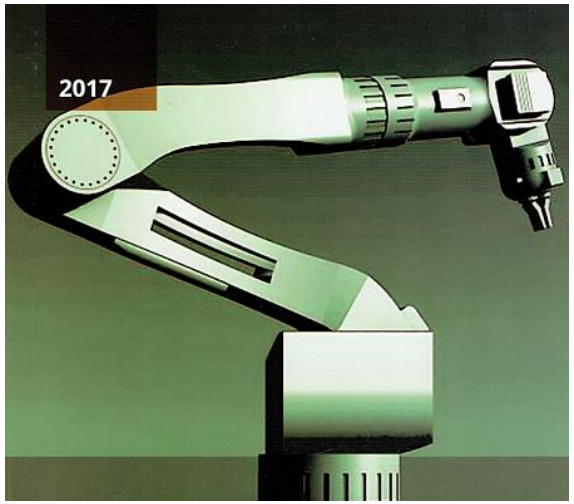
Milano, 12 Dicembre 2017

Fabio Pera

"L'evoluzione normativa dei sistemi di comando"

Seminario: "Il 9° rapporto INAIL sulla Sorveglianza del Mercato per la Direttiva Macchine"



Dipartimento innovazioni tecnologiche e sicurezza degli impianti prodotti e insediamenti antropici

Revisione della norma EN ISO 13849-1
Attuale stato: WD-2
Obiettivi:

- Incorporazione della parte normativa della EN ISO 13849-2 (Validazione) all'interno della ISO 13849-1
- - Si sta prendendo in considerazione il riesame della definizione di componenti Well Tried (ben provati) e dei Principi di Sicurezza Well Tried
- Miglioramento della struttura della EN ISO 13849-1 per renderla più comprensibile
- Revisione della parte software (notevoli cambiamenti)
- Revisione della metodologia per la determinazione del PL_r (Annesso A)
- Revisione dei criteri semplificati per determinare il DC (All. E) ed il CCF (All. F)
- Revisione della lista delle Safety Functions
- Introduzione delle formule per il calcolo del PFHD (al momento sarebbero accettate solo in allegato)
- Miglioramento degli aspetti non quantificabili (CCF, guasti sistematici….)

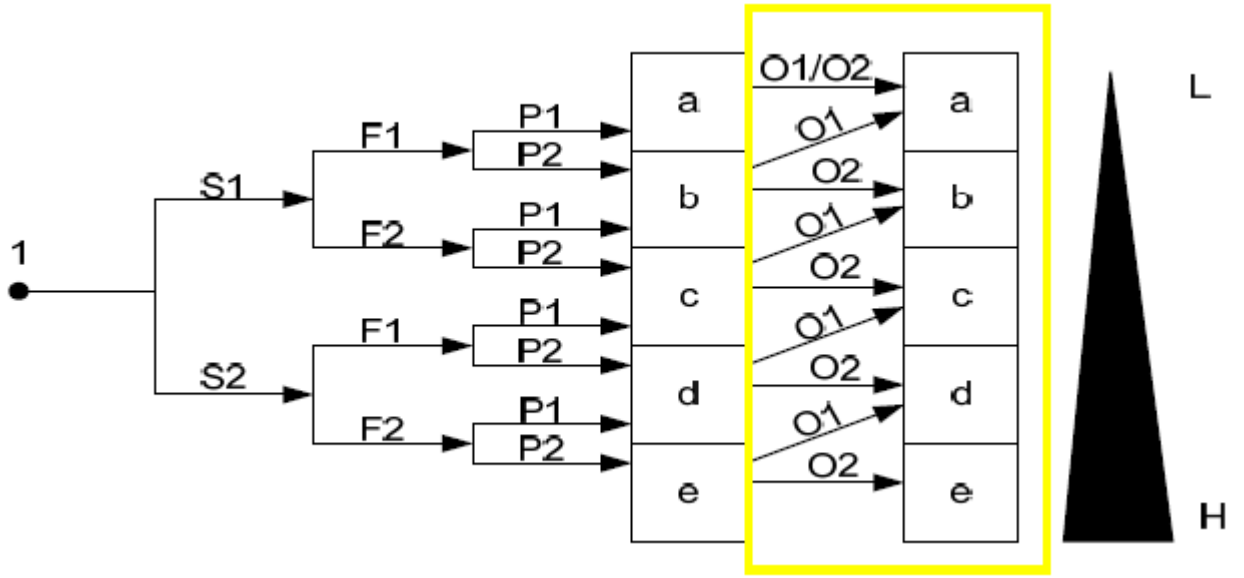
Revisione della norma EN ISO 13849-1

Criticità:

- Impiego di componenti (ad es.: PLC, inverter, sensori…) per i quali non sono rispettati i requisiti richiesti per il software incorporato (Safety Related Embedded Software: SRESW) e per i quali è consentito l'uso solo se:
  - la SRP/CS ha un Pl_r ="a" o un Pl_r ="b" con struttura in Categoria B, 2 o 3
  - la SRP/CS ha un Pl_r ="c" o un Pl_r ="d" e può usare più componenti per i due canali nelle categorie 2 o 3 . I componenti dei due canali devono usare diverse tecnologie.
- Compatibilità elettromagnetica dei prodotti per applicazioni di sicurezza: riferimento alle norme per immunità aumentata (Increased Immunity) quando non esiste una norma di prodotto
- Software
- Metodo semplificato per la valutazione del PL_r (All. A)

Revisione della norma EN ISO 13849-1

Modifica dell'albero per la scelta del PL_r: introduzione del parametro O per la probabilità che si verifichi l'evento pericoloso



Basso contributo alla riduzione del rischio

Alto contributo alla riduzione del rischio

- S:severità del danno
- F: frequenza e o durata dell'esposizione al pericolo
- P: possibilità di evitare il pericolo o limitare il danno
- O: probabilità che si presenti l'evento pericoloso

Revisione della norma EN ISO 13849-1

Metodo semplificato per la valutazione del PL_r: parametri P1 e P2 per la possibilità di evitare l'evento pericoloso e parametri O1 ed O2 per la probabilità che si presenti l'evento pericoloso

- E' stato realizzato un sistema semi-quantitativo per decidere fra P1 e P2 e fra O1 ed O2, mediante tabelle a punteggio, contenenti aspetti che, in funzione di quanto sono importanti, influenzano la scelta di uno o dell'altro valore.
- Per P1 e P2 sono stati presi in considerazione:

  - la qualifica dell'operatore (1), la velocità con cui si presenta il pericolo (2), lo spazio per sfuggire al pericolo (3), la possibilità di riconoscere il pericolo (4), la complessità del lavoro (5)

- Per O1 e O2 sono stati presi in considerazione:

  - il carico di lavoro paragonato ai limiti della macchina(1), la frequenza di impiego paragonata ai limiti della macchina (2), il monitoraggio dei guasti nel processo(3), l'accuratezza della manutenzione (4)

Revisione della norma EN ISO 13849-1
Software: i livelli SW

La norma considera 3 differenti livelli di software:

- SW level A: caratterizzato dall'impiego di hardware pre-valutato con software interno idoneo per applicazioni di sicurezza (moduli software con ingressi ed uscite limitati a valori predefiniti). E' di ridotta complessità, si può applicare il V-model semplificato e può raggiungere PL e. Per i moduli software si usa in genere LVL.
- SW level B: caratterizzato dall'impiego di hardware con software interno per applicazioni non necessariamente di sicurezza in LVL. E' di maggiore complessità perché utilizza sistemi hardware e software non pre-valutati per applicazioni di sicurezza, si applica il V-model dettagliato e può raggiungere PL d. Sono possibili diverse soluzioni progettuali dette «routes» che dipendono dai criteri applicati (es. categoria, diversità, IEC 61508, ISO 13849-1) e che determinano il PL.
- SW level C: caratterizzato dall'uso di un linguaggio diverso dall'LVL ed è tipicamente utilizzato in software embedded. E' anch'esso di maggiore complessità per gli stessi motivi del SW level B, si applica il V model dettagliato e può raggiungere PL e, in funzione della «route» scelta.

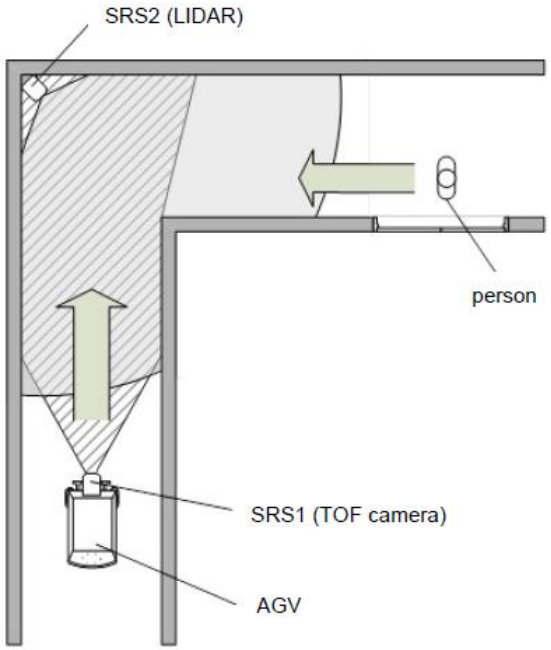
Revisione della norma EN ISO 13849-1
Software: caratteristiche di un livello SW

La norma considera per ogni livello SW:

- Il modello del ciclo di vita (V-model) applicabile
- Il progetto del software
- Il progetto del modulo
- Il codice (regole)
- Il test del modulo
- Il test di integrazione del software
- Il test del software
- La documentazione
- La configurazione e la modifica

La norma IEC 62998-721 (Attuale stato: CD)

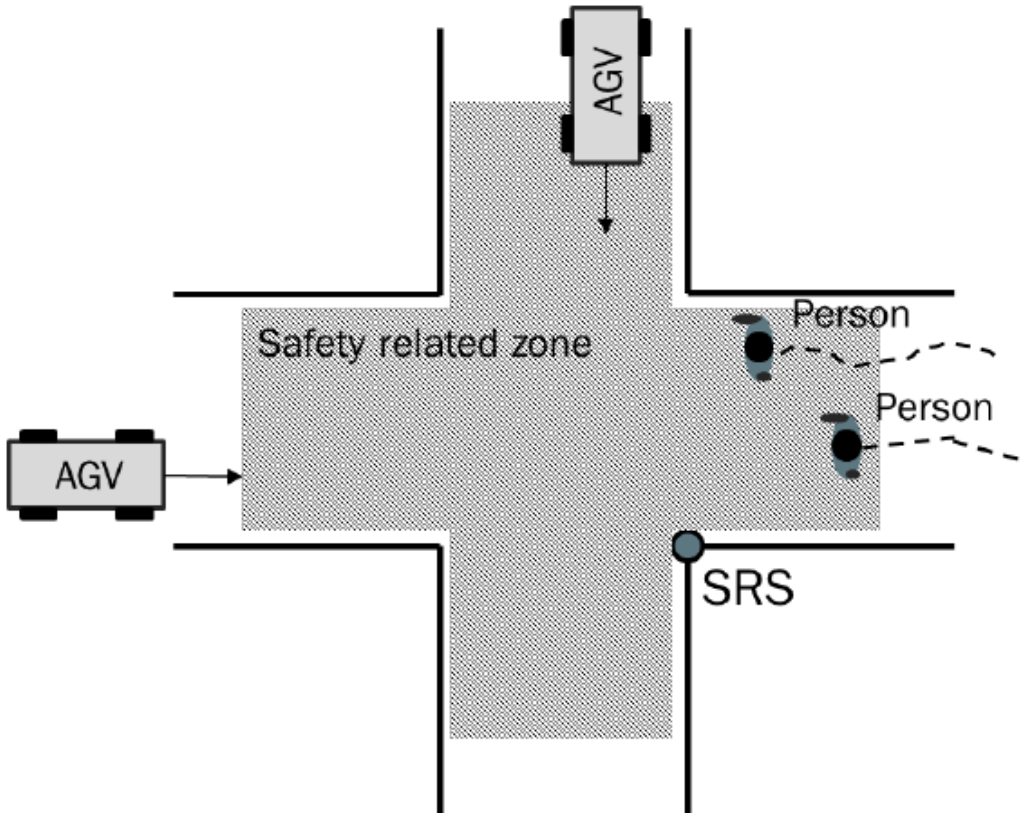
”Sicurezza delle macchine – Dispositivi di protezione elettrosensibili - Sensori relativi alla sicurezza utilizzati per la protezione delle persone ”



- Si tratta di sensori di sicurezza applicati a macchine che presentano un rischio di danno per le persone: sono in grado di riportare la macchina in una condizione sicura prima che la persona possa essere posta in pericolo
- Sono sensori di nuova tecnologia come Radar, ultrasuoni, Lidar……
- Hanno un nuovo tipo di funzione di rilevamento : classificazione di oggetti, posizione di oggetti….
- Possono essere combinati in un sistema di sensori
- Sono richiesti per AGV, Service Robotics e Sistemi di interazione Uomo – Macchina
- La norma IEC 62998-721 riempie il vuoto lasciato dalle norme sulla sicurezza funzionale IEC 61508 (Generica), IEC 62061 ed ISO 13849 fra la progettazione di questi prodotti e la loro applicazione

La norma IEC 62998-721

Sensori e sistemi di sensori relativi alla sicurezza

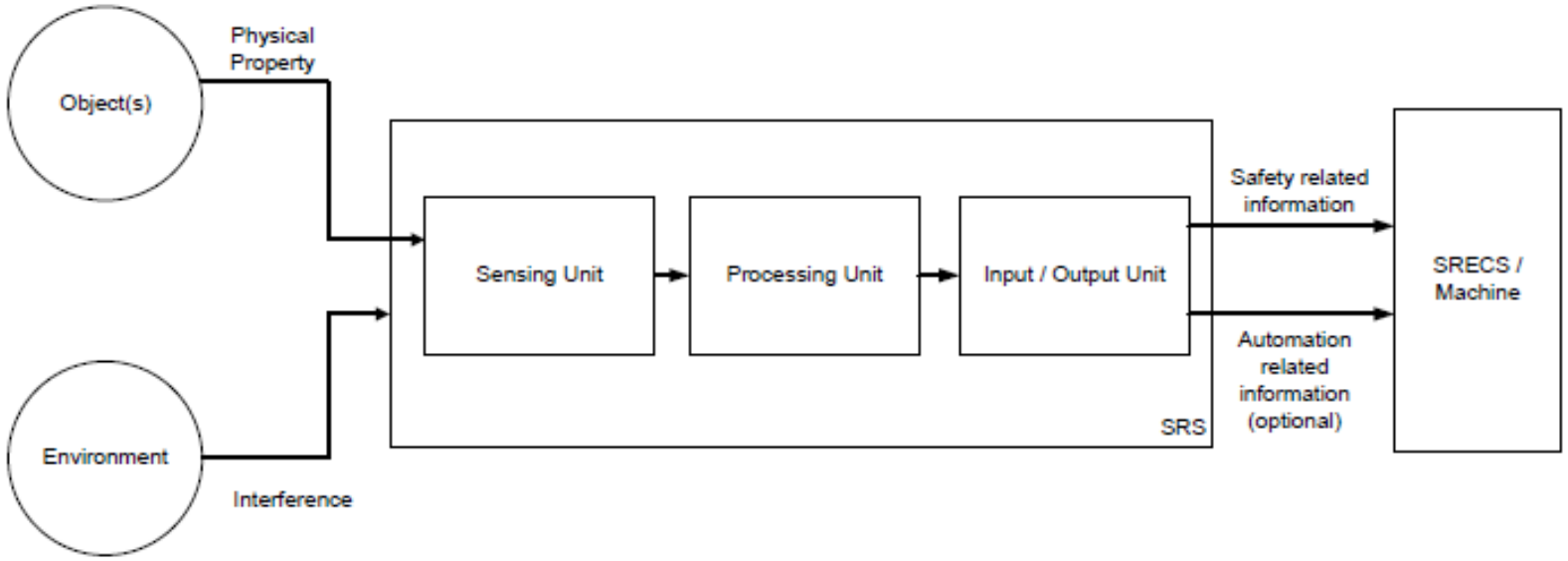


- Ciclo di vita SRS/SRSS
- Fase di progettazione e sviluppo
- Fase di integrazione e installazione
- Fasi di operatività, manutenzione e modifica
- Verifica e validazione

La norma IEC 62998-721

UN SRS consiste al minimo di:

- un sensore;
- Un'unità di processamento;
- un'unità di output.



La norma IEC 62998-721

Classi di Performance

E’ definita una corrispondenza fra le Classi di Performance della IEC 62998-721 ed i livelli di SIL delle IEC 61508 ed IEC 62061 e di PL della ISO 13849

Table 1 – Correspondence between level of safety performance and minimum required SRS/SRSS performance class

	SRS/SRSS performance class A	SRS/SRSS performance class B	SRS/SRSS performance class C	SRS/SRSS performance class D	SRS/SRSS performance class E	SRS/SRSS performance class F
ISO 13849	PL_a	PL_b	PL_c	PL_d	PL_e	
IEC 62061			SIL_{cl} 1	SIL_{cl} 2	SIL_{cl} 3	
IEC 61508			SIL 1	SIL 2	SIL 3	SIL 4

La norma IEC 62998-721

Il costruttore di un SRS/SRSS dovrà effettuare:

- Un’analisi del rischio
- Progetto e sviluppo
- Integrazione ed installazione
- Operatività, manutenzione e modifica
- Verifica e validazione

Grazie per l’attenzione