DI FABIO ANDREOLLI*

SICUREZZA FUNZIONALE IN AMBITO INDUSTRIALE: LA **NUOVA IEC 61508/2010**

L'INTERNATIONAL ELECTROTECHNICAL COMMISSION (I.E.C.) HA PUBBLICATO LA NUOVA EDIZIONE DI UNO DEGLI STANDARD PIÙ IMPORTANTI E DI MAGGIORE IMPATTO APPLICATIVO IN AMBITO INDUSTRIALE: SI TRATTA DELLA NORMA IEC 61508 DEDICATA ALLA SICUREZZA FUNZIONALE O MEGLIO ALLE *FUNZIONI DI SICUREZZA*

La IEC 61508, sviluppata in prima edizione nel 1998, è una norma generica che contiene metodologie generali da applicarsi nello sviluppo dei sistemi per la sicurezza funzionale o per lo sviluppo di una norma applicativa di settore.
Al momento la norma non è cogente ma è citata come testo di riferimento trasversale e generale sulla sicurezza funzionale per molti ambiti tecnologici per i quali si sviluppano norme applicative specifiche di settore rispecchiandone la struttura e i contenuti mediante dettagliate e puntuali prescrizioni.
Per esempio per il macchinario la norma applicativa di settore è la CEI EN 62061 e la corretta applicazione permette la realizzazione di una macchina conforme alla direttiva di riferimento e la sua marcatura CE.
Per la misura e il controllo degli impianti di processo industriale, la norma è la CEI EN 61511 e la sua corretta applicazione permette di ottemperare ai requisiti previsti da:

- D.Lgs. n. 334/99 Attuazione Direttiva 96/82/CE "Seveso";
- Direttiva ATEX (94/9 - 99/92 CE);
- Direttiva PED (94/9 - 98/37 CE);
- Disposizioni del DM 04/05/1998 (decreto attuativo DPR 12/01/98), blocchi di emergenza degli impianti tec-

nologici.
Riguardo alla produzione di energia, fatta eccezione per gli impianti fotovoltaici, si ricade sempre nell'ambito di applicabilità della norma IEC 61508 con la CEI EN 61511 (tutto il termico, incluso solare, biomasse e idroelettrico), la CEI EN 62061 (eolico) e la CEI EN 61513 (nucleare).
Inoltre IEC cita esplicitamente la 61508[1] tra le norme da considerare nello sviluppo dei sistemi di protezione e controllo del sistema elettrico per le *smart grid* (reti intelligenti di trasmissione e distribuzione).
Nei prossimi mesi ci saranno sicuramente novità riguardo gli azionamenti (61800-5-2), l'EMC (61326-3-X), le comunicazioni (61784-3), il ferroviario (serie 50126/8/9), l'automobilistico e i dispositivi di sicurezza.
La norma ricalca il formato precedente, costituito da una parte introduttiva (0) e dalle seguenti sette parti:
1. requisiti generali;
2. requisiti per i sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza;
3. requisiti del software;
4. definizioni e 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.

Le principali novità sono le seguenti:
- aggiornati i requisiti di sicurezza;
- è modificato il ciclo di vita in sicurezza;
- è introdotto il concetto di integrità di sicurezza anche ai sottosistemi;
- è introdotto il requisito di "security" (antintrusione informatica e non);
- il manuale di sicurezza diventa obbligatorio e sono definiti i requisiti sia per hardware sia per software;
- è fornita una seconda via per determinare la ridondanza in applicazioni con componenti "*proven use*";
- è rivisto il calcolo della frazione di guasti sicuri dei componenti SFF (Safe Failure Fraction);
- è considerato l'impiego di tecnologia ASICS (Application Specific Integrated Circuits);
- sono maggiormente esplicitati i metodi per definire i SIL (Safety Integrity Level);
- sono meglio dettagliati i software, i tool e la programmazione a oggetti;
- sono descritte nuove possibili architetture dei sistemi di sicurezza;
- sono state aggiunte e rivisitate le definizioni.

Prima parte - 61508-1 Requisiti generali

Il ciclo di vita in sicurezza è ancora suddiviso in sedici fasi come nell'edizione precedente, ma sono state riviste:
- le fasi di realizzazione dei SrS (Safety related System) e in particolar modo le fasi di specificazione dei requisiti e di realizzazione dei sistemi E/E/PE (Elettrici/Elettronici/Elettronici Programmabili), fasi nove e dieci, precedentemente svolti nella fase nove;
- le fasi nove e dieci dell'edizione 1, dedicate rispettivamente ai Sistemi relativi alla Sicurezza (SrS) realizzati con altre tecnologie (valvole di sicurezza, dischi di rottura, eccetera) e con altri mezzi di riduzione del rischio (serbatoi di convogliamento, vasche di contenimento, eccetera). Queste sono invece state raggruppate nella nuova fase undici che diventata ora il riferimento per la descrizione e la realizzazione di tutti gli altri sistemi di riduzione del rischio diversi dai SIS (Safety Instrumented System), oggetto principale della norma in esame.

Inoltre, le competenze del personale coinvolto nei progetti della sicurezza funzionale, dapprima relegate come informative nell'Allegato A, sono ora diventate parte della norma e definite all'art 8.
La sicurezza funzionale 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 (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.

Seconda parte - 61508-2 Hardware

I requisiti delle diverse fasi del ciclo di vita in sicurezza che si riferiscono alla realizzazione dell'hardware dei sistemi E/E/PE sono ulteriormente approfonditi nell'art. 7 e nella fase dieci.
L'approvazione dell'impiego di tecnologia ASICS permetterà lo sviluppo e l'omologazione di componenti evoluti come quelli in bus di campo.

Terza parte - 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'art. 7 e nella fase dieci.
In entrambe le parti due e tre, l'art. 7 esamina e approfondisce i requisiti concernenti, l'integrazione, la validazione e modificazione dei sistemi E/E/PE, mentre l'ultimo articolo normativo 8 dettaglia la valutazione della sicurezza funzionale che, riferendosi ai requisiti dell'analogo art. 8 della prima parte, deve sempre rispondere ai requisiti di pianificazione, esecuzione, completezza, cor-

1. http://www.iec.ch/smartgrid/standards/

rettezza e precisione. In altre parole, quello che è stato specificato deve essere realizzato nonché validato per l'applicazione in sicurezza richiesta.
La tolleranza ai guasti hardware HFT (Hardware Fault Tolerance) oltre che con il 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 in 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 determinazione dei guasti hardware casuali è stata:
- rilevata dall'utilizzo in campo in similari applicazioni di processo e ambientali;
- elaborata statisticamente secondo Norme Internazionali IEC 20300-3-2 o ISO 14224;
- valutata in accordo alle quantità di dati di ritorno dall'utilizzazione, da test e da giudizi.

Il manuale di sicurezza è diventato obbligatorio; ogni componente e/o sistema ne dovrà essere dotato e dovrà contenere almeno i seguenti elementi:
- la specifica funzionale delle funzioni realizzate;
- l'identificazione dell'hardware e del software per consentire l'integrazione;
- le istruzioni e i vincoli da rispettare per evitare guasti sistematici.

Inoltre, per ogni funzione devono essere specificati:
- 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 hardware e software;
- la fault tolerance hardware e software;
- la classificazione in tipo A e tipo B;
- la configurazione raccomandata;
- le istruzioni per l'installazione.

Le rimanenti parti 4, 5, 6 e 7 sono state revisionate aggiornando la bibliografia, aggiungendo esempi riguardo alle metodologie di determinazione del SIL, inserendo maggiori informazioni sul calcolo della probabilità e miglior descrizione sulle tecniche di modellazione probabilistica: *reliability block, fault tree, Markov*.
Alla revisione della norma hanno contribuito i membri del SottoComitato 65A - *Aspetti di sistema* del CEI con commenti che sono stati inclusi nel nuovo documento.
Ci piace citare tra questi, con riferimento alla parte quarta, relativa alle definizioni, la rivisitazione del termine *harm - danno.*

Harm - Danno
Danno fisico o danneggiamento della salute del personale, o un danno all'ambiente o alla proprietà.
La proprietà (tangibile o intangibile) deve essere salvaguardata solo quando **non in contrasto** con quella della salute delle persone o dell'ambiente.

La versione precedente era ambigua ai fini della valutazione del rischio mentre la nuova esplicita che la macchina non è equiparabile all'uomo e all'ambiente, cosa non da poco conto nel rispetto della tecno-etica.
Siamo così riusciti a tradurre alcuni concetti, precedentemente relegati alla *science fiction*, in realtà da applicarsi quotidianamente.

Acronimi
ASICS = Appliacation Specific Integrated Circuits
E/E/PE = Elettrici/Elettronici/Elettronici Programmabili
EUC = Equipment Under Control
HFT = Hardware Fault Tolerance
SFF = Safe Failure Fraction
SIS = Safety Instrumented System
SrS = Safety related System

** Perito Industriale Laureato - Delegato del Collegio dei Periti Industriali e dei Periti Industriali Laureati delle province di Milano e Lodi presso il Comitato Elettrotecnico Italiano (CEI) al SC65A - Aspetti di Sistema*