FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE

CONFINDUSTRIA

DAL 1945 IL VALORE DELL'INNOVAZIONE

Sicuri… ma quanto?

Introduzione alla Sicurezza Funzionale nei sistemi impieganti azionamenti elettrici ed alla normativa di riferimento.

Marco Franchi
Ansaldo Sistemi Industriali

Gruppo Azionamenti Elettrici

ASSOAUTOMAZIONE
ASSOCIAZIONE ITALIANA
AUTOMAZIONE E MISURA

Introduzione

1- **Un robot non può recare danno a un essere umano, né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno.**

2- **Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge.**

3- **Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima e la Seconda Legge.**

[Isaac Asimov, Le Tre Leggi della Robotica]

Sicurezza nei sistemi:

- Sicurezza elettrica, termica ed energetica [Safety]
- Sicurezza funzionale [Functional Safety]
- Fidatezza [Dependability]

Sicurezza Funzionale

- La sicurezza funzionale è la parte della sicurezza di sistema che dipende dal corretto comportamento del sistema o dell'apparecchiatura in risposta agli ordini dati.

[cfr. IEC, Introductory Brochure to IEC61508].

Sicurezza funzionale in un sistema:

- Sistema: insieme di dispositivi e/o sottoassiemi di dispositivi interconnessi, costituenti una singola entità logica atta a fornire un servizio;
- se la fornitura anomala, indesiderata o mancata di uno o più aspetti del servizio può generare pericolo, la sicurezza funzionale del sistema è critica.

Apparecchiature e Sicurezza Funzionale

- Le Apparecchiature Elettriche e/o Elettroniche e/o Programmabili (E/E/PE) sono sistemi sovente complessi e sono sempre più spesso impiegate per svolgere funzioni di sicurezza.
- Misure e criteri atti a garantire il livello di Sicurezza Funzionale delle apparecchiature E/E/PE devono essere adottati fin dalla fase di progetto, allo scopo di prevenire il verificarsi di guasti catastrofici o quantomeno di mantenere il controllo su quanti di questi inevitabili.

[cfr. IEC, Guide to IEC 61508] .

Possibili cause di eventi catastrofici

-> carenze od omissioni nella definizione dei requisiti di sicurezza funzionale;

-> carenze od omissioni nell'implementazione delle funzioni per le quali è richiesta sicurezza funzionale (ad esempio, mancata applicazione dei criteri di Sicurezza Funzionale per ciascuno dei modi e delle condizioni di funzionamento);

-> guasti casuali o sistematici dell'hardware;

-> errori nel software;

-> comportamenti indesiderati dovuti all'ambiente (sollecitazioni meccaniche, elettromagnetiche, climatiche, ecc.);

-> guasti o comportamenti indesiderati dovuti all'alimentazione,

-> eccetera...

[cfr. IEC, Giude to IEC 61508]

E/E/PE Safety Related System

- Lo Standard **CEI EN 61508** norma la Sicurezza Funzionale per tutte le apparecchiature Elettriche e/o Elettroniche e/o Programmabili (E/E/PE) indipendente dal tipo di apparecchiatura, applicazione e di impiego.
- Solo le apparecchiature appositamente progettate, costruite, installate, documentate e verificate per tale scopo possono garantire -o meno- un livello definito di Sicurezza Funzionale per ciascuna delle funzioni svolte.

Struttura della CEI EN 61508:

“Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza -

- **Parte 1: Requisiti generali**
- **Parte 2: Requisiti per i sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza**
- **Parte 3: Requisiti del software**
- **Parte 4: Definizioni ed abbreviazioni**
- **Parte 5: Esempi di metodi per la determinazione dei livelli di integrità di sicurezza**
- **Parte 6: Guida all’applicazione delle IEC 61508-2 e IEC 61508-3**
- **Parte 7: Panorama delle tecnologie e delle misure tecniche**

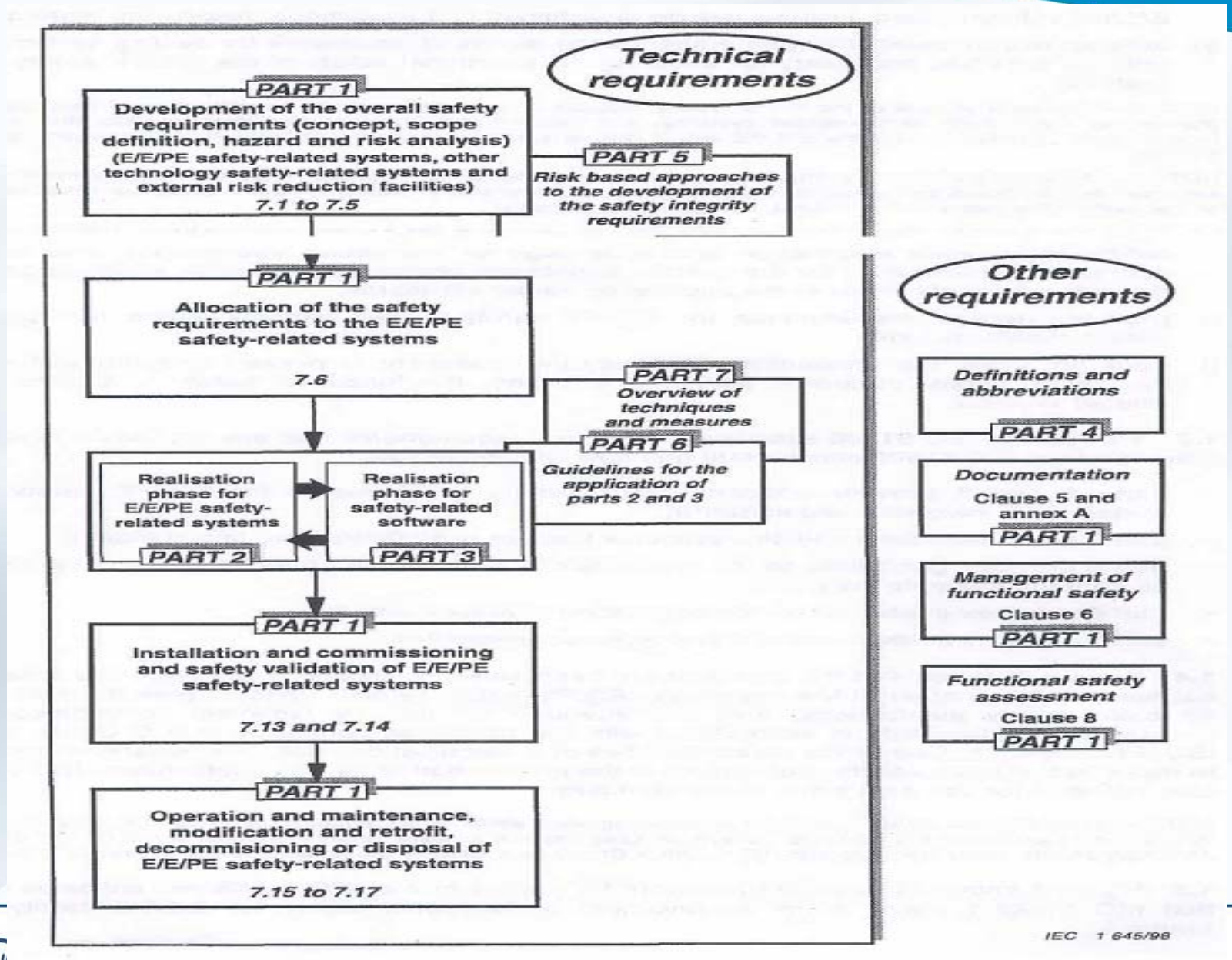
Norma “trasversale”...

… in quanto definisce i criteri e le linee guida da adottare come riferimento per la Sicurezza Funzionale in tutte le apparecchiature E/E/PE.

E’ lasciato alla Norma di Prodotto, ove esistente e se necesssario, definire i dettagli specifici per ciascuna apparecchiatura.

… destinata ad essere riferimento per ...

- Costruttori (di sistema e di ogni livello di sottoassieme);
- Integratori di sistema;
- Utilizzatori finali;
- Manutentori;
- Enti certificatori;
- Analisti.


Technical requirements
PART 1
Development of the overall safety requirements (concept, scope definition, hazard and risk analysis)
(E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities)
7.1 to 7.5
PART 5
Risk based approaches to the development of the safety integrity requirements
PART 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
PART 7
Overview of techniques and measures
PART 6
Guidelines for the application of parts 2 and 3
Realisation phase for E/E/PE safety-related systems
PART 2
Realisation phase for safety-related software
PART 3
PART 1
Installation and commissioning and safety validation of E/E/PE safety-related systems
7.13 and 7.14
PART 1
Operation and maintenance, modification and retrofit, decommisioning or disposal of E/E/PE safety-related systems
7.15 to 7.17
Other requirements
Definitions and abbreviations
PART 4
Documentation
Clause 5 and annex A
PART 1
Management of functional safety
Clause 6
PART 1
Functional safety assessment
Clause 8
PART 1
IEC 1 645/98

Qualche definizione

- Low Demand Mode: la funzione SR è richiesta meno di una volta l'anno o meno del doppio dell'intervallo di manutenzione; in caso contrario si tratta di
- High Demand (o Continuous) Mode.

Safety Integrity Level

- SIL: livello di integrità. Sovente è diverso per ciascuna delle funzioni SR del sistema.

Low Demand Mode SIL	probabilità di comportamento indesiderato alla richiesta
4	da $\geq 10^{-5}$ a $> 10^{-4}$
3	da $\geq 10^{-4}$ a $> 10^{-3}$
2	da $\geq 10^{-3}$ a $> 10^{-2}$
1	da $\geq 10^{-2}$ a $> 10^{-1}$

Hih Demand Mogde SIL	probabilità per ora di comportamento indesiderato
4	da $\geq 10^{-9}$ a $> 10^{-8}$
3	da $\geq 10^{-8}$ a $> 10^{-7}$
2	da $\geq 10^{-7}$ a $> 10^{-6}$
1	da $\geq 10^{-6}$ a $> 10^{-5}$

Norme SR di Prodotto

- CEI EN 61508 norma criteri e principi per la Sicurezza Funzionale nelle Apparecchiature Elettriche/Elettroniche/Programmabili.
- Ove ritenuto necessario sono state preparate e sono in preparazione Norme legate alle specifiche funzioni dell'Apparecchiatura (affiancate allo Standard di Prodotto, ad esempio: CEI EN 62061, ed.1: 2005, [macchinario])

Azionamenti Elettrici a Sicurezza Funzionale

- Azionamenti Elettrici a Velocità variabile (PDS): Norma in preparazione a cura IEC come 61800-5-2 "Adjustable speed electrical power drive systems - Part - 5: safety requirements - Section 2: functional".
- Data pubblicazione prevista: estate/autunno 2007

- Norma del gruppo 61800- -> norma di prodotto.
- Gli Azionamenti Elettrici aventi una o più funzioni di sicurezza funzionale secondo la futura Norma dovrebbero essere denominati **Safety Related Power Drive Systems** o **PDS(SR).**

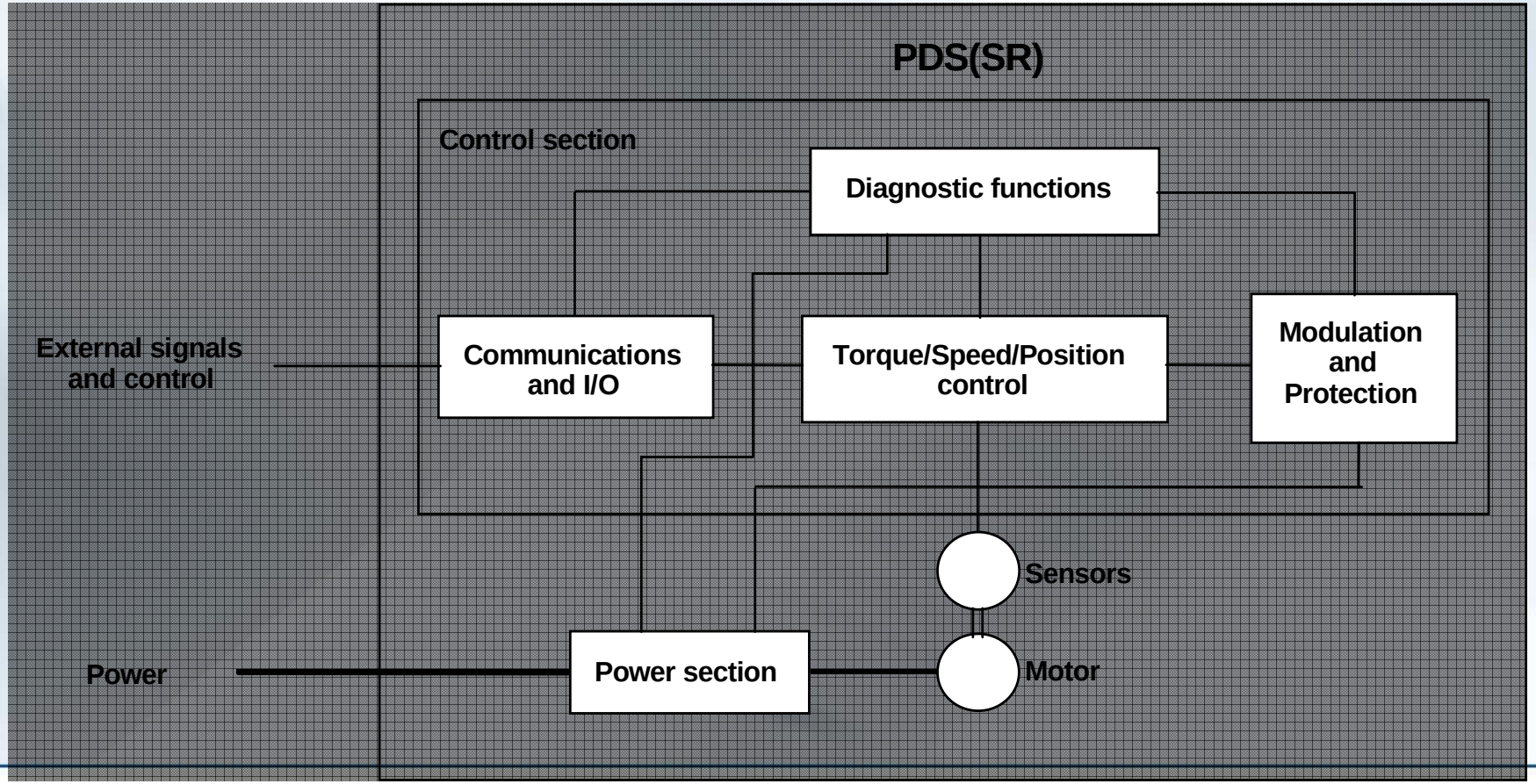
Scope of 61800-5-2

-> Norma di prodotto per gli Azionamenti Elettrici a Velocità variabile che ne definisca requisiti e raccomandazioni per

- progetto,
- sviluppo,
- integrazione e
- validazione

per quanti di questi debbano essere impiegati in contesti che richiedano funzioni a sicurezza funzionale come genericamente definito nel contesto dello Standard CEI EN 61508.

Campo di applicabilità della futura 61800-5-2



Limiti e confini

In un PDS(SR) le funzioni Safety Related sono tali per il solo PDS, inteso quale sottoassieme avente come confini le interfacce alle funzioni Safety Related del PDS(SR) stesso.

Sono estranei allo scopo della Norma e del PDS(SR):

- la verifica di congruenza dei comandi ricevuti;
- i calcoli di analisi di rischio per l'applicazione;
- l'identificazione delle funzioni SR legate all'applicazione e la definizione del SIL associato ad esse;
- il carico;
- i rischi secondari (legati al processo produttivo);
- tutto quanto concerne sicurezza elettrica, termica ed energetica.

- Non è solitamente sufficiente impiegare sottoassiemi aventi funzioni SR per implementare nel sistema caratteristiche di sicurezza funzionale.

PDS (SR)

- Un azionamento Elettrico a Velocità Variabile (PDS) dispone di parecchie funzioni: ciascuna può essere SR con un diverso SIL o non essere per niente SR.

- Per esempio, un PDS (SR) potrebbe presentare:
- funzione Annullamento Coppia Sicuro a SIL 3;
- funzione Arresto Sicuro a SIL 3;
- funzione Limite di Accelerazione Sicuro a SIL 1;
- tutte le altre funzioni non Safety Related.

Esempio di funzioni SR in un PDS (SR)

- Annullamento Coppia Sicuro
- Arresto Sicuro
- Limite di accelerazione Sicuro
- Limite di Velocità Sicuro
- Limitazione Campo di Velocità Sicuro
- Limite di Coppia Sicuro
- Senso di Rotazione Sicuro
- Controllo della frenatura Sicuro
- Segnale monitor della velocità Sicuro
- Marcia a impulso Sicuro
- ……

Le Vostre domande sono benvenute

Grazie per l'attenzione