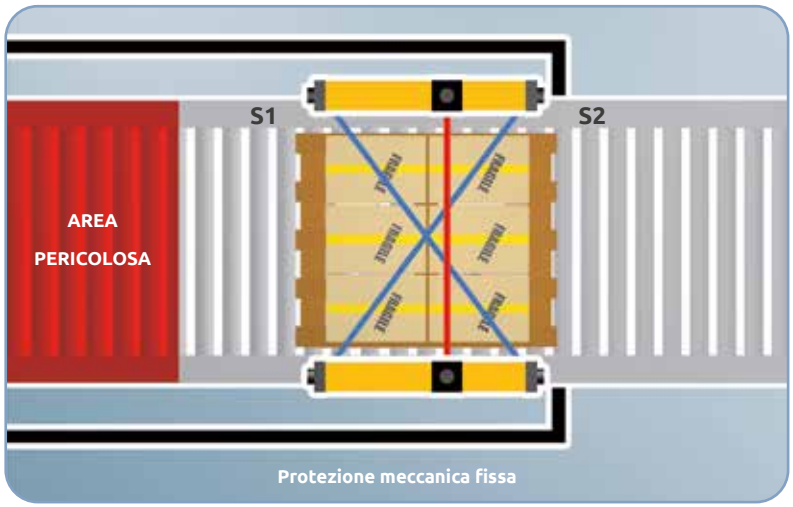
La funzione di Muting può esistere sia in barriere di tipo 2 che di tipo 4.



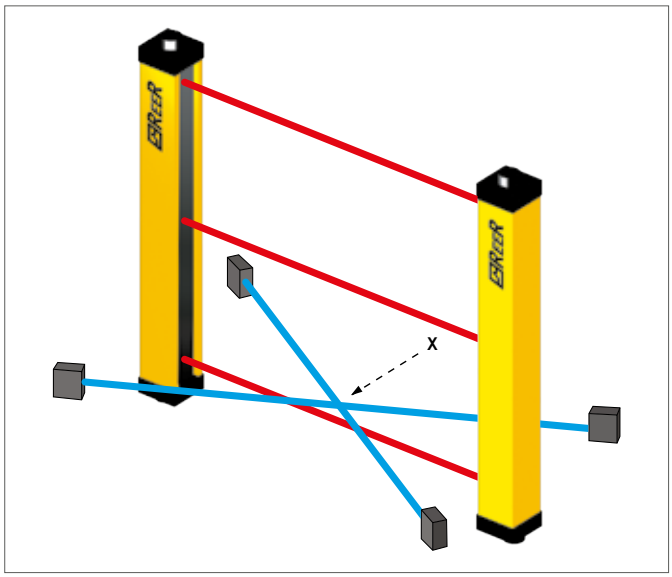
Geometrie più comuni per il posizionamento dei sensori di Muting

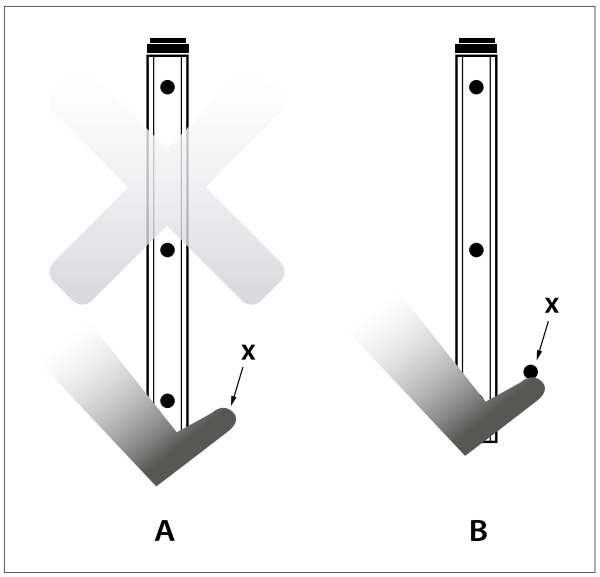
Muting a 2 sensori a raggi incrociati – Configurazione a "T" con controllo di contemporaneità e transito bi-direzionale pallet:

- Il punto di incrocio dei due raggi deve rigorosamente trovarsi nella zona pericolosa segregata oltre la barriera
- È obbligatorio un timer di sicurezza che limiti la funzione di Muting al solo tempo necessario al materiale per l'attraversamento del varco
- La funzione di Muting può essere attivata solo se i due sensori di Muting vengono oscurati contemporaneamente: (t2(S2) – t1(S1) = 4 secondi max)
- I due raggi devono essere oscurati con continuità dal pallet per tutto il periodo di transito fra i sensori
- Un oggetto cilindrico opaco D=500 mm (corrispondente alle possibili dimensioni di una persona) non deve essere in grado di attivare la funzione di Muting



Il punto di incrocio dei due raggi dei sensori di Muting deve essere posizionato più in alto o, al massimo, allo stesso livello del raggio più basso della barriera per evitare la possibilità di manomissioni o attivazioni inconsapevoli del Muting.

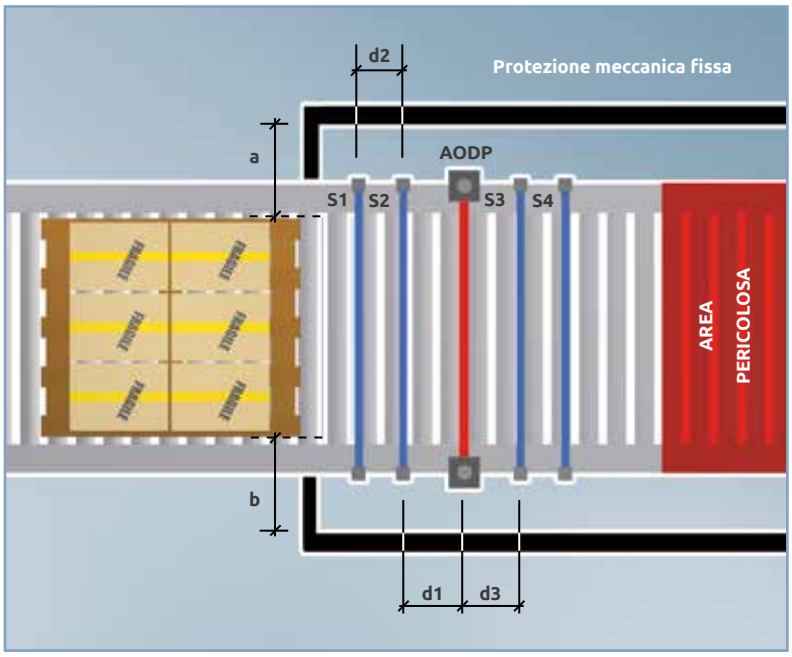




BARRIERE FOTOELETTRICHE DI SICUREZZA

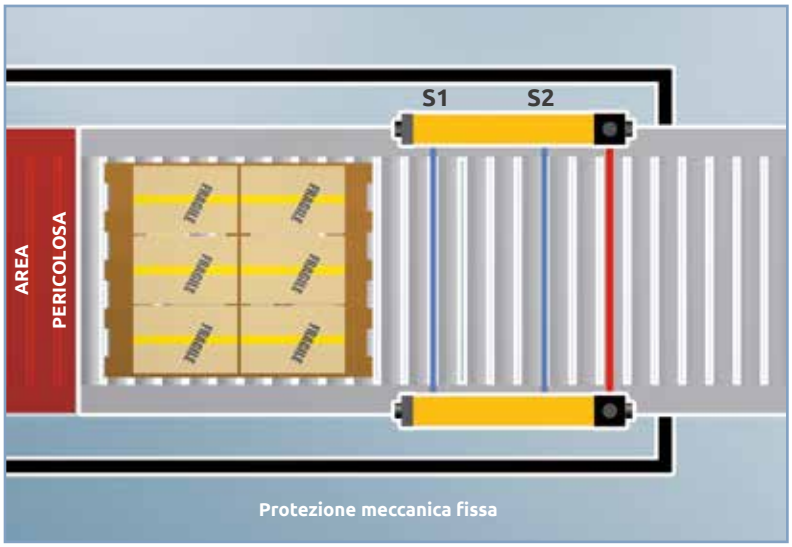
Muting a 4 sensori a raggi paralleli – Configurazione a "T" con controllo di contemporaneità e/o sequenza e transito bi-direzionale pallet:

- Per un breve periodo di tempo i 4 sensori di Muting devono risultare tutti simultaneamente intercettati (occupazione e liberazione sequenziale dei 4 sensori)
- Le distanze fra sensori e barriera fotoelettrica devono rispettare quindi i seguenti valori:
  - d1 e d3 < 200 mm — per evitare che una persona possa entrare senza essere rilevata precedendo o seguendo il pallet durante la fase di Muting
  - d2 > 250 mm — per evitare che una parte di una persona (gamba, pantalone) oscurando contemporaneamente due sensori possa attivare il Muting.



Muting a 2 sensori a raggi incrociati o paralleli – Configurazione a "L" con controllo di contemporaneità e transito pallet solo in uscita dalla zona pericolosa:

- I sensori di Muting devono essere posizionati oltre la barriera nella zona pericolosa
- La funzione di Muting deve essere disattivata appena la barriera viene liberata e comunque non oltre 4 sec. dal momento in cui viene liberato il primo dei due sensori di Muting. Il timer che controlla i 4 sec. deve essere di sicurezza



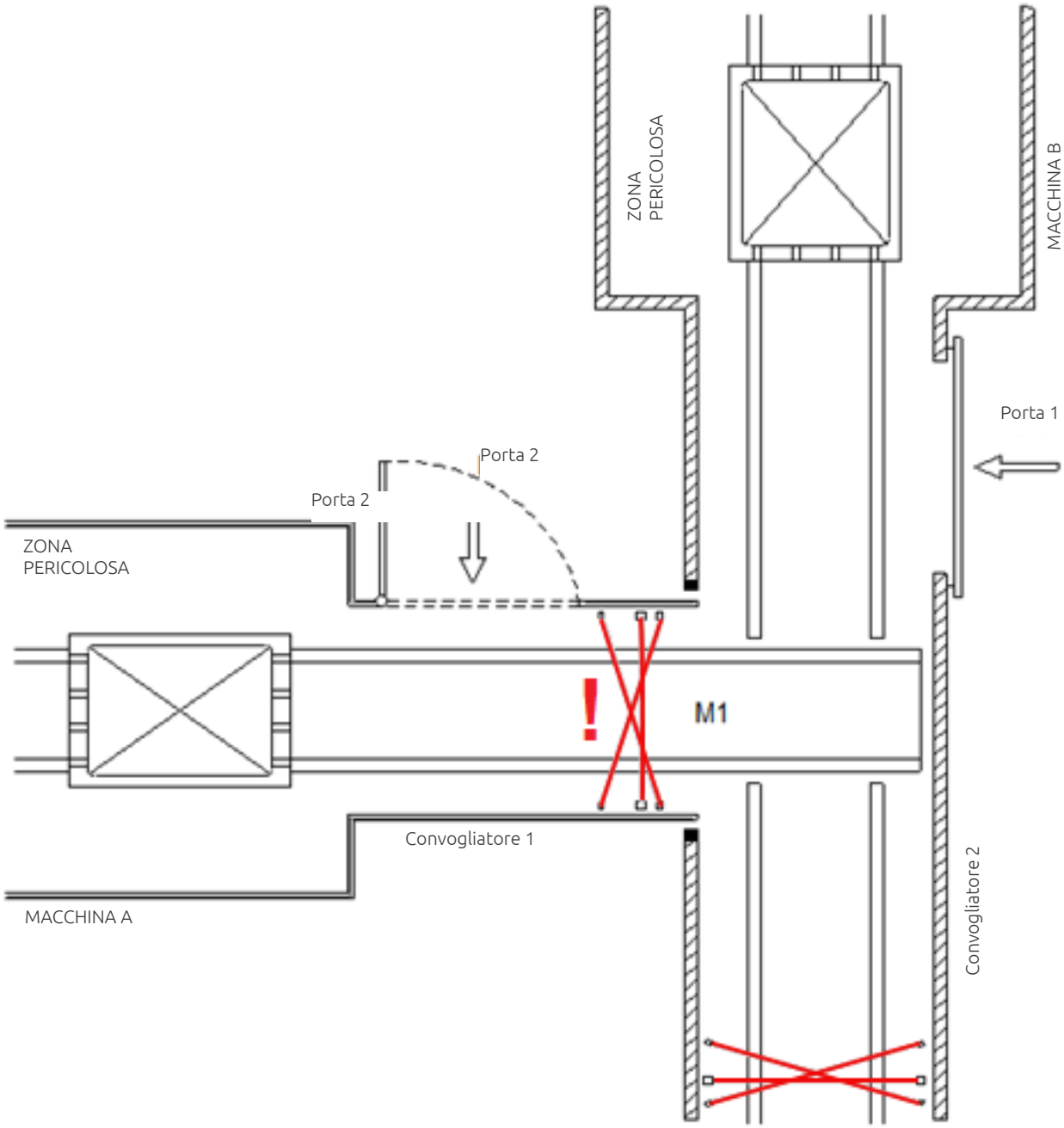
Protezione di due sistemi di trasporto funzionanti in modo coordinato

L'esempio mostra una parte di una linea di produzione comprendente due macchine, A e B, e due linee di trasporto. I pallet si muovono dall'area pericolosa associata al trasportatore 1 all'area pericolosa associata al trasportatore 2.

Il sistema di Muting M1 a due sensori a T consente ai pallet di transitare dal trasportatore 1 al trasportatore 2.

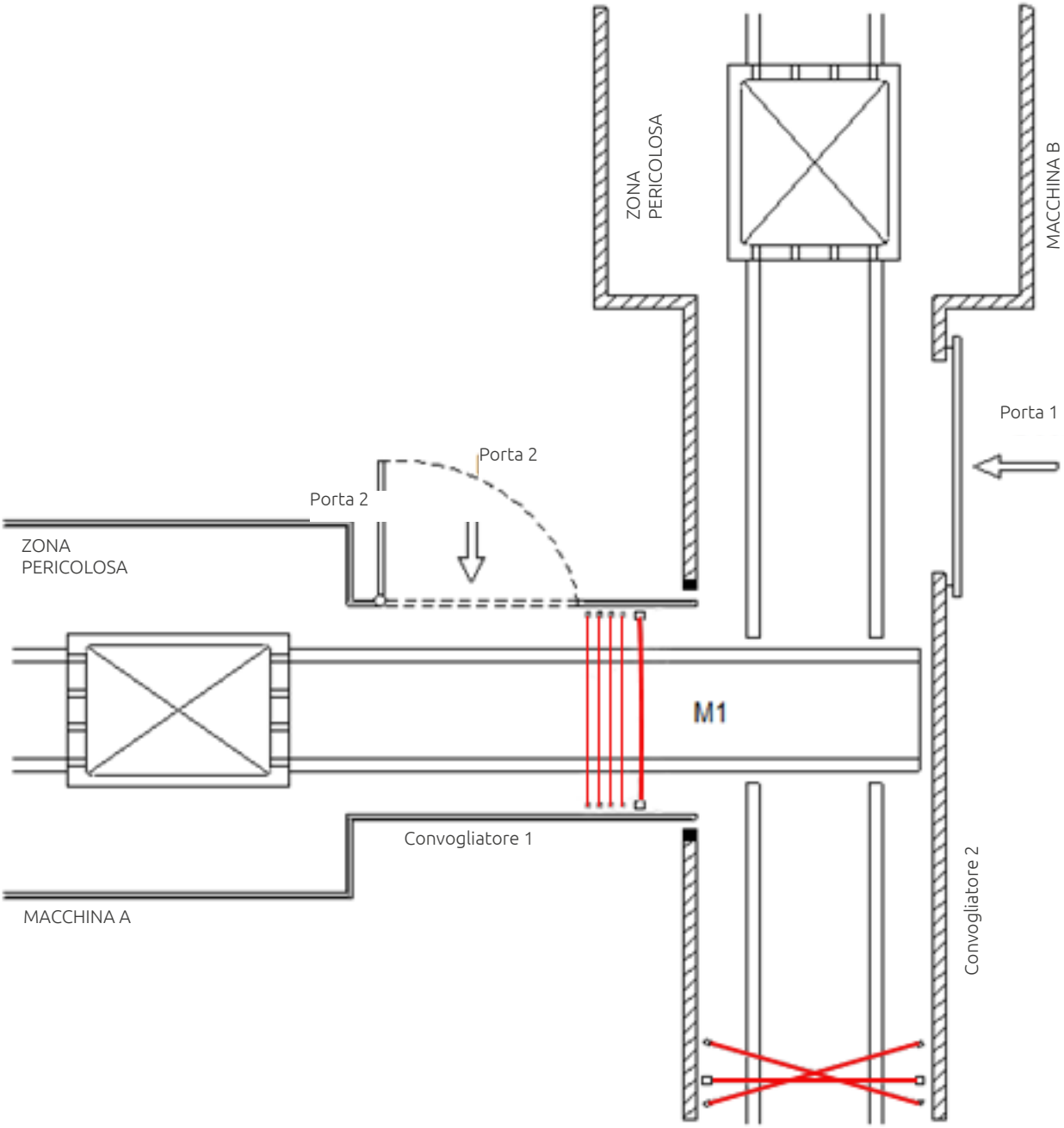
Se l'operatore apre la porta 1, l'area pericolosa associata alla macchina B viene resa sicura mentre il sistema di Muting M1 impedirà all'operatore di accedere, passando sul sistema di trasporto, all'area pericolosa associata alla macchina A.

Se l'operatore invece apre la porta 2, l'area pericolosa associata alla macchina A viene resa sicura, ma il sistema di Muting M1 non può fornire alcuna protezione all'operatore se questi cerca di raggiungere l'area pericolosa associata alla Macchina B passando sul sistema di trasporto poiché l'operatore può attivare il Muting prima di aver interrotto l'area sensibile della barriera, per esempio passando sul punto di intersezione dei due sensori di muting. Il sistema di Muting a due sensori a T non è perciò idoneo.



BARRIERE FOTOELETTRICHE DI SICUREZZA

Per questa applicazione è necessario usare un sistema di muting a quattro sensori con controllo della temporizzazione o della sequenza.



Le barriere con 4 sensori di muting a raggi paralleli:

- consentono il transito bidirezionale di pallet tra una macchina e l'altra
- non attivano il muting e se una persona tenta di attraversare, in entrambi in sensi, il varco protetto.

Funzione di Blanking

Il Blanking è una funzione ausiliaria delle barriere fotoelettriche di sicurezza che consente, in presenza di determinate condizioni, l'introduzione di oggetti opachi nel campo protetto della barriera senza che questo causi l'arresto della macchina controllata.

Questa funzione è quindi particolarmente utile quando il campo protetto dalla barriera fotoelettrica deve poter essere intercettato dal materiale oggetto della lavorazione oppure da una parte fissa o mobile della macchina.

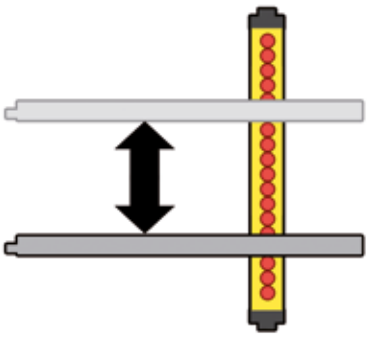
In pratica, è possibile mantenere le uscite di sicurezza della barriera nello stato di ON, e dunque la macchina in funzione, anche se un numero predeterminato di raggi viene intercettato.

Il **Blanking fisso** (fixed Blanking) permette che una parte fissa del campo protetto (per esempio un insieme definito di raggi) venga intercettata, mentre gli altri raggi funzionano normalmente.

Il **Blanking mobile** (floating Blanking) permette all'oggetto intercettato di muoversi liberamente entro il campo protetto occupando un numero definito di raggi, a condizione che i raggi occupati siano adiacenti e che il loro numero non sia più alto di quello previsto in configurazione.

Il **Blanking mobile con obbligo di presenza oggetto** fa si che, limitatamente alla parte del campo protetto che si trova in Blanking, la barriera funzioni con logica inversa. Ciò vuol dire che la parte in Blanking del campo protetto deve risultare sempre occupata durante la fase di Blanking: pertanto l'oggetto deve trovarsi dentro il campo protetto per far si che la barriera rimanga in stato di ON. Anche in questo caso l'oggetto può muoversi liberamente entro il campo protetto, purché le condizioni sopra esposte vengano rispettate.

I requisiti riguardanti la funzione di Blanking si possono trovare nella Specifica Tecnica IEC/TS 62046 che descrive i mezzi aggiuntivi necessari a impedire che una persona raggiunga l'area pericolosa attraverso la parte del campo protetto che si trova in Blanking.



ATTENZIONE!

L'utilizzo della funzione di Blanking ed il tipo di configurazione prescelta dipendono dalle caratteristiche dell'applicazione da proteggere. Verificare in base all'analisi dei rischi della propria applicazione se l'uso di tale funzione è permesso o no e quale configurazione è eventualmente possibile usare.

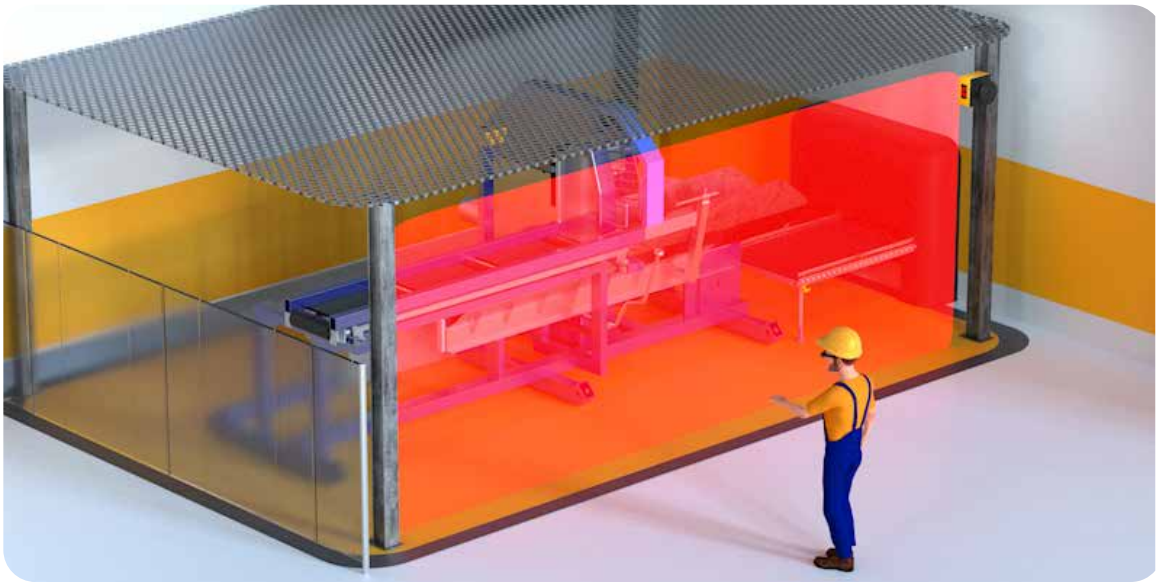
La funzione di Blanking, consentendo l'intercettamento di uno o più raggi, provoca in corrispondenza dei raggi stessi un

peggioramento della risoluzione della barriera che deve essere considerato nel calcolo della distanza di sicurezza.

Elementi caratteristici

Il laser scanner (Active Opto-electronic Protective Device responsive to Diffuse Reflection) misura la distanza fra sé e gli oggetti che rientrano nel suo campo di azione per mezzo di quella piccola frazione di energia che viene re-diffusa dagli oggetti stessi in asse con la direzione di emissione.

Gli AOPDDR, non avendo bisogno di un target cooperante per il loro funzionamento, trovano applicazione soprattutto dove l'area protetta è mobile come è il caso degli AGV, oppure dove è necessario variare la posizione e la dimensione dell'area protetta durante il processo produttivo



Con riferimento alla Norma **EN 61496-3,** i laser scanner possono essere classificati come sensori di sicurezza al massimo di Tipo 3.

Con riferimento alle Norme **IEC 61508, IEC 62061, ISO 13849-1,** gli stessi possono essere usati per realizzare funzioni di sicurezza fino a SIL 2 - PL d.

Con il Laser Scanner è possibile creare aree protette orizzontali, programmabili con precisione e di forma variabile. Ad esempio semicircolare, rettangolare o segmentata e adatte a tutte le applicazioni, senza necessità di utilizzare un riflettore o un ricevitore separato.

È inoltre possibile utilizzare lo scanner posizionato in modo verticale per proteggere il varco di accesso ad una zona pericolosa. In tal caso, secondo **IEC EN 62046,** è obbligatoria la rilevazione del bordo del varco.

L'ingresso o la presenza di una persona o di un eventuale altro ostacolo nella zona controllata di sicurezza producono, attraverso le uscite statiche di sicurezza autocontrollate del dispositivo, un comando di arresto in sicurezza del movimento pericoloso della macchina protetta.

L'occupazione della zona controllata di pre-allarme consente, attraverso un'uscita separata del dispositivo, di inviare un segnale di avviso alla macchina. Questo comando può essere utilizzato per avvisare l'operatore, per esempio mediante un segnale ottico o acustico, dell'avvicinamento alla zona pericolosa oppure, nel caso di applicazione su AGV, per provocare un rallentamento del veicolo prima di un eventuale arresto in caso di occupazione della zona di sicurezza.

I profili delle aree da controllare, così come gli altri parametri di funzionamento, sono impostabili grazie ad un software dedicato di interfaccia utente, installato su laptop o PC e collegato al dispositivo tramite interfaccia seriale.

Il Laser Scanner può anche effettuare il rilievo automatico dell'area da controllare tramite la funzionalità teach-in (auto-apprendimento).

Zone controllate

Zona di sicurezza

È la zona effettivamente protetta, nella quale il laser scanner è in grado di garantire il rilevamento di un ostacolo avente una riflettività minima pari al 1,8%, cioè ogni persona con ogni possibile indumento.

L'occupazione di questa zona provoca la commutazione delle 2 uscite di sicurezza che comandano l'arresto di emergenza della macchina.

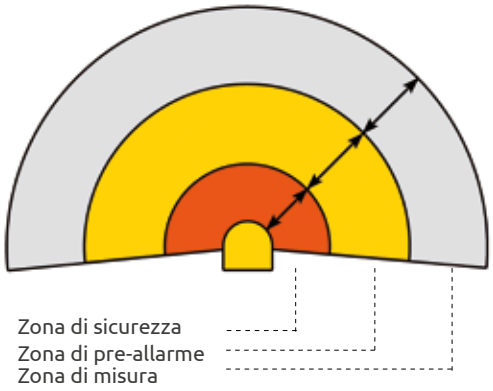
La forma della zona è programmabile secondo le esigenze dell'applicazione.

Zona di pre-allarme

È la zona nella quale il laser scanner è in grado di rilevare la presenza di un ostacolo che si sta avvicinando alla zona di sicurezza.

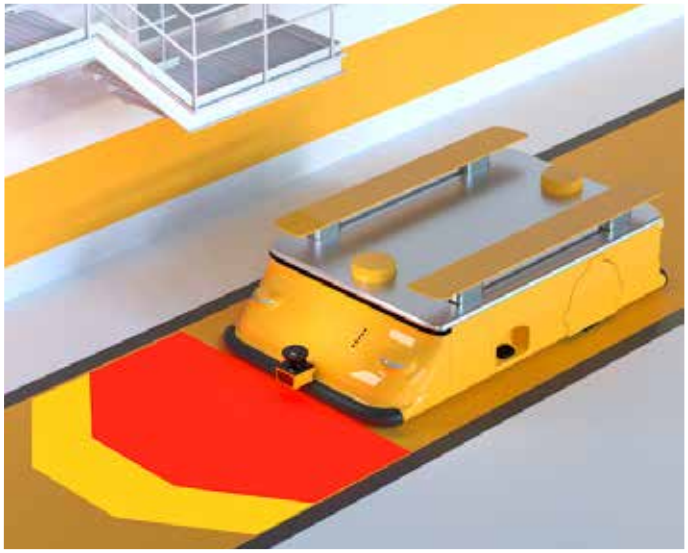
L'occupazione di questa zona provoca la commutazione di un'uscita supplementare che può essere utilizzata per segnalazioni visive o acustiche oppure per procedere al rallentamento di un movimento pericoloso.

La dimensione di questa zona è generalmente maggiore rispetto a quella di sicurezza. Anche in questo caso la forma della zona è programmabile secondo le esigenze dell'applicazione.



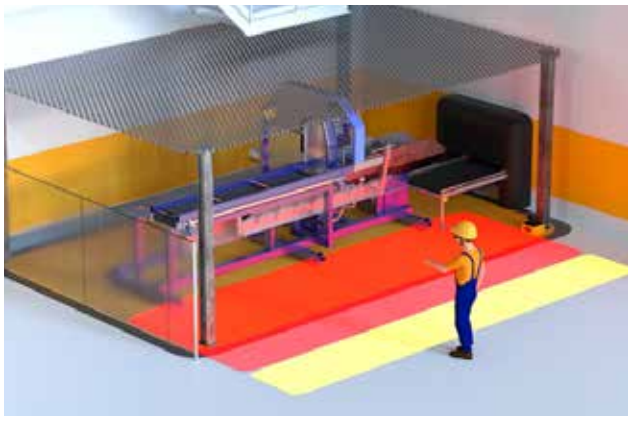
Vantaggi del laser scanner

- Assenza di elementi ricevitori e riflettori
- Zone controllate di forme variabili facilmente programmabili
- Controllo e protezione di aree di grandi dimensioni
- Utilizzo in orizzontale per il rilevamento della presenza del corpo in area pericolosa
- Utilizzo in verticale per il rilevamento delle mani, delle braccia o del corpo nel controllo di accesso
- Utilizzo su veicoli in movimento
- Rilevamento dimensionale, di forma e posizione di oggetti
- Installazione rapida e affidabile.



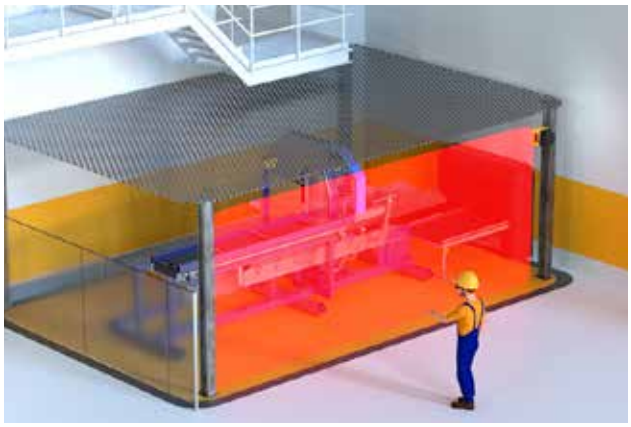
LASER SCANNER DI SICUREZZA

Applicazioni



Controllo di area

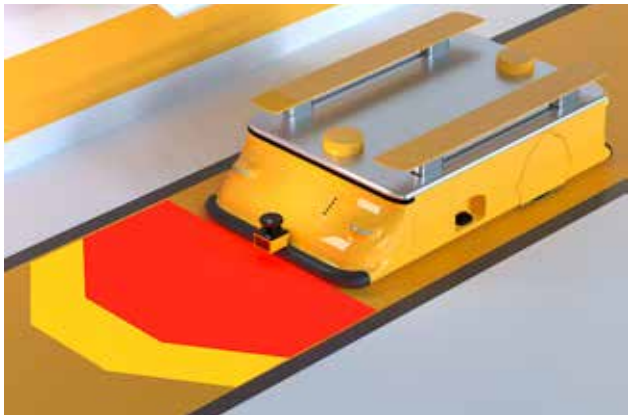
È possibile proteggere un'area, anche di grandi dimensioni, posizionando il piano controllato in orizzontale per il rilevamento degli arti inferiori o del corpo.



Controllo di accesso

È anche possibile proteggere un accesso posizionando il piano controllato in verticale per il rilevamento delle mani, delle braccia o del corpo.

Per le applicazioni in verticale come controllo di accesso è obbligatorio il rilevamento del contorno.



Protezione di veicoli a guida automatica (AGV)

La vasta area controllata consente di raggiungere velocità più elevate rispetto alla protezione con bumper.

L'area di pre-allarme permette di diminuire preventivamente la velocità in presenza di ostacoli.

Attraverso l'interfaccia seriale è possibile trasmettere al veicolo i dati misurati dal sensore perché siano utilizzati come ausilio alla navigazione.

Rilevamento dimensionale

Il sensore è prima di tutto uno strumento di misura. È quindi anche possibile utilizzare i dati di misurazione dell'ambiente circostante, sempre disponibili durante il funzionamento, anche per il rilevamento dimensionale, di profilo e di posizione di oggetti nell'automazione industriale.

Sensori RFID di sicurezza

La tecnologia RFID consente ai sensori Magnus RFID di essere individualmente codificati in tre modi diversi, consentendo all'utilizzatore di adottare la tecnologia che più si addice al livello di protezione anti-manomissione richiesto dall'applicazione.

Le configurazioni più sicure sono quelle dove ogni sensore è accoppiato con un solo attuatore.

La tecnologia RFID utilizzata consente di raggiungere il livello di sicurezza PL e / SIL 3 (secondo la normativa EN ISO 13849-1) anche quando i sensori vengono connessi in serie.

Sensori Magnetici di sicurezza

I sensori Magnetici della serie Magnus MG devono essere connessi al controllore di sicurezza Mosaic (livello di sicurezza PL e) o alla unità di controllo dedicata MG d1 (livello di sicurezza PL d).

I sensori MG collegati a Mosaic formano un sistema di sicurezza certificato PL e.

Sensori induttivi di sicurezza

Una gamma completa di sensori per il rilevamento della posizione.

- Certificato secondo lo standard EN 60947-5-3
- Garantisce la sicurezza di persone e macchinari
- Non necessita di attuatore specifico
- Collegamento dei sensori a interfacce, controllori o PLC di sicurezza (ad esempio: AD SR1, Mosaic)

Tutti i modelli della gamma raggiungungono il livello di sicurezza PL d / SIL2.

Il modello PI M30 NF K raggiunge il livello di sicurezza PL e / SIL3.

Interruttori di sicurezza con dispositivo di blocco integrato

Si definisce un dispositivo interbloccato, un interblocco meccanico, elettrico o di altra natura, il cui scopo è impedire il funzionamento delle operazioni pericolose delle macchine, in specifiche condizioni (generalmente fino a quando i ripari non sono chiusi).

La norma di riferimento è la EN 14119. Questa norma mette in evidenza che le funzioni di "Interblocco" e di "Blocco" sono 2 funzioni di sicurezza distinte, con livelli di sicurezza richiesti (PL r) che possono essere diversi. Spesso il livello di sicurezza richiesto per la funzione di blocco è minore di quello richiesto per la funzione di Interblocco.

Analizzeremo, come esempio, la protezione di un movimento pericoloso di un macchinario tramite un cancello di protezione perimetrale effettuando un'analisi di rischio (semplificato) secondo la norma EN 13849.

Lo strumento che viene utilizzato per stabilire quale dovrà essere il contributo alla riduzione del rischio fornito dalla funzione di sicurezza è il "Grafico delle decisioni per determinare il valore di PLr se la probabilità (Pthe) del verificarsi di un evento pericoloso può essere giudicata bassa" che porta ad individuare in modo univoco il valore di PL r. Se vengono individuate più funzioni di sicurezza, per ognuna di esse occorre definire il PLr.

Funzione di sicurezza interblocco

1. Quando il cancello si apre il movimento pericoloso deve essere fermato e quindi rimanere fermo.
2. In caso di incidente, facendo riferimento al grafico in alto, ipotizziamo che:
   - Il danno che si può generare sia irreversibile S_2
   - La frequenza di esposizione al rischio sia continua (il macchinario è sempre in funzione) F_2
   - La possibilità di limitare il rischio sia scarsa e inevitabile in caso di partenza inaspettata del macchinario, P_2.

Quindi, sulla funzione di sicurezza di interblocco, il PLr dovrà essere PLe.

Funzione di sicurezza blocco

Dobbiamo anche considerare che il macchinario ha un'inerzia tale per cui la distanza di sicurezza (calcolata secondo la norma EN 13855) è maggiore di quella tra il cancello e la zona pericolosa. Di fatto è possibile aprire il cancello e raggiungere il macchinario ancora in movimento. Per questa ragione è opportuno utilizzare una serratura che blocchi in sicurezza il cancello impedendo l'ingresso fino a quando il macchinario è in movimento.

Devono quindi essere utilizzati dei sistemi di sicurezza in grado di svolgere questa funzione. Ad esempio:

- Verificare che gli organi in movimento siano fermi (Controllo della velocità) prima di permettere l'apertura
- Autorizzare l'apertura solo dopo un tempo prefissato (Delay) a seguito di un comando di arresto.

Abbiamo quindi una nuova funzione di sicurezza, quella sul blocco del cancello.

Sempre utilizzando il grafico di pagina precedente, analizziamo il rischio anche per la funzione di blocco. Ipotizziamo che:

1. Il danno che si può generare sia irreversibile S_2
2. La frequenza di esposizione al rischio sia rara (devo entrare nella zona pericolosa raramente) F_1
3. La possibilità di evitare il rischio o di limitare il danno è alta P_1 per due motivi:
   - L'operatore è in grado di vedere il movimento pericoloso del macchinario (comportamento umano) e decidere di non entrare
   - Si stanno utilizzando usando sistemi molto affidabili per controllare il movimento della macchina (Safety speed monitor, Safety PLC….), P1.

Quindi, sulla funzione di sicurezza del blocco porta, il PL r sarà PLc.

Livelli di sicurezza

In generale, nei dispositivi di questo tipo, un singolo guasto può interrompere la funzione di sicurezza, tipicamente una rottura della linguetta attuatore o di qualche altra parte del collegamento meccanico. Il singolo guasto meccanico, può far sì che la sicurezza del riparo non sia garantita oppure che i contatti trasmettano un segnale errato circa lo stato di chiusura o apertura del riparo di protezione.

Quindi, la funzione di sicurezza di blocco interblocco di questi dispositivi è (in generale) di categoria Cat. 1:

- Non c'è ridondanza, quindi Cat. 4 e Cat. 3 vanno escluse. Il singolo guasto interrompe la condizione di sicurezza.
- La Cat. 2 è impraticabile perché è impossibile testare il funzionamento della ritenuta meccanica.
- La Cat. 1 è raggiungibile grazie alla affidabilità dei componenti ($MTTF_D$ alto).

Dalla norma ISO 13849-1 - tabella 5, vediamo che alla Cat. 1 corrispondono i livelli di sicurezza PLc e PLd.

Come aumentare il livello di sicurezza della funzione di blocco e interblocco

Per aumentare il livello di sicurezza di queste funzioni ci sono diverse alternative:

- La **ridondanza**, ovvero duplicando i dispositivi di blocco e interblocco
- Sempre per la ridondanza, possiamo affiancare ai dispositivi elettromeccanici un sensore di tecnologia più raffinata, per esempio un sensore RFID, da utilizzare come dispositivo di Interblocco
- **Esclusione dei guasti**, ovvero procedere a una analisi dettagliata di tutti quelli che possono essere i guasti pericolosi e prendere iniziative per escludere tutti i casi in cui possono accadere. Con questo metodo, utilizzando un solo dispositivo, è possibile raggiungere la Cat. 3 / PLd (PLe non prevede l'uso della esclusione dei guasti). Si tratta di una attività complessa che va eseguita secondo la norma EN 13849-1/2 e giustificata in ogni suo aspetto.

Riassumiamo ora questi concetti con un esempio basato sui prodotti ReeR.

- Safelock — Dispositivo di blocco e Interblocco elettromeccanico
- Magnus RFID — Sensore contactless RFID con uscite OSSD utilizzato come sensore di interblocco.
- Magnus — Sensore contactless magnetico Reed con 2 contatti N.A. utilizzato come sensore di interblocco
- Relè di sicurezza — (ADSR3, ADS4, AD SR1)
- MOSAIC — Controllore di sicurezza

Funzione di blocco Categoria / Livello sicurezza	Funzione di interblocco Categoria / Livello sicurezza	Codifica	Dispositivi
Fino a Cat. 1 / PL c (Nota)	Fino a Cat. 1 / PL c	Bassa	Safelock + Interfaccia di sicurezza PL d per controllo arresti di emergenza e ripari mobili ADSR3 oppure un ingresso di Mosaic
Fino a Cat. 1 / PL c (Nota)	Fino a Cat. 3 / PL d	Bassa	Safelock + Interfaccia di sicurezza PL d per controllo arresti di emergenza e ripari mobili ADSR3 oppure 2 ingressi di Mosaic + Esclusione dei guasti (Vedi Nota)
Fino a Cat. 1 / PL c (Nota)	Fino a Cat. 4 / PL e	Alta	Safelock + Magnus + 2 Interfacce di sicurezza PL e per controllo arresti di emergenza e ripari mobili ADSR4 oppure 4 ingressi di Mosaic
Fino a Cat. 1 / PL c (Nota)	Fino a Cat. 4 / PLe	Alta	Safelock + Magnus RFID + Relè di sicurezza AD SR1 o 2 ingressi di Mosaic (Solo per Magnus)
Fino a Cat. 4 / PL e	Fino a Cat. 3 / PL d	Bassa	2 Safelock + Interfaccia di sicurezza PL d per controllo arresti di emergenza e ripari mobili ADSR3 oppure 2 + 1 ingressi di Mosaic (FBK necessario)
Fino a Cat. 4 / PL e	Fino a Cat. 4 / PL e	Bassa	2 Safelock + 2 Interfacce di sicurezza PL e per controllo arresti di emergenza e ripari mobili ADSR4 oppure 4 + 2 ingressi di Mosaic (FBK necessario)

(Nota) È possibile raggiungere Cat. 3 / PL d attraverso una esclusione dei guasti. E' ammessa l'esclusione dei guasti secondo il punto 7.3 della EN ISO 13849-1.

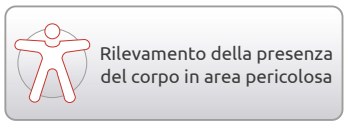
GUIDA ALLA SELEZIONE

	EOS 4 A	EOS 4 X	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK
Sensore	Barriera	Barriera	Barriera	Barriera	Barriera
Livello di sicurezza	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e
Risoluzione (mm)	14	14	14	14	14
Altezza aree controllate (mm)	160 ...1960	160 ...1960	160 ...1810	160 ...1810	160 ...1810
Portata max (m)	6	6	5	5	5
Start/Restart interlock integrato	-	si	-	si	-
EDM integrato	-	si	-	si	-
Blanking	-	-	-	-	si, floating
Versioni Master/Slave	-	si (1/2 slave)	-	si (1 slave)	si, master

	EOS 4 A	EOS 4 X	SAFEGATE SM - SMO	SAFEGATE SMPO	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK	JANUS M
Sensore	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera
Livello di sicurezza	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SIL 3 – PL e
Risoluzione(m)	20, 30, 40	20, 30, 40	30, 40	30, 40	20, 30, 40	20, 30, 40	20, 40	30, 40
Altezza aree controllate (mm)	160 ... 2260	160 ... 2260	310 ... 2260	310 ... 2260	160 ... 2260**	160 ... 2260**	160 ... 2260**	310 ... 1810
Portata max (m)	12 o 20	12 o 20	4 o 8	4 o 8	18	18	18	16 o 60
Start/Restart interlock integrato	-	si	si	si	-	si	-	si
EDM integrato	-	si	si	si	-	si	-	si
Blanking	-	-			-	-	si, floating	-
Muting integrato	-	-	si	si	-	-	-	si
Lampada Muting integrata	-	-	Modello SMO	si	-	-	-	-
Programmabile	-	-	-	si	-	-	-	-
Versioni Master/Slave	-	si (1/2 slave)	-	-	-	si (1 slave)	si master	-
Versioni Long Range	-	-	-	-	-	-	-	si (fino a 60 m)

** Per la famiglia ADMIRAL (modelli AX, AD e AX BK) sono disponibili, su richiesta, barriere di sicurezza con altezza protetta fino a 2260 mm per le risoluzioni (30 mm, 40 mm, 50 mm e 90 mm).
Nel dettaglio le nuove altezze protette sono: 1960 mm, 2110 mm e 2260 mm.
I modelli Master e Slave non sono invece disponibili per queste nuove altezze.
* Versioni VISION VXL e MXL con risoluzione 30 mm: altezza massima area controllata 1210 mm.

GUIDA ALLA SELEZIONE



DEFINIZIONI	
Start/Restart interlock	Funzione di interblocco (necessità di riarmo manuale) alla partenza o alla ripartenza della macchina
EDM	External Device Monitoring: controllo della commutazione dei contattori esterni tramite ingresso di feedback
Master/Slave	Due o tre barriere possono essere collegate in cascata; tutte le uscite sono gestite da una sola di queste (Master)
Blanking	La barriera può essere programmata per ignorare un solo oggetto di dimensioni definite anche maggiori della risoluzione. Vedere “Funzione di Blanking”
Muting	La funzione di protezione della barriera può essere inibita sotto determinate condizioni di sicurezza. Vedere “Funzione di Muting”
Modelli I	Modelli con connessioni per sensori di Muting esterni
Modelli L, T	Modelli con sensori di Muting integrati in kit preassemblati per sola uscita pallet (L) o ingresso/uscita (T)

JANUS J	LASER SCANNER UAM	EOS 2 A	EOS 2 X	VISION V	VISION VX	VISION VXL	VISION MXL
Barriera	Laser scanner	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera
Tipo 4 SIL 3 – PL e	Tipo 3 SIL 2 – PL d	Tipo 2 SIL 1 – PL c	Tipo 2 SIL 1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c
40	30, 50 , 70 selez.	30, 40	30, 40	20, 30, 40	20, 30, 40	30, 40	30, 40
610 ... 1210	-	160 ... 2260	160 ... 2260	160 ... 1810	160 ... 1810	160 ... 1810*	160 ... 1810*
16 o 60	5 (raggio)	12	12	16	18	8	8
si	si	-	si	-	si	si	si
si	si	-	si	-	si	si	si
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	si
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	si (1/2 slave)	-	si (1 slave)	-	-
si (fino a 60 m)	-	-	-	-	-	-	-

GUIDA ALLA SELEZIONE

	EOS 4 A	EOS 4 X	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK	JANUS M	JANUS J
Sensore	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera
Livello di sicurezza	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e
Risoluzione (mm)	50, 90	50, 90	50, 90	50, 90	40,90	40, 90	40
Altezze aree controllate (mm)	160 ... 2260	160 ... 2260	310 ... 2250**	310 ...2250**	310 ... 2250**	310 ... 1810	610 ... 1210
Portata max (m)	12 o 20	12 o 20	18	18	18	16 o 60	16 o 60
Start/Restart interlock integrato	-	si	-	si	-	si	si
EDM integrato	-	si	-	si	-	si	si
Blanking	-	-	-	-	si, floating	-	-
Muting integrato	-	-	-	-	-	si	-
Versioni Master/Slave	-	si (1/2 slave)	-	si (1 slave)	si (master)	-	-
Versioni Long Range	-	-	-	-	-	si (fino a 60 m)	si (fino a 60 m)

	EOS 4 A	EOS 4 X	SAFEGATE SM - SMO	SAFEGATE SMPO	ADMIRAL AD	ADMIRAL AX	JANUS M	JANUS J
Sensore	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera
Livello di sicurezza	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SILCL3 – PL e	Tipo 4 SIL 3 – PL e	Tipo 4 SIL 3 – PL e
Numero raggi	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4
Risoluzione (mm)	-	-	-	-	-	-	-	-
Altezze aree controllate (mm)	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910
Portata max (m)	12 o 20	12 o 20	4 o 12	4 o 12	18	18 o 60	16 o 60	16 o 60
Start/Restart interlock integrato	-	si	si	si	-	si	si	si
EDM integrato	-	si	si	si	-	si	si	si
Muting integrato	-	-	si	si	-	-	si, modelli I, L e T	-
Versioni Master/Slave	-	si (1/2 slave)	-	-	-	si	-	-
Lampada Muting integrata	-	-	Modello SMO	si	-	-	-	-
Programmabile	-	-	-	si	-	-	-	-
Versioni TRX con elemento passivo	-	-	si	si	-	-	si	si
Versioni Long Range	-	-	-	-	-	si (fino a 80 m)	si (fino a 60 m)	si (fino a 80 m)

LASER SCANNER UAM	EOS 2 A	EOS 2 X	VISION V	VISION VX
Laser scanner	Barriera	Barriera	Barriera	Barriera
Tipo 3 SIL 2 – PL d	Tipo 2 SIL 1 – PL c	Tipo 2 SIL 1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c
30, 50 , 70 selez.	50, 90	50, 90	50, 90	50, 90
-	160 ... 2260	160 ... 2260	310 ... 1810	310 ... 1810
5 (raggio)	12	12	16	18
si	-	si	-	si
si	-	si	-	si
-	-	-	-	-
-	-	-	-	-
-	-	si (1/2 slave)	-	si (1 slave)
-	-	-	-	-

LASER SCANNER UAM	EOS 2 A	EOS 2 X	VISION V	VISION VX	VISION VXL	VISION MXL	ILION	ULISSE
Laser scanner	Barriera	Barriera	Barriera	Barriera	Barriera	Barriera	Raggio singolo	Raggio singolo
Tipo 3 SIL 2 – PL d	Tipo 2 SIL 1 – PL c	Tipo 2 SIL 1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c	Tipo 2 SILCL1 – PL c
-	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	1, 2, 3, 4	1, 2, 3, 4
-	-	-	-	-	-	-	-	-
-	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	-	-
5 (raggio)	12	12	16	18 o 60	8	8	8 o 20	6
Si	-	si	-	si	si	si	si con unità AU SX o AU SXM	si con unità AU SX o AU SXM
Si	-	si	-	si	si	si	si con unità AU SX o AU SXM	si con unità AU SX o AU SXM
-	-	-	-	-	-	si	si con unità AU SXM	si con unità AU SXM
-	-	si (1/2 slave)	-	si (1 slave)	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	
-	-	-	-	-	-	-	-	-
-	-	-	-	si (fino a 60 m)	-	-	-	-

Poiché l'ESPE sarà integrato nel sistema di controllo di sicurezza della macchina, la scelta del suo Livello di sicurezza dipenderà dal risultato dell'analisi del rischio e conseguentemente dal valore del parametro PL, SIL o Categoria della corrispondente funzione di sicurezza.

Le norme di prodotto (Norme di tipo C) generalmente raccomandano il tipo di ESPE più adatto per ogni funzione di sicurezza interessata. Se non si hanno a disposizione norme di tipo C conviene usare le raccomandazioni contenute nelle norme ISO 13849-1 e IEC 62061. È necessario tener conto che l'integrità di sicurezza complessiva della catena: ingresso-unità di controllo- attuatori, non potrà che essere uguale o inferiore a quella del dispositivo più debole.

Regole per una corretta interconnessione dei dispositivi di protezione al sistema di controllo della macchina

L'interconnessione fra le uscite di sicurezza dell'ESPE (OSSD) ed i dispositivi di arresto della macchina, la disposizione e la scelta dei pulsanti di ripristino deve essere fatta in modo che non venga ridotto o peggio annullato il grado di "safety integrity" assegnato al sistema di controllo di sicurezza della macchina.

L'esempio di figura seguente mostra il caso più comune quello cioè dove il sistema di comando e controllo della macchina (es. Il PLC) non assolve a funzioni di sicurezza. In questo caso il sistema di controllo di sicurezza che gestisce i dispositivi di protezione ad esso connessi deve funzionare in modo indipendente e deve essere collegato fra il PLC e l'organo di arresto della macchina stessa.

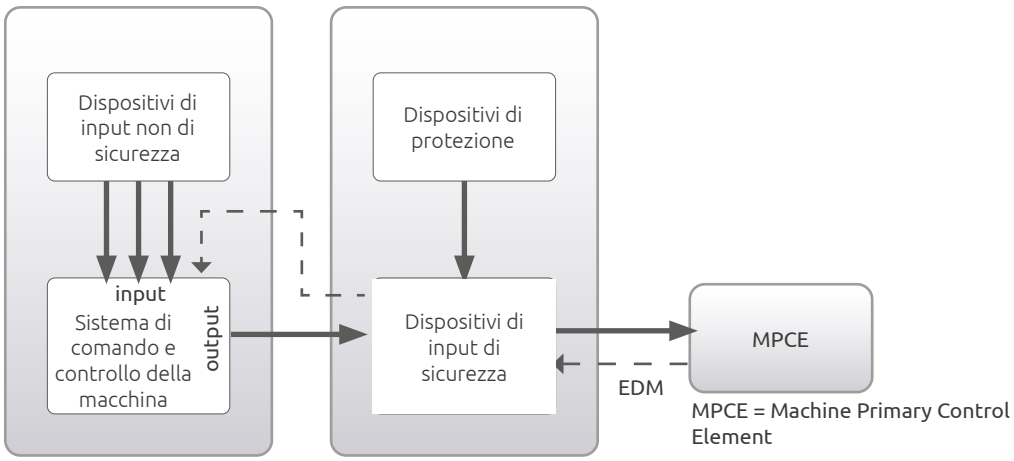


Fig. 43. Sistema di comando e controllo della macchina (es. Il PLC) non assolve a funzioni di sicurezza.

Nel caso invece che la macchina disponga di un sistema centrale di controllo e governo di sicurezza (PLC di sicurezza), come mostrato in figura seguente, conviene che le funzioni operative della macchina e le funzioni di sicurezza attuate dai dispositivi di protezione vengano coordinate dal sistema di sicurezza centrale.

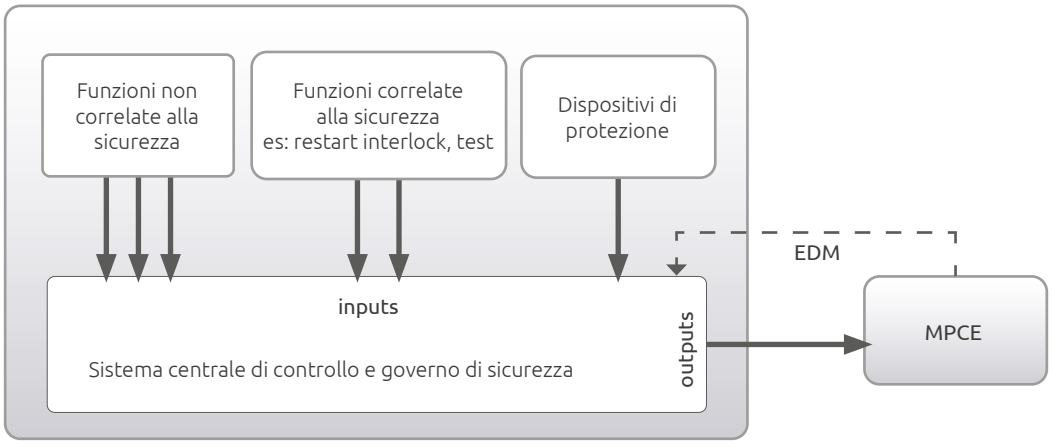


Fig. 44. Sistema centrale di controllo e governo di sicurezza (PLC di sicurezza)

Posizionamento delle barriere di sicurezza per la protezione delle persone negli impianti di pallettizzazione

Questo approfondimento normativo cerca di rispondere a queste 2 domande:

- A che altezza dal piano di riferimento deve essere posizionato il primo raggio della barriera?
- Quale è il criterio di selezione per determinare il numero di raggi della barriera?

Di seguito tre esempi di pallettizzatori dove le barriere di sicurezza sono posizionate:

- Esempio 1
  direttamente sul pavimento

- Esempio 2
  sul convogliatore sollevato dal pavimento

- Esempio 3
  sul convogliatore sollevato da terra ma facilmente accessibile dalla persona per mezzo di scale

Per ognuna di queste condizioni la EN 415-10 stabilisce:

- A che altezza deve essere posizionato il primo raggio della barriera
- Quanti raggi deve avere la barriera stessa

Quando l'apertura comprende il pavimento o un piano facilmente accessibile come nell'esempio seguente gli AOPD devono comprendere almeno 3 raggi disposti in verticale e posizionati a 300mm, 700mm e 1100mm dal piano di accesso.

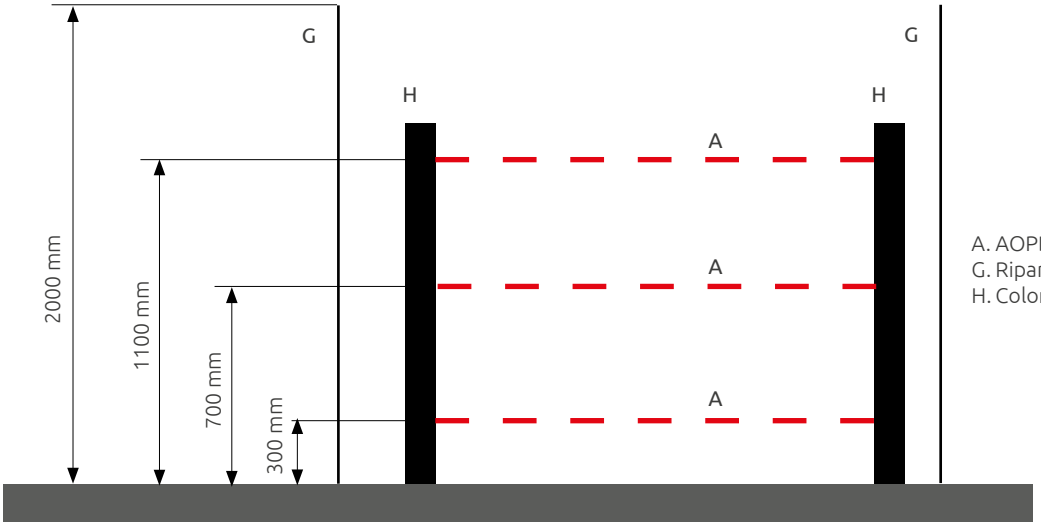


Fig. 45. pavimento o un piano facilmente accessibile

Quando l'apertura si trova su un convogliatore , l'AOPD deve avere almeno due raggi posizionati a 400mm e 900mm

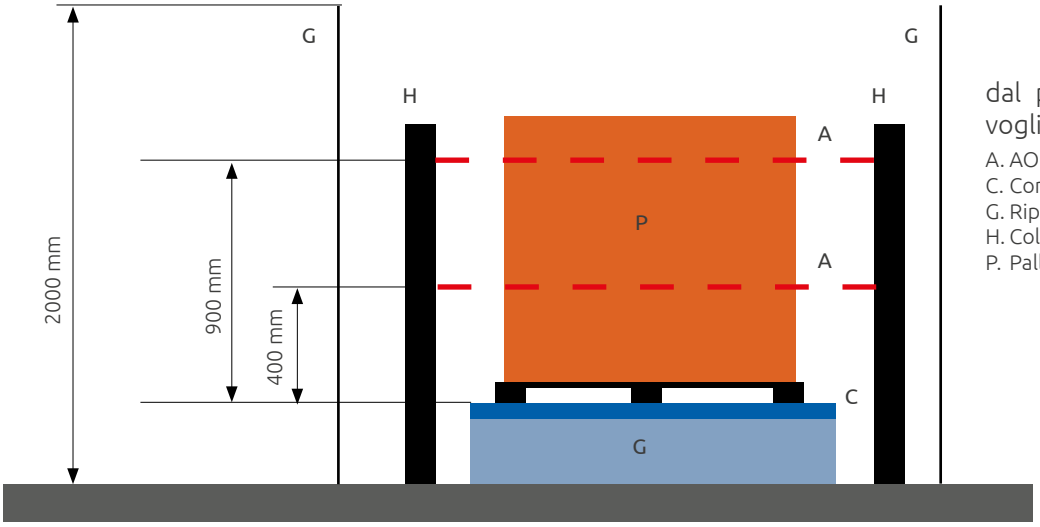


Fig. 46. apertura si trova su un convogliatore

La distanza di sicurezza va calcolata con la formula della ISO 13855:2010: **S = 1600 x T + 850**

Se è possibile raggiungere il punto pericoloso sporgendosi oltre il raggio più alto allora occorre usare la formula: **S = 1600 x T + C_{ro}** (dove C_{ro} si ricava dalla tabella 1 della ISO 13855:2010)

Oppure si sceglie un AOPD con un numero maggiore di raggi.

Utilizzo di ostacoli meccanici

Per impedire che una persona possa "strisciare" sotto il raggio più basso e raggiungere la zona pericolosa senza essere intercettato dall'AOPD si possono usare degli ostacoli meccanici.

Processi termici industriali

Controllo in sicurezza di tutte le applicazioni in cui si utilizzano dei bruciatori o, in generale, dei processi termici industriali. Ad esempio: Forni, Essiccatori per ceramica o cereali, pistole per retrazione, ecc.

Le richieste più comuni per questo tipo di applicazioni sono le seguenti:

- Controllo della fiamma che, secondo la normativa ISO/13849-1 deve raggiungere il livello di sicurezza PL e.
- Controllo pressione gas e olio combustibile (PL d)
- Controllo presenza gas nei tubi dopo il lavaggio (PL d)
- Controllo dello spegnimento delle ventole per l'aria comburente (PL d)

Occorre evidenziare un fattore fondamentale per quanto riguarda questo tipo di applicazioni: non si deve creare una confusione tra il dispositivo "bruciatore" e l'impianto o processo termico in cui questo viene utilizzato.

Il bruciatore deve rispettare delle normative specifiche che richiedono funzioni di lettura analogica della miscela aria gas e molte altre funzioni logiche relative.

Esiste invece la normativa EN 746-2 che regola le applicazioni dei bruciatori e definisce i livelli di sicurezza richiesti e le normative applicabili.

Sensoristica prevista dalla normativa vigente:

- Controllo dello spegnimento della fiamma.
  Normalmente vengono utilizzati sensori di presenza fiamma (spesso ottici, non di sicurezza) anche se si dovrebbero utilizzare rilevatori di fiamma SIL3 oppure 2 rilevatori di fiamma SIL2. Più facilmente vengono utilizzati dei sistemi integrati di controllo del bruciatore (BMS) che includono il controllo di fiamma e sono certificati. Il segnale digitale SIL3 o i due segnali SIL2 vengono ricevuti da questi dispositivi
- Pressostati per il controllo della pressione del gas. Esistono solamente SIL2 ma non SIL3
- Sensori per il controllo della temperatura della fiamma pilota (SIL3)
- Sensori per il controllo del lavaggio dei tubi che possono contenere gas (rilevatori di gas SIL2 o SIL3)
- Sensori per il controllo delle ventole di areazione (sensori di portata SIL2)
- Pressostati per il controllo dell'aria comburente (pressostati SIL2)

Lo schema a blocchi rappresentato in figura indica le relazioni tra i diversi componenti dell'impianto.

Nello schema è evidente dove può intervenire un controllore di sicurezza tipo Mosaic. In base agli input forniti dai sensori e dai sistemi di sicurezza le uscite OSSD di Mosaic vanno ad agire sugli erogatori di gas ed aria che permettono la combustione.

Controllo di processo (a)

1. 1. Controllo e strumentazione dell'impianto
   - controllo livelli
   - controllo dei processi
   - regolazioni
   - interfaccia operatore
2. 2. Sistemi di sicurezza
   - e-stop
   - dispositivi di protezione interbloccati
   - lavaggio e controllo tubi
   - unità di controllo del bruciatore
   - controllo ventilazione dei gas di scarico
   - controllo rapporto aria/gas
   - sensori di pressione e di flusso
   - sensori di temperatura

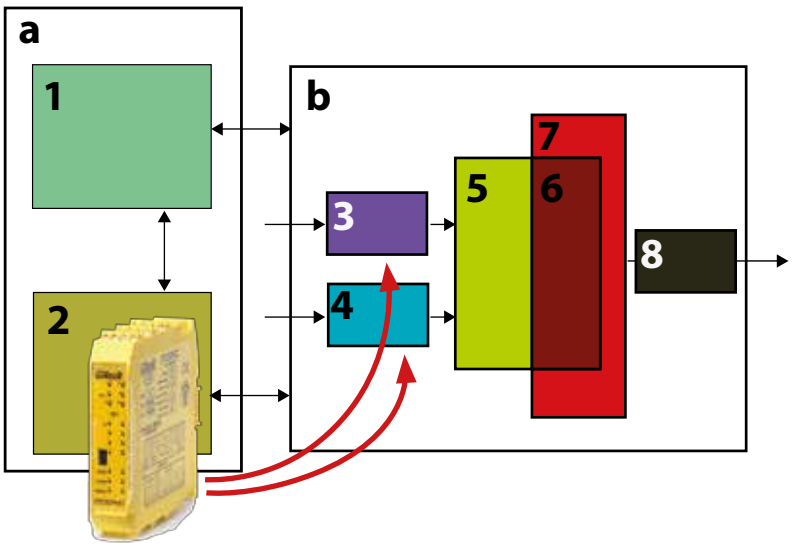


Fig. 47. Schema di apparecchiatura di processo termico industriale

Sistema di riscaldamento (b)

3. 3. Erogazione del combustibile (gas)
4. 4. Erogazione del comburente (aria)
5. 5. Bruciatore e dispositivi per iniezione di gas e aria
6. 6. Camera di combustione
7. 7. Camera per il processo termico
8. 8. Gas di scarico

Le norme di riferimento

La normativa di riferimento per questo tipo di impianti è la EN 746-2 - "Sicurezza per apparecchiature di processo termico industriale - Sicurezza per la combustione e per la movimentazione ed il trattamento dei combustibili" del 2010.

È una norma europea di tipo C e fa parte della serie di 8 norme di sicurezza che compongono la EN 746 "Apparecchiature di processo termico industriale".

La norma EN 746-2 presuppone che l'apparecchiatura non possa dare origine ad atmosfere potenzialmente esplosive e sia posta in luoghi ventilati.

La norma stabilisce i requisiti che deve avere il sistema di protezione e sicurezza per questi dispositivi:

- Il sistema di protezione è un insieme di dispositivi, unità di controllo e circuiti di sicurezza che hanno come scopo principale la protezione delle persone, dell'impianto e dell'ambiente.
- fanno parte del sistema di protezione tutti i componenti richiesti per realizzare le funzioni di sicurezza:
  - Sensori che permettono il monitoraggio dei parametri di funzionamento (temperatura della fiamma, pressione aria, ecc.)
  - Dispositivi che consentono l'interruzione di flusso del combustibile o del comburente (valvole)
  - Dispositivi per il controllo della ventilazione della camera di combustione e di protezione del bruciatore

Tipicamente il sistema di protezione e sicurezza è costituito da sensori, logiche di controllo, dispositivi di attuazione e da un sistema multi-canale che ne permette la comunicazione. È quindi necessario un controllo in sicurezza dei canali di comunicazione e dei dispositivi stessi.

La norma definisce anche le condizioni che devono essere soddisfatte dal sistema di protezione e sicurezza realizzato. Vengono definite 4 condizioni come indicate nella tabella seguente:

Condizione	Componente	Norma di riferimento
Sistema cablato in cui tutti i componenti sono conformi alle normative di prodotto indicate nei paragrafi da 5,2 a 5,6 della norma	Bruciatore	EN 298
	Valvole per controllo di tenuta	EN 1643
	Sensori di pressione	EN 1854
	Valvole automatiche di intercettazione carburante	EN 161
	Dispositivi di regolazione del rapporto aria-gas per bruciatori a gas e apparecchi a gas	EN 12067-2
Sistema cablato con una combinazione di: componenti conformi alle normative di prodotto indicate nei paragrafi da 5,2 a 5,6 della norma componenti conformi ai livelli di sicurezza PL e SIL definiti rispettivamente secondo le norme EN ISO 13849-1 e EN 62061	Bruciatore	EN 298
	Valvole per controllo di tenuta	EN 1543
	Sensori di pressione	EN 1854
	Valvole automatiche di intercettazione carburante	EN 161
	Dispositivi di regolazione del rapporto aria-gas per bruciatori a gas e apparecchi a gas	EN 12067-2
	Funzioni di controllo (esempio pressione del gas e temperatura) realizzate da componenti per i quali non esistono norme di prodotto, devono essere conformi almeno al livello di sicurezza: SIL 2 / PLd	IEC 62061 (SIL) EN ISO 13849 (PL)
	Funzioni di controllo che possono determinare un rischio immediato in caso di guasto (controlli di fiamma, rapporto gas/aria) realizzate da componenti per i quali non esistono norme di prodotto, devono essere conformi almeno al livello di sicurezza: SIL 3 / PLe	
Sistema basato su di un PLC e da una combinazione di: componenti conformi alle normative di prodotto indicate nei paragrafi da 5,2 a 5,6 della norma componenti conformi ai livelli di sicurezza PL e SIL definiti rispettivamente secondo le norme EN ISO 13849-1 e EN 62061	Bruciatore	EN 298
	Valvole per controllo di tenuta	EN 1543
	Sensori di pressione	EN 1854
	Valvole automatiche di intercettazione carburante	EN 161
	Dispositivi di regolazione del rapporto aria-gas per bruciatori a gas e apparecchi a gas	EN 12067-2
	Funzioni di controllo (esempio pressione del gas e temperatura) realizzate da componenti per i quali non esistono norme di prodotto, devono essere conformi almeno al livello di sicurezza: SIL 2 / PLd	IEC 62061 (SIL) EN ISO 13849 (PL)
	Funzioni di controllo che possono determinare un rischio immediato in caso di guasto (controlli di fiamma, rapporto gas/aria) realizzate da componenti per i quali non esistono norme di prodotto, devono essere conformi almeno al livello di sicurezza: SIL 3 / PLe	
	Il software di gestione delle funzioni di sicurezza dovrebbe essere separato dalla altre funzioni di controllo e deve essere conforme ai requisiti delle norme EN ISO 13849 e EN 62061.	
	Il PLC utilizzato per le funzioni di sicurezza deve essere conforme ai requisiti delle norme EN ISO 13849-1 e EN 62061.	
Sistema basato su di un PLC e da componenti tutti conformi ai livelli di sicurezza PLe e SIL 3 definiti rispettivamente secondo le norme EN ISO 13849-1 e EN 62061 compreso il software di gestione	In questo caso il sistema di sicurezza deve essere conforme alle norme EN ISO 13849-1 e EN 62061.	IEC 62061 (SIL) EN ISO 13849 (PL)

Protezioni perimetrali

Applicazione combinata delle barriere di sicurezza e degli specchi deviator. Per le protezioni perimetrali fino a 4 lati possono essere utilizzate delle colonne con specchi deviatori in combinazione alla barriere di sicurezza. Un esempio di applicazione è illustrata nella figura seguente.

Fig. 48. Protezione perimetrale di una macchina per taglio laser

La gamma di colonne con specchi deviatori offerta da ReeR è la seguente:

Modelli	FMC-S2	FMC-SB2	FMC-S3	FMC-SB3	FMC-S4	FMC-SB4	FMC-S1700	FMC-S2000
Codice ordinazione	1200620	1200645	1200621	1200646	1200622	1200647	1200625	1200623
Descrizione	specchio unico per barriere a 2 raggi	2 specchi per barriere a 2 raggi	specchio unico per barriere a 3 raggi	3 specchi per barriere a 3 raggi	specchio unico per barriere a 4 raggi	4 specchi per barriere a 4 raggi	altezza controllata fino a 1360 mm	altezza controllata fino a 1660 mm
Altezza totale con base (mm)	1055		1255		1385		1725	2025

Le colonne che utilizzano specchi multipli sono ideali per la realizzazione di protezioni perimetrali di aree pericolose con accessi su più lati che prevedono grandi distanze tra gli elementi di protezione.

Normalmente le barriere utilizzate in questo tipo di applicazioni sono quelle a 2, 3 e 4 raggi per il rilevamento della presenza del corpo in area pericolosa. Sono però utilizzabili anche barriere con altre risoluzioni. In questo caso però non valgono le misure riportate della tabella di pagina seguente ma occorre valutare le distanze di sicurezza a seconda della tipologia di impianto. La disposizione delle barriere di sicurezza e delle colonne con gli specchi deviatori dipendono chiaramente dal tipo e dalle specifiche esigenze del sistema di protezione che si intende realizzare. Ci sono però 3 fattori di cui tener conto nel calcolare le distanze tra barriere di sicurezza e colonne:

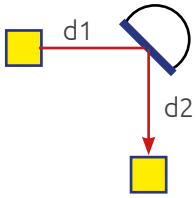
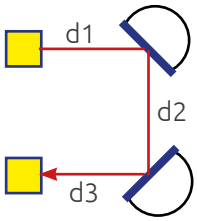
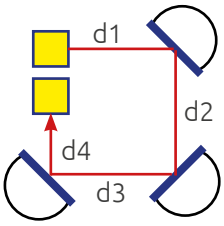
- Divergenza tra i raggi della barriera - Occorre tener conto del fatto che i raggi emessi dall'emettitore della barriera presentano un certo grado di divergenza, quindi non sono mai perfettamente paralleli
- Eventuali problemi di planarità dello specchio - Questo fattore, come il precedente aumenta la sua influenza con l'aumentare delle distanze
- Fattore di assorbimento degli specchi - Per ogni specchio utilizzato occorre tener conto della riduzione di potenza del fascio ottico emesso dall'emettitore della barriera. Fare riferimento allo schema seguente:
  - FMC (S2 - S3 - S4) - 15% per barriere con portata fino a 20 m
    - 20% per barriere con portata superiore a 20 m.
  - FMC (SB2 - SB3 - SB4) - 10% per barriere con portata fino a 20 m
    - 15% per barriere con portata superiore a 20 m.

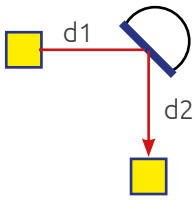
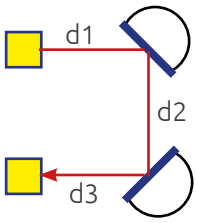
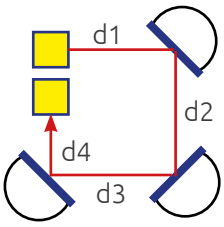
  Questa riduzione è dovuta alla caratteristiche specifiche dello specchio e tiene conto dello sporco e polvere che si deposita sullo stesso, specie in ambiente industriale. Questo fattore riduce la portata del sistema specchio/barriera.

Questi 3 fattori determinano sia la scelta della modello di barriera, sia le distanze minime per il posizionamento degli

elementi del sistema di protezione. La tabella seguente intende fornire una guida per:

- la scelta del tipo di colonna e di barriera da utilizzare
- definire le distanze massime permesse per il posizionamento corretto dei dispositivi tenendo conto dei fattori indicati in precedenza e della portata massima della barriera utilizzata

			TIPO DI INSTALLAZIONE - SPECCHIO SINGOLO		
TIPO DI COLONNA CON SPECCHIO	MODELLO DI BARRIERA DI SICUREZZA	PORTATA BARRIERA			
			Distanza massima	Distanza massima	Distanza massima
FMC S2 FMC S3 FMC S4	EOS	4 - 12 m	(d1+d2) < 10 m	(d1+d2+d3) < 8,5 m	(d1+d2+d3+d4) < 6,5 m
	SAFEGATE	4 - 12 m	(d1+d2) < 10 m	(d1+d2+d3) < 8,5 m	(d1+d2+d3+d4) < 6,5 m
	EOS H	10 - 20 m	(d1+d2) < 17 m	(d1+d2+d3) < 14,5 m	(d1+d2+d3+d4) < 12 m
	ADMIRAL	6 - 18 m	(d1+d2) < 15 m	(d1+d2+d3) < 13 m	(d1+d2+d3+d4) < 11 m
	VISION	6 - 16 m	(d1+d2) < 13,5 m	(d1+d2+d3) < 11,5 m	(d1+d2+d3+d4) < 9,5 m
	JANUS LR	30 - 60 m	(d1+d2) < 48 m	(d1+d2+d3) < 38 m	(d1+d2+d3+d4) < 30 m
	ADMIRAL LR	22 - 60 m			
	VISION LR	22 - 60 m			
	JANUS LR ILP	40 - 80 m	(d1+d2) < 64 m	(d1+d2+d3) < 51 m	(d1+d2+d3+d4) < 41 m

			TIPO DI INSTALLAZIONE - SPECCHI INDIPENDENTI		
TIPO DI COLONNA CON SPECCHIO	MODELLO DI BARRIERA DI SICUREZZA	PORTATA BARRIERA			
			Distanza massima	Distanza massima	Distanza massima
FMC SB2 FMC SB3 FMC SB4	EOS	4 - 12 m	(d1+d2) < 11 m	(d1+d2+d3) < 10 m	(d1+d2+d3+d4) < 9 m
	SAFEGATE	4 - 12 m	(d1+d2) < 11 m	d1+d2+d3) < 10 m	(d1+d2+d3+d4) < 9 m
	EOS H	10 - 20 m	(d1+d2) < 18 m	(d1+d2+d3) < 16 m	(d1+d2+d3+d4) < 14,5 m
	ADMIRAL	6 - 18 m	(d1+d2) < 16 m	(d1+d2+d3) < 14,5 m	(d1+d2+d3+d4) < 13 m
	VISION	6 - 16 m	(d1+d2) < 14,5 m	(d1+d2+d3) < 13 m	(d1+d2+d3+d4) < 11,5 m
	JANUS LR	30 - 60 m	(d1+d2) < 51 m	(d1+d2+d3) < 43 m	(d1+d2+d3+d4) < 36,5 m
	ADMIRAL LR	22 - 60 m			
	VISION LR	22 - 60 m			
	JANUS LR ILP	40 - 80 m	(d1+d2) < 68 m	(d1+d2+d3) < 58 m	(d1+d2+d3+d4) < 49 m

Per piccole distanze è sufficiente la colonna con specchio singolo; per distanze maggiori, che amplificano tutti i fattori indicati in precedenza, sono necessari gli specchi multipli che consentono di recuperare le divergenze di parallelismo dei raggi.

ReeR Customer Service

Mettiamo sempre il cliente al primo posto

Il servizio post-vendita di ReeR supporta i clienti che necessitano di una guida tecnica per quanto riguarda la funzionalità, la gestione e l'installazione dei prodotti

Linea diretta Servizio Clienti
011 24 82 215
Da Lunedì a Venerdì 8.30 - 12.30 e 13.30 - 18.00

in alternativa
aftersales@reer.it

Per ulteriori informazioni consultare il sito www.reersafety.it

Your future's safe!

Oltre 60 anni di qualità ed innovazione

Fondata a Torino nel 1959, ReeR si distingue per il forte contributo all'innovazione e alla tecnologia.

La costante crescita attraverso gli anni consente a ReeR di affermarsi come punto di riferimento globale nel settore della sicurezza per l'automazione industriale.

La Divisione Sicurezza è infatti oggi un leader mondiale nello sviluppo e produzione di sensori optoelettronici di sicurezza e controllori di sicurezza.

ReeR è certificata ISO 9001, ISO 14001 e ISO 45001.

Made in Italy
since 1959

ReeR SpA
Via Carcano, 32
10153 Torino

T 011 248 2215
F 011 859 867

www.reersafety.it | info@reer.it

Edizione 2 - Rev. 1.4
Giugno 2022
8946221
GUIDA ALLA SICUREZZA - Italiano

Stampato in Italia