Studio Valeri Vanni
Consulenze aziendali per la sicurezza delle macchine e degli impianti
Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

"SICUREZZA FUNZIONALE" SECONDO LE NORME: EN ISO 13849-1 ed EN IEC 62061

LA EN 954-1 VA IN PENSIONE

A fine 2011, **esattamente a partire dal 31.12.2011** (da di entrata in vigore della nuova direttiva macchine 2006/42/CE), la norma EN 954-1 concernente l'affidabilità delle funzioni di controllo legate alla sicurezza delle macchine sarà ritirata e sostituita dalla EN ISO 13849-1.

La nuova norma introduce il concetto di Performance Level (PL) quale **indicatore del livello di affidabilità di una funzione di sicurezza**.

Il PL necessario per una determinata funzione di sicurezza deve essere determinato in base alla valutazione del rischio e ottenuto mediante la scelta di un'architettura adeguata, l'impiego di componenti idonei, l'eventuale adozione di ridondanze e di sufficiente copertura diagnostica.

Il PL della funzione di sicurezza complessiva è espresso in termini di **probabilità media di guasto pericoloso/ora** e deve essere calcolato in base al tasso di guasto dei componenti assemblati ed alla configurazione utilizzata per la realizzazione della funzione di sicurezza. Nel corso della conversazione verranno illustrati i contenuti della norma EN ISO 13849-1 e saranno presentati alcuni esempi di calcolo del Performance Level

SICUREZZA DEI SISTEMI DI COMANDO E CONTROLLO DI MACCHINE PROGETTARE I SISTEMI DI COMANDO CORRELATI ALLA SICUREZZA IN CONFORMITÀ CON LA NUOVA NORMA EN ISO 13849-1

SITUAZIONE NORMATIVA

La EN ISO 13849-1 "Sicurezza del macchinario — Parti dei sistemi di comando legate alla sicurezza — Parte 1: Principi generali per la progettazione", che segue la EN 954-1, è la norma centrale per la progettazione dei sistemi di sicurezza nell'ambito della "Sicurezza delle macchine".
La EN ISO 13849-1 (ora nella versione 2008) è stata approvata nel 2006 come versione europea.
La EN ISO 13849-1 è inoltre pubblicata nella Gazzetta Ufficiale della UE come norma armonizzata nell'ambito della Direttiva Macchine.
Per questa norma vale il principio di presunzione di conformità. La EN 954-1 formalmente non è più in vigore, ma può essere utilizzata ancora fino alla fine di dicembre 2011.

QUALI SONO STATE LE RAGIONI PRINCIPALI PER LA REVISIONE DELLA EN 954-1?

La norma (ancora) attuale EN 954-1, che dal 1996 descrive i circuiti elettrici di sicurezza nell'ambito della sicurezza delle macchine, non include requisiti sufficienti relativi ai sistemi elettronici programmabili. Un altro punto critico è che la relazione tra entità del rischio e categoria non appariva sempre plausibile. Da qui la decisione di includere riflessioni probabilistiche insieme alle considerazioni sulla sicurezza.

Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

QUALI SONO LE NOVITÀ?

Una tra le principali novità della norma EN ISO 13849-1 è l'approccio probabilistico per la valutazione dei sistemi di comando correlati alla sicurezza. La revisione della norma EN 954-1 è stata finalizzata all'inserimento di metodi probabilistici nella valutazione dei moderni sistemi di comando. Il passo decisivo in questa direzione è stato preso per poter continuare ad utilizzare le categorie ed allo stesso tempo per poter valutare quantitativamente le funzioni rilevanti ai fini della sicurezza.
Un ruolo importante nelle categorie è l'utilizzo del cosiddetto Performance Level (PL), descritto dalle seguenti grandezze:

- categoria (requisito strutturale),
- tempo medio ad un evento pericoloso (MTTFd)
- grado di copertura diagnostica (DC) e
- guasti per cause comuni (CCF).

Il PL è il livello di affidabilità per realizzare la riduzione richiesta di rischio per ogni funzione di sicurezza, ovvero la capacità di un sistema di comando e controllo di svolgere una funzione di sicurezza sotto determinate condizioni, al fine di ottenere la prevista riduzione dei rischi.

OBIETTIVO RAGGIUNTO IN 6 MOSSE

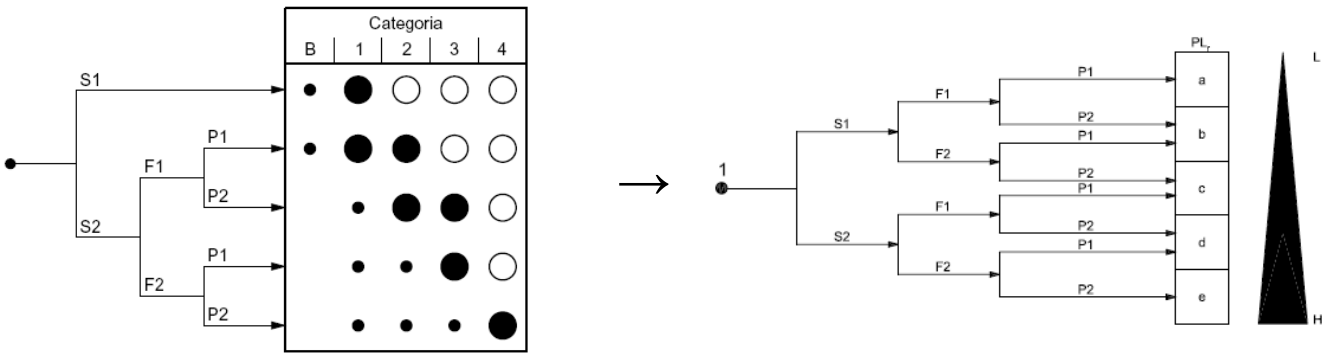
L'introduzione della EN ISO 13849-1 ha comportato nuovi requisiti procedurali anche nella costruzione delle macchine. La realizzazione di parti di sicurezza dei sistemi è un processo iterativo che si compie in diverse fasi.

Fase 1 - definizione dei requisiti delle funzioni di sicurezza

E' necessario stabilire le caratteristiche necessarie per ogni funzione di sicurezza. Questa è la fase più importante e al contempo la più difficile. Ad esempio, per garantire la sicurezza di un riparo mobile di una macchina è necessario interrompere i movimenti pericolosi all'apertura del riparo stesso; non è possibile consentire un riavvio con il riparo mobile aperto.

Fase 2 – determinare il necessario Performance Levels PL

Tanto maggiore è il rischio, tanto più elevato è il requisito del sistema di controllo.
Il contributo all'affidabilità e alla struttura può variare a seconda della tecnologia utilizzata.
Il livello per ogni situazione pericolosa viene suddiviso in cinque livelli, dalla "a" alla "e".
Con PL "a" il contributo della funzione di controllo alla riduzione del rischio è basso, con PL "e" è elevato.
A seconda dei grafici del rischio viene determinato il Performance Level richiesto (PLr) per le funzioni di sicurezza sopra descritte.



Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

Gravità della lesione (S)
S1 = lesione leggera (normalmente reversibile)
S2 = lesione grave (normalmente irreversibile), anche mortale

Frequenza e/o durata dell'esposizione al rischio (F)
F1 = da rara a frequente e/o di breve durata
F2 = da frequente a costante e/o di lunga durata

Possibilità di evitare il pericolo (P)
P1 = possibile in determinate condizioni
P2 = praticamente impossibile

Fase 3 - progettazione e realizzazione tecnica delle funzioni di sicurezza

La funzione di sicurezza "Blocco del riparo mobile" descritta nella fase 1 viene realizzata a livello tecnico. Per il blocco del riparo mobile è necessario utilizzare finecorsa di sicurezza codificato.
E' così possibile commutare più ripari mobili in serie, senza che le funzioni di controllo perdano efficacia.
A questo scopo il Codifica offre un elevato livello di protezione contro la manipolazione.
La relativa verifica dei sensori avviene tramite un sistema di sicurezza multifunzionale. L'arresto del motore avviene tramite due relè con contatti a guida forzata.

Fase 4 - determinazione del Performance Level e valutazione quantitativa

Per determinare il Performance Level ottenuto, la funzione di sicurezza viene analizzata nelle sue singole parti: sensore (=rilevatore dell'informazione), logica (=elaborazione) e attuatore (=apparecchio di manovra).
Ogni parte di questo sistema apporta un proprio contributo alla funzione di sicurezza.
L'applicazione dei PL comporta però la necessità di calcolare e validare i parametri che li compongono: categoria del circuito, affidabilità (MTTF), copertura diagnostica (DC) e cause comuni di guasto (CCF).

Fase 5 - Verifica

Questa fase spiega la domanda a che livello il Performance Level raggiunto corrisponda anche al Performance Level necessario.
Il PL raggiunto deve essere uguale o superiore rispetto al PLr stabilito dalla valutazione del rischio.
Ciò significa "via libera" alla costruzione di macchine.

Fase 6 - Convalida

Oltre a quanto previsto dai requisiti puramente qualitativi, nella realizzazione dei sistemi di sicurezza è anche importante evitare errori sistematici.

Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

DALLA “SICUREZZA” ALLA “SICUREZZA FUNZIONALE”

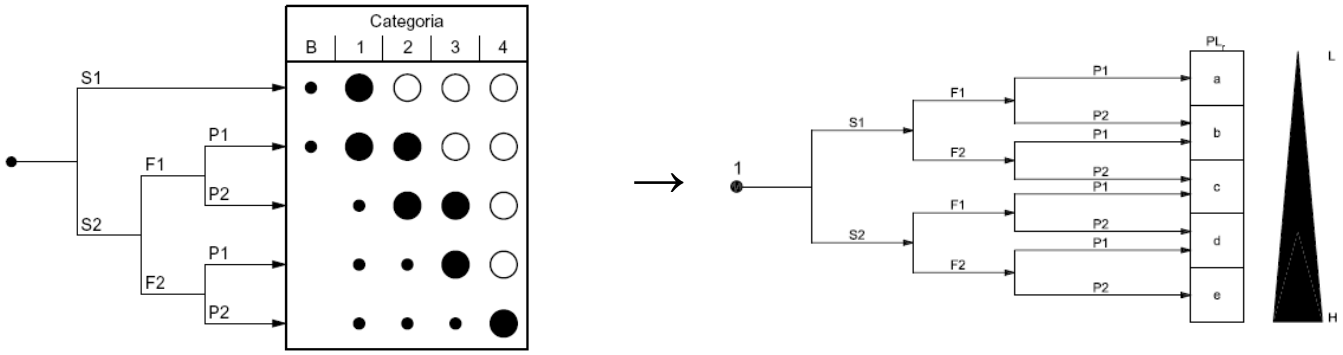
La pubblicazione delle norme EN ISO 13849-1 e della EN IEC 62061 ha determinato il passaggio della progettazione delle macchine: si è passati dal concetto di “sicurezza” al concetto di **sicurezza funzionale**:

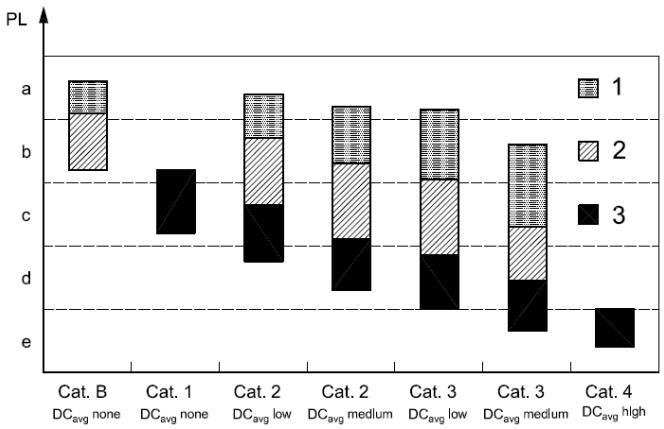
1. **sicurezza**: rappresenta l’assenza di rischi inaccettabili di danni fisici o danni diretti alla salute delle persone, oppure danni indiretti generati a beni ed all’ambiente.
2. **sicurezza funzionale (safety functional)**: rappresenta la parte della sicurezza della macchina che dipende dal funzionamento corretto di un sistema di comando e controllo in risposta a segnali d’ingresso.

PARTI DEI SISTEMI DI COMANDO LEGATE ALLA SICUREZZA: passaggio da “categoria di sicurezza” a “PL” o “SIL”

La pubblicazione delle norme EN ISO 13849-1:2006 e della EN IEC 62061:2005 ha determinato l’esigenza di non pensare più alle **categorie di sicurezza** secondo la EN 954-1:1997 (approccio deterministico), ma di **valutare l’affidabilità** delle parti dei sistemi di comando e controllo relativi alla sicurezza e realizzate sia con tecnologie pneumatiche, idrauliche, elettromeccaniche ma anche elettroniche (approccio probabilistico).
Per ogni funzione di sicurezza, l’obbiettivo non è più quello di determinare la categoria di sicurezza secondo la EN 954-1:1997 ma:

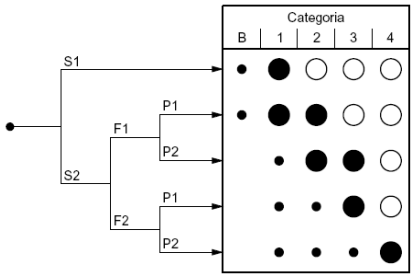
1. **PL (performance level),** articolato in n. 5 livelli: a, b, c, d, e. PL è il livello di affidabilità per realizzare la riduzione richiesta di rischio per ogni funzione di sicurezza, ovvero la capacità di un sistema di comando e controllo di svolgere una funzione di sicurezza sotto determinate condizioni, al fine di ottenere la prevista riduzione dei rischi.





Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

2. **SIL (sfety integrità level),** articolato in n. 3 livelli: 1, 2, 3. SIL è il livello discreto per specificare le relative prescrizioni di integrità della sicurezza delle funzioni di controllo da assegnare alla funzione di sicurezza



Valutazione del rischio e misure di sicurezza

Documento numero:
Parte di:

Prodotto:
Emesso da:
Data:

☐ Valutazione del rischio prima delle misure
☐ Valutazione intermedia del rischio
☐ Valutazione del rischio a posteriori

Aerea nera = Misure di sicurezza richieste
Area grigia = Misure di sicurezza raccomandate

Conseguenze	Gravità Se	Classe CI 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequenza e durata Fr		Probabilità dell'evento pericoloso Pr		Evitabilità Av	
Morte, perdita di un occhio o di un braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<=1 h	5	Molto alta	5		
Permanente: perdita di dita	3		OM	SIL 1	SIL 2	SIL 3	Da > 1 h a <= giorno	5	Probabile	4		
Reversibile: intervento medico	2			OM	SIL 1	SIL 2	Da >1 giorno a <= 2 settimane	4	Possibile	3	Impossibile	5
Reversibile: pronto soccorso	1				OM	SIL 1	Da > 2 settimane a <= 1 anno	3	Scarsa	2	Possibile	3
							> 1 anno	2	Trascurabile	1	Probabile	1

Pertanto nell'approccio probabilistico si devono ora tenere in considerazione dei nuovi parametri:

1. PFH_d : probabilità media di guasti pericolosi all'ora
2. $MTTF_d$: tempo medio di guasto pericoloso all'ora
3. λ_d : tasso di guasto pericoloso
4. $B10_d$: il numero di cicli di funzionamento entro cui il 10% dei componenti ha subito un guasto pericoloso
5. $T10_d$: periodo di tempo espresso in anni in cui il 10% dei componenti subisce un guasto pericoloso. Pertanto una volta superato il tempo calcolato, il componente deve essere sostituito.
6. DC : copertura diagnostica
7. CCF o β : cause comuni di guasto
8. SFF: frazione di guasto in sicurezza
9. T_1 : valore inferiore tra l'intervallo della prova diagnostica (proof test) ed il ciclo di vita (mission time)
10. T_2 : intervallo di prova diagnostica

RELAZIONE TRA PL E SIL

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]	SIL [EN 61508-1 (IEC 61508-1)] for information
a	≥ 10^{-5} to < 10^{-4}	No special safety requirements
b	≥ 3 x 10^{-6} to < 10^{-5}	1
c	≥ 10^{-6} to < 3 x 10^{-6}	1
d	≥ 10^{-7} to < 10^{-6}	2
e	≥ 10^{-8} to < 10^{-7}	3

Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

ESEMPI DI ALCUNI CALCOLI SECONDO LA EN ISO 13849-1

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{t_{cycle}}$$

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

dove:

hop = ore operative al giorno (ore per giorno)
dop = giorni operativi all'anno (giorni per anno)
tcycle = tempo medio tra l'inizio di due cicli successivi (sec per ciclo)
T10d = tempo medio prima che il 10% dei componenti si guasti in modo pericoloso

Determination of the $MTTF_d$ per channel

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{d,j}}$$

The following applies to diverse systems:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,C1} + MTTF_{d,C2} - \frac{1}{\frac{1}{MTTF_{d,C1}} + \frac{1}{MTTF_{d,C2}}}\right]$$

Evaluation	$MTTF_d$
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ < 100 years

Determination of the degree of diagnostic coverage (DC)

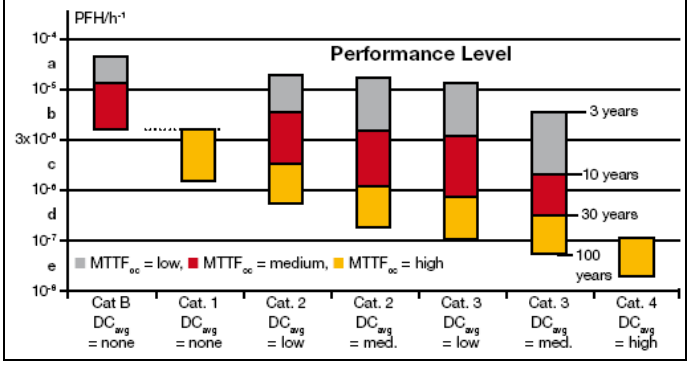
Diagnostic coverage: $DC = \sum\lambda_{DD} / \sum\lambda_{Dtotal}$

Average DC:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

Diagnostic coverage	Range of DC
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

Relationship between the categories DC, $MTTF_d$ and PL



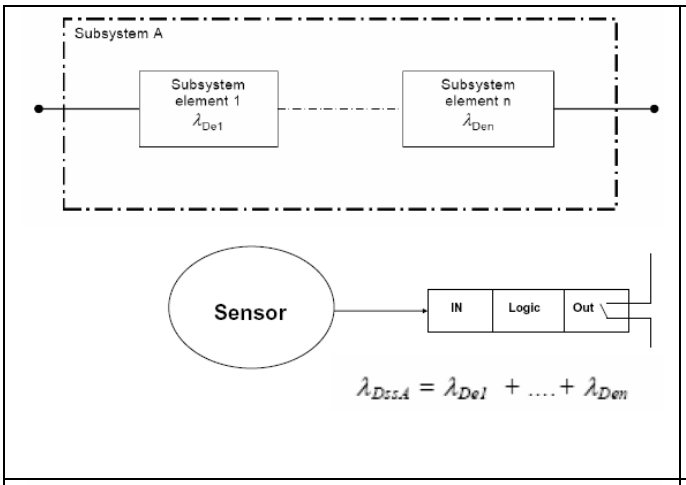
Determination of common cause failures

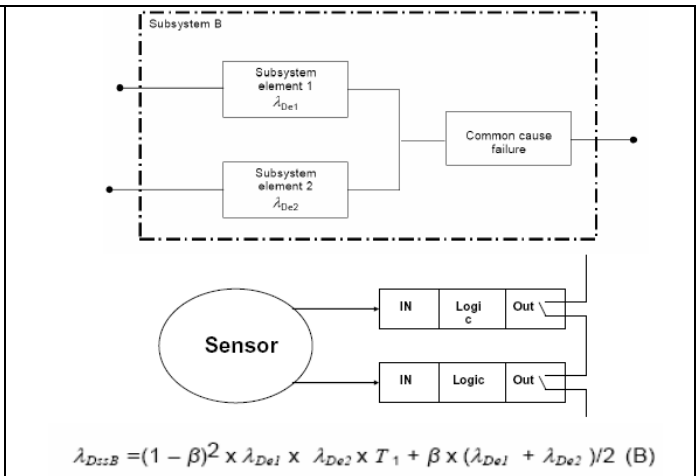
SIL points	Requirement	PL points
25	Physical separation of safety circuits and other circuits	15 %
38	Diversity (use of diverse technologies)	20 %
2	Design/application/experience	20 %
18	Assessment/analysis	5 %
4	Competence/training	5 %
18	Environmental influences (EMC, temperature, ...)	35 %

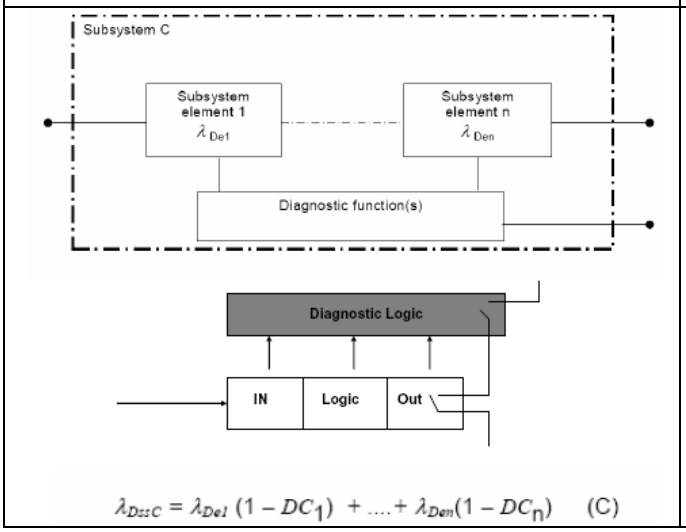
Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

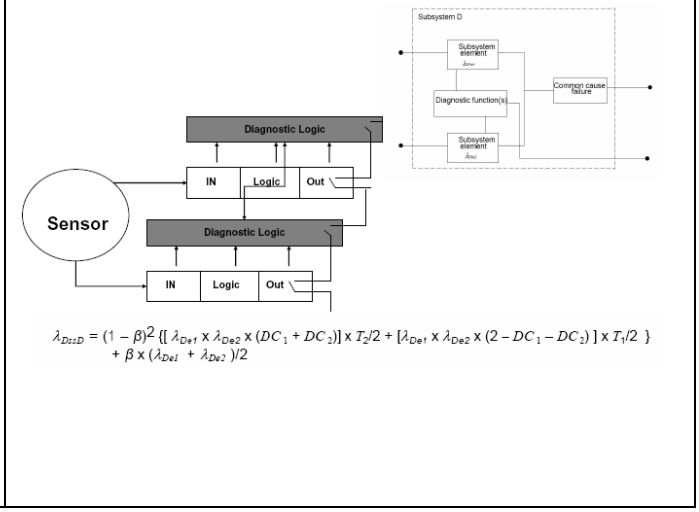
ESEMPI DI ALCUNI CALCOLI SECONDO LA EN IEC 62061

Architettura	Struttura
1001	Singolo canale - Zero fault tolerance
1001D	Singolo canale con monitoraggio - Zero fault tolerance
1002	Doppio canale senza monitoraggio – single fault tolerance
1002D	Doppio canale con monitoraggio – single fault tolerance









Architectural constraints on subsystems

$$SFF = \frac{\sum\lambda_{SD} + \sum\lambda_{SU} + \sum\lambda_{DD}}{\sum\lambda_{SD} + \sum\lambda_{SU} + \sum\lambda_{DD} + \sum\lambda_{DU}} = \frac{\sum\lambda_{S} + \sum\lambda_{DD}}{\sum\lambda_{Dtotal}}$$

Safe failure fraction (SFF)	Hardware fault tolerance 0	Hardware fault tolerance 1	Hardware fault tolerance 2
< 60 %	not permitted	SIL 1	SIL 2
60 % – < 90 %	SIL 1	SIL 2	SIL 3
90 % – < 99 %	SIL 2	SIL 3	SIL 3
99 %	SIL 2	SIL 3	SIL 3

Via Calamone, 1 - 61025 Montelabbate (PU)
Tel. - Fax.: +39 0721 472036 - Cell.: +39 339 6410508 – E-mail info@vannivaleri.it
http://www.vannivaleri.it posta elettronica certificata: vanni@pec.vannivaleri.it

PROCEDIMENTO RIASSUNTIVO

1. eseguire l'analisi dei rischi:
   - identificare i pericoli,
   - valutare i rischi e determinare i parametri S, F e P
2. valutare il **PLr** (livello di prestazione richiesto) od il **SILr** (livello di integrità della sicurezza richiesto) idoneo sulla base del grafico della valutazione dei rischi
3. progettare e realizzare la funzione di sicurezza richiesta (con o senza ridondanza, con o senza monitoraggio, etc…)
4. valutare il **livello di prestazione** o **livello di integrità della sicurezza** ottenuto attraverso i parametri caratteristici: PFH_d, $MTTF_d$, λ_d , $B10_d$, $T10_d$, DC , CCF o β , SFF, T_1 , T_2 :
5. confronto tra **PL** (livello di prestazione) od il **SIL** (livello di integrità della sicurezza) ottenuto e quello richiesto
6. eventuale riprogettazione e realizzazione della funzione di sicurezza.

SERVIZI SPECIFICI OFFERTI ALLE AZIENDE

Pertanto sia **le analisi dei rischi** sia i **documenti delle Vs macchine** (per. es. fascicolo tecnico, manuale delle istruzioni per l'uso, etc…), potrebbero **non essere aggiornati** secondo il comparto normativo vigente.

Per. Ind. Valeri Vanni con il proprio staff tecnico è referente tecnico per Cobest. S.r.l. partecipata UCIMU Sistemi Per Produrre (Associazione Costruttori Italiani Macchine Utensili) attraverso SOFIMU. Questa collaborazione porta alla **fornitura di un servizio ingegneristico, specialistico e costantemente aggiornato con l'evoluzione tecnica nel settore della sicurezza delle macchine e degli impianti**, nel centro Italia.

Per. Ind. Valeri Vanni si propone come referente per la risoluzione delle problematiche legate all'applicazione delle disposizioni legislative e regolamentari vigenti.

Per. Ind. Valeri Vanni possiede adeguate competenze tecniche nel settore per l'analisi dei rischi, lo sviluppo della documentazione a carico del PRODUTTORE e tutte le ulteriori attività formative nel settore, in merito a:

1. Incontri tecnici - corsi di formazione,
2. Aggiornamento delle analisi dei rischi (in virtù delle nuove norme tecniche)
3. Esecuzione dei calcoli al fine di identificare il PL
4. Aggiornamento dei fascicoli tecnici (in virtù delle nuove norme tecniche)
5. Aggiornamento dei manuali delle istruzioni per l'uso (in virtù delle nuove norme tecniche)