Attività di normazione tecnica sulla sicurezza funzionale: stato attuale e sviluppi futuri

Emanuele Ciapessoni

Il tema della sicurezza dei sistemi d'automazione viene considerato in ambito CEI e IEC sotto due aspetti: Sicurezza Funzionale (SF) e Security dei sistemi e delle comunicazioni. La Sicurezza Funzionale (SF) è quella parte della sicurezza globale dei processi e sistemi (Equipment Under Control), inclusivi dei relativi sistemi di controllo, che dipende dal corretto funzionamento dei sistemi elettrici, elettronici ed elettronici programmabili (E/E/EP) per applicazioni di sicurezza, di altri sistemi tecnologici per applicazioni di sicurezza, di dispositivi esterni per la riduzione del rischio. La Security dei sistemi e delle comunicazioni è quella parte della sicurezza che dipende da meccanismi di protezione da intrusioni informatiche nei sistemi di automazione, controllo e protezione. L'articolo introduce i problemi relativi alla sicurezza in ambito industriale e illustra lo stato e gli sviluppi futuri delle attività di normazione tecnica nell'ambito del TC65 dell'IEC. Il lavoro presentato è basato sulle attività di ricerca svolta dal CESI (Centro Elettrotecnico Sperimentale Italiano Giacinto Motta), nell'ambito del progetto Norme/Automazione della Ricerca di Sistema[1] sulla tematica della sicurezza dei sistemi di automazione.

Keyword
Normativa, Sicurezza, Sicurezza Funzionale, Safety, Security.

Oramai da decenni, le funzioni vitali per la gestione degli impianti sono affidate a sistemi automatici di protezione, controllo, monitoraggio e supervisione. Questi stessi sistemi sono generalmente distribuiti all'interno degli impianti e dipendono da una rete di comunicazione locale e/o da collegamenti remoti che ne consente il controllo distribuito e remoto.
Le mutate politiche aziendali, i vantaggi in termini di costo, d'interoperabilità e di disponibilità stanno portando sempre più ad utilizzare prodotti HW e SW di mercato, spesso personalizzabili su esigenze specifiche, consentendo di salvaguardare e supportare specifiche esigenze dell'utente. In questo quadro, il corretto funzionamento e la sicurezza degli impianti viene sempre più a dipendere dalle prestazioni, in termini di *affidabilità* e *sicurezza*, dei sistemi d'automazione e dell'infrastruttura di comunicazione. Pertanto la sicurezza dei sistemi è sempre più un obiettivo imprescindibile e un bene sociale, cui è associato anche un valore economico.
A livello normativo questo tema è considerato in particolare nell'ambito dell'attività normativa relativa ai sistemi di misura e controllo dei processi industriali e cioè dal TC 65 dell'IEC: infatti, la progettazione, la realizzazione e l'esercizio di sistemi automatici per la protezione, il controllo e l'automazione degli impianti, richiede profonde conoscenze di tipo sistemistico.
La normativa tecnica di supporto dello sviluppo dei sistemi d'automazione riflette il loro carattere trasversale ed è conseguentemente molto vasta e articolata, riguardando sia i sistemi nel loro complesso, attività sviluppata nell'ambito SC 65A, sia i vari elementi che lo costituiscono, con riferimento il SC 65B, sia le comunicazioni, nel SC 65C.

SC-65 in particolare

Il SC 65A (sottocomitato A del comitato tecnico TC 65) ha sviluppato la norma trasversale IEC 61508 relativa alla SF "Functional safety of Electrical/ Electronic/Programmable Electronic safety-related systems", che rappresenta un riferimento per l'intera industria e sulla sua base sono stati definiti, e sono in corso di definizione, standard settoriali specifici per l'industria di processo, per il nucleare, in ambito elettromedicale, e in prospettiva per il sistema elettrico.
Il SC 65C, dopo aver sviluppato la normativa relativa alle

Emanuele Ciapessoni, CESI Ricerca S.p.A.

[1]Attività finanziata nell'ambito della "Ricerca di Sistema" per il Settore Elettrico (Decreto 28.02. 2003, "Modalità di gestione del Fondo per il finanziamento delle attività di ricerca e sviluppo di interesse generale per il sistema elettrico nazionale", Ministero per le Attività Produttive")

Terminologia

Fidatezza: è la proprietà di un sistema per cui si può giustificabilmente avere fiducia nel servizio fornito da un sistema. La fidatezza di un sistema richiede diverse sotto-proprietà complementari: l'affidabilità, la disponibilità, la manutenibilità, la safety e la security, essenziali per il servizio o a missione.

Affidabilità *: è la capacità di un sistema ad adempiere alla funzione richiesta per un periodo di tempo stabilito ed in determinate condizioni operative. Matematicamente, l'affidabiltà R(t) è una funzione del tempo che esprime la probabilità condizionale che un servizio soddisfi la funzione del sistema (servizio corretto) durante l'intervallo di tempo $[t_0, t]$, quando un servizio corretto è eseguito al tempo t_0.

Disponibilità: è la capacità di un sistema o di un componente di svolgere una funzione richiesta in determinate condizioni a un dato istante, o durante un dato intervallo di tempo, supponendo che siano assicurati i mezzi esterni eventualmente necessari. Matematicamente, la disponibilità A(t) è la probabilità che un servizio svolga la funzione del sistema (servizio corretto) al tempo t.

Manutenibiltà: è l'attitudine a consentire riparazioni ed evoluzione del servizio. Maintainability è una misura del tempo di ripristino (dal servizio scorretto al servizio corretto) dall'ultimo failure sperimentato. Matematicamente, la maintainability M(t) è la probabilità condizionale che un servizio non soddisfi la funzione di sistema (servizio scorretto) durante l'intervallo $[t_0, t]$, quando un servizio non corretto è consegnato al tempo t_0.

Safety: è la capacità di un sistema di evitare rischi inaccettabili.
Tra i rischi si possono considerare i danni alla salute delle persone, i guasti agli impianti e i problemi alla missione o al servizio con le conseguenti perdite economiche. La safety richiede il conseguimento del migliore bilanciamento dei vari fattori (inclusi quelli non tecnici, quale il comportamento umano) che elimina i rischi evitabili di danni a persone, cose [UNI CEI EN 45020].

Sicurezza Funzionale (Functional Safety): è una specializzazione della Safety ed è quella parte della sicurezza globale dei processi e dei sistemi (Equipment Under Control - EUC), inclusivi dei relativi sistemi di controllo, che dipende dal corretto funzionamento dei sistemi Elettrici, Elettronici ed Elettronici Programmabili (E/E/EP) per applicazioni di sicurezza, di altri sistemi tecnologici per applicazioni di sicurezza, di dispositivi esterni per la riduzione del rischio.

Security: è la fidatezza di un sistema rispetto alla prevenzione di accessi non autorizzati e/o di trattamenti indesiderati delle informazioni e richiede la conservazione di: riservatezza (garantire che le informazioni siano accessibili solo a chi è autorizzato ad averne accesso); integrità (salvaguardare l'accuratezza e la completezza delle informazioni e dei beni collegati quando necessario); disponibilità (assicurare che gli utenti autorizzati abbiano accesso alle informazioni ed ai beni collegati quando necessario).

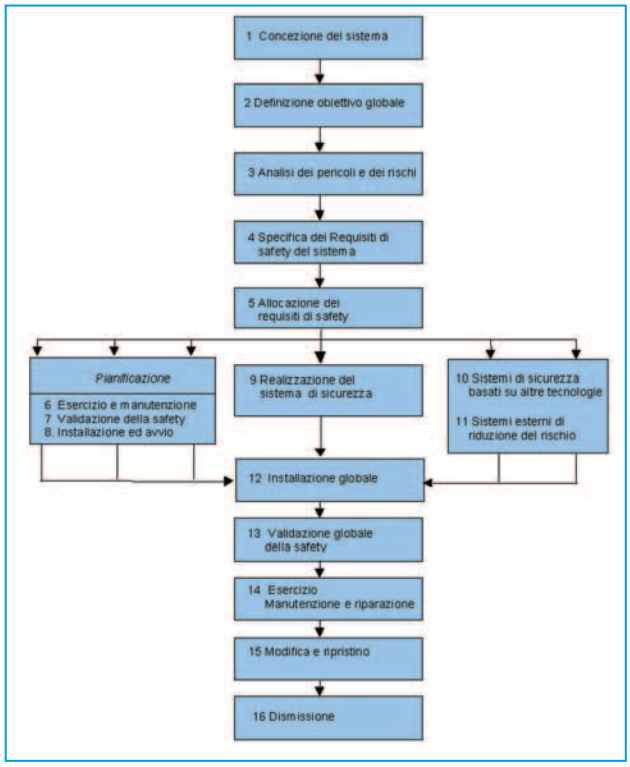
** Quando la missione ha una durata definita, viene anche utilizzato [MIL-STD-785B] il concetto di affidabilità della missione. Questa è la capacità di un sistema di svolgere la funzione richiesta per la durata della missione.*
Matematicamente l'affidabiltà di missione è la probabilità che un sistema, funzionante al tempo t_1, risulti ancora funzionante al tempo t_1+t_m, dove t_m è il tempo di missione. L'affidabilità di missione è una misura della fornitura continua del servizio corretto durante la missione di un sistema. In altre parole, è la probabilità che, sotto condizioni stabilite, il sistema continui ad operare correttamente, per tutta la durata della missione, supposto che esso sia in condizioni di perfetta operatività all'inizio della missione stessa.

comunicazioni industriali (fieldbus), sulla base della IEC 61508 sta definendo i profili di comunicazione per applicazioni safety critical: "Digital data communications for measurement and control - Part 3: Profiles for functional safe communications in industrial networks". Il problema riguarda la definizione dei profili di comunicazione delle reti utilizzate in ambito industriale che garantiscano livelli di SF adeguati nella protezione/controllo e automazione dei sistemi, comprendendo anche gli impianti elettrici.
Analogamente, sulla base delle norme esistenti relative alla security, nel SC 65C si stanno definendo i profili per la comunicazione sicura nelle reti industriali e le modalità da adottare per garantire la security delle comunicazioni industriali. Il TC 65 sta definendo norme trasversali per la security industriale dei sistemi di automazione. Tra i nodi affrontati c'è l'individuazione delle modalità più opportune per trattare le relazione tra safety e security e l'individuazione di metodologie per lo sviluppo di sistemi che garantiscano un adeguato livello di security.

Gli standard sulla sicurezza dei sistemi

Considerate le crescenti esigenze di sicurezza dei sistemi, questa tematica sta ricevendo una particolare attenzione nell'ambito del TC 65. Il carattere trasversale della normativa sui sistemi di misura e controllo dei processi ha portato, infatti, a considerare il TC 65 un comitato pilota per alcuni temi particolarmente importanti e di carattere emergente come quello della sicurezza dei sistemi elettrici, elettronici ed elettronici programmabili (E/E/EP) destinati a funzioni di sicurezza, la cosiddetta *Sicurezza Funzionale* (SF) e quello della *Security industriale* dei sistemi e delle comunicazioni, e cioè quella parte della sicurezza globale che dipende da meccanismi di protezione da intrusioni informatiche, verso il quale negli ultimi anni sta crescendo l'interesse e la sensibilità nell'ambiente industriale. Affrontare questi problemi richiede di considerare in modo globale il problema del rischio per garantire l'affidabilità del servizio e i necessari requisiti di robustezza, integrità e sicurezza degli impianti e dei sistemi d'automazione. Un fatto analogo sta succedendo con riferimento al tema della security.

Il TC 65 e i sistemi di misura e controllo dei processi industriali
L'attività normativa relativa sui sistemi di misura e controllo dei processi industriali è svolta a livello internazionale principalmente dalla IEC (International Electrotechnical



Il ciclo di vita della sicurezza come definito dallo standard IEC 61508

Commission), e più precisamente dal Comitato Tecnico TC 65 "Industrial process measurement and control", strutturato in quattro sottocomitati (SC A, B, C e D), che opera in collaborazione con il corrispondente Comitato Tecnico TC 184 "Industrial automation" della ISO (International Standardization Organization).

A livello italiano l'attività nel settore della normativa sui sistemi di controllo dei processi industriali è svolta dal comitato tecnico CT 65 del CEI, strutturato analogamente al corrispondente comitato della IEC. L'attività di questo comitato consiste essenzialmente nella partecipazione attiva ai lavori internazionali ed europei e nel recepimento a livello nazionale della totalità delle norme europee e di alcune norme internazionali IEC, che pur non avendo le corrispondenti CENELEC, sono state ritenute di particolare interesse per l'industria italiana.

La normativa tecnica sui sistemi di misura e controllo dei processi industriali, sviluppata nell'ambito del TC 65, si propone fondamentalmente di:

- definire le caratteristiche generali dei sistemi di misura e controllo dei processi industriali, sia di tipo continuo che discontinuo (batch);
- normalizzare i singoli elementi e sottosistemi, compresi quelli d'interfaccia e di comunicazione, dal punto di vista funzionale e delle prestazioni, per la loro integrazione nei sistemi completi.

Rientrano nella prima categoria le norme riguardanti: la terminologia, le condizioni ambientali, la compatibilità elettromagnetica (EMC), la sicurezza funzionale dei sistemi, la valutazione delle proprietà dei sistemi, la caratterizzazione dei sistemi di controllo batch.

Rientrano invece nella seconda categoria le norme riguardanti: i sensori, gli attuatori e gli analizzatori, i blocchi funzionali, i controllori programmabili, i sottosistemi di comunicazione, la valutazione delle prestazione dei singoli dispositivi, la sicurezza delle cabine degli analizzatori.

La sicurezza funzionale

La norma IEC 61508 "Functional safety of E/E/PE safety related systems", sviluppata dal SC 65A —che tratta appunto il tema della sicurezza funzionale e che dopo la pubblicazione IEC, è stata successivamente recepita dal CENELEC e adottata come Norma CEI nel 2002— non riguarda solo gli aspetti applicativi relativi ai sistemi di misura e controllo dei processi industriali, ma anche tutti gli aspetti relativi alle metodologie da applicare nello sviluppo dei sistemi per la sicurezza, non disponibili in altre norme di riferimento.

Invero, la norma IEC 61508 trae origine da altri standard relativi all'affidabilità dei sistemi e alla valutazione del rischio; la novità della normativa consiste, oltre al considerare l'affidabilità in termini quantitativi, nel porre la gestione di un progetto o lo sviluppo di un prodotto in uno schema organico di assicurazione degli obiettivi, che parte dalla sua concezione e si conclude con la sua dismissione.

Questa impostazione ha fatto sì che sono oggi disponibili sul mercato internazionale apparecchiature e sistemi per la sicurezza funzionale d'impianti certificati in conformità alla IEC 61508 e molte attività d'ingegneria, per le fasi di sviluppo e verifica del progetto dei sistemi strumentali e degli impianti in cui essi saranno installati, sono organizzate secondo i suoi criteri.

La norma definisce i criteri di progettazione e gestione dei sistemi E/E/PE utilizzati per garantire un livello di sicurezza adeguato in tutti i settori industriali in cui possono presentarsi rischi per le persone, l'ambiente o perdite economiche. Si

La sicurezza funzionale secondo la IEC 61508

Secondo la IEC 61508, la sicurezza funzionale è quella parte della sicurezza globale dei processi e sistemi (Equipment Under Control), inclusivi dei relativi sistemi di controllo, che dipende dal corretto funzionamento di: sistemi elettrici, elettronici ed elettronici programmabili (E/E/EP) per applicazioni di sicurezza; altri sistemi tecnologici per applicazioni di sicurezza; dispositivi esterni per la riduzione del rischio.

Ad esempio: un sistema di protezione che utilizzi un sensore termico sugli avvolgimenti di un motore elettrico e che agisca togliendo l'alimentazione prima che sopraggiunga il surriscaldamento, realizza una funzione di sicurezza necessaria alla sicurezza funzionale di un impianto. Questi sistemi per la sicurezza agiscono implementando delle funzioni di sicurezza (Safety Functions) il cui scopo è quello di mantenere il sistema da controllare in uno stato sicuro al verificarsi di un evento pericoloso.

noti che la norma richiede di specificare requisiti per la prevenzione delle *failure* e per il loro controllo; a valle della specifica, si progetterà e realizzerà il sistema di protezione, che dovrà poi essere verificato e validato rispetto ai requisiti.
A tal fine la norma introduce il ciclo di vita in sicurezza di un sistema (Safety-Life-cycle), che richiede: la concezione del sistema; l'analisi del contesto (ambiente) dell'impianto e la determinazione dei suoi confini; l'analisi dei rischi dell'impianto in tutte le possibili situazioni; l'allocazione delle *safety functions* nei sistemi strumentali per la sicurezza; la specifica funzionale delle *safety functions* e del loro necessario livello di integrità con l'obiettivo di minimizzare i rischi e di massimizzare il fattore di servizio; la pianificazione dell'esercizio e della manutenzione dei sistemi di sicurezza al fine di garantire la funzionalità e l'affidabilità nel tempo; l'analisi quantificata dell'affidabilità dell'HW dei sistemi strumentali per la sicurezza; un approccio rigoroso allo sviluppo del SW che realizza le funzioni di sicurezza; la validazione dei sistemi per la sicurezza funzionale (Functional Safety Assessment).
In tal senso la IEC 61508 non è solamente una guida alla gestione della sicurezza industriale: essa vuole introdurre i concetti fondamentali di gestione della *Safety* e di *Safety Engineering*. Si può notare come questi concetti non siano totalmente nuovi, ma provengono da quei mondi dell'ingegneria dove l'analisi dei requisiti rappresenta già un caposaldo, come ad esempio l'ingegneria del software.
L'innovazione di base introdotta dallo standard consiste nel richiedere un'attenta analisi del dominio applicativo (in altre parole della situazione di un impianto controllato relativamente alla safety), base per definire successivamente i requisiti che il sistema di protezione dovrà soddisfare al fine di garantire la safety del sistema (o, dualmente, per abbattere il rischio associato all'impianto controllato). In particolare, giacché non è possibile annullare i rischi, lo standard richiede di valutare il livello di rischio residuo per verificare il raggiungimento dei requisiti di sicurezza. Per sistemi critici, la certificazione dovrà quindi essere svolta da personale indipendente dai progettisti del sistema di sicurezza in modo da garantire l'oggettività del risultato.
La norma basa la progettazione dei sistemi di sicurezza sul concetto di *Safety Integrity Level* (SIL), livello d'integrità della sicurezza associato ad ogni *safety function*, e di conseguenza al sistema di strumentazione che la realizza e che deve essere identificato fin dalle prime fasi del ciclo di vita dei sistemi. L'adozione del concetto di SIL mira a semplificare la progettazione delle catene di strumentazione che realizzano le funzioni di sicurezza. A tal fine la Norma (vedi Tabella 1) definisce valori discreti di SIL da 1 a 4, in ordine crescente d'integrità, cui corrispondono intervalli decrescenti di probabilità di fallimento della funzione di sicurezza stessa.
Si noti la distinzione tra il funzionamento a bassa richiesta, per il quale si specifica la probabilità di fallimento per ogni singolo evento e quello ad alta richiesta (o continuo), per il quale si specifica la probabilità di fallimento per ora di funzionamento. Per la sua trasversalità e la complessità del tema affrontato, la IEC 61508 è suddivisa in sette parti, le prime tre si occupano di definire il processo di valutazione dei requisiti di safety, d'analisi del rischio e dell'implementazione delle funzioni di sicurezza; le successive quattro si occupano di fornire esempi e metodologie per l'analisi e la gestione del rischio. Essendo una norma di tipo generico, la IEC 61508 è utilizzabile direttamente sia nei diversi settori industriali in cui sono utilizzati sistemi E/E/PE per applicazioni di sicurezza, sia per la

Mappa dei requisiti sulle parti della IEC 61508

Parte 1 - Requisiti generali; descrive tutti requisiti ed i passaggi da compiere all'interno del safety lifecycle e si spiega come effettuare il functional safety assessment.
Parte 2 - Requisiti per i sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza; la fase del safety lifecycle, riguardante la specifica dei requisiti per le funzioni di sicurezza (fase 9), viene qui dettagliata nel contesto dell'utilizzo di sistemi basati prettamente sull'hardware per l'implementazione delle funzioni di sicurezza.
Parte 3 - Requisiti del software; Come nella 61508-2 si fa per l'hardware, la parte 3 dettaglia gli aspetti relativi all'utilizzo del software per l'implementazione delle funzioni di sicurezza (fase 9 del ciclo di vita della safety).
Parte 4 - Definizioni ed abbreviazioni; definisce i termini specifici relativi alla gestione della sicurezza funzionale utilizzati nello standard.
Parte 5 - Esempi di metodi per la determinazione dei livelli di integrità e sicurezza; fornisce definizioni ed esempi riguardanti il concetto di rischio, di SIL e di allocazione del SIL.
Parte 6 - Guida all'applicazione delle IEC 61508-2 e IEC 61508-3; oltre a fornire, come suggerisce il titolo, una guida all'applicazione dello standard, presenta le metodologie per valutare e calcolare le probabilità di guasto, l'effetto delle cause comuni di guasto (common cause failure) ed altro ancora.
Parte 7 - Panorama delle tecnologie e delle misure tecniche; è una rassegna di metodi per valutare e controllare i guasti hardware casuali e sistematici e per effettuare una corretta specifica del software.

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Probability of failure to perform its design function on demand)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per hour)
4	$>=10^{-5}$ to $<10^{-4}$	$>=10^{-9}$ to $<10^{-8}$
3	$>=10^{-4}$ to $<10^{-3}$	$>=10^{-8}$ to $<10^{-7}$
2	$>=10^{-3}$ to $<10^{-2}$	$>=10^{-7}$ to $<10^{-6}$
1	$>=10^{-2}$ to $<10^{-1}$	$>=10^{-6}$ to $<10^{-5}$

Tabella 1 - Livelli d'Integrità dei Sistemi

definizione di norme più specializzate per quei settori industriali ove si ritenga necessaria e opportuna una maggiore specificità delle prescrizioni d'affidabilità, con l'assistenza di un apposito gruppo di coordinamento del SC 65A: sicurezza funzionale dei sistemi di protezione e controllo degli impianti industriali di processo (IEC 61511); sicurezza funzionale dei sistemi di protezione e controllo del macchinario (IEC 62061); sicurezza funzionale dei sistemi di protezione e controllo degli impianti nucleari (IEC 61513). Per altri settori, come il settore elettrico nell'ambito della Ricerca di Sistema [4], sono in corso attività prenormative che mirano a identificare le esigenze specifiche di questi settori al fine di proporre lo sviluppo da parte dell'IEC di normative specifiche.
Per estendere ulteriormente l'applicabilità e la trasversalità della IEC 61508 nell'ambito del SC 65A del IEC è in corso una sostanziale revisione della norma stessa, che porterà a trasformarla in una norma di riferimento per le metodologie di sviluppo dei sistemi per la sicurezza funzionale. La nuova norma mantiene l'impostazione della norma attuale, in particolare nei principi di base relativi all'utilizzo dei SIL nella progettazione dei sistemi d'automazione. Al fine di rendere più rigoroso il processo di progettazione, sviluppo e verifica, cambia invece profondamente nei requisiti imposti nelle fasi del ciclo di vita dei sistemi. Sono inoltre considerate le tecnologie ASIC (Application Specific Integrated Circuits) e FPGA (Field Programmable Gate Array), le applicazioni di tipo Data Driven e Object Oriented non comprese nella norma in vigore.

La security nell'ambito dell'automazione

Il fatto che la *vulnerabilità* dei sistemi e quindi la loro *security* sia un problema cruciale nell'automazione, specialmente nei domini tradizionalmente considerati safety critical, come il nucleare, nelle industrie spaziale, in campo aeronautico, chimico o ferroviario, è un fatto riconosciuto a tutti i livelli. La sola sicurezza funzionale infatti, non è sufficiente per garantire la sicurezza degli impianti: il problema delle vulnerabilità dei sistemi distribuiti d'automazione è infatti sempre più critico per la sicurezza, in senso generale, degli impianti e delle infrastrutture di rete. Tuttavia paradossalmente, alcuni elementi di base dei sistemi, come i protocolli di comunicazione, sono stati definiti e progettati con scarsa attenzione alla sicurezza: il protocollo TCP/IP ad esempio, base dei protocolli più diffusi anche in ambito industriale, non prevede meccanismi d'identificazione, confinamento e recupero degli errori o d'identificazione delle intrusioni. Allo stato attuale questi meccanismi devono essere esplicitamente integrati nei sottosistemi di comunicazione, adottando estensioni dei protocolli che garantiscono i necessari requisiti di sicurezza (come ad esempio il Secure TCP e in futuro l'IPv6) o gestendo il problema della sicurezza a livello applicativo.
Ovviamente, l'utilizzo di protocolli standard come il TCP/IP non impone necessariamente l'adozione di reti di comunicazione aperte. Tuttavia, secondo una tendenza diffusa, la manutenzione del sistema stesso e delle sue componenti più importanti si appoggia spesso su reti aperte. Chiaramente in questa situazione le vulnerabilità dei sistemi d'automazione sono destinate a crescere e di conseguenza la sicurezza globale degli impianti a ridursi.
Quanto ai sistemi operativi, nell'ambito dei sistemi distribuiti d'automazione non è più sufficiente garantirne l'affidabilità, ma è necessario adottare misure cautelative tese ad evitare che vulnerabilità informatiche possano ridurre la sicurezza. Questo aspetto è particolarmente critico nel caso di sistemi utilizzati per la sicurezza funzionale degli impianti stessi.
Peraltro, la *security ICT* e la *security industriale* sono diverse sotto molti aspetti, cosa che rende più difficile la protezione dei sistemi d'automazione dalle vulnerabilità informatiche. Secondo il rapporto [ISA TR99], ad esempio: " ... i piani di security dei sistemi d'impianto e di controllo sono consistenti con l'esperienza, i programmi e la prassi maturata in ambito IT. Esistono tuttavia differenze operative critiche tra i sistemi IT e quelli d'impianto e di controllo che influenzano le modalità di applicazione delle specifiche misure ... "
Per il corretto funzionamento dei sistemi d'automazione risulta chiara la necessità di definire meccanismi in grado di garantire i necessari requisiti di *security industriale*. Difatti i meccanismi di protezione dell'ICT hanno obiettivi e adottano strategie non appropriate per i sistemi di protezione, controllo e automazione.
Un chiaro esempio delle differenze tra la security ICT e quella industriale è legato all'importanza attribuita nei due ambiti ai requisiti di base della security (vedi appendice sulla terminologia): nel caso dei sistemi ICT, secondo gli standard [ISO/IEC 17799], [ISO/IEC 15408], la riservatezza è considerata la proprietà più importante, seguita da *integrità* e *disponibilità*, che ha impatto solo sul servizio; nel caso dei sistemi d'automazione, per i quali i requisiti di real time sono spesso critici per la sicurezza, le proprietà più importanti sono la disponibilità e l'integrità.
Inoltre nell'ambito dell'automazione, le proprietà della security hanno caratteristiche specifiche che li distinguono dalle analoghe proprietà IT:
- *Disponibilità (real time)* delle informazioni: le funzioni di security non devono interferire con l'accesso alle informazioni necessario alla SF dei sistemi, salvo nel caso in cui questa interferenza sia richiesta per garantire altri obiettivi di security. Se compatibile con altri obiettivi, le funzioni di security dovrebbero permettere l'identificazione d'interferenze indebite con la disponibilità delle informazioni. Inoltre deve essere possibile identificare, con un ben definito livello di confidenza, ritardi o risequenzializzazioni non autorizzate dei messaggi;
- *Integrità*: modifiche non autorizzate o manipolazioni dei messaggi devono essere identificate con un ben definito livello di confidenza.

Si noti in particolare che nell'ambito dell'automazione, oltre a richiedere requisiti di real time, deve essere possibile garantire un ben definito livello di confidenza alle proprietà di disponibilità e integrità delle informazioni e nell'identifica-

segue a pag. 81

Security	Sistemi ICT	Sistemi d'automazione
Rischi	Perdita di fidatezza dei sistemi ICT. Perdita di risorse, tempo, denaro	Perdita di fidatezza dei sistemi di automazione. Conseguenze indirette sulla safety globale degli impianti
Disponibilità	Deve essere garantita nel normale orario d'ufficio	La perdita di disponibilità può causare problemi di sicurezza funzionale. Deve essere garantita 24/24h - 7/7gg
Integrità	Essenziale per il business	La perdita di integrità dei dati d'impianto può causare problemi di sicurezza funzionale
Riservatezza	L'accesso non autorizzato può comportare problemi legali	L'accesso non autorizzato può comportare problemi di sicurezza funzionale
Gestione delle emergenze	Chiusura delle applicazioni, Shutdown dei sistemi, Backup/Restore dei dati	Le reazioni devono essere tempestive. Può essere necessario lo shutdown dell'impianto
Architettura e prestazioni di rete	Le architetture sono a grafo, separazione intranet/internet Le prestazioni non sono critiche	Le architetture sono distribuite. Devono essere garantiti tempi di risposta definiti
Protocolli	TCP/IP è il protocollo standard	Protocolli standard di settore, come la IEC 61850, la IEC 870-5/101…104, …
HW e SW dei sistemi	Sistemi operativi di mercato collaudati per applicazioni d'ufficio o transazionali	HW e SW di base devono essere real time. I meccanismi di autenticazione e autorizzazione devono essere efficienti
Aggiornamenti HW e SW	Per garantire la security il SW è aggiornato frequentemente	Gli aggiornamenti richiedono verifiche di regressione (Regression Test)

Tabella 2 - La security nei sistemi ICT e nei sistemi d'automazione

zione/autorizzazione degli attori della comunicazione.
In questo quadro, un altro aspetto della normativa sviluppata nell'ambito del TC 65 sul quale è opportuno soffermarsi è quello relativo ai sottosistemi di comunicazione, in relazione soprattutto alla sicurezza dei sistemi d'automazione distribuiti.
L'attività di normazione tecnica relativa ai sistemi di comunicazione, svolta dal SC 65C, si è sviluppata dagli anni '80 a sostegno dell'automazione distribuita. Il primo tema affrontato è stato quello delle comunicazioni di campo (fieldbus), viste come lo strumento indispensabile per permettere alle applicazioni, distribuite su vari microprocessori embedded nei dispositivi di campo come attuatori e trasduttori, di cooperare per realizzare la soluzione specificata.

ISO	International organization for standardization	www.iso.org
IEC	International Electrotechnical Commission	www.iec.ch
CENELEC	European Committee for Electrotechnical Standardization	www.cenelec.org
CEI	Comitato Elettrotecnico Italiano	www.ceiweb.it
UNI	Ente Nazionale Italiano di Unificazione	www.uni.com
ISA	Instrument Society of America	www.isa.org

Tabella 3 - Enti normativi e associazioni

Dopo l'approvazione delle norme IEC 61158 e IEC 61784 per l'automazione distribuita degli impianti, che definiscono una serie di protocolli di comunicazione utilizzati nei sistemi di controllo industriale, nell'ambito del SC 65C è in corso la definizione di norme a supporto della sicurezza delle comunicazioni industriali: il WG12 e il WG13.
Il *WG12 del SC 65C* (Comunicazioni funzionalmente sicure) mira ad identificare i principi di base per l'implementazione dei requisiti della IEC 61508 per le comunicazioni *safety related*, considerando gli *errori di trasmissione*, i relativi *rimedi* e l'*integrità dei dati*. Inoltre la norma specifica profili per la comunicazione di dati *safety related* come estensioni dei *profili di comunicazione fieldbus*, che danno la necessaria garanzia nel trasporto dei messaggi o nell'individuazione delle *failure* in una rete di comunicazione safety related. Il Draft 2 è stato rilasciato nel luglio 2005; lo Standard è previsto per l'estate del 2007.
Il *WG13 del SC 65C* (Security delle comunicazioni industriali) identifica i principi di base necessari per

garantire la security delle comunicazioni industriali, includendo l'integrità dei messaggi, autenticità delle sorgenti, l'autorizzazione delle azioni, il trattamento dei ritardi e la non ripudiabilità dei messaggi. Questa norma definirà nuovi profili di comunicazione security-related per le diverse famiglie di profili di comunicazione industriale. Il Draft 1 è stato rilasciato nel luglio 2005; lo Standard è previsto per l'estate 2007.

Per completare il quadro delle attività di normazione tecnica in corso nell'ambito del TC 65, con l'obiettivo generale di garantire la security dei sistemi di automazione distribuiti, il WG10 del TC 65 sta definendo norme specifiche per *security industriale dei sistemi d'automazione* rivolte:

- Ai progettisti di sistemi d'automazione: per identificare i requisiti utente (ad esempio per identificare gli *asset* da *proteggere*); per identificare i *vincoli utente* (ad esempio la *security policy*, i *vincoli operativi*); per definire l'architettura del sistema di security (ad esempio i *domini di sicurezza* e i *punti di controllo*).
- Ai fornitori di componenti e per gli integratori di sottosistemi e sistemi: per specificare i *livelli di sicurezza*; per guidare l'implementazione dei *meccanismi di security*; per essere la base per la valutazione delle *funzionalità di security*.
- Agli utenti finali (responsabili dell'esercizio degli impianti): per guidare l'esercizio; per essere una base per gli *audit* e le valutazioni.

Lo standard fornirà linee guida e metodologie per la definizione dei requisiti di security, dei meccanismi e dell'architettura di protezione dei sistemi, considerando le esigenze di: *migrazione/evoluzione* dei sistemi esistenti ; *affidabilità/disponibilità* dei servizi di comunicazione sicura; *scalabilità* delle architetture, per garantire l'applicabilità dello standard in tutti i contesti industriali; *separazione* dei requisiti di sicurezza funzionale da quelli di security, introducendo modi di fallimento (fail-over modes) che siano sicuri per il processo.

Come nel caso della sicurezza funzionale, e per mantenere la compatibilità con la relativa normativa, la metodologia adottata per la definizione del livello di security richiesto ai sistemi e per la definizione delle funzioni di security (Security Functions), sarà basata sull'analisi dei rischi associati alle vulnerabilità di un sistema, considerando le minacce, la probabilità del loro verificarsi e l'impatto sugli impianti e tenendo conto delle contromisure scelte.

I meccanismi e le architetture che saranno adottati consentiranno di rendere sicura la trasmissione dei messaggi sia in una rete locale che geografica, trattando quindi anche gli aspetti di telecontrollo e di manutenzione remota. Altri aspetti considerati saranno la protezione dei programmi e dei dati, la verifica dell'identità dei dispositivi e degli operatori e la definizione delle relative autorizzazioni. Naturalmente per la comunicazione sarà previsto l'utilizzo di schemi di crittogra-

CEI 61508	Functional safety of E/E/PE safety related systems	IEC 2000
	Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza	CEI 2002
IEC 61508–0	Part 0 : Functional safety and IEC 61508.	
65A/413/DTR	A basic guide (Draft Technical Report).	IEC 2004
CEI 61508–1	Part 1 : General requirements	IEC 1998
	Parte 1 : Requisiti generali	CEI 2002
CEI 61508–2	Part 2 : Requirements for E/E/PE safety related systems	IEC 2000
	Parte 2 : Requisiti per i sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza	CEI 2002
CEI 61508–3	Part 3 : Software requirements	IEC 1998
	Parte 3 : Requisiti del software	CEI 2002
CEI 61508–4	Part 4 : Definitions and abbreviations	IEC 1998
	Parte 4 : Definizioni ed abbreviazioni	CEI 2002
CEI 61508–5	Part 5 : Examples of methods for the determination of safety integrity levels	IEC 1998
	Parte 5 : Esempi di metodi per la determinazione dei livelli di integrità e sicurezza	CEI 2002
CEI 61508–6	Part 6 : Guidelines on the application of IEC 61508-2 and IEC 61508-3	IEC 2000
	Parte 6 : Guida all'applicazione delle IEC 61508-2 e IEC 61508-3	CEI 2002
CEI 61508–7	Part 7 : Overview of measures and techniques	IEC 2000
	Parte 7 : Panorama delle tecnologie e delle misure tecniche	CEI 2002
CEI 61511	Functional safety – Safety instrumented systems for the process industry sector	IEC 2003
	Sicurezza funzionale dei sistemi di protezione e controllo degli impianti industriali di processo	CEI 2005
IEC 61511–1	Part 1: Framework, definitions, system, hardware and software requirements	IEC 2003

fia interoperabili, necessari a garantire la compatibilità dei sistemi d'automazione.

Conclusioni

Come si è visto, l'attività di normazione tecnica sviluppata dal TC 65 mira a definire metodi di sviluppo, basati sull'analisi del rischio, che possano garantire la safety e la security dei sistemi.
Dato il carattere generale della normativa sulla sicurezza funzionale, anche se all'interno della stessa sono compresi esempi e guide, la sua applicazione risulta alquanto difficile per i non addetti ai lavori e molte iniziative sono in atto per illustrarne e divulgarne le finalità e i contenuti; la stessa IEC, riconoscendo la centralità di questa normativa, ha predisposto un sito dedicato alla sicurezza funzionale [1]. La situazione sta in ogni caso evolvendosi nel senso che in tutti i settori interessati alla sicurezza funzionale (industria di processo, trasporti, macchinario, azionamenti, domotica, ecc.) sono nate o stanno nascendo norme di settore che sviluppano l'aspetto applicativo rimandando per gli aspetti metodologici alla serie IEC 61508.
Oltre a considerare la sicurezza funzionale, il TC 65 sta considerando il problema della security industriale, con l'obiettivo di standardizzare i criteri di progettazione e di gestione dei sistemi d'automazione che possono presentare vulnerabilità informatiche. Lo scopo è far sì che un sistema svolga la propria missione, e in particolare garantire la sicurezza degli impianti, anche in presenza di situazioni inattese, come attacchi informatici, che possono derivare dall'utilizzo improprio delle reti di comunicazione aperte. Presso il CESI, nell'ambito del progetto Norme/Automazione della Ricerca di Sistema per il settore elettrico, sono in corso studi e collaborazioni con i Gruppi di Lavoro nazionali (CEI) e internazionali (IEC) del TC 65, relativamente alla sicurezza funzionale e della security dei sistemi di protezione, controllo e automazione con particolare riguardo al sistema elettrico.

Riferimenti

[1] Sito IEC: www.iec.ch/zone/fsafety/fsafety_entry.htm
[2] J. C. Laprie, *Dependability: basic concepts and terminology*, Springer-Verlag, 1992
[3] J. C. Laprie, A. Avizienis, B. Randell, "Fundamental concepts of computer system dependability"; *IEEE Workshop on robot dependability*, Seoul, 2001
[4] E. Ciapessoni, L. Ferrarini, "Indagine sulla sicurezza funzionale dei sistemi di automazione delle reti elettriche", *Rapporto RdS progetto Norme Automazione*, Prot. A5052457

IEC 61511–2	Part 2 : Guidelines for the application of IEC61511	IEC 2003
IEC 61511–3	Part 3 : Giudance for the determination of required safety integrity levels	IEC 2003
IEC 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	IEC 2005 IEC 2001
IEC 61513	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	
IEC 62138	Nuclear power plants - Instrumentation and control important for safety Software aspects for computer-based systems performing category B or C functions	IEC 2004
IEC 61158 Part 1 - 8	Digital data communications for measurement and control - Fieldbus for use in industrial control systems	IEC 2003 - 2004
IEC 61784	Digital data communications for measurement and control - Part 1: Profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems	IEC 2003
ISO/IEC 15408	Information technology - Security techniques - Evaluation criteria for IT security	
ISO/IEC 15408-1	Part 1 : Introduction and general model	ISO/IEC 1999
ISO/IEC 15408-2	Part 2 : Security functional requirements	ISO/IEC 1999
ISO/IEC 15408-3	Part 3 : Security Assurance Requirements	in sviluppo
ISO/IEC 17799	Information Technology – Code of practice for information security management	ISO/IEC 2000
ISA-TR99.00.01	Security Technologies for Manufacturing and Control Systems	ISA TR 2004
ISA-TR99.00.02	Integrating Electronic Security into the Manufacturing and Control Systems Environment	ISA TR 2004
IEC 65/360/NP	Security for industrial process measurement and control Network and system security	WG10 del TC 65 IEC 2005