FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

Le nuove norme tecniche di settore per la sicurezza funzionale

La sicurezza funzionale

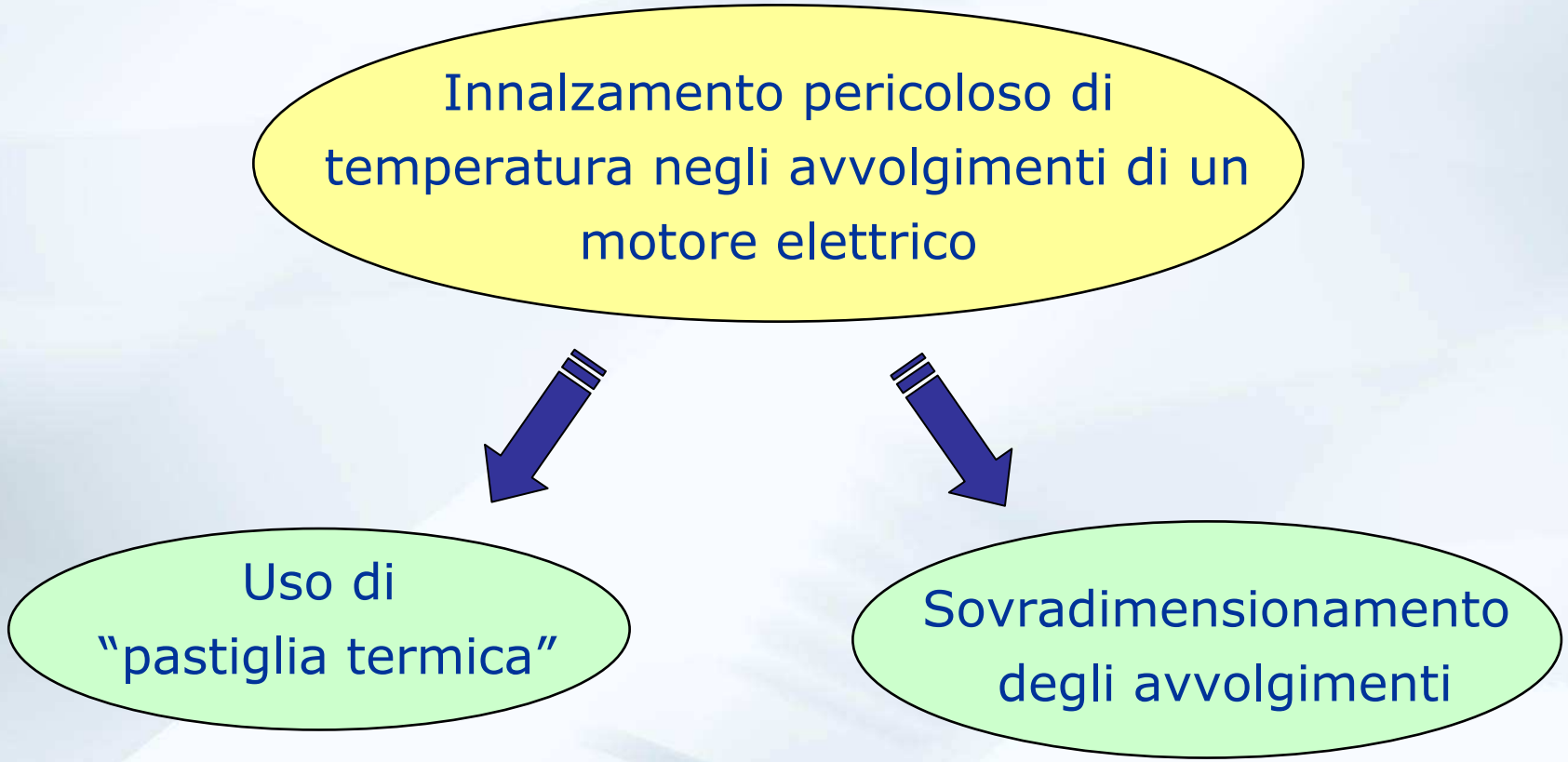
La definizione più autorevole di “Functional Safety” è contenuta all’interno della norma IEC 61508-4:

“Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functionning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities”

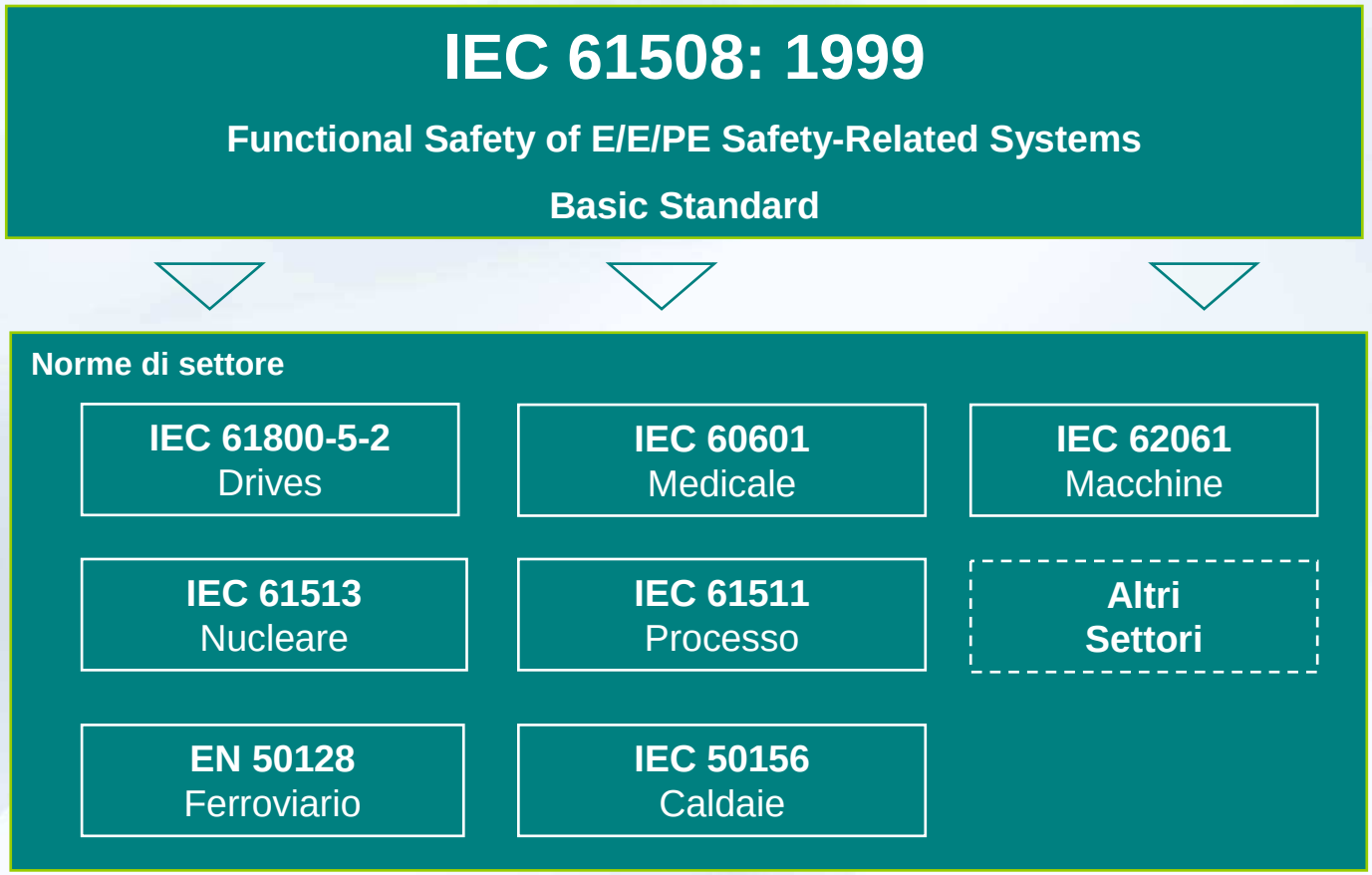
dove

EUC = Equipment Under Control
E/E/PE = Electrical/Electronic/Programmable Electronic

La sicurezza funzionale



La serie di norme IEC 61508:1999 e le relative norme di settore



Safety Integrity Level (SIL)

Il "Safety Integrity Level" (SIL) è l'indice di classificazione secondo livelli discreti della "integrità di sicurezza", dove per "integrità di sicurezza" si intende la probabilità che un sistema di controllo elettrico / elettronico / elettronico programmabile "di sicurezza" (SRECS) esegua in modo corretto la richiesta funzione di sicurezza (SRCF), secondo condizioni ben definite (SFS).

La norma IEC 62061:2005

Predisposizione di un piano per la sicurezza funzionale

- Esecuzione di un'analisi del rischio, definizione delle funzioni di sicurezza e delle corrispondenti SRCF.
- Definizione per ogni SRCF dei requisiti funzionali e del valore di SIL obiettivo.
- Scomposizione delle SRCF in blocchi funzione ed associazione delle stesse a sottosistemi di SRECS.
- Progettazione dei sottosistemi in accordo con il SIL obiettivo.
- Integrazione dei sottosistemi a formare lo SRECS.
- Elaborazione delle istruzioni d'uso.
- Validazione dello SRECS.

La norma ISO 13849-1:2006

Categorie di sicurezza EN 954-1:1996				
B	1	2	3	4

+

Affidabilità hardware dei componenti: $MTTF_d$
Diagnostic Coverage (DC) a partire da Cat. 2
Common Cause Failure (CCF) a partire da Cat. 2

=

Performance Level ISO EN 13849-1:2006				
a	b	c	d	e

Quale norma utilizzare?

ISO 13849-1

- Evoluzione della EN 954-1 con addizione di aspetti di affidabilità
- Utilizza metodi semplificati ma fornisce risultati cautelativi (sovradimensionamento della funzione)
- Non applicabile a sistemi elettronici complessi
- Da preferire per sistemi a complessità limitata

IEC 62061

- Norma derivata dalla norma IEC 61508
- Applicabile ai sistemi elettrici / elettronici senza limitazioni
- Risultati ottenuti mediante calcolo senza semplificazioni (funzione di sicurezza calibrata secondo le reali necessità)

Quale norma utilizzare?

Caso	Tecnologie	EN ISO 13849-1:2006	EN IEC 62061:2005
A	Tecnologie non elettriche (per esempio idraulica)	X	-
B	Tecnologia elettromeccanica (per esempio relè; no elettronica complessa)	Solo per alcune architetture, fino a PL "e"	Tutte le architetture, fino a SIL3
C	Elettronica complessa (per esempio logica programmabile)	Solo per alcune architetture, fino a PL "d"	Tutte le architetture, fino a SIL3
D	Caso A con caso B	Solo per alcune architetture, fino a PL "e"	X (EN ISO 13849-1:2006 per i sottosistemi non elettrici)
E	Caso B con caso C	Solo per alcune architetture, fino a PL "d"	Tutte le architetture, fino a SIL3
F	Caso A con caso C o caso A e caso B con caso C	X (IEC 62061 per i sottosistemi elettronici complessi)	X (EN ISO 13849-1:2006 per i sottosistemi non elettrici)