SICUREZZA DEI SISTEMI DI COMANDO

EN ISO 13849-1 | EN ISO 13849-2

Software SISTEMA IFA

Certifico S.r.l.

2022

EN ISO 13849-1

L'ITER NORMATIVO DELLA ISO 13849-1

Il testo della ISO 13849-1:2015 è stato elaborato dall'Organizzazione Internazionale di Normazione (ISO) ed è stato ripreso, senza alcuna modifica, come EN ISO 13849-1:2015 dal Comitato Europeo per la Normazione (CEN).

La norma ha acquisito dall'Ente Nazionale Italiano di Unificazione (UNI) lo status di norma nazionale come UNI EN ISO 13849-1:2016, che sostituisce EN ISO 13849-1:2008.

EN ISO 13849-1 è norma armonizzata per la Direttiva Macchine 2006/42/CE, infatti è inclusa nell'elenco pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GU).

EN ISO 13849-1

Comunicazione della Commissione nell'ambito dell'applicazione della direttiva 2006/42/CE del Parlamento europeo e del Consiglio relativa alle macchine e che modifica la direttiva 95/16/CE

(Pubblicazione di titoli e riferimenti di norme armonizzate ai sensi della normativa dell'Unione sull'armonizzazione)

(Testo rilevante ai fini del SEE)

(2017/C 183/02)

OEN ([1])	Riferimento e titolo della norma (e documento di riferimento)	Prima pubblicazione GU	Riferimento della norma sostituita	Data di cessazione della presunzione di conformità della norma sostituita Nota 1
CEN	EN ISO 13849-1:2015 Sicurezza del macchinario — Parti dei sistemi di comando legate alla sicurezza — Parte 1: Principi generali per la progettazione (ISO 13849-1:2015)	13.5.2016	EN ISO 13849-1:2008 Nota 2.1	30.6.2016

EN ISO 13849-1

APPENDICE ZA (informativa) della EN ISO 13849-1

RELAZIONE TRA LA PRESENTE NORMA EUROPEA E I REQUISITI ESSENZIALI DELLA DIRETTIVA UE 2006/42/CE

La presente norma europea è stata elaborata nell'ambito di un mandato conferito al CEN dalla Commissione Europea e dall'Associazione Europea di Libero Scambio per fornire un mezzo per soddisfare i requisiti essenziali della Direttiva del Nuovo Approccio 2006/42/CE Macchine.

Una volta che la presente norma è citata nella Gazzetta Ufficiale dell'Unione Europea come rientrante in quella Direttiva e che è stata adottata come norma nazionale in almeno uno Stato membro, la conformità ai punti normativi della presente norma conferisce, entro i limiti dello scopo e campo di applicazione della presente norma, una presunzione di conformità con i requisiti essenziali 1.2.1 dell'Allegato I di quella Direttiva e regolamenti EFTA associati.

AVVERTENZA: Altri requisiti e altre Direttive UE possono essere applicabili al/ai prodotto/i che rientra/rientrano nello scopo e campo di applicazione della presente norma.

EN ISO 13849-1

RESS 1.2.1 – Allegato I della DIRETTIVA MACCHINE 2006/42/CE

1.2. SISTEMI DI COMANDO

1.2.1. Sicurezza ed affidabilità dei sistemi di comando

(1° par. Requisiti di base per l'affidabilità e la sicurezza dei sistemi di comando)

I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose.

In ogni caso essi devono essere progettati e costruiti in modo tale che:

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

EN ISO 13849-1

RESS 1.2.1 – Allegato I della DIRETTIVA MACCHINE 2006/42/CE

(2° par. Principali eventi e situazioni di pericolo da evitare)

Particolare attenzione richiede quanto segue:

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

In caso di comando senza cavo deve essere attivato un arresto automatico quando non si ricevono i segnali di comando corretti, anche quando si interrompe la comunicazione.

EN ISO 13849-1

Quindi il requisito 1.2.1 della DIRETTIVA MACCHINE 2006/42/CE richiede sostanzialmente che:

- la progettazione e la costruzione del sistema di comando garantiscano un funzionamento sicuro ed affidabile della macchina;
- l'operatore riesca a far funzionare la macchina sempre in sicurezza e secondo le modalità previste;
- la progettazione dei sistemi di comando consideri l'errore umano ragionevolmente prevedibile durante il funzionamento.

EN ISO 13849-1

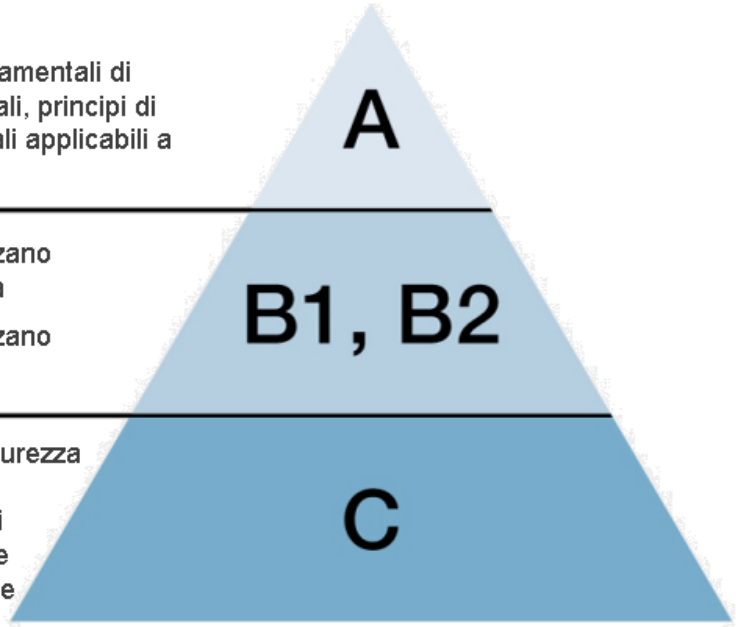
Tipologie norme tecniche

Norme di tipo A (norme fondamentali di sicurezza: concetti fondamentali, principi di progettazione e aspetti generali applicabili a tutti i macchinari

Norme di tipo B1, che analizzano aspetti specifici della sicurezza

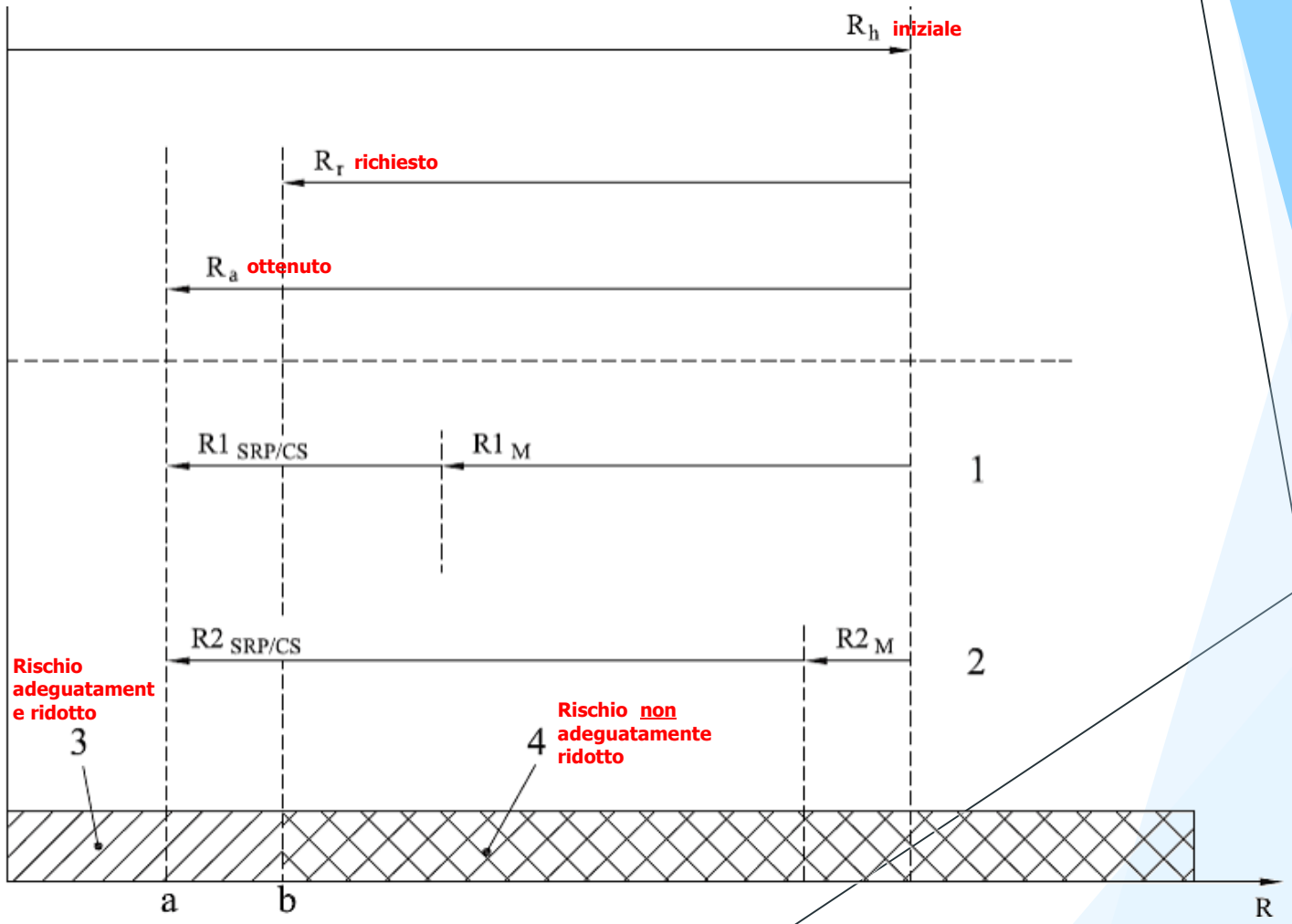
Norme di tipo B2, che analizzano i dispositivi di sicurezza

Norme di tipo C: norme di sicurezza per categorie di macchine), che trattano dettagliati requisiti di sicurezza per una particolare macchina o gruppo di macchine



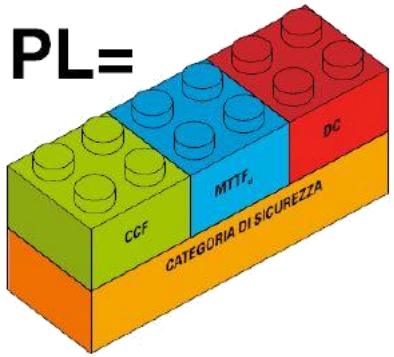
EN ISO 13849-1

PROCESSO DI RIDUZIONE DEL RISCHIO PER OGNI SITUAZIONE PERICOLOSA



EN ISO 13849-1

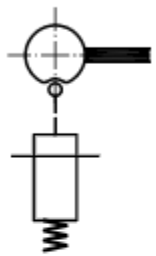
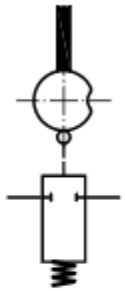
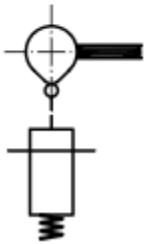
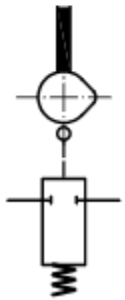
Non vi è correlazione diretta tra PL e le Categorie di Sicurezza della EN 954-1. La EN 13849 riutilizza i concetti delle categoria di sicurezza e della resistenza del sistema al guasto integrandoli con il calcolo di ulteriori nuovi parametri numerici MTTFd, DC e CCF



UNI EN ISO 14119

PRINCIPI DI SICUREZZA BEN PROVATI – SISTEMI ELETTRICI

EN ISO 14119 - MODI DI AZIONAMENTO DEI DISPOSITIVI DI INTERBLOCCO (tipo 1)

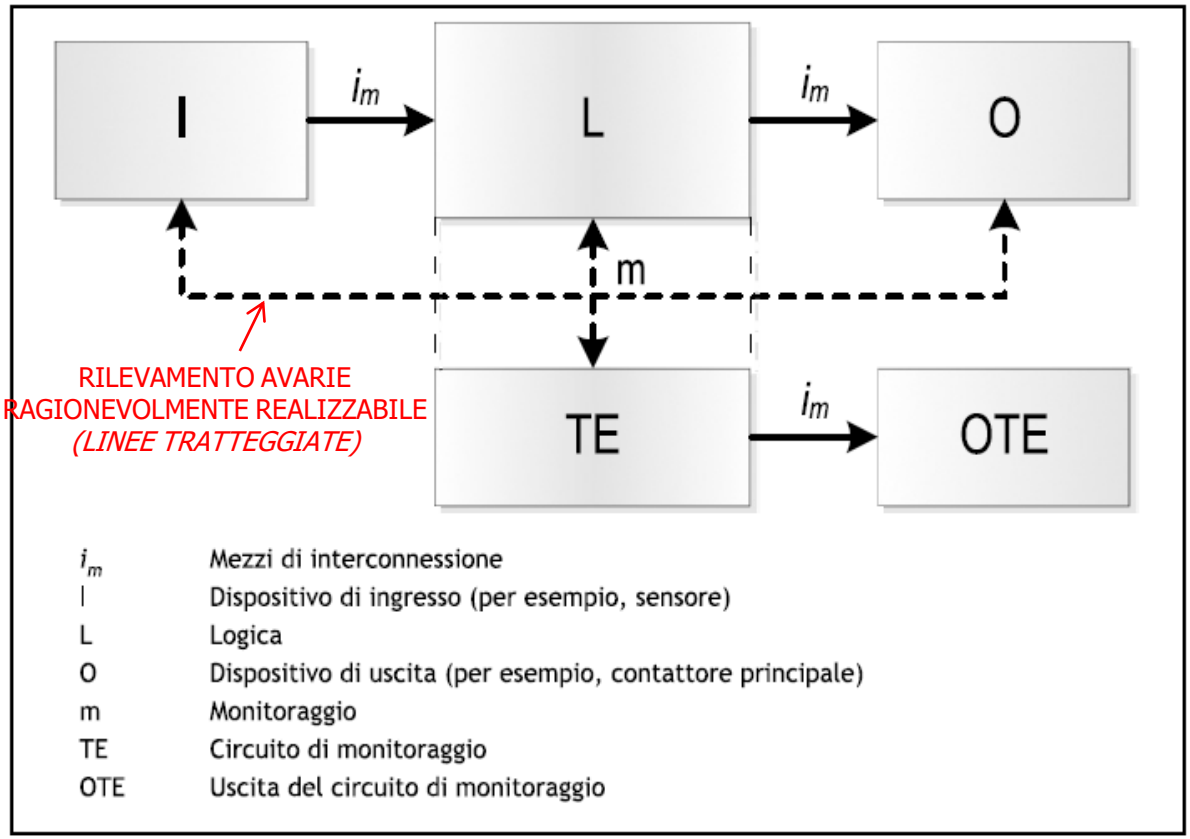
Mechanical action	Guard closed	Guard not closed	Working mode	Example of behaviour in case of failure (see 8.3.2)
Direct			Plunger held depressed by cam as long as guard is not closed When guard closed, output system changes its state as result of action of return spring	Output system remains in safe state when guard is not closed even if spring breaks
Non-direct			The plunger is held depressed by a cam as long as the guard is closed. When guard not closed, output system changes state as result of action of return spring.	If spring breaks, output system can go to unsafe state even if guard not closed.

EN ISO 13849-1

CAT.	REQUISITI	COMPORTAMENTO SISTEMA	PRINCIPIO
B	Principi di sicurezza di base.	Un'avaria può portare alla perdita della funzione di sicurezza.	Scelta dei componenti
1	Vedi cat. B. Componenti e principi di sicurezza ben provati.	Un'avaria può portare alla perdita della funzione di sicurezza, ma la probabilità è < di B.	Scelta dei componenti
2	Vedi cat. B e principi di sicurezza ben provati. La funzione di sicurezza controllata a intervalli opportuni mediante il sistema di comando della macchina.	Il verificarsi di un'avaria può portare alla perdita della funzione di sicurezza tra i controlli. La perdita della funzione di sicurezza è rilevata dal controllo.	Struttura
3	Vedi cat. B e principi di sicurezza ben provati. – una singola avaria in una SRP/CS non porti a una perdita della funzione di sicurezza; e – ogniqualvolta ragionevolmente fattibile, la singola avaria sia rilevata.	Quando si verifica una singola avaria la funzione di sicurezza è sempre eseguita. Alcune ma non tutte le avarie sono rilevate. L'accumulo di avarie non rilevate può portare alla perdita della funzione di sicurezza.	Struttura
4	Vedi cat. B e principi di sicurezza ben provati. – una singola avaria in una SRP/CS non porti a una perdita della funzione di sicurezza; e – la singola avaria sia rilevata durante o prima della successiva richiesta della funzione di sicurezza ma, se tale rilevamento non è possibile, l'accumulo di avarie non rilevate non deve portare alla perdita della funzione di sicurezza.	Quando si verifica una singola avaria la funzione di sicurezza è sempre espletata. Il rilevamento delle avarie accumulate riduce la probabilità della perdita della funzione di sicurezza (DC alta). Le avarie sono rilevate in tempo per prevenire la perdita della funzione di sicurezza.	Struttura

EN ISO 13849-1

CATEGORIA 2

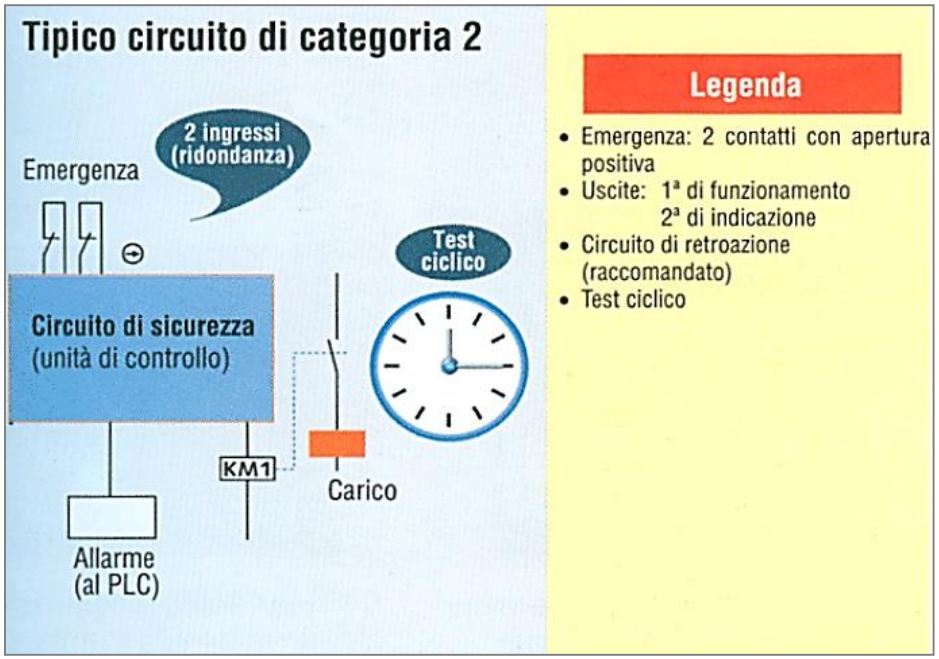


i_m	Mezzi di interconnessione
I	Dispositivo di ingresso (per esempio, sensore)
L	Logica
O	Dispositivo di uscita (per esempio, contattore principale)
m	Monitoraggio
TE	Circuito di monitoraggio
OTE	Uscita del circuito di monitoraggio

NOTA: Nel calcolo di MTTFd e DCavg non si considerano i blocchi del canale diagnostico.

EN ISO 13849-1

CATEGORIA 2: esempio



EN ISO 13849-1

CATEGORIA 3

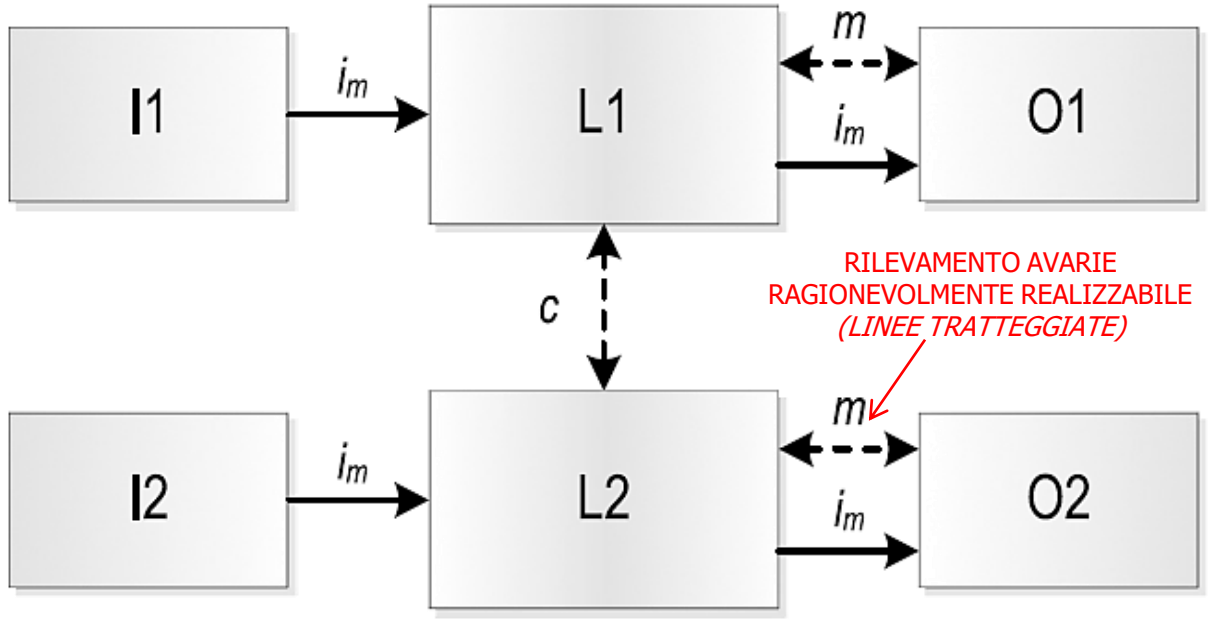
Si applicano i requisiti della categoria B, con aggiunta dei principi di sicurezza ben provati.
Un singolo guasto in qualsiasi sua parte NON DEVE comportare la perdita della funzione di sicurezza.
Quando possibile, tale guasto deve essere rilevato durante o prima della successiva richiesta della funzione di sicurezza.

Resistenza ai guasti	Quando si verifica un singolo guasto, la funzione di sicurezza è sempre eseguita. Alcuni guasti, ma non tutti, sono rilevati. L'accumulo di guasti non rilevati può portare alla perdita della funzione di sicurezza
Struttura tipica	Canale ridondante con monitoraggio
DC_{avg}	Da bassa a media
$MTTF_d$ di ciascun canale	Da basso ad alto
CCF	Deve essere soddisfatto
PL massimo raggiungibile	e

Il requisito del rilevamento di una singola avaria non significa che tutte le avarie siano rilevate. Di conseguenza, l'accumulo delle avarie non rilevate può portare ad un'uscita accidentale e a una situazione pericolosa nella macchina. Tipici esempi di misure attuabili per il rilevamento delle avarie sono l'utilizzo del feedback (ritorno) dei contatti di relè meccanicamente guidati e la sorveglianza delle uscite elettriche ridondanti.

EN ISO 13849-1

CATEGORIA 3



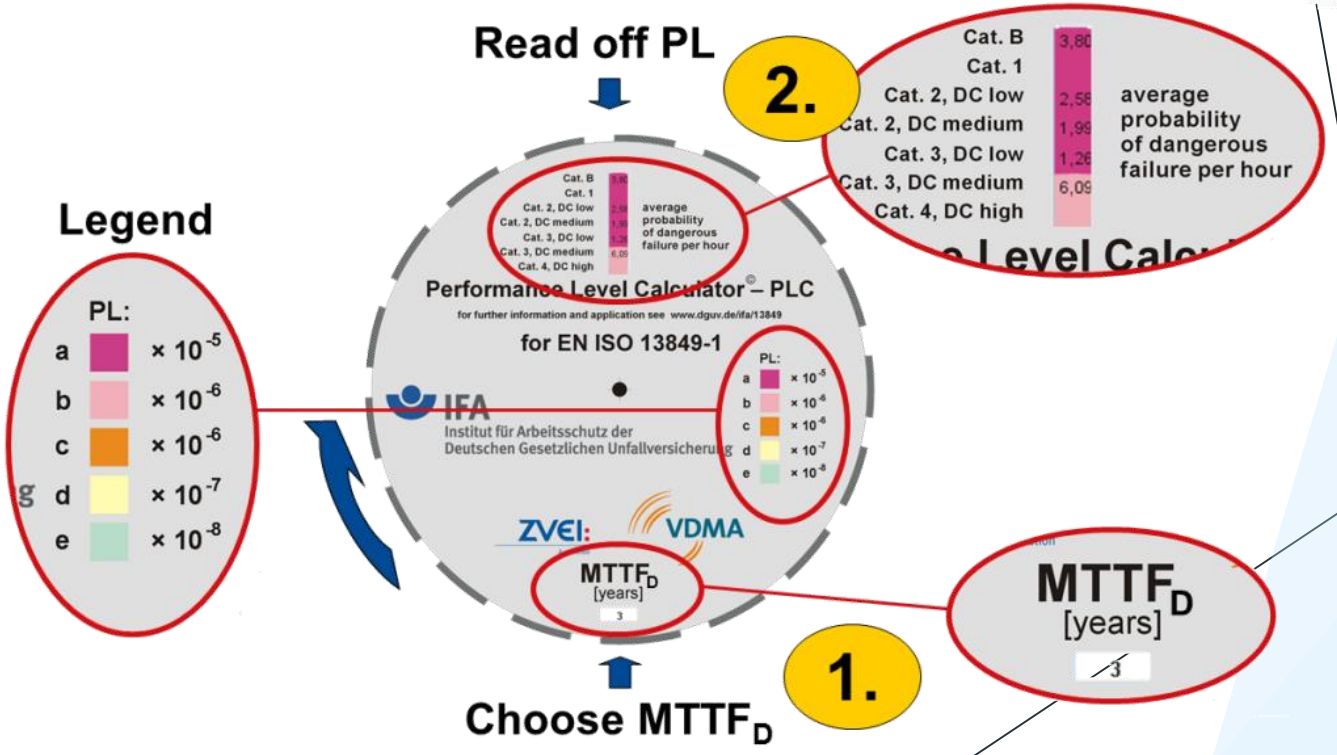
i_m	Mezzi di interconnessione
I1, I2	Dispositivi di ingresso (per esempio, sensori)
L1, L2	Logica
O1, O2	Dispositivi di uscita (per esempio, contattori)
m	Monitoraggio
c	Monitoraggio incrociato

Deve essere soddisfatto

EN ISO 13849-1

PERFORMANCE LEVEL CALCULATOR (PLC)

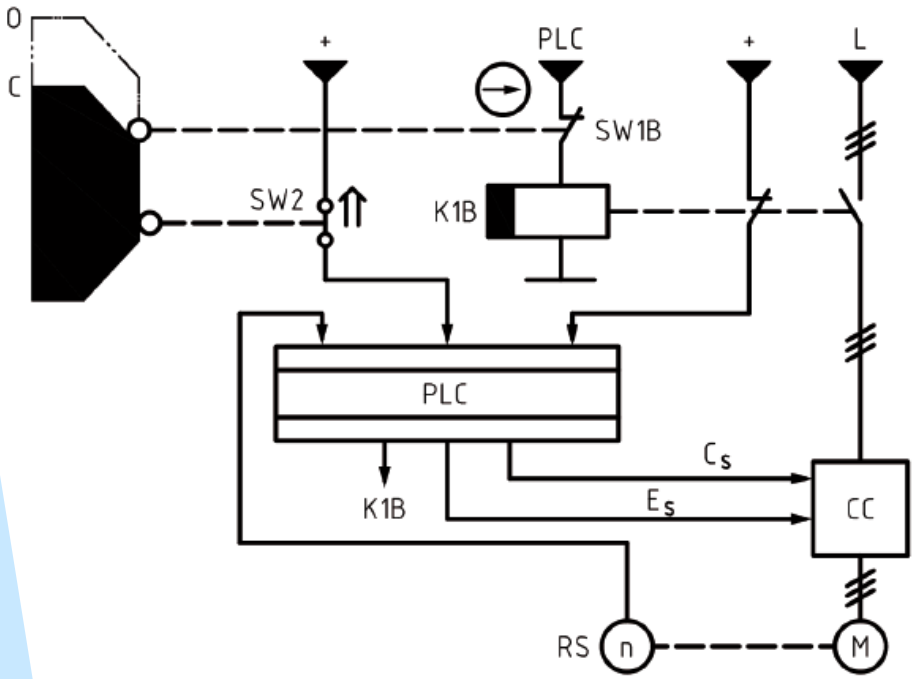
Disco per il calcolo del PL realizzato dalla BGIA o German Institute for Occupational Safety (sotto organizzazione dell'IFA, Institute for Occupational Health and Safety of the German Social Accident Insurance).



EN ISO 13849-1

ESEMPIO B (rif. EN ISO 13849-1, App. I)
CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

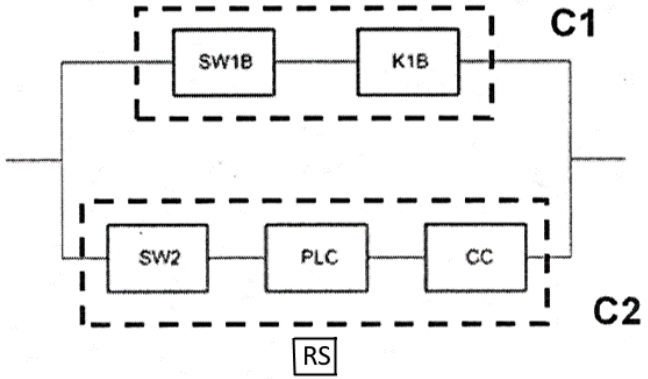
PLC	Controller a logica programmabile	C_s	Funzione di arresto (standard)
CC	Convertitore di corrente	E_S	Consenso (standard)
M	Motore	K1B	Relè contattore
RS	Sensore di rotazione	SW1B	Interruttore di posizione (NC)
o	Riparo interbloccante aperto	SW2	Interruttore di posizione (NO)
c	Riparo interbloccante non aperto	⇑	Apertura diretta

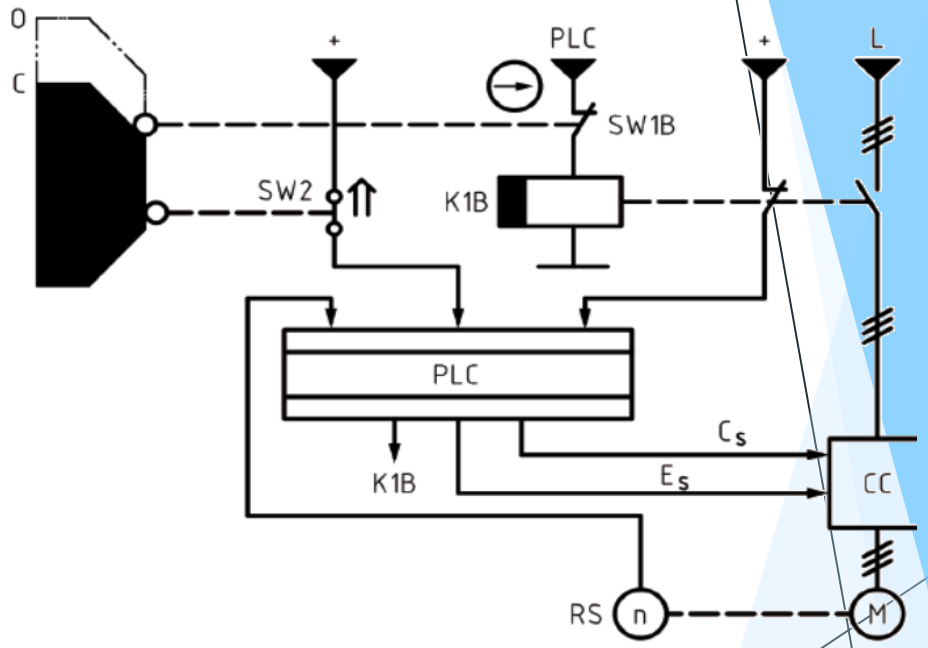


EN ISO 13849-1

ESEMPIO B (rif. EN ISO 13849-1, App. I)
CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

1° Step : Diagramma a blocchi relativo alla sicurezza :





2° Step : Calcolo di MTTFd:

Si suppongano i seguenti valori:

$MTTFd_{K1B}$ = 56 anni

MTTFdplc = MTTFdcc = 20 anni

MTTFdsw1b = 2778 anni

MTTFdsw2 = 139 anni

IL SW SISTEMA

IFA (Istituto per la Salute e la Sicurezza sul Lavoro dell'Assicurazione per gli Incidenti sul Lavoro in Germania), corrispettivo Tedesco di INAIL (ex-ISPESL), ha elaborato il SW

S.I.S.T.E.M.A.

Safety Integrity Software Tool for the Evaluation of Machine Applications

scaricabile gratuitamente per consentire il calcolo del PL per una funzione di sicurezza

(La versione italiana è a cura di ISPESL)

IL SW SISTEMA

SW SISTEMA

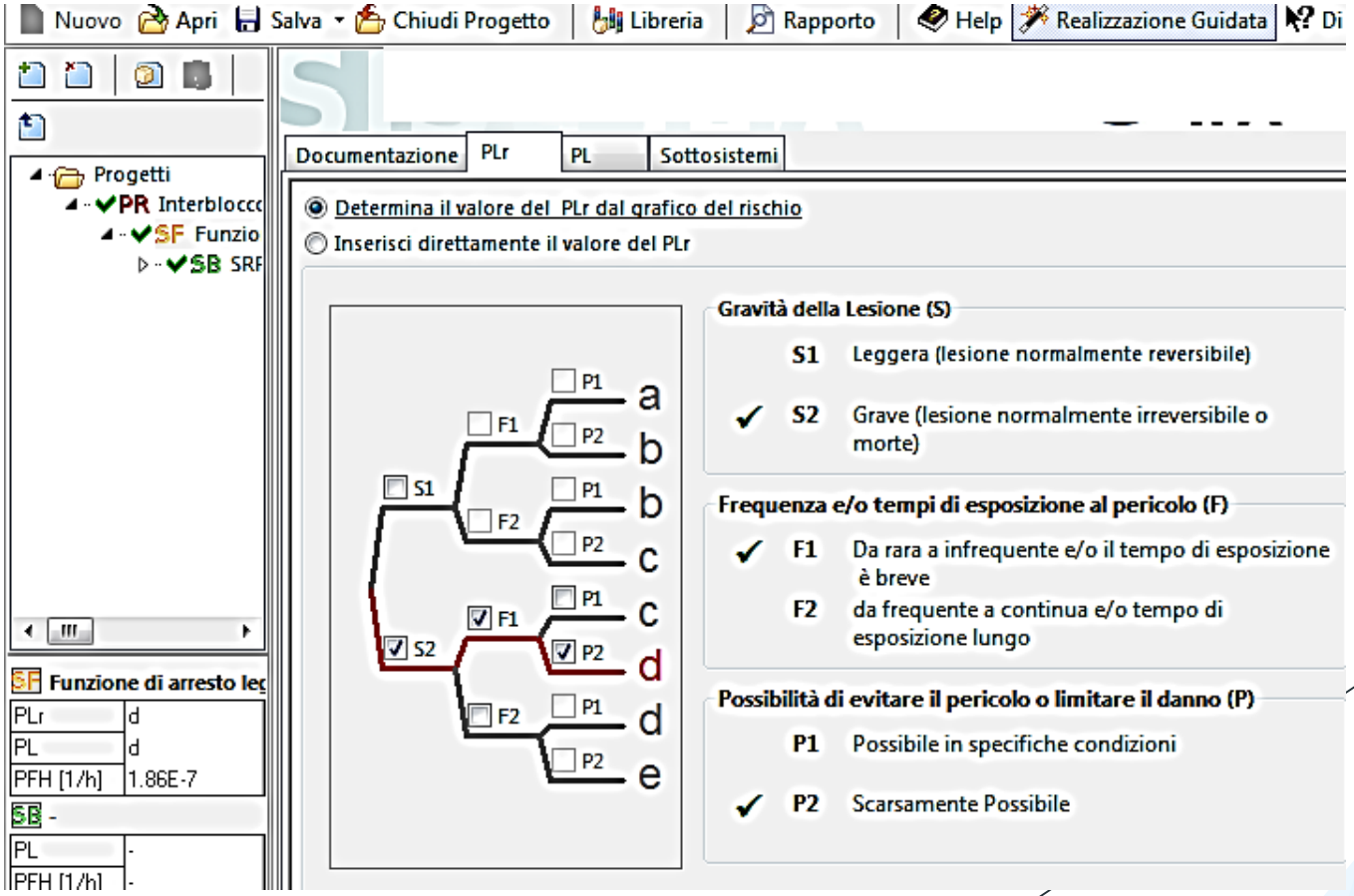
Uno strumento per la valutazione della sicurezza sui sistemi di controllo delle macchine. Un supporto per l'applicazione della norma EN ISO 13849-1.

Questo strumento consente di creare un modello della struttura realizzata con i componenti per il sistema di controllo relativo alla sicurezza sulla base delle architetture designate, permettendo in tal modo di calcolare automaticamente con diverso livello di dettaglio i parametri di affidabilita', compreso quello del Livello di Prestazione (PL) ottenuto.

Il SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)
CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

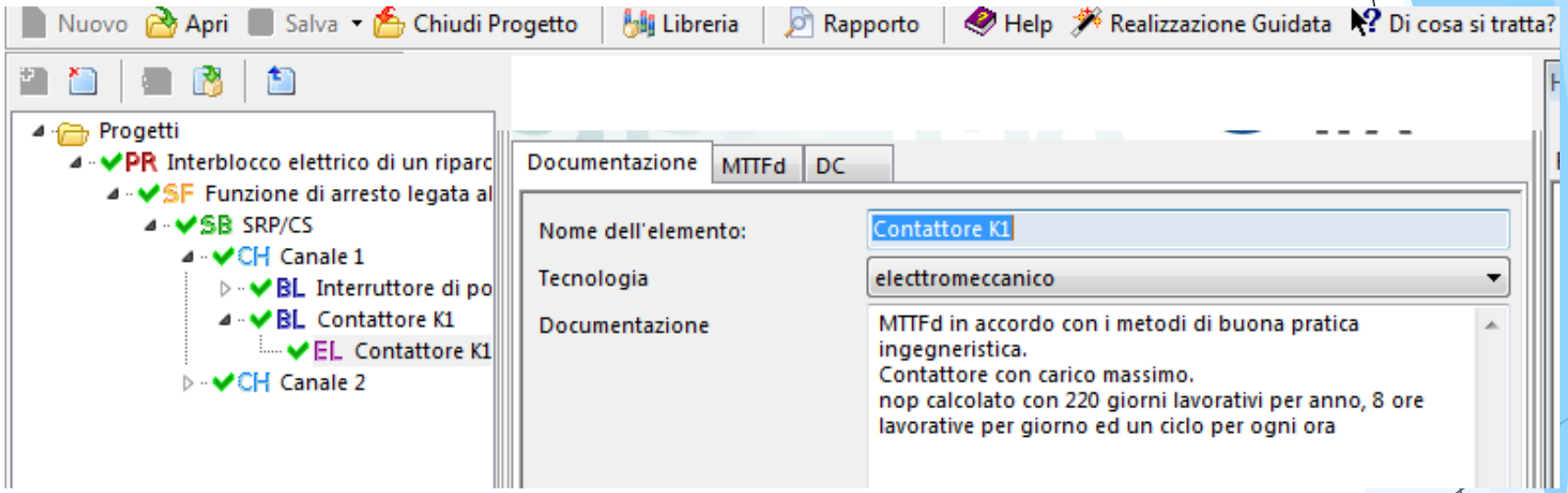
Definizione del PLr



Il SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)
CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Definizione dell'elemento



Il SW SISTEMA

Numerosi esempi di FUNZIONI DI SICUREZZA sono analizzati nel documento

BGIA Report 2/2008 Functional safety of machine controls – Application of EN ISO 13849-1

BGIA

Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

BG-Institute for Occupational Safety and Health

Emanazione di IFA

Per questi esempi esistono anche progetti già risolti con SISTEMA