White paper

ARCHITETTURA SICURA IN MODALITÀ DI SETUP

VALUTAZIONE DELLA SICUREZZA DI UN ENCODER ROTATIVO RIDONDANTE CON UTILIZZO DI UN PLC DI SICUREZZA

SCHMERSAL
THE DNA OF SAFETY

CONTENT

WHITE PAPER

ARCHITETTURA SICURA IN MODALITÀ DI SETUP

VALUTAZIONE DELLA SICUREZZA DI UN ENCODER ROTATIVO RIDONDANTE CON UTILIZZO DI UN PLC DI SICUREZZA BASATO SU UN ESEMPIO DI FUNZIONE DI SICUREZZA E SULLA SUA QUANTIFICAZIONE CON IL SOFTWARE "SISTEMA"

Per la modalità di setup o per la ricerca dei guasti nelle macchine, la funzione di sicurezza "Velocità limitata con riparo aperto" è estremamente rilevante. Il presente White Paper preparato da Schmersal e Wachendorff mostra un esempio di soluzione sicura che utilizza un encoder e un modulo di sicurezza e valuta le soluzioni in accordo con la EN ISO 13849.

Autori: Christian Lumpe, Product Manager for Controllers, Schmersal Group, e Steffen Negeli, Product Manager & Technical Sales, Wachendorff Automation GMBH & CO KG

SITUAZIONE INIZIALE

Consideriamo una tipica linea di produzione come la potremmo trovare nell'industria del packaging.

L'operatore è protetto da potenziali movimenti pericolosi per mezzo di adeguati ripari per cui l'ingresso nella zona di rischio è impedita tramite un accesso controllato. Dal punto di vista della sicurezza della macchina, il requisito minimo indispensabile è che l'operatore non sia in pericolo quando il riparo è aperto, l'azionamento cioè non dovrebbe essere in grado di muoversi. Si dovrebbe inoltre considerare in molti casi la possibilità di arrestare il sistema con un pulsante di emergenza.

Fig. 1: Linea di produzione nell'industria del packaging

Per semplificare il setup della linea di produzione o la ricerca dei guasti, una buona soluzione è quella di configurare il Sistema in maniera tale che il movimento pericoloso abbia una velocità ridotta anche con il riparo aperto.

Contemporaneamente a

- 'Una protezione contro gli avviamenti inattesi' e a
- Una funzione di sicurezza con 'Arresto tramite pulsante di emergenza', un'ulteriore protezione deve essere considerata, e cioè
- Una 'Velocità limitata sicura (SLS*) con riparo aperto'

*Safely Limited Speed – secondo la EN ISO 61800-5-2

LA SICUREZZA DEL MACCHINARIO – LA NORMA EN ISO 13849

Applicheremo la EN ISO 13849 alla nostra macchina per determinare e verificare il livello di sicurezza richiesto. Se comparata alla IEC 62061, questa norma ha il vantaggio di essere più semplice da utilizzare a condizione che la sua implementazione preveda alcune accortezze.
Una parte del concetto base della EN ISO 13849 sta nel fatto di poter dimostrare la capacità di eseguire una determinata funzione di sicurezza in condizioni predefinite. Questa capacità è espressa usando il Performance Level (PL), che corrisponde in sostanza ad una probabilità di guasto. La norma specifica 5 livelli di PL che sono indicati da “a” ad “e” in ordine ascendente di efficacia e di capacità di ridurre il rischio. In corrispondenza esiste la valutazione del rischio di una macchina che solitamente usa il grafico sottostante per illustrare un Performance Level target, il cosiddetto PLr (r = richiesto).

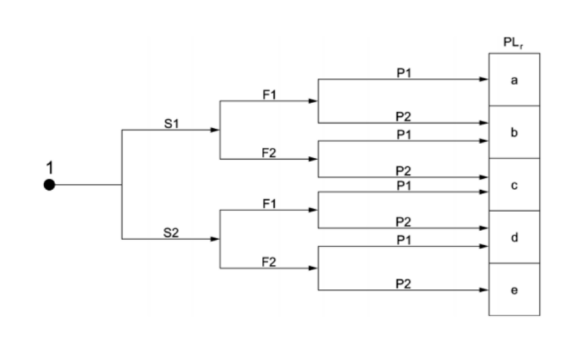

Fig. 2: Matrice di rischio © Beuth Verlag

La valutazione del rischio per la macchina presa ad esempio in questo White Paper ha prodotto un PLr pari a d. Questo PL può essere raggiunto in diversi modi. La norma dà una prima valutazione tramite lo schema seguente:I target, il cosiddetto PLr (r = richiesto).

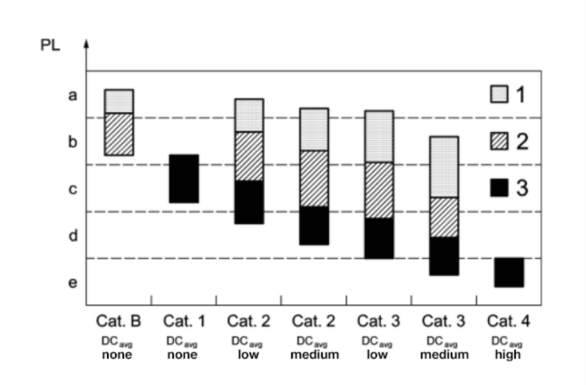

Fig. 3: Possibile combinazione tra categorie, MTTFD e DC
© Beuth Verlag

La Categoria 3 è generalmente adatta all’impiego poiché consente di fare a meno di un canale di test che invece sarebbe richiesto in Categoria 2. Tale test è spesso difficile da applicare, in particolare con componenti meccanici. La Categoria 3 richiede una sicurezza contro il singolo guasto che può essere soddisfatta con una configurazione a 2 canali.

COMPONENTI STANDARD NELLE FUNZIONI DI SICUREZZA

Si può usare un encoder rotativo per misurare la velocità. Il mercato offre molteplici dispositivi certificati per applicazioni di sicurezza. In funzione dell’applicazione, potrebbe valere la pena utilizzare componenti standard, questo sia per ragioni di costo, dato che il maggiore sforzo progettuale del costruttore è controbilanciato dal risparmio sul costo dei componenti, oppure perché i componenti standard offrono in ultima analisi una migliore soluzione nel caso specifico.

La validazione richiesta della soluzione per applicazioni di sicurezza è più facilmente soddisfatta con componenti già certificati, poiché i costruttori di tali componenti garantiscono la conformità con le norme di riferimento.

Rimane comunque responsabilità dell’utilizzatore assicurarne la corretta installazione tenendo in considerazione le prevedibili condizioni ambientali della macchina includendo temperatura e compatibilità elettromagnetica.

Se vengono usati component standard in una funzione di sicurezza, il progettista della macchina o l’integratore è responsabile della scelta. La trattazione che segue funge da linea guida, ma in ogni caso non esime dall’applicazione delle norme e delle direttive applicabili.

STRUTTURA DELLA FUNZIONE DI SICUREZZA

Quali componenti concorrono in una funzione di sicurezza? Oltre all'encoder rotativo, che è utilizzato per il controllo della velocità, senz'altro la logica, come per esempio il PLC di sicurezza PSC1 di Schmersal, il motore stesso, ma anche il monitoraggio del riparo che deve essere incluso nel dimensionamento, dato che è il componente che attiva la funzione SLS. Naturalmente altre soluzioni sono possibili, la procedura da seguire sarà tuttavia identica.

Nell'architettura sopra menzionata, le considerazioni sull'encoder rotativo sono di particolare rilevanza. Gli altri elementi sono di sicurezza per cui il PL complessivo è ottenuto semplicemente sommando i singoli valori.

L'approccio più semplice per ottenere il sistema a due canali richiesto sarebbe quello di usare due encoder separati da installare in posizioni diverse per costituire effettivamente i due canali anche meccanicamente. In pratica però questa soluzione è ovviamente dispendiosa e complicata. E' decisamente più pratico poter usare un unico componente. L'encoder rotativo di Wachendorff combina queste due proprietà. Include due encoder completamente indipendenti utilizzando tecnologie diverse, in un solo involucro. Questo consente una installazione molto semplice e, al contempo, la ridondanza interna soddisfa le specifiche della Categoria 3.

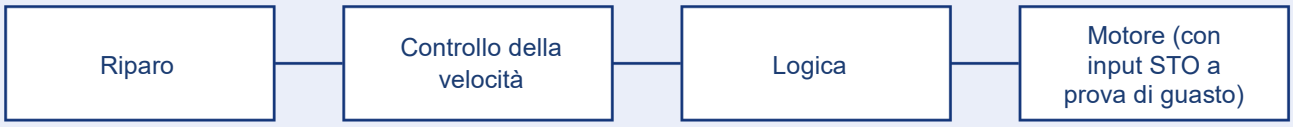

Fig. 4: Struttura della funzione di sicurezza

STRUTTURA DI UN ENCODER ROTATIVO RIDONDANTE

In linea di principio, un encoder rotativo ridondante comprende due encoder rotativi standard pienamente autonomi, il che significa che l'elettronica dell'encoder può essere considerata come un sistema a due canali. Solamente la struttura meccanica che comprende un albero e l'insieme dei cuscinetti è a canale singolo nella sua configurazione. La norma per i motori elettrici, EN 61800-5-2 prevede di considerare il guasto che si determina quando viene meno il collegamento meccanico tra l'encoder rotativo e il motore. In molti casi, l'esclusione del guasto è richiesta dato che il PLC non riesce necessariamente a rilevare tali eventualità. L'esclusione di tale evento può essere giustificata solo da un appropriato dimensionamento degli elementi di connessione e usando un collegamento meccanico affidabile al 100% (per esempio un giunto di bloccaggio tra l'albero e il sistema di azionamento con sistema a chiavetta o spina).

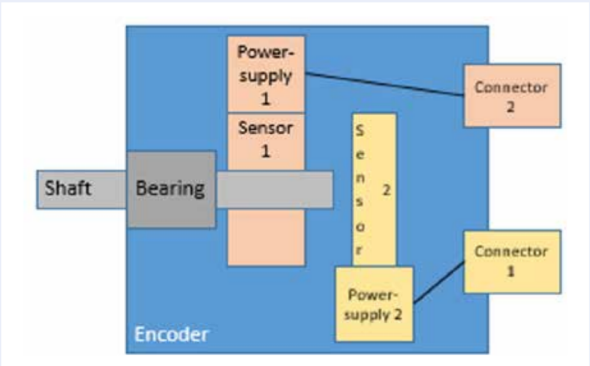

Fig. 5: Struttura di un encoder rotativo ridondante

TIPOLOGIE DI ENCODER ROTATIVI RIDONDANTI

Wachendorff offre tre modelli di encoder rotativi ridondanti, il WDGR (incrementale ottico/-incrementale magnetico), il WDGE (incrementale ottico/assoluto magnetico) e il WDGB (assoluto ottico/assoluto meccanico). Questo assicura la massima flessibilità nell'applicazione e nell'uso di componenti aggiuntivi poiché permette di scegliere tra un'ampia gamma di prodotti standard non certificati. Tutti e tre i modelli si basano sul principio della diversità, il che vuol dire che la resistenza al guasto aumenta usando principi di rilevamento differenti e impiegando il minor numero possibile di componenti di uguale tecnologia. La filosofia di fondo, che sta alla base di questa procedura, è che differenti tipologie di sensori rispondono con gradi diversi di sensibilità, o insensibilità, a malfunzionamenti di vario genere e di conseguenza non cessano di funzionare regolarmente in maniera concomitante, permettendo così al sistema elettronico di rilevare in maniera affidabile il guasto potenziale. Nel configurare questo approccio, Wachendorff ha usato la propria gamma di sensori ad alta affidabilità sviluppati nel corso degli anni. L'encoder rotativo standard ridondante fornisce segnali differenziati (magnetici e ottici) che sono generati indipendentemente l'uno dall'altro ma che, nonostante ciò, possono essere correlati tra di loro.
Anche l'alimentazione elettrica è separata per ciascun sensore. Questo è vero sia per gli encoder rotativi incrementali ottici e magnetici sia per quelli magnetici assoluti.

Fig. 5a: Encoder incrementale rotativo ridondante WDGR di Wachendorff

SOTTOSISTEMA DI "RILEVAMENTO DELLA VELOCITA'"

Il nocciolo della EN ISO 13849 è il calcolo della probabilità di guasto dell'architettura di controllo del sistema. L'approccio puramente matematico, cioè basato esclusivamente sui valori del MTTFD non è sufficiente di per sé stesso. Piuttosto devono essere considerate le influenze ambientali e sistemiche, come per esempio se i componenti sono stati progettati per le condizioni di lavoro previste.
Come mostrato in Fig. 3, un PLr=d richiede componenti con elevati valori di MTTFD (tempo medio tra guasti pericolosi), superiori a 30 anni come minimo, e/o un alto valore (> di 90%) di copertura diagnostica (DC). Considerando solo il sottosistema encoder e logica, abbiamo il seguente schema a blocchi:

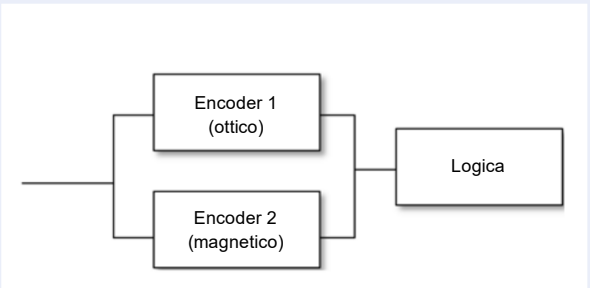

Fig. 6: Schema a blocchi della struttura dell'encoder rotativo e della logica di controllo

Come spiegato, la Categoria 3 necessita di un rilevamento del singolo guasto che è dato dalla capacità in doppio canale di rilevare in maniera continua la velocità/direzione nell'encoder rotativo. La diagnostica (DC) che viene richiesta non è integrata nell'encoder ma deve essere effettuata dalla logica.

Il PLC di sicurezza PSC1 di Schmersal ne è un ottimo esempio. Se richiesto dall'applicazione, possono essere monitorati fino a 12 assi tramite gli encoder rotativi facilmente connessi tramite interfacce D-sub. Incrociando i segnali dei due encoder o, nel caso di encoder seno-coseno, valutando la funzione $sen^2+cos^2=1$, eventuali errori possono essere rilevati ed è possibile reagire con una risposta adeguata agli errori stessi.

Fig. 7a:
PLC di Sicurezza PSC1

Inoltre il software di programmazione SafePLC2 per il PSC1 integra i blocchi funzionali per le principali funzioni di sorveglianza come ad esempio SLS, SOS o SCA, in accordo con la EN 61800-5-2.

Questi possono essere facilmente integrati nel programma come illustrato dall'immagine seguente che mostra la logica di programmazione per il nostro esempio di funzione di sicurezza.

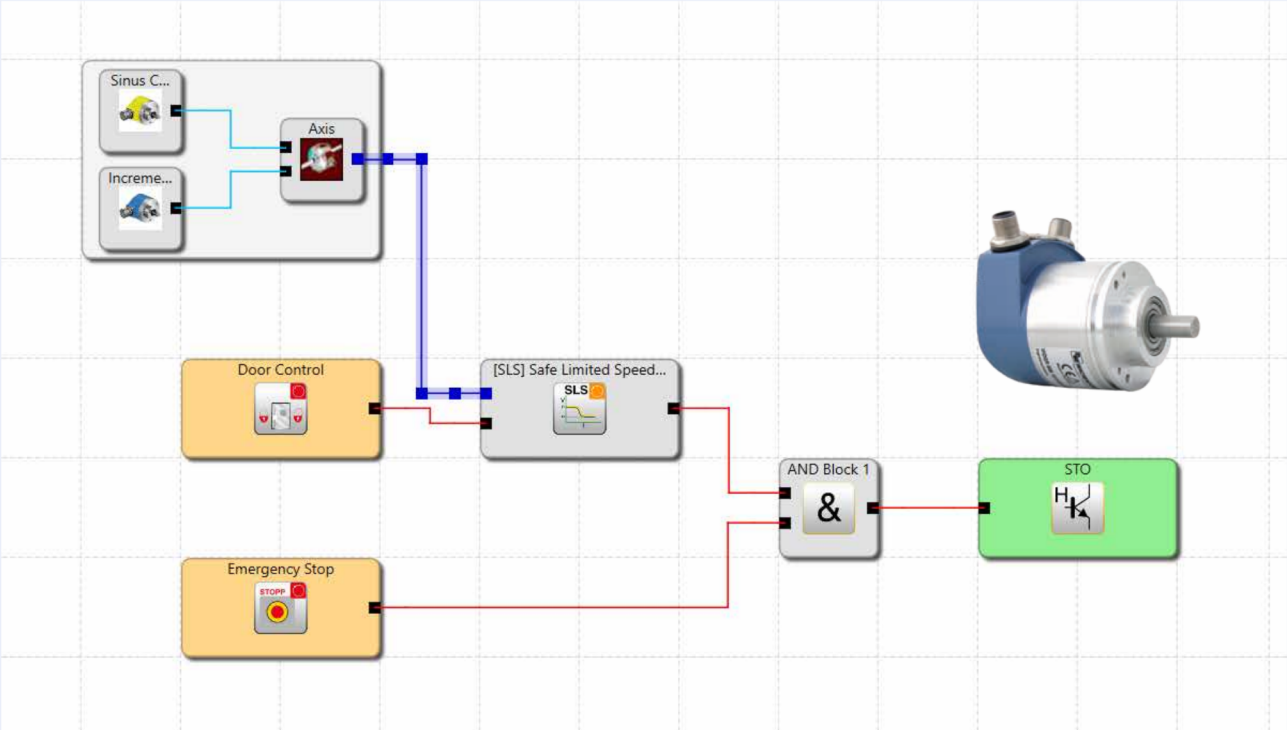

Fig. 7b: Programmazione in SafePLC2

Grazie alla programmazione intuitiva, la probabilità di errori è minima e la tracciabilità del programma in termini di validazione o nel caso di estensioni della macchina è decisamente semplificata.

La necessaria parametrizzazione del percorso dell'encoder, come per esempio la risoluzione, può essere effettuata in maniera semplice all'interno delle finestre di dialogo.

ESCLUSIONE DEL GUASTO NEL COLLEGAMENTO MECCANICO TRA ALBERO ED ENCODER

Una particolare attenzione deve essere posta al collegamento meccanico tra albero e motore che è progettato di fatto come un sistema a canale singolo. Quest'ultimo necessita di una esclusione del guasto per quanto riguarda il collegamento dato che anche un singolo guasto può risultare pericoloso.

La norma permette l'esclusione di questo tipo di guasto sempre che sia documentato e circostanziato (EN ISO 13849-1, sez. 7.3). In termini di guasto meccanico, la motivazione è abitualmente fondata su un sovradimensionamento adeguato dell'organo. Ma cosa si intende per "adeguato" in questo caso? Un'occhiata alla

EN 61800-5-2 offre alcuni approfondimenti dati dalla tab. D.8, che fornisce informazioni sulla giustificazione dell'esclusione del guastoOltre alla verifica della portata massima dei cuscinetti del collegamento (matematica o tramite test), la norma richiede anche un'analisi FMEA sul caso specifico.

- FMEA (Failure Mode and Effects Analysis)
  L'FMEA considera la valutazione degli effetti e della probabilità di accadimento di diverse modalità di guasto e definisce come contrastarle, cioè le misure da prendere o le limitazioni da imporre.

Un esempio di FMEA è mostrato qui di seguito:

FMEA Subject: Redundant-diverse encoder on small safety controller PSC1

26.02.2021

CHLU, DABR, ULBE, STNE, HAPO

SCHMERSAL THE DNA OF SAFETY

No.	Component / Process	Function / Feature	Possible Error	B	Possible Error	Current / planned measures for error detection	E	Possible causes of errors	Current / planned measures for error prevention	A	RZ	Note
1	Connection Encoder-Shaft	Flange	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection is overloaded by excessive torque and thus loosens	none	10	1000	
				10		**Fault exclusion**	10		Oversizing for the application. Used values are given in BA. Proof of loadability via calculation	7	700	Current solution with grub screw/cam flattening probably not suitable. Alternative connections are being examined
				10		Target/actual comparison	5			7	350	
	Connection Encoder-Shaft	Clutch	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed f	none	10	Connection is overloaded by external thrust	none	10	1000	
				10		**Fault exclusion**	10		Oversizing for the application, note in BA. Recommendation if necessary	1	100	
				10		Target/actual comparison	5			1	50	
	Mounting encoder-machine	Bolting	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection loosens	none	10	1000	
				10		**Fault exclusion**	10		Correct dimensioning of the screws. Visual inspection, QEP	1	100	
				10		Target/actual comparison	5			1	50	
	Connection Encoder-Shaft	Grub screw	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Connection loosens	none	10	1000	
	Encoder	Detection of movement	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed on one channel	none	10	Damage due to e.g. vibration, shock, e.g. loosening of the pulse disc or the magnet	none	10	1000	
				10		Error detection in safety controller	1		Diverse encoder technologies	1	10	
	Encoder	Wiring	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Short circuits due to mechanical damage to the cables	none	10	1000	
				10		Error detection in safety controller	1		Separate cable routing	5	50	
	Encoder	Power-supply	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Power supply fails or overvoltage	none	10	1000	
				10		Error detection in safety controller plus supervision of power supply	1		Separate power supplies Prescribe PELV power supplies in manual	5	50	
	Encoder	Generating SSI-Signal	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	Error in FW	none	10	1000	
				10		Error detection in safety controller	1		Diversity of encoder technologies at SSI/incremental. With SSI different FW and HW realisation	2	20	
	Encoder	General	Speed too low or wrong position. For example, standstill could be detected -> safety door could be unlocked.	10	Encoder delivers wrong position/speed	none	10	EMC	none	10	1000	
				10		Error detection in safety controller	1		Reference to compliance with environmental conditions in manual. Diverse structure	2	20	

Fig. 8: Esempio di FMEA

Ciononostante, è responsabilità del progettista, come del resto lo è anche nel caso si utilizzino encoder certificati, assicurarsi che le condizioni ambientali non eccedano i valori ammissibili.

Cos'altro deve essere considerato?

I paragrafi seguenti esplicitano gli aspetti ulteriori di cui bisogna tenere conto in accordo con la EN ISO 13849 per accertarsi che la Categoria 3 sia soddisfatta.

■ Principi fondamentali e di provata sicurezza

Questi devono essere rispettati sia per le prestazioni meccaniche che elettriche. Ciò include l'uso di materiali resistenti agli stress ambientali come l'umidità e le sollecitazioni elettromagnetiche (EMC) o il sovradimensionamento degli organi meccanici.

■ CCF (Common Cause Failure)

Oltre al calcolo della probabilità di guasto, debbono essere implementate delle misure preventive che evitino guasti da cause comuni. Questo per assicurare che un guasto singolo non possa determinare un problema contemporaneamente su entrambi i canali, il che creerebbe una situazione di pericolo.

Le misure che si possono adottare contro un CCF sono valutate tramite un punteggio nella EN ISO 13849. La Categoria 3 richiede un minimo di 65 punti per dimostrare una sufficiente tutela contro i guasti aventi una causa comune.

I criteri seguenti sono soddisfatti nel Sistema con encoder considerato:

		Note
Separazione	15	Separazione fisica tra segnali tramite: - Architettura elettrica separata - Alimentazione separata - Cablaggio separato - Distanze adeguate a prevenire strisciamenti e interferenze
Diversità	20	Differenti tecnologie e/o principi fisici
Competenza	5	Formazione ai progettisti sulla comprensione delle cause di guasto e delle loro conseguenze
Ambiente (meccanico -> ambiente)	10	Valutazione delle condizioni ambientali
Design/applicazione/esperienza	15	Protezione contro sovraccarichi, sovrapressioni, sovracorrenti, sovratemperature, etc.
	65	

■ Guasti sistematici

L'encoder rotativo usa differenti principi fisici (magnetico, ottico) per i due canali così come alimentazioni indipendenti e mutualmente isolate. Guasti sistematici nel software del PLC di Sicurezza devono essere contemplati nella scrittura del software secondo le indicazioni della norma (SRASW).

■ $MTTF_D$

Il periodo di tempo per giungere a un guasto pericoloso è definito per entrambi i sensori ed è significativamente superiore ai 100 anni anche se la norma prevede un tetto massimo di 100 anni. Quindi il valore per il sottosistema encoder, anche dopo la simmetrizzazione dei canali si attesta su un MTTFD di 100 anni.

■ DC

L'encoder in sé non ha un sistema di rilevamento del guasto di alcun tipo nei sotto-canali individuali né ha una logica integrata di livello elevato. IL PLC di sicurezza identifica i guasti per mezzo di un costante controllo incrociato delle informazioni riguardanti velocità e direzione rilasciate dall'encoder.

Se i due valori deviano l'uno dall'altro, una procedura di sicurezza viene inizializzata. La funzione "Safe speed" è un segnale dinamico. Le due alimentazioni vengono anch'esse monitorate. Il tasso di rilevamento del guasto è del 99%.

Come sopra indicato, viene esclusa la rottura dell'albero. Nonostante ciò il rilevamento del guasto può essere condotto tramite il PLC di sicurezza assumendo che nel caso di guasto dell'albero, la velocità misurata sia inferiore a quella prevista.

Se viene usato un bus di campo di più alto livello, i valori di velocità possono essere letti dal PLC e poi direttamente comparati con i valori del sistema di controllo del motore. Se tale opzione non fosse disponibile, un ulteriore segnale "motore in rotazione" proveniente dal PLC, potrebbe essere utilizzato per effettuare un controllo di plausibilità dal PLC di sicurezza.

Questa modalità di rilevamento del guasto non ha conseguenze sulle specifiche della Categoria 3 per il rilevamento del guasto singolo, ma se l'implementazione fosse possibile, questa misura aggiuntiva dovrebbe essere applicata.

CALCOLO DEL PL

Se consideriamo di nuovo l'intera struttura otteniamo il calcolo seguente nelle seguenti ipotesi:

Controllo del riparo: Un sensore di sicurezza di tipo 4 è utilizzato come richiesto dalla EN ISO 14119.
Il valore PFHD è dichiarato dal costruttore in 5.2E-10/h.

PES: Il PLC di Sicurezza è certificato PLe. Il valore PFHD è 1.38E-8.

STO: La probabilità di guasto della funzione STO è dichiarata dal costruttore dell'inverter in 3.2E-7 e corrisponde a un PL= d.

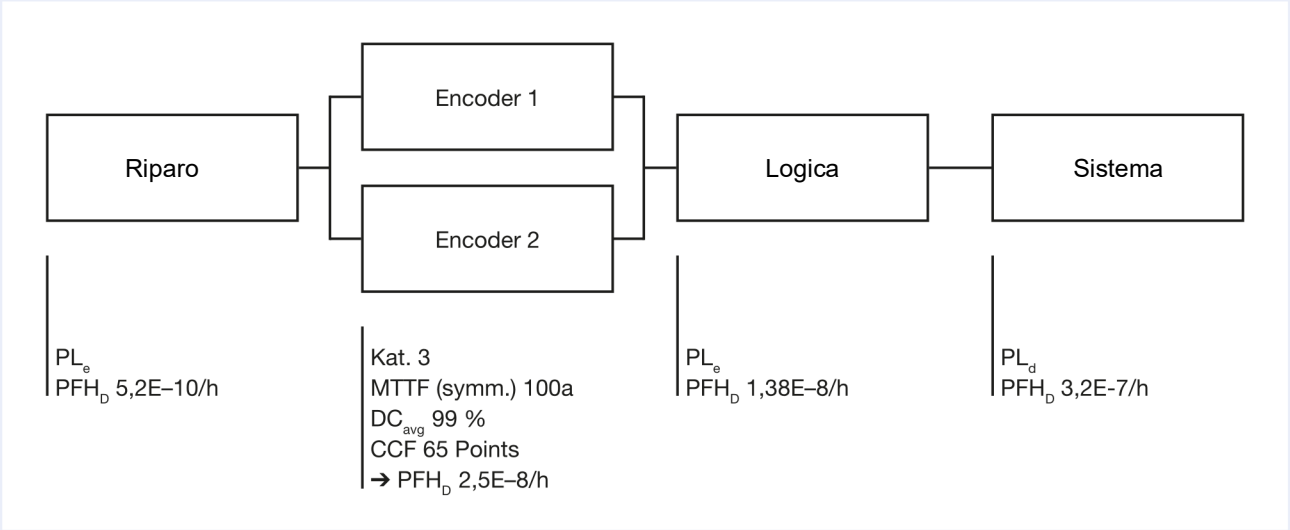

Fig. 9: Diagramma a blocchi generale

CONCLUSIONE

La struttura delineata permette il raggiungimento di un Performance Level pari a d. Il PL potenziale nel nostro esempio è largamente inficiato dal PL dell'inverter. Un alto livello di sicurezza può essere raggiunto nonostante l'uso parziale di componenti standard. Inoltre, l'uso di un encoder ridondante semplifica l'installazione.

La combinazione con il PSC1 facilita le funzioni di sicurezza aggiuntive come, per esempio, il pulsante di emergenza o il monitoraggio di altri circuiti di sicurezza nello stesso dispositivo.

Authors:
Christian Lumpe
Product Manager for Controllers
Schmersal Group

Steffen Negeli
Product Manager & Technical Sales
Wachendorff Automation GMBH & CO KG

About the Schmersal Group:
The Schmersal Group is an international market leader in the challenging field of machine safety. With the world's most comprehensive range of safety switchgear products, the Schmersal Group develops safety systems and solutions for special requirements in a variety of user industries. Schmersal's tec.nicum business division offers a comprehensive service portfolio to complement the range of solutions offered by Schmersal.

Founded in 1945, the company is represented by seven manufacturing sites on three continents with its own companies and sales partners in more than 60 countries.

Contact:
K.A. Schmersal GmbH & Co. KG
Phone: +49 202 6474-0
info@schmersal.com
Möddinghofe 30
42279 Wuppertal
Germany

www.schmersal.com
www.tecnicum.com