La sicurezza nell'innovativa norma IEC 61508 funzionale

di **Fabio Andreolli*** **e Iuri Mazzarelli****

LA NORMA SULLA SICUREZZA FUNZIONALE È ILLUSTRATA DETTAGLIATAMENTE IN TUTTE LE SUE CARATTERISTICHE E IMPLICAZIONI. L'ADOZIONE DI QUESTI STANDARD (INTEGRATI DA NORME COLLEGATE) COSTITUISCE IL GIUSTO COLLANTE TRA EVOLUZIONE TECNOLOGICA E ASSICURAZIONE DEI PRINCIPI DI SAFETY NELL'UTILIZZO DI ATTREZZATURE E IMPIANTI

Lo stato dell'automazione nei sistemi di sicurezza di macchine ed impianti si evolve rapidamente a seguito della continua ricerca in settori portanti quali l'elettronica e l'elettronica programmabile (PLC, DCS, DSP, ecc.).
Le norme di prodotto sono in genere obbligate ad inseguire tale progresso nei processi di fabbricazione; talvolta si pensa che l'assenza di adeguati riferimenti normativi sia a vantaggio delle condizioni di garanzia nel funzionamento di attrezzature e impianti, mentre in altri casi si trascura (data la non obbligatorietà dell'applicazione normativa) l'esistenza di standard normativi utilissimi che costituiscono la regola dell'arte.
In quest'ultima casistica rientra certamente la norma IEC 61508 che indica i criteri di realizzazione al fine di ottenere un livello di *"sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili (E/E/EP) per applicazioni di sicurezza"*.
La prima versione della norma è del 1998; l'ultima revisione è stata recepita dall'IEC nel 2001 e riprende in modo organico concetti espressi da più norme relative ad aspetti connessi fra loro, ad esempio blocchi di sicurezza, affidabilità dei sistemi e valutazione del rischio.
La serie di norme IEC 61508 è stata recepita dal CENELEC e successivamente adottata dal CEI nel 2002 con validità dal 01/01/2003; è in lingua originale inglese (non è attualmente tradotta in italiano) ed è costituita da sette parti come riportato in tabella 1.
E' una norma di tipo "stand alone", in quanto non contiene solo gli aspetti applicativi relativi ai sistemi di misura e controllo dei processi industriali, ma anche tutti gli aspetti generali di descrizione delle metodologie, proponendo un metodo che considera l'affidabilità in termini *quantitativi*.
E' in atto una revisione della serie IEC 61508 che la dovrebbe trasformare in una norma di base e di riferimento per le metodologie di carattere generale, da utilizzarsi come supporto a settori differenti ovvero a tipologie di attrezzature differenti; si spera che nel tempo diventi norma armonizzata alle varie direttive di prodotto.
Su analoghi principi e metodi della IEC 61508 sono state emanate norme applicabili a settori o apparecchi specifici; ad esempio industria di processo (IEC 61511), sicurezza delle macchine (IEC 62061), segnaletica di controllo nel settore ferroviario (EN 50126 - EN 50128 – EN 50129), centrali elettriche a combustibile nucleare (IEC 61513), regolazioni

Tabella 1

IEC	CENELEC	CEI	Argomento
IEC 61508-1	EN 61508-1	CEI 65-74	Requisiti generali
IEC 61508-2	EN 61508-2	CEI 65-75	Requisiti dei sistemi E/E/PE
IEC 61508-3	EN 61508-3	CEI 65-76	Requisiti del software
IEC 61508-4	EN 61508-4	CEI 65-77	Definizioni ed abbreviazioni
IEC 61508-5	EN 61508-5	CEI 65-78	Esempi di determinazione dei livelli di integrità di sicurezza
IEC 61508-6	EN 61508-6	CEI 65-79	Guida all'applicazione delle 61508-2 e 61508-3
IEC 61508-7	EN 61508-7	CEI 65-80	Panorama delle tecnologie e delle misure tecniche

Si veda la figura 1 per i contenuti delle varie parti della norma

di velocità e carico negli azionamenti (IEC 61800-5-1).
A breve verranno completate le fasi di approvazione per altri settori a rischio specifico, ad esempio aerospaziale, automobilistico, marino, medicale.
Alcune norme armonizzate a particolari direttive di prodotto fanno espresso riferimento alla IEC 61508 per regolare gli aspetti legati alla sicurezza funzionale, la Norma UNI EN 574 ed UNI EN 954 armonizzate alla Direttiva Macchine 93/68/CE, la EN 13463-6 ed EN 15089 armonizzate alla Direttiva ATEX 94/9/CE (prodotti destinati ad atmosfere esplosive) e la EN 764-7 armonizzata alla Direttiva PED 97/23/CE (attrezzature in pressione).
L'argomento, vasto e complesso, richiede una specifica professionalità nell'approccio e nel metodo. Probabilmente la mancanza del requisito di armonizzazione della norma ne limita attualmente un'applicazione diffusa e una corretta comprensione. La stessa IEC fornisce nel proprio web site uno specifico spazio (http://www.iec.ch/zone/fsafety/) dove oltre a brevi descrizioni introduttive sullo standard è possibile scaricare gratuitamente alcuni documenti divulgativi.
E' da notare, tuttavia, come settori ad elevata automazione abbiano comunque destinato parte degli investimenti allo studio ed alla ricerca su nuovi prodotti conformi ai requisiti della IEC 61508, oltre a richiedere ulteriori approfondimenti in EMC e *Security* (fig. 1).

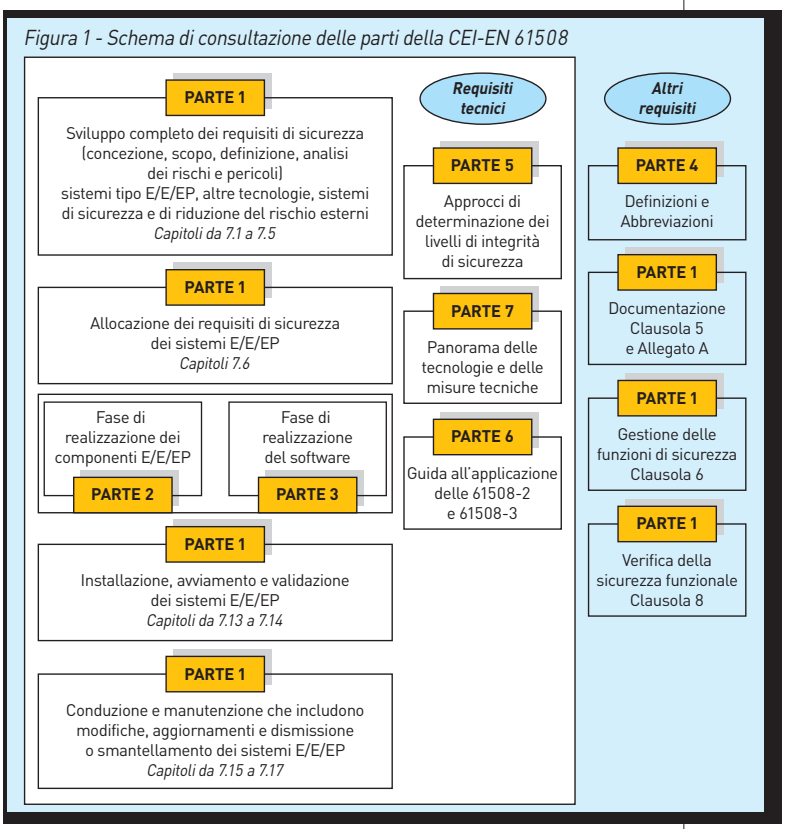
Definizioni di base della IEC 61508

Alcune definizioni di base contenute nella norma sono le seguenti.
Electrical/Electronic/Programmable Electronic System ovvero sistemi per il controllo, protezione, osservazione che hanno uno o più apparati elettrici, elettronici, elettronici programmabili. Includono tutti gli elementi del sistema come alimentazione elettrica, sensori, ed altri apparati di input, data highways (reti di comunicazione dati), ed altri sistemi di comunicazione, attuatori ed altre attrezzature di emissione comando.
Safety Function (funzione di sicurezza) ovvero la funzione che deve essere implementata per ridurre un pericolo o mantenere uno stato di sicurezza per l'attrezzatura sotto controllo rispetto ad uno specifico evento pericoloso.
Safety Related System ovvero il sistema progettato per ottenere, da solo o con altri sistemi E/E/SEP (dispositivi elettrosensibili) o con altre tecnologie, il livello di integrità richiesto dalle funzioni di sicurezza identificate.
Safety Integrity Level (SIL) ovvero la probabilità richiesta ad un sistema di sicurezza per effettuare correttamente le sue funzioni in tutte le condizioni previste. Il SIL è funzione dell'affidabilità dei componenti selezionati e della frequenza di prova stabilita. **Quindi la funzione di sicurezza deve rientrare in una condizione di affidabilità misurata dal SIL.**

La Sicurezza Funzionale

Una volta valutato, quantitativamente o dimensionalmente, un rischio ci si pone l'obiettivo di ridurlo fino ad un livello accettabile. Per ottenere questo si interpongono dei livelli di sicurezza che sottraggono quantità di rischio fino ad un livello, denominato residuo, che dovrà corrispondere o, meglio ancora, superare i nostri obiettivi iniziali. Ogni livello sarà composto di elementi specifici che potranno essere inerenti, sia interni che esterni. Dimensionando a seconda delle specifiche peculiarità o necessità ogni elemento si avranno contributi diversi e quindi quantità di rischio proporzionalmente sottratta (fig. 2).
La sicurezza funzionale aumenta il livello di *protezione inerente*.
Un tipico esempio è quello di evitare il superamento del livello di rischio definito accettabile, come quello di una pressione ammissibile per un'attrezzatura. Questa funzione di sicurezza (o sicurezza funzionale) potrebbe essere svolta da una valvola di regolazione che assicuri un livello di pressione su una linea in determinate condizioni di rischio dell'impianto e nel contempo garantisca valori di regolazione nel funzionamento ordinario.
Verificate le probabilità numeriche che la catena di sicurezza fallisca alla richiesta di intervento in caso di anomalie di esercizio (inclusi gli errori umani e di funzionamento valutati come rischio), senza trascurare il fatto che il medesimo componente svolge numerose operazioni nel funzionamento ordinario, que-

Figura 1 - Schema di consultazione delle parti della CEI-EN 61508



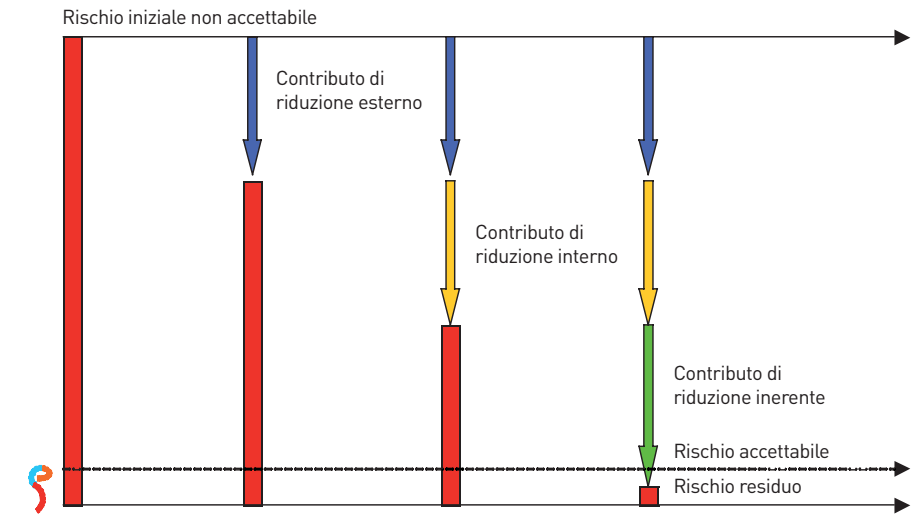


Figura 2 - Riduzione del rischio ad un livello accettabile

sta potrebbe affiancarsi o addirittura sostituire una protezione passiva (ad esempio un riduttore di pressione a coefficiente volumetrico fisso).

Si intuisce che, se da un lato l'adozione estensiva della sicurezza funzionale incentiva la sempre minor adozione di dispositivi attivi di mitigazione (esempio valvole di sicurezza, dischi di rottura, ecc.), dall'altro impone uno standard tecnologico di elevata affidabilità e costantemente in funzione per ricoprire nuove funzioni di prevenzione.

Tutte le Direttive di prodotto che fondano la sicurezza sul principio di affidabilità, associano a tale requisito quello di autodiagnosi del sistema di sicurezza al fine di assicurarne la *Continua Disponibilità*. Spesso le norme armonizzate impongono anche l'adozione di alimentazioni di sicurezza elettriche (si veda la Norma CEI-EN 64-8 per i requisiti di tali alimentazioni oppure la UNI 10616).

Essenzialmente il SIL è legato ai tassi di guasto dei singoli componenti e la valutazione del SIL trae origine da metodologie di calcolo di affidabilità della catena specifica adottata.

Si impone pertanto l'impiego di dispositivi di qualità elevata che il mercato ha recepito con una rapida ed importante immissione di prodotti ad alta fidatezza e di informazioni sui tassi di guasto dei singoli componenti.

E' facile notare, nella determinazione del SIL, che tale analisi numerica va oltre i requisiti cogenti di una Direttiva di prodotto, la quale in genere non regolamenta accuratamente aspetti legati alla manutenzione. L'approccio della IEC 61508 invece impone la scelta di tempi di controllo (*Interval Test - proof test*) e dell'eventuale ripristino dei requisiti del singolo componente della catena (tempo medio di riparazione MTTR).

Spesso il livello di SIL determina anche la ridondanza da adottare (ad esempio logiche 2/3, ecc.).

Lo standard di realizzazione deve essere associato ad uno standard elevato di verifica, la Norma IEC 61508 introduce la figura dell'*Advisor/Assessor* (Esperto di supporto/Perito): questi è deputato a validare ogni procedura concepita dal fabbricante nella realizzazione del prodotto, presunto conforme, e ad assisterlo nella corretta realizzazione del fascicolo tecnico da allegarsi al prodotto.

I fabbricanti si devono perciò avvalere di una *Terza Parte* che può essere ricercata, in modo facoltativo, all'interno della loro azienda ma con funzioni esterne al processo di produzione, oppure di un Professionista o di un Ente Notificato. Il fascicolo con relativa dichiarazione di conformità sarà poi reso disponibile al certificatore di impianto.

Un sostanziale e immediato obiettivo da perseguire nell'adozione di sistemi di sicurezza programmabili è quello di evitare la manipolazione non autorizzata o non intenzionale del software o di altri elementi della catena. In effetti anche se la CEI-EN 61508-3 (requisiti del software) ha in via di sviluppo il concetto di *security*, non richiama espressamente tale eventualità, mentre le norme armonizzate (esempio la UNI-EN 764-7) impongono tale requisito all'intero sistema di sicurezza.

E' importante ricordare che la Norma CEI-EN 61508 può essere sempre utilizzata come riferimento per il corretto approccio della sicurezza funzionale in qualunque campo tecnologico di applicazione, invece non è applicabile la valenza tra norme di settore: ad esempio non si possono avere ambivalenze tra la CEI-EN 61511 (impianti di processo) e la CEI-EN 62061 (equipaggiamento macchine).

Al momento, non è possibile sostenere analoghi ragionamenti per i sistemi di comando di macchine legati alla sicurezza così come descritti ed adottati da UNI-EN 954-1 (ISO-TC199).

Applicazione nell'industria di processo

La Norma IEC 61508 è stata ispiratrice della Norma IEC 61511 specifica per la sicurezza funzionale nell'industria di processo.

Anche la IEC 61511 è in lingua originale inglese; attualmente non è tradotta in italiano ed è in vigore dal 01/04/2006; il titolo completo è: CEI EN 61511 - *"Functional safety – Safety instrumented systems for the process industry sector"* e si compone delle parti riportate in tabella 2.

Il recepimento integrale della stessa norma da ANSI/ISA (ente normativo statunitense), con la pubblicazione S84.01 che contiene in più la *"Grandfather Clause"* relativa alla valutazione del rischio, è da consi-

Tabella 2

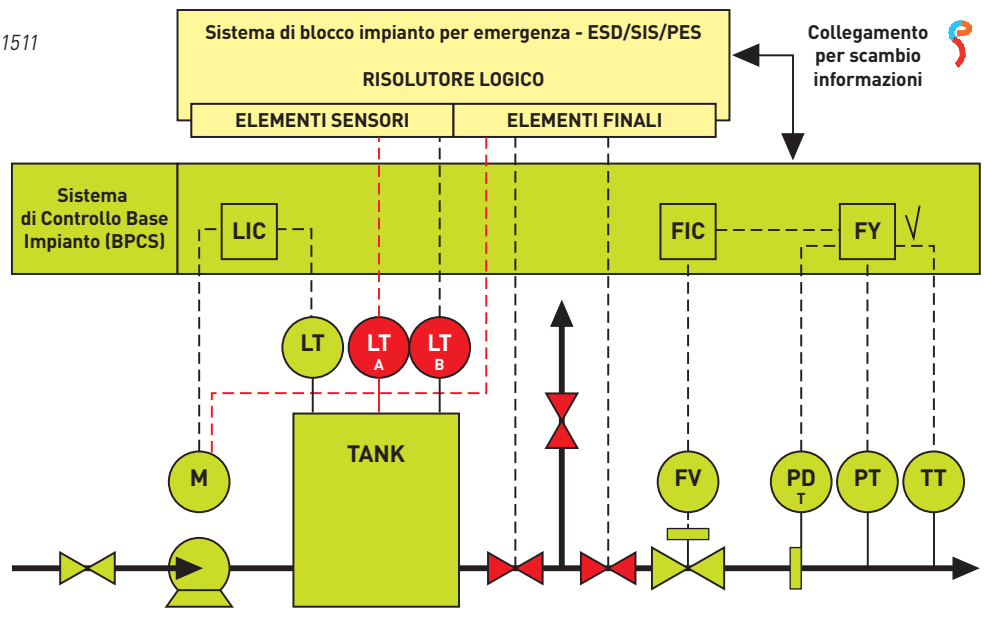
IEC	CENELEC	CEI	Argomento
IEC 61511-1	EN 61511-1	CEI-90	Struttura, definizioni, sistema, requisiti hardware e software
IEC 61511-2	EN 61511-2	CEI-91	Guida all'applicazione della EN 61511-1
IEC 61511-3	EN 61511-3	CEI-92	Guida alla determinazione dei livelli di integrità di sicurezza

derarsi una piccola vittoria europea in ambito internazionale.
L'applicabilità di tale norma è ristretta all'industria di processo, adegua il SIL a tale settore specifico, estende la catena relativa alla sicurezza (SIS) con le definizioni *sensors* (elementi sensibili) - *logic solver* (risolutore logico) - *final elements* (elementi di controllo finali).
Per aumentarne la divulgazione sarà emessa, prevedibilmente nel 2007, la traduzione in lingua italiana, mentre per incrementarne la corretta applicazione i membri del sottocomitato 65A stanno lavorando ad una guida applicativa aderente alla realtà nazionale da pubblicarsi successivamente.
Anche in questo caso deve essere prodotto un fascicolo con dichiarazione di conformità da sottoporsi al certificatore, esteso all'impianto e pertanto redatto dal costruttore dell'impianto e non limitato a quello di prodotto. L'applicazione della IEC 61511 è utile per ottenere *i sistemi di allarme e blocco automatico*, per i parametri operativi critici e i *blocchi di emergenza degli impianti tecnologici* da attuare per i rapporti di sicurezza previsti dal D.Lgs. 334/99 "Attuazione della Direttiva 96/82/CE, concernente il controllo dei pericoli di incidenti rilevanti connessi con determinate sostanze pericolose".
Sempre riguardo ai grandi impianti, questa si integra con la rivelazione incendio e gas (Fire & Gas System, fig. 3).

UNI-EN 764-7 e i Sistemi di Misurazione Controllo e Regolazione per la Sicurezza (SRMCR)

Appare evidente che finché la IEC 61508 non assume il carattere di norma armonizzata è auspicabile un continuo richiamo obbligatorio ad essa da parte di norme armonizzate a direttive di prodotto specifiche. Ad esempio la UNI-EN 764-7 (Sistemi di sicurezza per attrezzature a pressione non esposte a fiamma) introduce già espressamente come riferimento normativo la IEC 61508 quale requisito da ottenere per i *Sistemi di Misurazione Controllo e Regolazione per la Sicurezza (SRMCR).*
Questi sistemi, per mezzo di un'attrezzatura di controllo automatico funzionante indipendentemente da altre funzioni di controllo del processo, evitano che i parametri di esercizio superino i limiti ammissibili di pressione.
Il SRMCR può gestire il processo (ovvero regolarlo entro i limiti ammissibili) interromperlo (chiusura all'entrata materiale), isolare le cause di sovrapressione o le fonti di riscaldamento (blocchi compressori e pompe, ecc.).
La progettazione del SRMCR **deve** avvenire utilizzando i principi esposti nella IEC 61508 e deve essere progettato con *SIL* idoneo per lo svolgimento della funzione necessaria.
Tale condizione di affidabilità (*SIL*) deve essere determinata da una valutazione dei rischi; la CEI-EN 61508 sarà appunto adottata per il processo di riduzione dei rischi (concetto richiamato quale principale misura di tutela dalle Direttive Sociali, D.Lgs. 626/94).
Un altro aspetto rilevante dei sistemi di sicurezza funzionale è quello dell'indipendenza da altre funzioni di controllo. Ciò non vieta di usare i segnali provenienti

Figura 3 - Esempio applicativo CEI-EN 61511



dai sistemi per altre funzioni, quanto piuttosto impone di separare le funzioni di attuazione, regolate dal sistema di sicurezza, da altre funzioni non riguardanti la sicurezza legata alla grandezza su cui intervenire.
Questo assicura la mancanza di interferenze o reazioni non volute del sistema stesso; in tal caso l'interferenza deve essere intesa in senso ampio, inclusi i recenti concetti di compatibilità elettromagnetica (Direttiva 2004/108/CE).
In ultimo il sistema di sicurezza deve avere un'indicazione di stato, deve essere dotato di indicatori visivi e uditivi o segnali di avvertimento per il controllo della disponibilità del sistema/componente e dello stato di attivazione.
L'indicazione dello stato del sistema deve essere situata presso il pannello di controllo del processo oppure presso il sistema di controllo distribuito. L'indicazione dello stato dei componenti deve essere situata in posizioni simili o presso il dispositivo, in base alle necessità. Tale requisito è stato spesso adottato per derogare ad eventuali obblighi normativi, come la conduzione dell'impianto direttamente nel sito di installazione (nel caso dei generatori di vapore), con meno rischiose conduzioni da sale controllo.

Conclusioni

La Norma CEI-EN 61508 costituisce un validissimo ed utile supporto a valutazioni numeriche direttamente collegabili ai principi per la valutazione del rischio della UNI-EN 1050, norma armonizzata alle principali direttive di prodotto.
L'applicazione dei concetti espressi dalla CEI-EN 61508 deve essere correlata necessariamente ai requisiti essenziali di sicurezza richiesti dalle direttive stesse (affidabilità, ridondanza, fail-safe, autocontrollo).
In alcuni casi i regolamenti o le specifiche tecniche nazionali per varie tipologie di impianti sono datati e non evolvendosi nel tempo risultano incoerenti con l'elevato livello di automazione esistente, procurando limiti applicativi e qualche volta barriere indirette nell'evoluzione tecnologica.
Per questo motivo l'adozione di standard normativi come la CEI-EN 61508, seppur integrati da norme collegate, correttamente applicati e verificati, risulta il giusto collante tra evoluzione tecnologica e assicurazione dei principi di sicurezza nell'utilizzo di attrezzature e impianti.

Fonti - Bibliografia

CEI-EN-EN 61508 - *Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza*
UNI-EN 764-7 - *Attrezzature a pressione. Sistemi di sicurezza per attrezzature a pressione non esposte a fiamma*
ANSI/ISA - *The Instrumentation, Systems, and Automation Society*
Iuri Mazzarelli, *"L'attuale quadro normativo per le attrezzature a pressione ed il miglioramento delle specifiche tecniche nazionali"* - ISPESL Dipartimento di Milano

*Fabio Andreolli, delegato del Collegio dei Periti Industriali e Periti Industriali Laureati delle Province di Milano e Lodi presso il Comitato Elettrotecnico Italiano (CEI), Sottocomitato 65A - Sistemi.
**Iuri Mazzarelli, ISPESL Dipartimento di Milano, delegato UNI