U&C

Unificazione&Certificazione

LA RIVISTA DELLA NORMAZIONE TECNICA

DOSSIER: GESTIONE RIFIUTI

L'Assemblea Generale dell'ISO 2010

A L'Aquila esperti a confronto sul restauro dei beni culturali

Responsabilità sociale: una novità assoluta nel panorama delle norme ISO

10
Novembre/Dicembre 2010
Anno LV

La sicurezza funzionale: la nuova edizione della IEC 61508

di F. Andreolli, A. Brunelli, E. Ciapessoni

È stata pubblicata da IEC (International Electrotechnical Commission), la nuova edizione di uno degli standard più importanti e di maggiore impatto applicativo in ambito industriale: si tratta della serie di norme IEC 61508 dedicate alla sicurezza funzionale.

La nuova edizione subentra alla prima edizione del 1998 citata all'interno di Direttive Europee e testo di riferimento trasversale e generale sulla sicurezza funzionale per molti settori tecnologici che a loro volta sviluppano le norme applicative specifiche per il loro settore: per il controllo di processo (serie 61511), le macchine (serie 62061), gli azionamenti (61800-5-2), l'EMC (61326-3-X), le comunicazioni (61784-3), il ferroviario (serie 50126/8/9), il nucleare (serie 61513), ecc.

Nei prossimi mesi, tutti questi comitati IEC oltre a quelli CEN, CENELEC e ISO che fanno riferimento alla sicurezza funzionale, saranno impegnati nel valutare il recepimento degli aggiornamenti e l'eventuale revisione dei propri documenti normativi, che l'ACOS (IEC - Advisory Committee On Safety) ha stimato in oltre 170 documenti.

La nuova versione della norma, ricalca il formato della versione 1 precedente, suddiviso in sette parti:

1. requisiti generali
2. requisiti per sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza
3. requisiti del software
4. definizioni ed abbreviazioni
5. esempi di metodi per la determinazione dei livelli di integrità di sicurezza
6. guida all'applicazione delle IEC 61508-2 e IEC 61508-3
7. panorama delle tecnologie e delle misure tecniche.

A tal proposito, la figura 1 evidenzia, in termini di requisiti tecnici ed altri, l'applicazione delle varie parti della IEC 61508, allo scopo di indirizzare l'utilizzatore ad una corretta applicazione delle varie parti normative (1, 2, 3, 4) seguendo anche le esemplificazioni e le linee guida riportate nelle rimanenti parti informative (5, 6, 7).

La nuova norma Internazionale IEC 61508 sarà presto recepita dal CENELEC come norma europea EN 61508 e, successivamente, dal CEI come norma nazionale CEI EN 61508, abrogando così la norma attualmente in vigore.

Novità principali

Le novità principali introdotte dalla seconda edizione della IEC 61508 (emessa nel 2010) sono essenzialmente le seguenti:

- sono aggiornati i requisiti di sicurezza;
- viene modificato il ciclo di vita in sicurezza;
- viene introdotto il concetto di integrità di sicurezza anche ai sottosistemi;
- viene introdotto anche il requisito di "security" (antintrusione informatica e non);
- il manuale di sicurezza diventa obbligatorio e ne vengono definiti i requisiti sia per HW che SW;

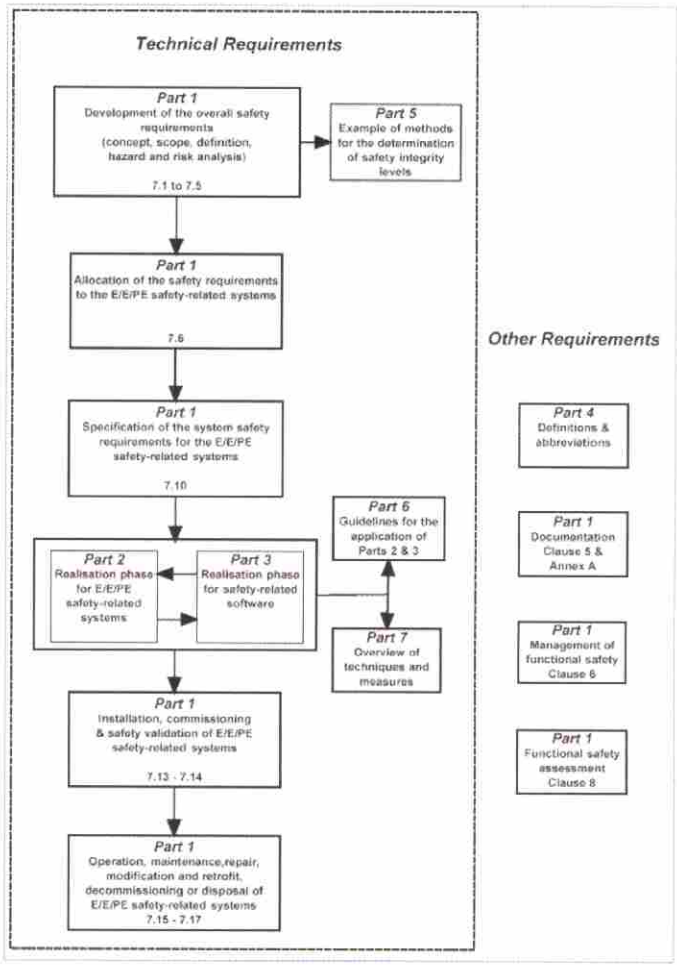

Figura 1 - Guida all'applicazione delle parti normative e informative (Figura 1: IEC 61508-1)

- viene fornita una seconda via per determinare la ridondanza in applicazioni con componenti "proven use";
- viene rivisto il calcolo della frazione di guasti sicuri dei componenti SFF (Safe Failure Fraction);
- viene considerato l'impiego di tecnologia ASICS (Appilcation Specific Integrated Circuits);
- vengono maggiormente esplicitati i metodi per definire i SIL (Safety Integrity Level);
- sono meglio dettagliati i software, i tools e la programmazione a oggetti;
- sono descritte nuove possibili architetture dei sistemi di sicurezza;
- sono state aggiunte e rivisitate le definizioni alcune delle quali verranno evidenziate e dettagliate nel prosieguo.

Ciclo di vita in sicurezza (Parte 1)

Il nuovo ciclo di vita in sicurezza, illustrato in figura 2, diviso in 16 fasi come nell'edizione precedente, è stato rivisto:

- nelle fasi di realizzazione dei SrS (Safety related System), ed in particolar modo nelle fasi di specificazione dei requisiti e di realizzazione dei sistemi E/E/PE (Elettrici / Elettronici / Elettronici Programmabili), fasi 9 e 10, precedentemente svolti nella fase 9,
- mentre le fasi 9 e 10 dell'edizione 1, *dedicate rispettivamente ai Sistemi relativi alla Sicurezza (SrS) realizzati con altre tecnologie (valvole di sicurezza, dischi di rottura,ecc.) e con altri mezzi di riduzione del rischio (serbatoi di convogliamento, vasche di contenimento, ecc.)*, sono state raggruppate nella nuova fase 11, che è diventata il riferimento per la specificazione e realizzazione di tutti gli altri sistemi di riduzione del rischio, diversi dai SIS (Safety Instrumented System), oggetto principale della normativa in esame.

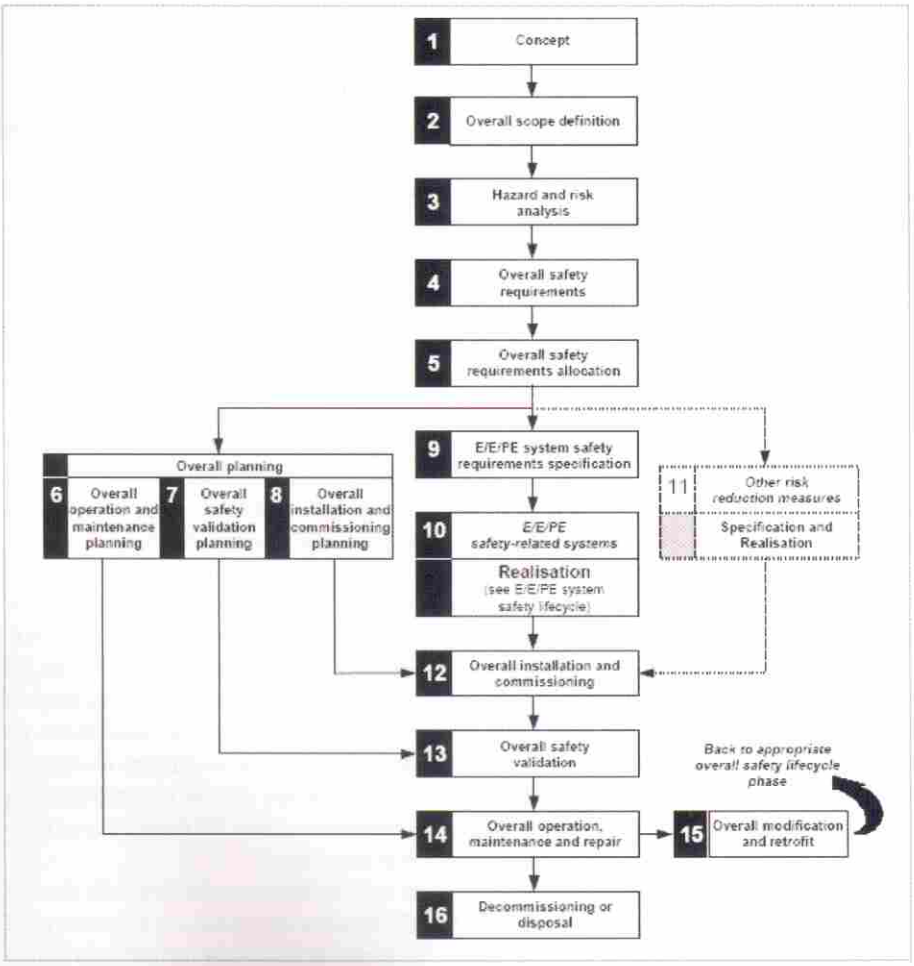

Figura 2 - Nuovo schema di flusso del ciclo di vita in sicurezza (Figura 2: IEC 61508-1)

Safety lifecycle phase		Objectives	Scope	Requirements subclause	Inputs	Outputs
Figure 2 box number	Title					
9	E/E/PE system safety requirements specification	7.10.1: To define the E/E/PE system safety requirements, in terms of the E/E/PE system safety functions requirements and the E/E/PE system safety integrity requirements, in order to achieve the required functional safety.	E/E/PE safety-related systems	7.10.2	Information and results of the overall safety requirements allocation.	Specification of the E/E/PE system safety requirements.
10	E/E/PE safety-related systems: realisation	7.11.1 and parts 2 and 3: To create E/E/PE safety-related systems conforming to the specification for the E/E/PE system safety requirements (comprising the specification for the E/E/PE system safety functions requirements and the specification for the E/E/PE system safety integrity requirements).	E/E/PE safety-related systems.	7.11.2, IEC 61508-2 and IEC 61508-3	Specification of the E/E/PE system safety requirements.	Realisation of each E/E/PE safety-related system according to the E/E/PE system safety requirements specification.
11	Other risk reduction measures: specification and realisation	7.12.1: To create other risk reduction measures to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).	Other risk reduction measures.	7.12.2	Other risk reduction measures safety requirements specification (outside the scope and not considered further in this standard).	Realisation of each other risk reduction measure according to the safety requirements for that measure.

Tabella 1 - Stralcio dei requisiti del ciclo di vita in sicurezza (Tabella 1: IEC 61508-1)

Per far chiarezza a tal proposito sono stati rivisti i contenuti della tabella 1: IEC 61508-1, che evidenzia a fronte delle nuove fasi del ciclo di vita in sicurezza (Safety Life Cycle):

- 9: Specificazione dei requisiti dei sistemi E/E/PE
- 10: Realizzazione dei sistemi E/E/PE
- 11: Specificazione e realizzazione degli altri sistemi di riduzione dei rischi.

Gli scopi e gli obiettivi della fase, corredati degli input e degli output necessari e richiesti per soddisfare i requisiti di tutti i sistemi relativi alla sicurezza, sia strumentati (SIS), sia non strumentati, sebbene non oggetto diretto della IEC 61508.

Inoltre, nella IEC 61508-2 (hardware), i requisiti delle diverse fasi del ciclo di vita in sicurezza relativi alla realizzazione dell'Hardware dei sistemi E/E/PE, sono ulteriormente approfonditi nell'articolo 7, e la fase 10 di realizzazione e dettagliata nella figura 2, con ulteriori dettagli realizzativi riportati nella relativa tabella 1.

Similarmente, nella IEC 61508-3 (software), i requisiti delle diverse fasi del ciclo di vita in sicurezza relativi alla realizzazione del software dei sistemi E/E/PE, sono ulteriormente approfonditi nell'articolo 7, e la fase 10 di realizzazione e dettagliata nella figura 3, con ulteriori dettagli realizzativi riportati nella relativa tabella 1.

In entrambe le parti 2 e 3 della IEC 61508, l'articolo 7, esamina e approfondisce i requisiti relativi all'integrazione, validazione, modificazione dei sistemi E/E/PE, mentre l'ultimo articolo normativo 8 dettaglia sulla valutazione della sicurezza funzionale che riferendosi ai requisiti dell'analogo articolo 8 della IEC 61508-1, deve sempre rispondere ai requisiti di pianificazione, esecuzione, completezza, correttezza e precisione, ovvero quello che è stato specificato, sia stato realizzato e sia stato anche validato per l'applicazione in sicurezza richiesta.

Introduzione di nuovi concetti di sicurezza (Parte 1)

La sicurezza funzionale (safety) finora considerata solo nei confronti dei pericoli dell'EUC (Equipment Under Control) è stata estesa anche alla sicurezza antintrusione (security) contro pericoli provocati da azioni non autorizzate e male volenti (Punto 7.4.2.3: IEC 61508-1), che possono portare e/o provocare rischi di pericolo per il personale, l'ambiente e l'impianto industriale.

Competenza e indipendenza del personale (Parte 1)

Le competenze del personale coinvolto nei progetti della funzione sicurezza, dapprima relegate come informative nell'allegato A della vecchia IEC 61508-1, ora sono state riportate e ridefinite nell'articolo 8 della nuova IEC 61508-1.

A titolo di esempio si riporta in tabella 2, la tabella 5: IEC 61508-1, che definisce in funzione del richiesto livello di integrità di sicurezza SIL, l'indipendenza del personale coinvolto nella valutazione della sicurezza funzionale rispetto l'organizzazione che realizza il sistema strumentato di sicurezza SIS.

Minimum level of independence	Safety integrity level/Systematic capability			
	1	2	3	4
Independent person	X	X1	Y	Y
Independent department		X2	X1	Y
Independent organization			X2	X
NOTE See 8.2.15, 8.2.16 and 8.2.18 for details on interpreting this table.				

Tabella 2 - Indipendenza del personale coinvolto nella valutazione della sicurezza funzionale

In particolare, secondo la "nota" riportata in tabella 2, in relazione al richiesto SIL (1, 2, 3, 4), l'indipendenza del personale di valutazione della sicurezza funzionale è:

- X : sufficiente;
- X1, X2 : sufficiente in alternativa;
  : X2 appropriato per sistemi a maggior grado di complessità, novità o tecnologia;
- Y : insufficiente.

Determinazione della tolleranza ai guasti hardware (Parte 2)

La tolleranza ai guasti hardware HFT (Hardware Fault Tolerance) oltre che col classico metodo della frazione dei guasti sicuri SFF (Safe Failure Fraction) denominata Route 1_H, si può ora determinare, anche attraverso la nuova Route 2_H (Punto 7.4.4.3: IEC 61508-2) sia per i componenti ad alta complessità tipo B (purché con copertura diagnostica DC maggiore del 60%), sia per i componenti a bassa complessità tipo A, che sono stati selezionati sulla base di utilizzazioni precedenti - "proven use" (analogamente all'attuale IEC 61511).

In queste situazioni di Route 2_H, è richiesto un HFT minore:

a) 2 per SIL 4
b) 1 per SIL 3
c) 0 per SIL 2
d) 0 per SIL 1

Inoltre, i componenti a bassa complessità tipo A, sono considerati "proven in use" se la quantificazione dei guasti hardware casuali sono stati:

a) rilevati dall'utilizzo in campo in similari applicazioni di processo e ambientali;
b) elaborati statisticamente secondo norme Internazionali IEC 20300-3-2 o ISO 14224;
c) valutati in accordo alle quantità di dati di ritorno dall'utilizzazione, da test e da giudizi.

Requisiti normativi del manuale di sicurezza (Parte 2 e 3)

Il manuale di sicurezza deve definire gli attributi di ogni componente dei sottosistemi di sicurezza, i vincoli HW e SW che l'integratore deve considerare e le proprietà principali, le caratteristiche funzionali ed i comportamenti in caso di guasto.

Il manuale è ora normativo sia per HW e SW (rispettivamente allegati D della parte 2 e 3), e deve contenere almeno i seguenti elementi:

a) la specifica funzionale delle funzioni realizzate;
b) l'identificazione dell'HW e SW per consentire l'integrazione;
c) le istruzioni ed i vincoli da rispettare per evitare guasti sistematici.

Poi per ogni funzione si deve almeno specificare:

- i modi di guasto casuali della funzione (rilevati e non rilevati dalla diagnostica);
- i tassi di guasto relativi (rilevati e non rilevati dalla diagnostica);
- i requisiti e gli intervalli della diagnostica;
- gli stati delle uscite in caso di guasto;
- la configurazione HW (& SW);
- la fault tolerance HW (& SW);
- la classificazione in tipo A e tipo B;
- la configurazione raccomandata;
- le istruzioni per l'installazione;
- ecc..

Altri dettagli sulle altre Parti della IEC 61508:2010

La parte 4 "Termini e Definizioni" introduce i concetti di element safety function, overall safety function, systematic capability, ecc.

Nella parte 5 "Esempi di metodi per la determinazione del SIL" sono state estesi gli esempi di metodologie di determinazione del SIL.

Nella parte 6 "Linee guida di applicazione della IEC 61508-2 &I EC 61508-3" sono state riportate maggiori informazioni sul calcolo della probabilità e miglior descrizione sulle tecniche di modellazione probabilistica: Reliability block, Fault tree, Markov, ecc.

Infine, è stata aggiornata la parte 7 "Bibliografia".

Conclusioni

Si tratta, dunque, di una revisione sostanziale: le novità riguardano da un lato, metodologie alternative per la determinazione della tolleranza ai guasti hardware HFT (Route 2_H, già contemplata in qualche maniera anche dalla IEC 61511:2003 rivolta alla sicurezza funzionale nell'industria di processo) e dall'altro lato, le richieste normative essenzialmente per la competenza e indipendenza del personale che conduce la valutazione della sicurezza funzionale e per la redazione del manuale di sicurezza. Pertanto si può ritenere che la nuova edizione 2 della IEC 61508:2010 avrà un l'impatto industriale favorevole, sia per la maggiore facilità di interpretazione e la maggiore generalità e completezza, sia perché in applicazioni che prevedono funzioni strumentate di sicurezza SIF, realizzate con componenti provati e/o utilizzati precedentemente, si può avere un credito di ridondanza rispetto SIF realizzate con componenti con ratei di guasto non documentati.

Sebbene le novità introdotte dalla nuova norma basilare sulla sicurezza funzionale IEC 61508:2010 non siano sostanziali per l'esperto, per il neofita che si avvicina alla sicurezza funzionale nell'industria di processo sono abbastanza rilevanti, perché dovendo seguire la norma specifica sull'industria di processo IEC 61511:2003 che fa spesso riferimenti trasversali con la IEC 61508, talvolta con corpo normativo articolato in ben 10 parti si potrebbe anche smarrire.

Per questo motivo il CEI ha messo a calendario un corso sui sistemi strumenti di sicurezza SIS, che partendo dalla linea guida nazionale di applicazione della IEC 61511, delinea una corretta implementazione della IEC 61511 e degli articoli normativi di riferimento trasversali della IEC 61508 con esempi applicativi di determinazione dei livelli di integrità di sicurezza SIL, attraverso un pratica modellistica consolidata mediante i grafici e le matrici di rischio, al fine di far rientrare il processo entro i limiti di rischio consentiti dalla regolamentazione legale e societaria, nei confronti dei possibili danni all'ambiente, alle persone e alle cose.

Fabio Andreolli
Membro CEI SC65A
Alessandro Brunelli
Segretario CEI SC65B
Emanuele Ciapessoni
Membro CEI SC65A

FUNCTIONAL SAFETY: THE NEW EDITION OF IEC 61508

The International Electrotechnical Commission (IEC) has recently published a new edition of one of the most important applicative standard affecting the industry: the IEC 61508 series, dedicated to Functional Safety, that also has multiple links with many other standards in several sectors. This brief article aims to illustrate the relevant news regarding the revision of the IEC 61508 Ed. 2 and the consequences of this update on the Process Industry.