tutorial

Fonte: www.irlandando.it

SIL: Safety Integrity Level

LUCA MARANI

La norma IEC 62061 definisce i livelli d'integrità della sicurezza e i vincoli ai quali attenersi per evitare pericoli a persone e cose

Le norme SIL si collocano nell'ambito delle normative di sicurezza funzionale relative a dispositivi elettrici ed elettronici programmabili. Per una loro corretta comprensione è necessario avere un quadro completo delle diverse norme vigenti in questo settore. La norma generale a cui fare riferimento è la IEC 61508, che si applica a dispositivi elettronici, ad esempio sistemi elettromeccanici, sistemi elettronici allo stato solido e sistemi basati su PC, che sono utilizzati in ambienti con problematiche di sicurezza. Da questa norma ne derivano altre specifiche per diversi settori di applicazione o sottosistemi, ad esempio macchine, settore di processo o nucleare ecc. In particolare, dalla IEC 61508 deriva la IEC EN 62061, dove trovano definizione i livelli SIL, il cui titolo esatto è "Sicurezza del macchinario - Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili correlati alla sicurezza". La norma si applica ai sistemi di controllo utilizzati individualmente o in associazione, per eseguire funzioni di controllo relative alla sicurezza su macchinari non mobili e non portatili, mentre sono in funzione, compresi i gruppi di macchinari che operano insieme in modo coordinato. Essa si riferisce esclusivamente alle prescrizioni per la sicurezza funzionale, destinate a ridurre il rischio di lesioni o di danni alla salute di persone nelle immediate vicinanze del macchinario o direttamente coinvolte nell'uso dello stesso. È limitata ai rischi direttamente derivanti dai pericoli della macchina o di un gruppo di macchinari che operano insieme in modo coordinato; non specifica prescrizioni per le prestazioni di elementi di controllo non elettrici, che sono soggette ad altra norma (generalmente EN 954-1); non tratta i rischi elettrici derivanti dalla stessa apparecchiatura di controllo. La norma ha lo scopo di definire l'utilizzo anche di sistemi elettronici complessi per funzioni legate alla sicurezza, eventualità fino a non molto tempo fa mal vista, anche alla luce di un'incertezza legata alle prestazioni tecnologiche di questi sistemi. Lo scopo è raggiunto fornendo una metodologia in grado di assegnare il livello d'integrità di sicurezza richiesto per ogni funzione di controllo da realizzare, mediante Srecs (Sistemi di controllo elettrici relativi alla sicurezza).

Il valore dell'"integrità"

Con 'integrità della sicurezza' la norma indica la probabilità che uno Srecs o il suo sottosistema esegua in modo soddisfacente le funzioni prescritte relative alla sicurezza, in tutte le condizioni dichiarate. Più è elevato il livello d'integrità dell'elemento, minore è la probabilità che esso non svolga la funzione di controllo prescritta relativa alla sicurezza. L'integrità della sicurezza comprende un aspetto

hardware, relativo alle prescrizioni riguardanti la probabilità di guasti casuali pericolosi all'hardware e vincoli all'architettura, e un aspetto software, relativo alla capacità di quest'ultimo, in un sistema elettronico programmabile, di svolgere le sue funzioni di controllo relative alla sicurezza in tutte le condizioni dichiarate e in un intervallo di tempo dichiarato. Per comodità i livelli d'integrità della sicurezza sono stati discretizzati a tre, dove il livello 1 si colloca al gradino più basso e il 3 presenta la massima sicurezza. Il livello 4 non è presente in questa norma, ma si trova nelle norme IEC 61508-1 e IEC 61508-2 ed è riservato a impianti ad alta pericolosità, quali quelli di ambito petrolchimico. I livelli SIL si collegano al valore della probabilità di un guasto pericoloso per ora, secondo i valori riportati nella tabella 1. I dati con cui si assegna un valore di SIL sono basati su: stima qualitativa del rischio, frequenza e durata dell'esposizione, probabilità di evitare o limitare il danno,

Livello di integrità sicurezza	Probabilità di un guasto pericoloso per ora
3	≥ 10-8 a 10-7
2	≥ 10-7 a 10-6
1	≥ 10-6 a 10-5

Tabella 1: I livelli SIL si collegano al valore della probabilità di un guasto pericoloso per ora

Conseguenze	Gravità (Se)
Irreversibile: morte, perdita di un occhio o di un braccio	4
Irreversibile: rottura di uno o più arti, perdita di uno o più dita	3
Reversibile: richiede l'intervento di un medico	2
Reversibile: richiede le cure di un pronto soccorso	1

Tabella 2: Classificazione di gravità del danno per fare una stima del rischio

probabilità del verificarsi di un evento pericoloso. A titolo di esempio nella tabella 2 è riportata la classificazione di gravità del danno da utilizzare per la stima del rischio. Nella tabella 3, invece, si indica lo schema per la definizione del livello SIL in base alla classificazione della gravità del

Gravità (Se)	Classe CI				
	3-4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

Tabella 3: Definizione del livello SIL in base alla classificazione della gravità del danno e al parametro CI

danno e a un parametro CI. Quest'ultimo deriva da una somma di valori relativi a frequenza e durata dell'esposizione, probabilità di evitare o limitare il danno, probabilità del verificarsi di un evento pericoloso. Le norma afferma inoltre che i circuiti di sicurezza hanno una degradazione nel tempo, quindi devono essere soggetti a un'attività di controllo; la macchina deve essere corredata di un fascicolo tecnico (calcoli relativi alla sicurezza) e di un manuale di istruzioni per la manutenzione.

Indicazioni per il software

L'appendice C della norma tratta della progettazione e dello sviluppo del software incorporato per la realizzazione di funzioni di controllo relative alla sicurezza in uno Srecs. L'obiettivo principale è fornire una guida generale alla prevenzione dei guasti al software e di qualsiasi altro comportamento inatteso dello stesso, suscettibile di portare a guasti pericolosi nel sistema. La norma parla di vincoli imposti al software dall'architettura dell'hardware, vincoli che dovrebbero essere definiti e documentati. Le conseguenze di qualsiasi interazione hardware/software sulla sicurezza della macchina o del sistema monitorato dovrebbero essere identificate e valutate dal progettista, il quale deve tenerne conto nella realizzazione del software. Tra i vincoli sono annoverati: protocolli e formati, frequenze d'ingresso/uscita per fronte di salita o di discesa, per livelli di dati d'ingresso utilizzando logiche inverse ecc. L'elenco di tali vincoli permette la loro valutazione fin dall'inizio dell'attività di sviluppo e riduce il rischio d'incompatibilità tra software e hardware, quando il primo è installato nell'hardware indicato. Sono interessanti anche le specifiche relative alla progettazione del software, che devono comprendere: una descrizione dell'architettura del software, struttura definita per soddisfare le specifiche; ingressi e uscite, ad esempio sotto forma di un vocabolario dati interno ed esterno, per tutti i moduli che costituiscono l'architettura del software; interrupt; dati globali; ogni modulo di software (ingressi/uscite, algoritmo, particolarità di progettazione ecc.); moduli o librerie dati utilizzati; software preesistente utilizzato. Il software dovrebbe essere modulare e scritto in modo logico per facilitarne la verifica o la manutenzione. In particolare, ogni modulo o gruppo di moduli dovrebbe corrispondere, se possibile, a una funzione nelle specifiche e le interfacce tra i moduli dovrebbero essere le più semplici possibili. Le caratteristiche generali di una corretta architettura del software possono essere quindi riassunte nel modo seguente: un modulo dovrebbe possedere un livello elevato di coesione funzionale e una semplice interfaccia con l'ambiente. Inoltre, si dovrebbero limitare il numero o l'estensione delle variabili globali e controllare la disposizione delle matrici nella memoria, per evitare il rischio di superamento di memoria. Da quanto riportato la norma diventa per l'utilizzatore non solo un vincolo imprescindibile per quanto concerne gli aspetti legali, ma anche uno strumento di miglioramento della qualità del livello progettuale. ■