SICUREZZA DEI SISTEMI DI COMANDO

EN ISO 13849-1:2023

EN ISO 13849-2:2012

Software SISTEMA IFA

Certifico S.r.l Rev. 1.0 2025

Certifico S.r.l.
Via Antonio De Curtis 28 - 06135 Perugia – IT
Via Madonna Alta 138A - 06128 Perugia - IT
Tel. + 39 075 599 73 63 | + 39 075 599 73 43
Assistenza 800 14 47 46
P.IVA IT02442650541

certifico.com

Testata editoriale iscritta al n. 22/2024 registro periodici
Tribunale di Perugia 19.11.2024

PARTE 1

EN ISO 13849-1:2023

Sicurezza del macchinario – Parti del sistema di comando legate alla sicurezza
Parte 1: Principi generali di progettazione

EN ISO 13849-1

ITER NORMATIVO DELLA ISO 13849-1

Il testo della ISO 13849-1:2023 è stato elaborato dall'Organizzazione Internazionale di Normazione (ISO) ed è stato ripreso, senza alcuna modifica, come EN ISO 13849-1:2023 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 13849-1:2023, che sostituisce la UNI EN ISO 13849-1:2016.

La 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

CEN	EN ISO 13849-1:2023 Sicurezza del macchinario - parti dei sistemi di comando legate alla sicurezza - parte 1: Principi generali per la progettazione (ISO 13849-1:2023)	15.05.2024			Con Decisione di esecuzione (UE) 2024/1329 La norma è pubblicata
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	Con Decisione di esecuzione (UE) 2024/1329 La norma è soppressa dal 15.05.2027

EN ISO 13849-1

PRESUNZIONE DI CONFORMITÀ E NORME ARMONIZZATE

Direttiva Macchine 2006/42/CE, art. 2, lettera l):

Definizione di NORMA ARMONIZZATA: specifica tecnica adottata da un organismo di normalizzazione europeo (CEN, CENELEC, ETSI) a seguito di un mandato rilasciato dalla Commissione Europea e non avente carattere vincolante.

Direttiva Macchine 2006/42/CE, art. 7, c. 2:

«2. Le macchine costruite in conformità di una norma armonizzata, il cui riferimento è stato pubblicato nella Gazzetta ufficiale dell'Unione europea, sono presunte conformi ai requisiti essenziali di sicurezza e di tutela della salute coperti da tale norma armonizzata.»

EN ISO 13849-1

- L'applicazione delle norme armonizzate non è obbligatoria.
- L'applicazione delle loro specifiche conferisce una presunzione di conformità ai requisiti essenziali di sicurezza e di tutela della salute (RESS) oggetto della norma.
- I requisiti essenziali di sicurezza e di tutela della salute (RESS) della Direttiva Macchine 2006/42/CE sono obbligatori in quanto disposizioni di legge.
- Direttiva Macchine 2006/42/CE entrata in vigore il 29/12/2009.
- D.Lgs. 17/2010 (Attuazione della direttiva 2006/42/CE, relativa alle macchine e che modifica la direttiva 95/16/CE relativa agli ascensori) entrato in vigore il 06/03/2010. Il recepimento italiano della Direttiva Macchine le conferisce lo status di legge nazionale.
- Regolamento Macchine 1230/2023 si applica dal 14/01/2027.

EN ISO 13849-1

APPENDICE ZA (informativa) della UNI EN ISO 13849-1

Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered

The relevant essential Requirements of Directive 2006/42/EC	Clause(s)/subclause(s) of this EN	Remarks/Notes
1.1.6	9	
1.2.1	6, 7, 10	
1.2.3	5.2.2.4	This subclause only deals with the restart function
1.2.4.1	5.2.2.2	This subclause only deals with those safety-related stop function achieving stop category 0 or 1.
1.2.4.2	5.2.2.2	This subclause only deals with those safety-related stop function achieving stop category 2.
1.2.4.3	5.2.1	This subclause only deals with the safety requirements specification (SRS) of an emergency stop function
1.2.5	5.2.2.9	
1.2.6	5.2.1.3 item i), 5.2.2.8	
1.6.1	11	
1.6.2	11	
1.6.4	11	
1.7.4.2 (e, g, i, r, s)	13	This subclause only deals with the instruction for safety functions.

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.

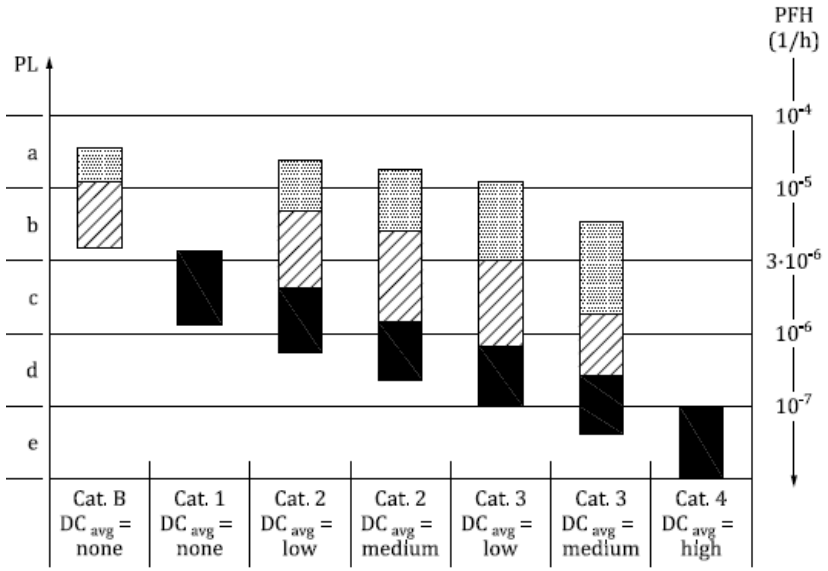
EN ISO 13849-1

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.

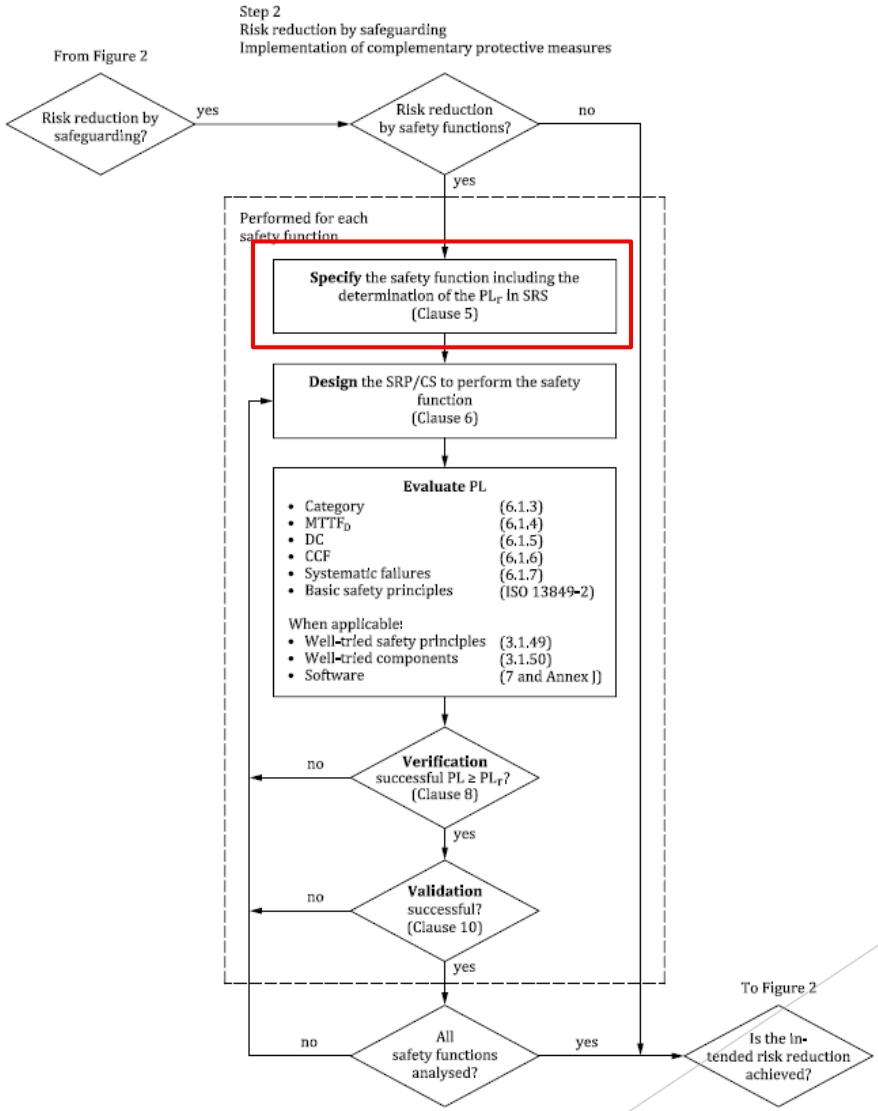
EN ISO 13849-1

RAPPRESENTAZIONE GRAFICA DEI LIVELLI DI PRESTAZIONE



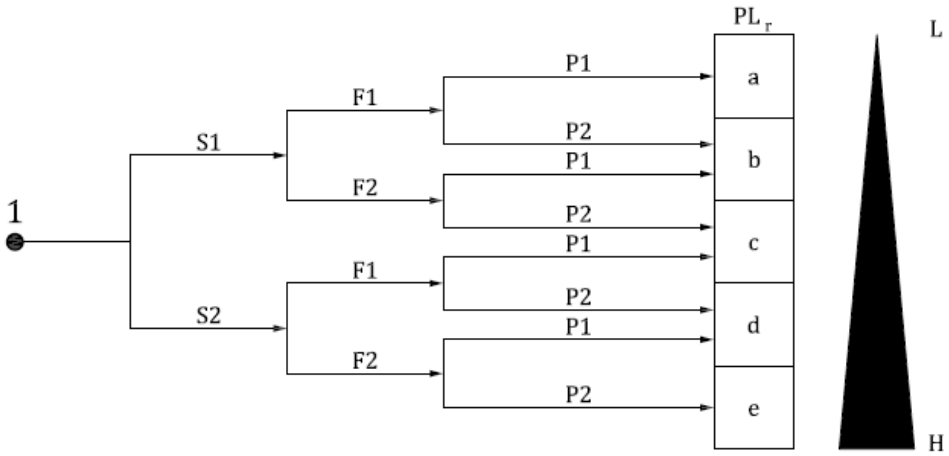
EN ISO 13849-1

PROCESSO ITERATIVO PER LA PROGETTAZIONE DI UN SRP/CS



EN ISO 13849-1

DETERMINAZIONE LIVELLO DI PRESTAZIONE RICHIESTO (PLr)

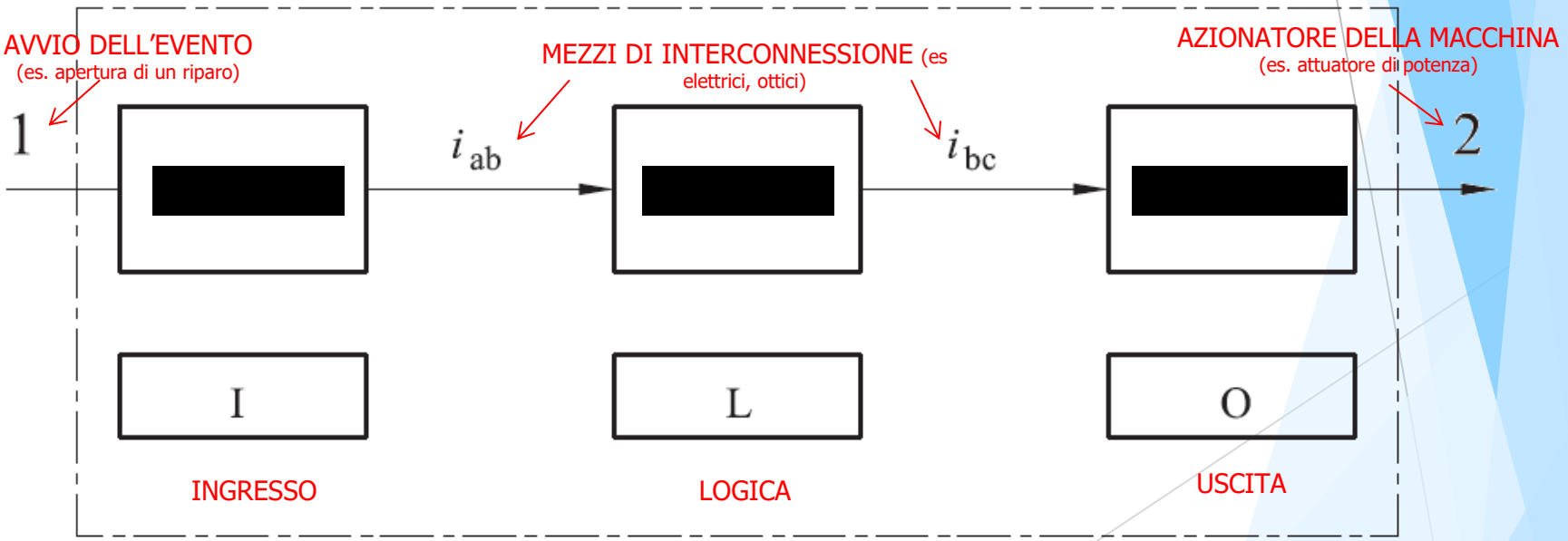


EN ISO 13849-1

PROGETTAZIONE DELLA SRP/CS

Progettazione e realizzazione tecnica della funzione di sicurezza con identificazione delle parti legate alla sicurezza che eseguono la SF mediante modellizzazione.

ESEMPIO



EN ISO 13849-1

COMPONENTI E APPARECCHIATURE GIA' CERTIFICATE

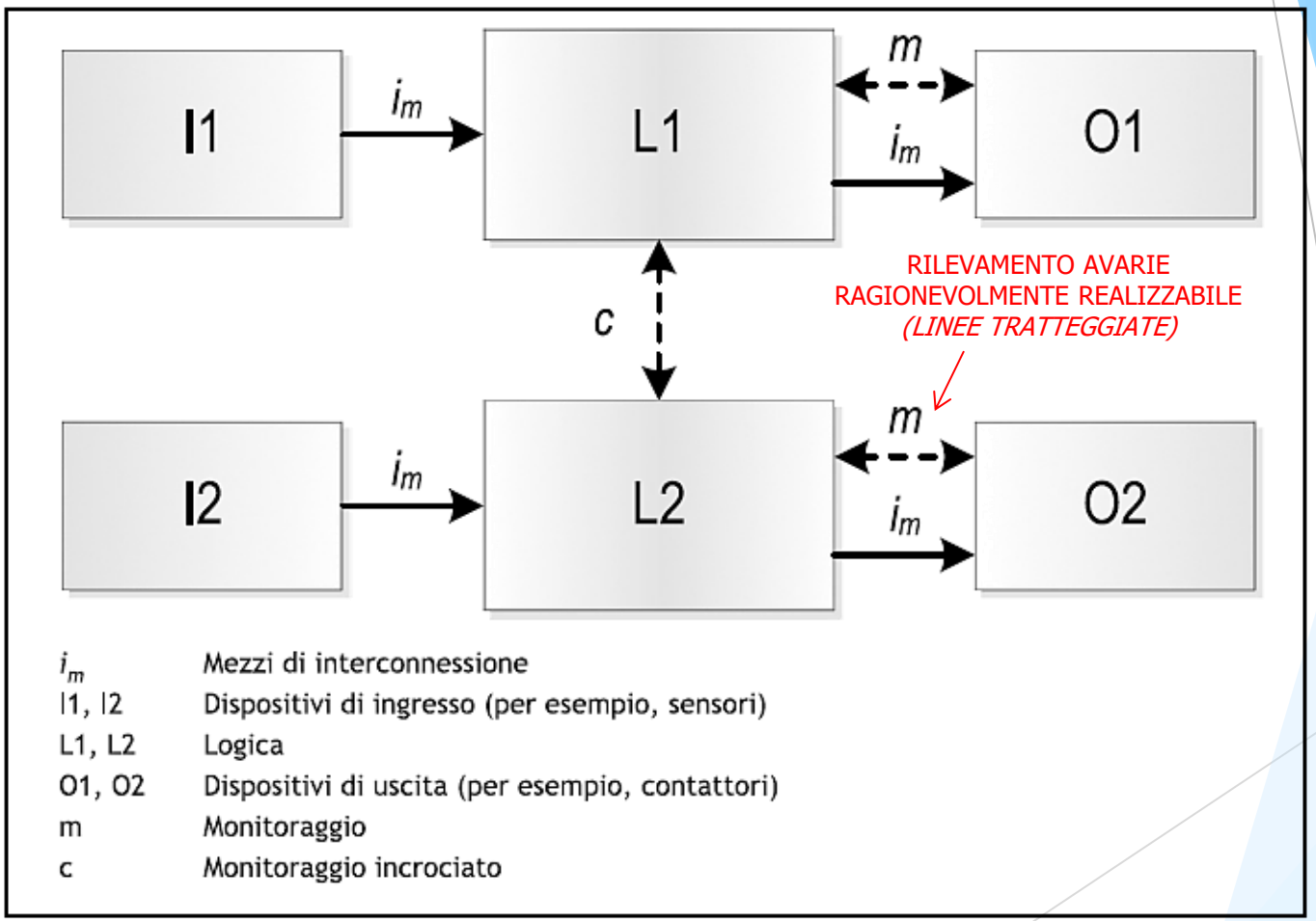
Sempre più frequentemente i costruttori certificano i loro componenti assegnando un Performance Level (in PFH) già sui Data Sheet (moduli di sicurezza, PLC di sicurezza, dispositivi «incapsulati» in genere). Se questi componenti sono utilizzati come sottosistemi in un canale di una SRP/CS, il PFH dichiarato può essere utilizzato come stima del MTTFd di questa Black Box:

$$MTTF_d = \frac{1}{\lambda_d} \cong \frac{1}{PFH}$$

Caso tipico dei moduli di sicurezza

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

EN ISO 13849-1

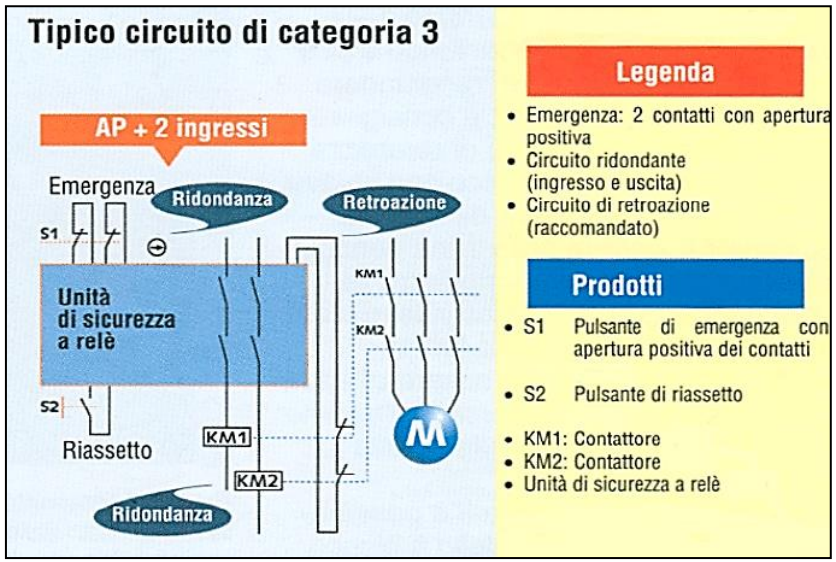
CATEGORIA 3

- *Quando si verifica il singolo guasto la funzione di sicurezza viene sempre assicurata (RIDONDANZA)*
- *Vengono rilevati alcuni ma non tutti i guasti (SORVEGLIANZA)*
- *L'accumulo dei guasti non rilevati può portare alla perdita della funzione di sicurezza*

Oltre alla sorveglianza viene introdotto nell'architettura il CONCETTO DI RIDONDANZA, cioè in caso di guasto di un canale la sicurezza è garantita da un altro canale. La perdita della funzione viene immediatamente rilevata.

EN ISO 13849-1

CATEGORIA 3: esempio



EN ISO 13849-1

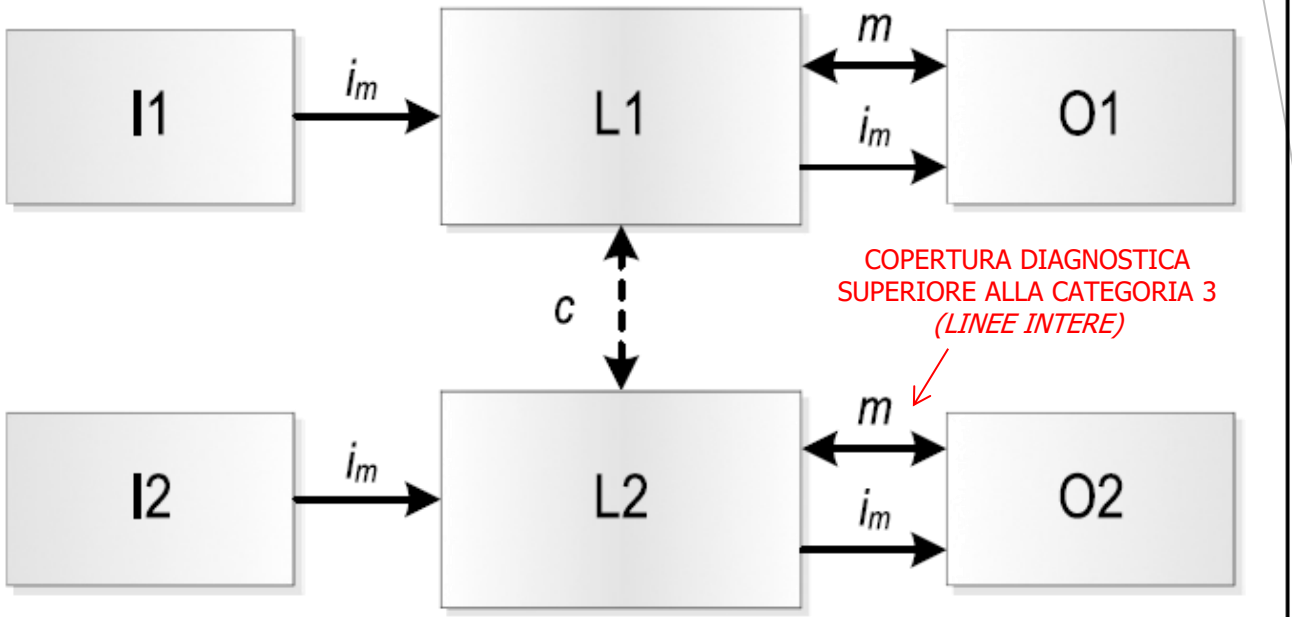
CATEGORIA 4

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. Il singolo guasto DEVE essere rilevato prima della successiva richiesta della funzione di sicurezza (p.es.: all'accensione o alla fine del ciclo operativo). Quando ciò non è possibile, la somma di più guasti non rilevati NON DEVE comunque causare la perdita della **funzione di sicurezza**.

Resistenza ai guasti	Quando si verifica un singolo guasto, la funzione di sicurezza è sempre eseguita. I guasti sono rilevati in tempo per prevenire la perdita della funzione di sicurezza. Anche l'accumulo di più di un guasto non rilevato, non comporta la perdita della funzione di sicurezza; nella pratica, è sufficiente considerare la combinazione di due guasti
Struttura tipica	Canale ridondante con monitoraggio
DC_{avg}	Alta
$MTTF_d$ di ciascun canale	Alto
CCF	**Deve essere soddisfatto**
PL massimo raggiungibile	e

EN ISO 13849-1

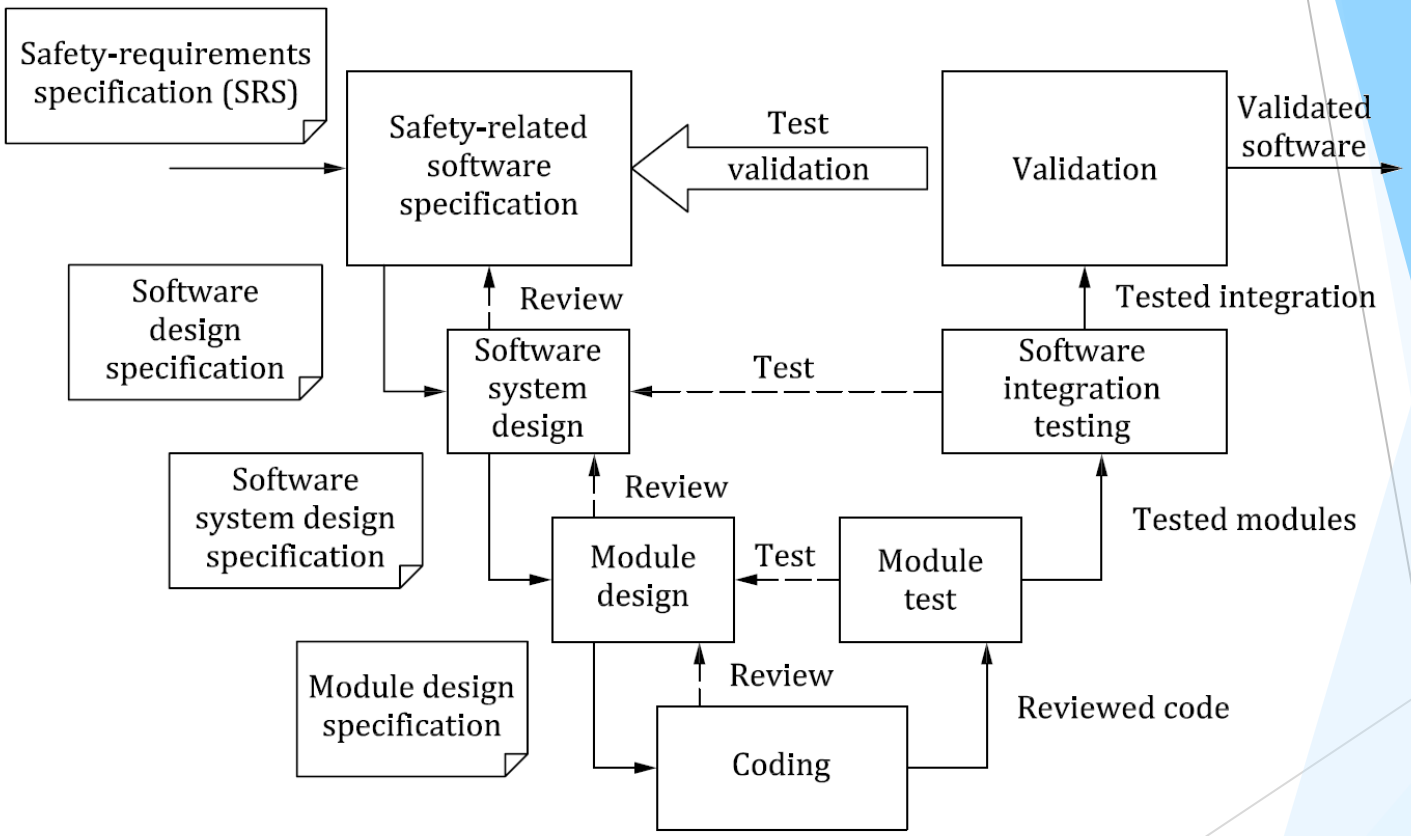
CATEGORIA 4



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

EN ISO 13849-1

CICLO DI VITA DI SICUREZZA DEL SW: MODELLO A V

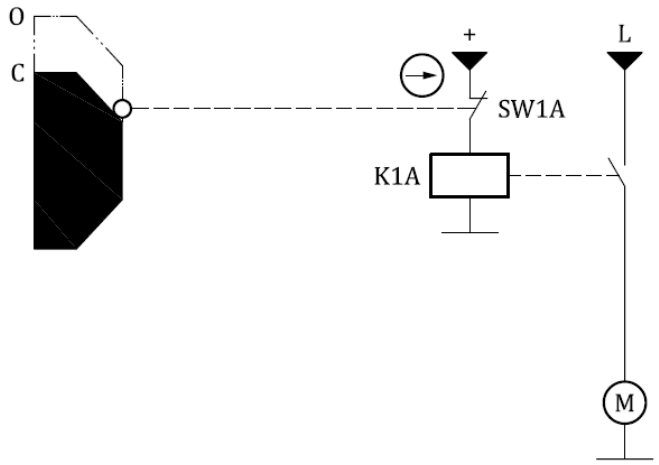


a) Simplified V-model of software safety lifecycle

EN ISO 13849-1

ESEMPIO A (rif. EN ISO 13849-1, App. I)

CIRCUITO A SINGOLO CANALE ELETTROMECCANICO



Key

O	guard interlocking is open
C	guard interlocking is not open
M	motor
K1A	contactor relay
SW1A	position switch (NC)
L	power supply
⊖	direct opening

NOTA: I dettagli funzionali che non contribuiscono alla funzione di sicurezza dell'interblocco (come interruttori di avvio e di arresto) sono omessi.

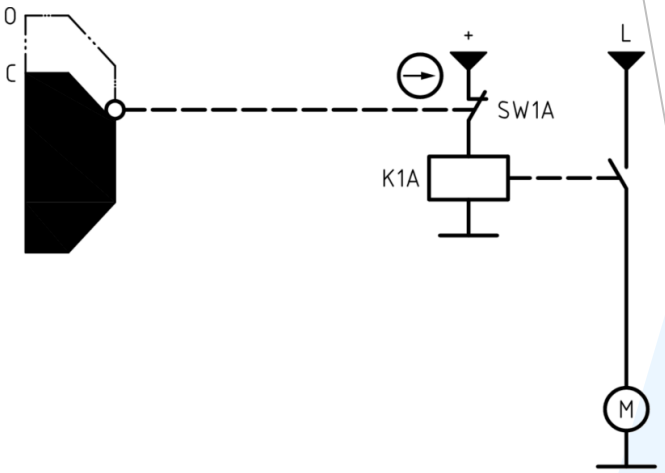
EN ISO 13849-1

ESEMPIO A (rif. EN ISO 13849-1, App. I)

CIRCUITO A SINGOLO CANALE ELETTROMECCANICO

1° Step : Diagramma a blocchi relativo alla sicurezza :

2° Step : Calcolo di MTTFd:



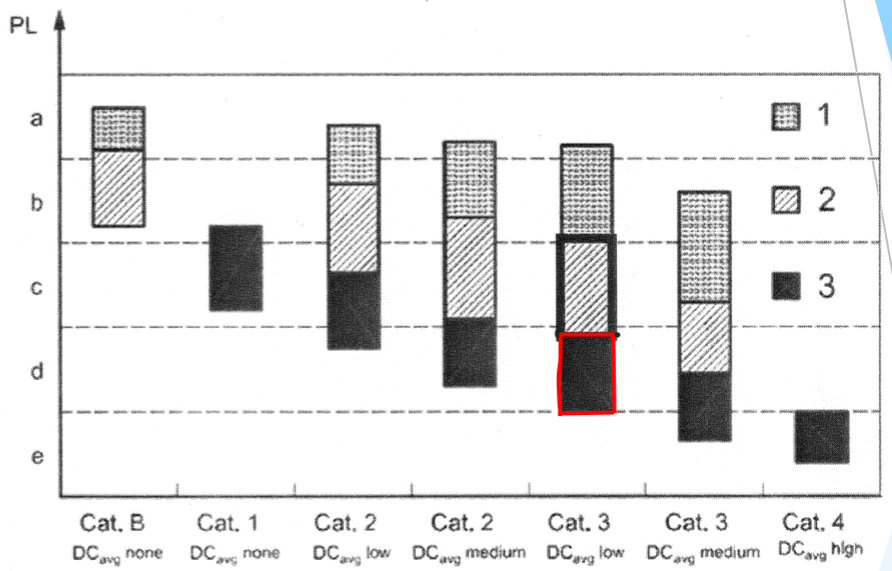
EN ISO 13849-1

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Riassumendo, per il sistema in esame si ha:

1. MTTFd = alto
2. DC_{AVG} = basso
3. CCF = soddisfatto
4. Categoria = 3



Secondo la figura, l'SRP/CS considerato raggiunge i requisiti conformi a: Categoria 3 PL d

ISO 13849-1 Categoria 3 PL d

PARTE 2

Il Software SISTEMA per il calcolo del PL

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

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.

SW SISTEMA

SW SISTEMA

Parametri di base come i parametri del rischio per la determinazione del Livello di Prestazione (PLr) richiesto, la Categoria, le misure contro i guasti per causa comune (CCF) su sistemi multicanale, la qualità media dei componenti (MTTFd) e la qualità media della diagnostica (DCavg) di componenti e blocchi, vengono inseriti passo passo in schede. Una volta che i dati richiesti sono stati inseriti in SISTEMA, i risultati sono prodotti e visualizzati istantaneamente. Un vantaggio pratico per l'utente è che ogni cambiamento di parametro si riflette immediatamente sull'interfaccia utente insieme al suo impatto sull'intero sistema.

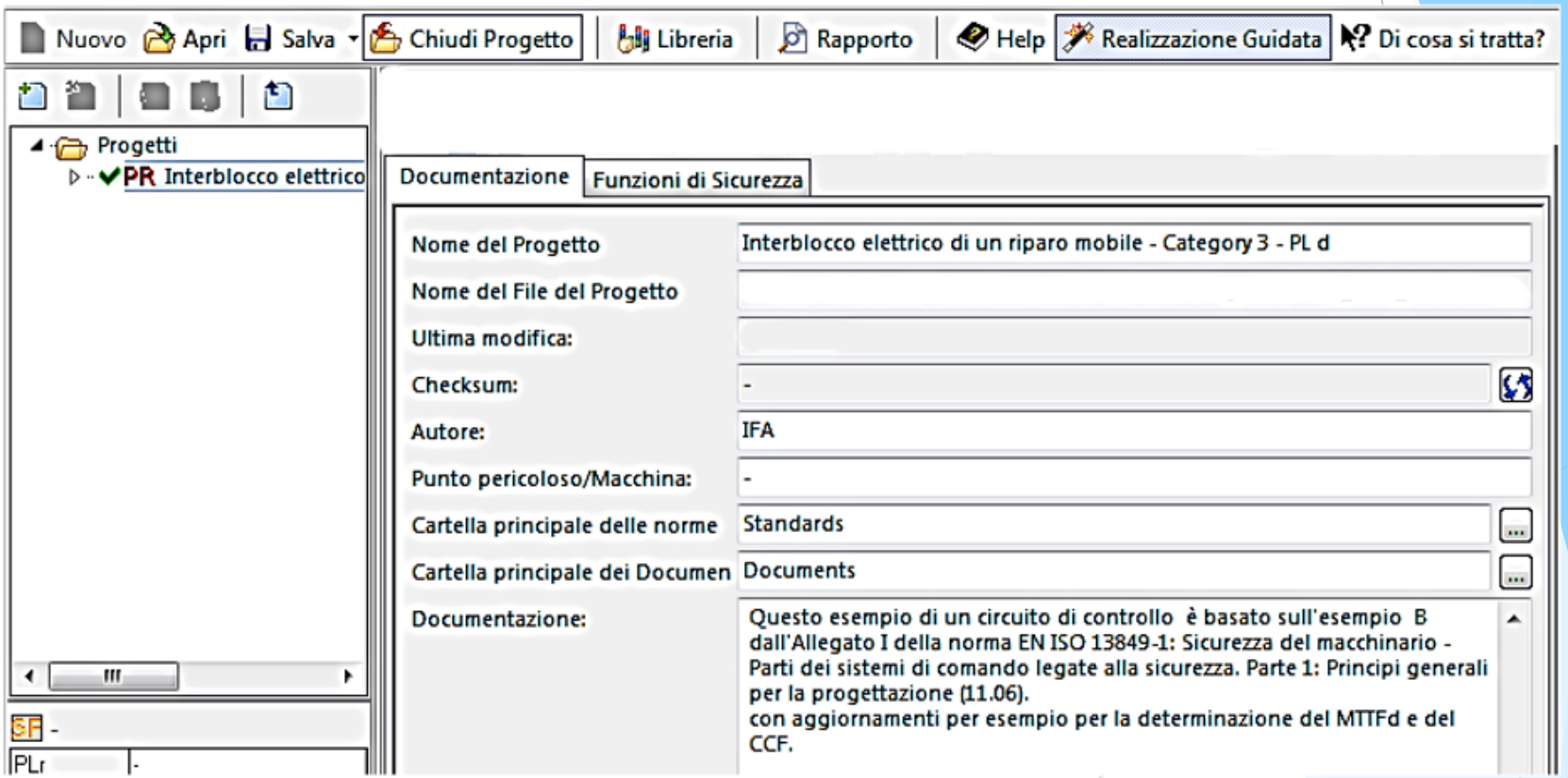
Il tempo da dedicare alla consultazione di tabelle ed al calcolo delle formule (calcolo del MTTFd per mezzo del metodo della conta delle parti, simmetrizzazione del MTTFd per ciascun canale, stima del DCavg, calcolo del PFH e PL, ecc.), viene impiegato dal software. Questo permette di "giocare" con i valori dei parametri e così di valutare l'effetto globale delle modifiche con uno sforzo minimo.

SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Inserimento del Progetto (PR)

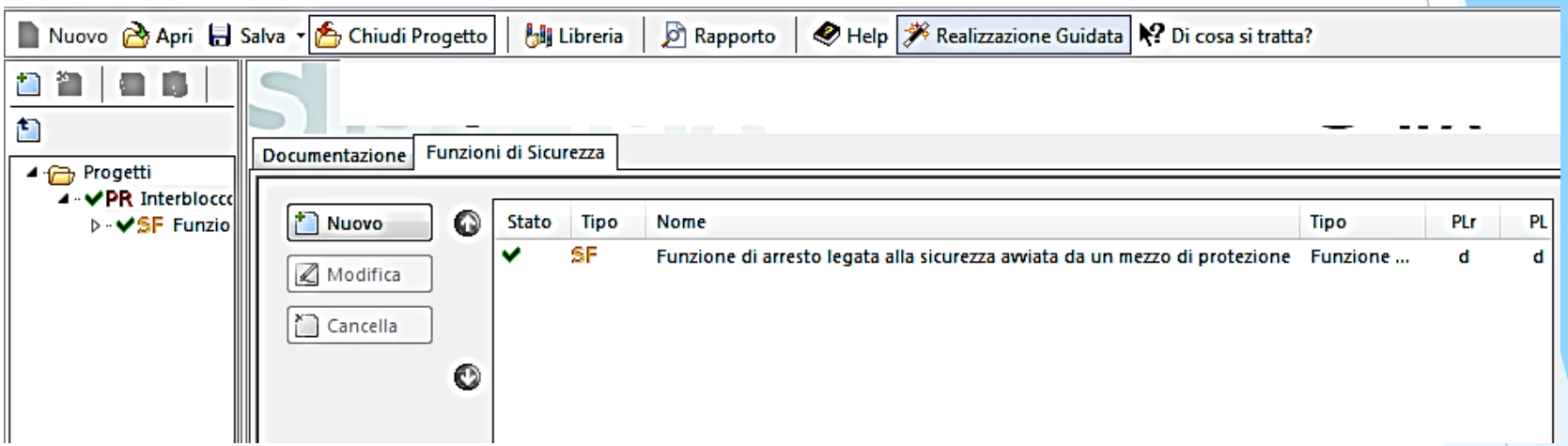


SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

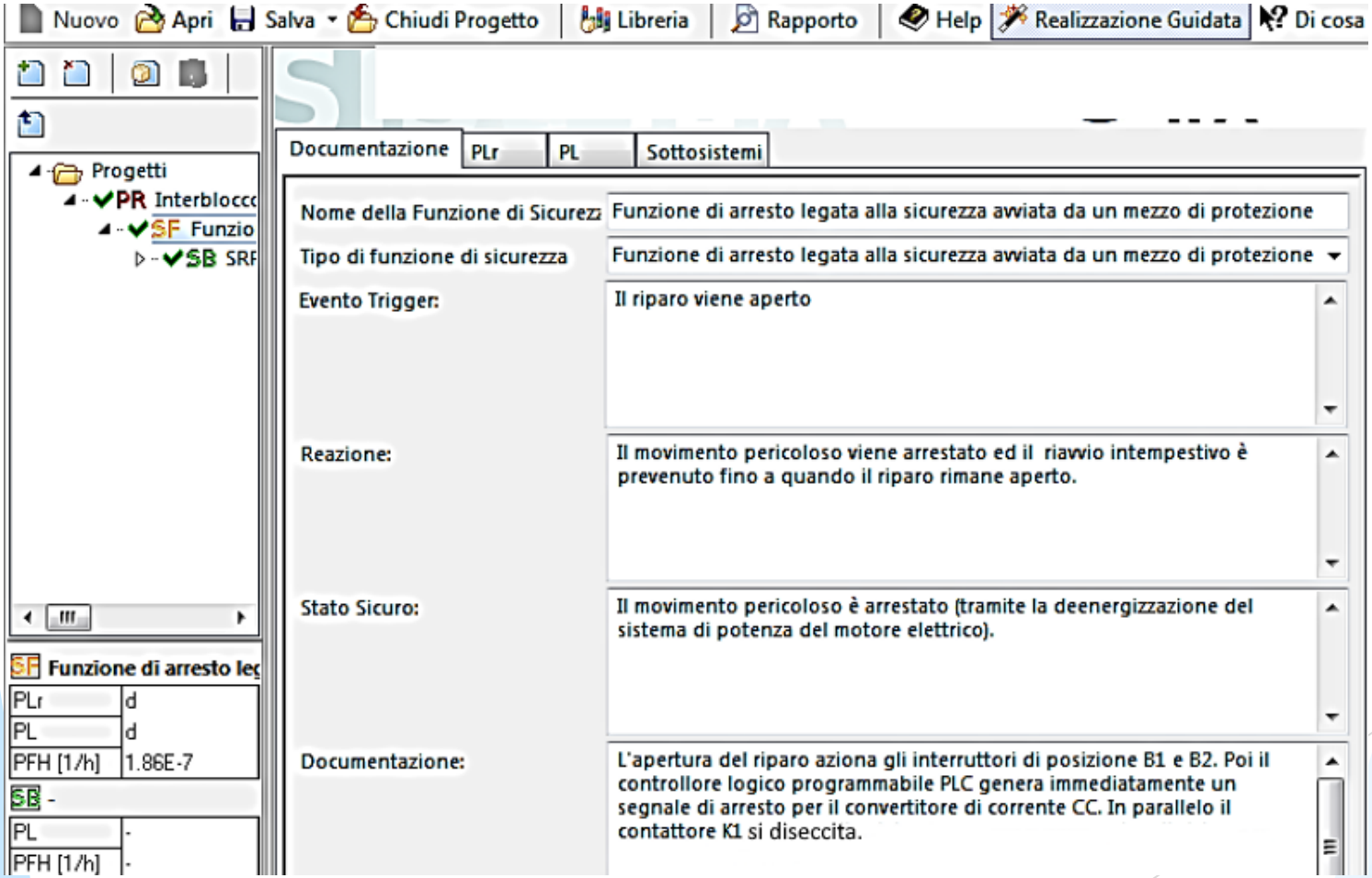
Inserimento delle Funzioni di Sicurezza (SF)



SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

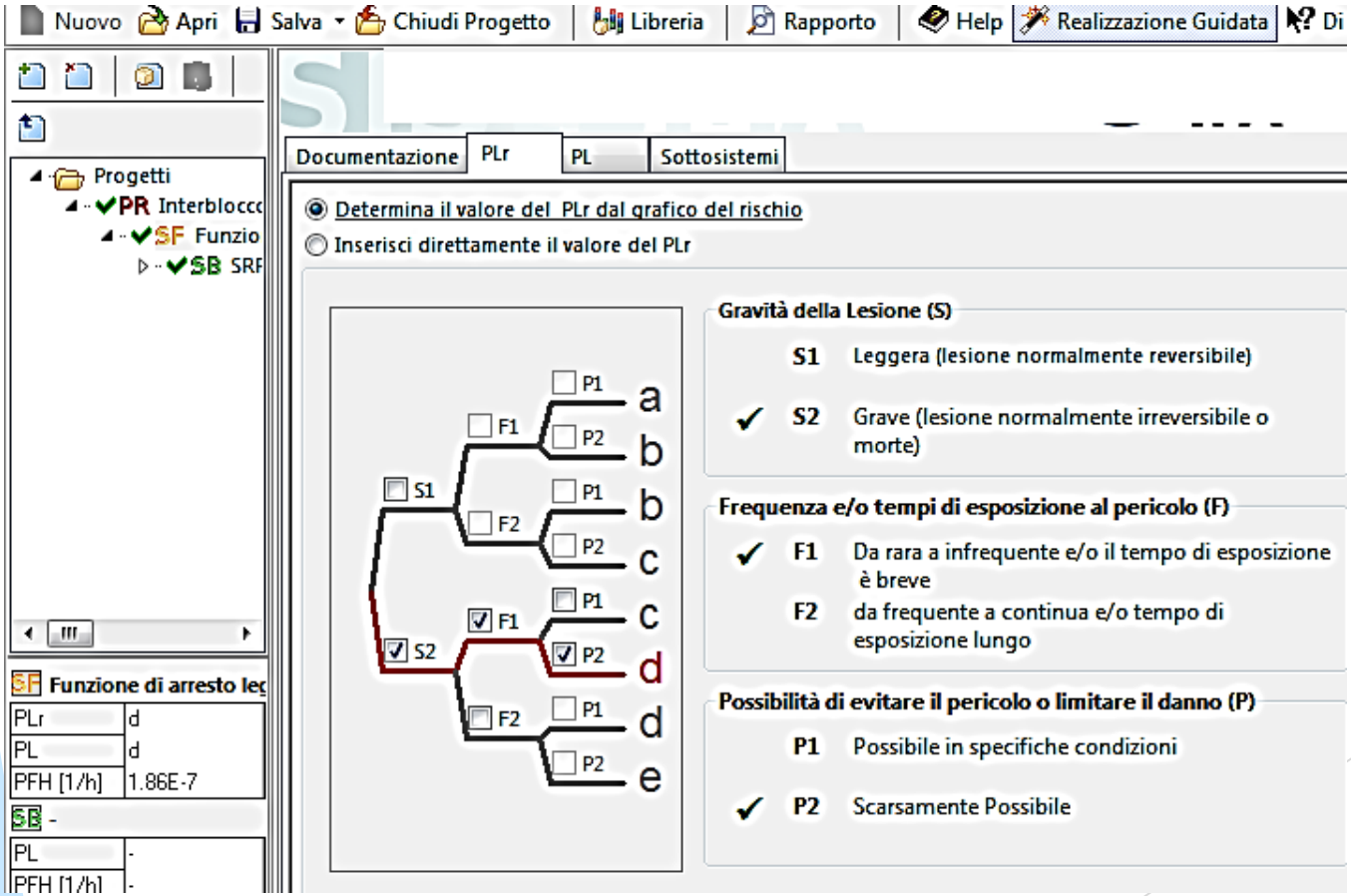


SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Definizione del PLr



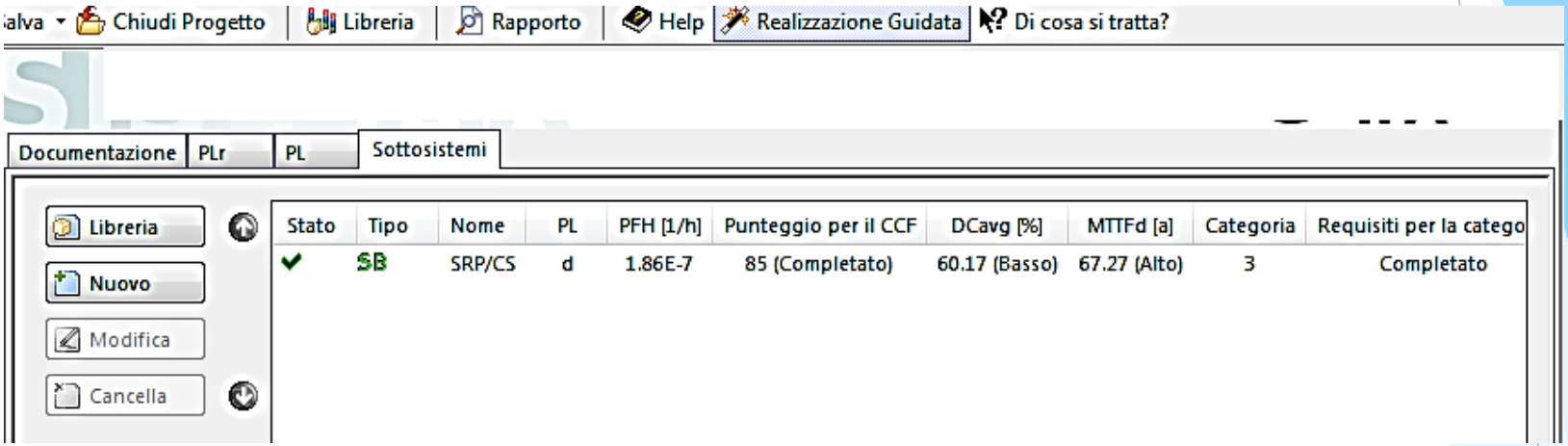
SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Inserimento di un sottosistema della SRP/CS

(in questo caso coincide con l'SRP/CS)

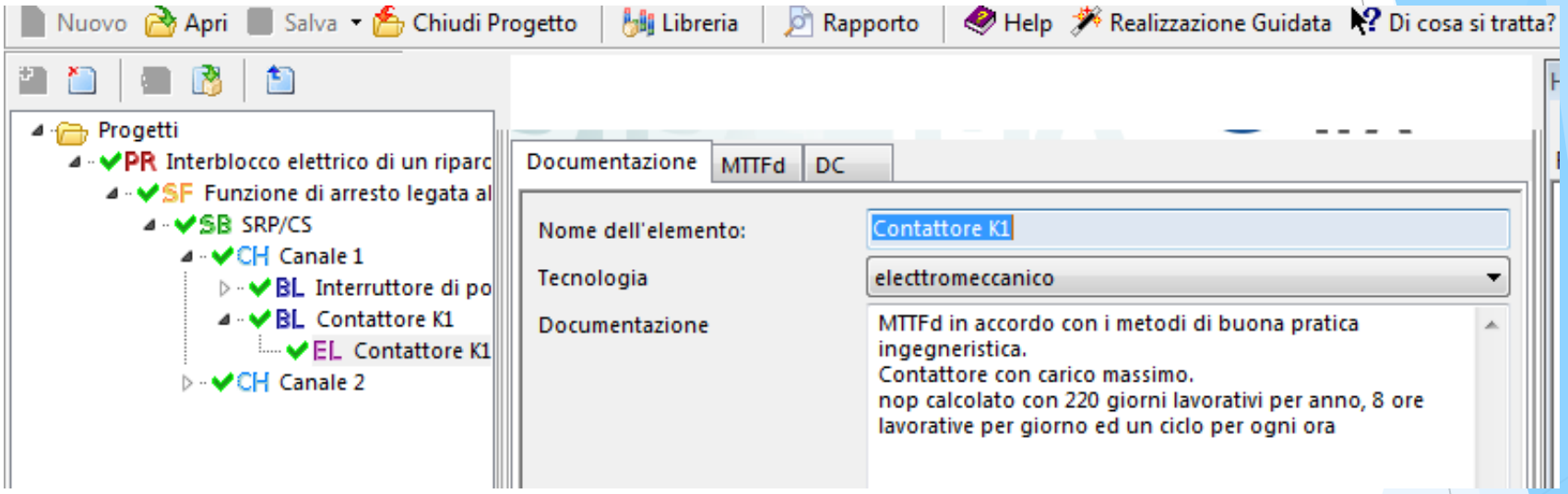


SW SISTEMA

ESEMPIO B (rif. EN ISO 13849-1, App. I)

CIRCUITO RIDONDANTE ELETTRICO/ELETTRONICO

Definizione dell'elemento



Grazie

per l’attenzione