PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3765 di giovedì 21 aprile 2016

Una breve illustrazione della norma EN 61508-6:2010

Uno degli obblighi di un professionista della security è quello di tenersi aggiornato sulla evoluzione normativa anche relativa a problemi di sicurezza afferenti alle persone. La serie normativa IEC 61508. A cura di Adalberto Biasiotti.

Questa norma è una preziosa linea guida sull'applicazione di una serie di norme afferenti alla **sicurezza di apparecchiature elettriche, elettroniche o programmabili**, che vengono utilizzate nel garantire che macchinari di vario tipo possono essere utilizzati senza presentare un rischio per l'operatore.

A mio avviso, uno degli obblighi che incombe ad un professionista della security è quello di tenersi sempre aggiornato sulla evoluzione normativa, soprattutto quando essa fa riferimento a problemi di sicurezza non solo anticrimine, ma anche a problemi di sicurezza afferenti alle persone.
Questa è la ragione per la quale ho deciso di illustrare brevemente questa norma, che aiuta gli utenti ad applicare correttamente la **serie normativa IEC 61508-1, -2, -3, -4**.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[DVD018] ?#>

In molti macchinari, le funzioni di protezione dell'operatore e di sicurezza intrinseca del macchinario sono affidati ad elementi elettrici o elettronici, ormai da moltissimi anni. Anche i sistemi basati su computer, vale a dire sistemi a programmazione elettronica, vengono utilizzati spesso per sviluppare non solo funzioni non legate alla sicurezza, come la gestione automatica dei macchinari, ma anche funzioni legate alla sicurezza, per proteggere gli operatori.
A questo punto, un aspetto critico nella progettazione di questi macchinari è quello legato alla garanzia che gli apparati elettrici ed elettronici o computerizzati possano funzionare in modo affidabile, proteggendo in particolare la salute e l'integrità fisica dell'operatore.

Questa norma internazionale indica un approccio generico per la **progettazione di attività legate alla installazione di sistemi di protezione**, sia basati su componenti elettrici, sia su componenti elettronici o su sistemi ad elettronica programmabile, vale a dire computer. Questo approccio unificato è stato adottato per sviluppare in modo omogeneo le linee guida per queste apparecchiature critiche.
Una strategia di sicurezza deve prendere in considerazione non solo tutti gli elementi che si trovano all'interno di un sistema, come ad esempio i sensori, gli attuatori e simili, ma deve anche esplorare globalmente le relazioni tra questi apparati, onde garantire il rispetto di soddisfacenti livelli di sicurezza.
Questa linea guida introduce dei livelli di integrità dei dispositivi che permettono di raggiungere un soddisfacente livello di garanzia circa il fatto che le funzioni di questi apparati verranno rispettate e quindi i livelli di sicurezza saranno raggiunti.
Vengono anche indicati dei livelli di affidabilità funzionale, in modo che la probabilità media di una avaria pericolosa del dispositivo sia dell'ordine di una su 1.000.000, anche se il dispositivo è in funzione ventiquattr'ore su 24.

La linea guida stabilisce anche le regole per cercare di mettere sotto controllo dei guasti sistematici, che nascono dall'esperienza pratica accumulata in tanti anni nell'industria del settore. Anche se evidentemente non è possibile stabilire in forma analitica la probabilità che si verifichi un guasto sistematico, l'analisi storica di determinati apparati e architetture funzionali può offrire preziose indicazioni per il progettista.

Purtroppo, alla luce delle tecnologie utilizzate, la norma non riesce a raggiungere una definizione esplicita del concetto di "*fail safe*" anche se tali concetti, come pure il concetto di sicurezza intrinseca, possono essere applicati dal progettista, per soddisfare i requisiti imposti dallo standard.

La norma, assai corposa, perché ci troviamo davanti a 150 pagine di norma, analizza il quadro di riferimento afferente alla serie normativa 61508, con una serie di figure, e illustra quali siano le architetture da utilizzare, i livelli di affidabilità che possono essere raggiunti ed illustra anche un albero del guasto, connesso allo schema a blocchi, che illustra l'affidabilità.
Altre tavole sono dedicate alla verifica del software, all'architettura da adottare, alle modalità di prova ed alle funzioni di integrazione sistemistica.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.
