Certification

FUNCTIONAL SAFETY

Il rapido sviluppo dell'automazione e dell'intelligenza distribuita ha portato a un esponenziale incremento di macchinari, impianti, dispositivi e di prodotti in genere con sistemi di comando e controllo elettronici o elettronici programmabili, cui sono affidate **funzioni di sicurezza**.
Quando la funzionalità di un elemento all'interno di un sistema può pregiudicarne la sicurezza, la sicurezza primaria non basta più, deve esserne garantita la sicurezza funzionale. I temi trattati dalla norma IEC/EN 61508 e dalle norme da essa derivate (ISO 13849-1, ISO 16232, IEC 62061, IEC 61800-5-2, IEC 61496, EN 50495, ecc.), costituiscono lo stato dell'arte e il riferimento normativo per la progettazione e la gestione dei sistemi di sicurezza negli impianti, con particolare attenzione ai sistemi elettrici, elettronici ed elettronici programmabili e trovano largo impiego in **svariati settori industriali** come chimico, petrolchimico, raffinazione, nucleare, trasporti, elettromedicale, automazione industriale e automotive.

FUNCTIONAL SAFETY MANAGEMENT di TÜV INTERCERT è un **servizio modulare volontario** strutturato **a fasi** che nasce per supportare i costruttori che, nel progettare hardware e software sicuri, devono adottare tecniche specifiche come **ridondanza**, **diversità** e **test diagnostici interni** con l'obiettivo di aumentare la robustezza del prodotto verso errori casuali o sistematici.

Step 1: INITIAL ASSESSMENT

Verifica on-site del sistema; caratterizzazione del sistema; identificazione dei pericoli; analisi delle specifiche dei requisiti di sicurezza da soddisfare; verifica della documentazione tecnica (*data sheet* componenti, schemi elettrici, ecc.).

Step 2: RISK ASSESSMENT

Identificazione delle normative tecniche applicabili al sistema; analisi quali-quantitativa dei componenti del sistema (QFD – FMEA – FTA); analisi di affidabilità e disponibilità dei componenti del sistema; redazione della relazione di analisi dei rischi / gap analysis rispetto requisiti di sicurezza definiti; condivisione dei suoi contenuti.

Step 3: FOLLOW-UP

Controllo e verifica delle eventuali modifiche apportate al sistema dal cliente; verifica delle modifiche alla documentazione tecnica.

Step 4: SIL/PL EVALUATION

Verifica di sicurezza del concept design; analisi delle funzioni di sicurezza; analisi dei requisiti di sicurezza; analisi hardware/software; eventuali *witness testing*; valutazione del SIL/PL raggiunto; test sul software (analisi statica e test di modulo); test di integrazione hardware/software; esecuzione di eventuali prove di tipo (meccaniche e elettriche).

Step 5: FINAL REPORT & SIL/PL ATTESTATION

Rilascio del rapporto di fine attività e dell'attestazione del livello SIL/PL raggiunto per ciascuna funzione di sicurezza.

TÜV INTERCERT ITALIA
Via D. F. Cecati 1/1
42123 Reggio Emilia
t. 0522 409611
info@tuv-intercert.org
www.tuv-intercert.org

NORMATIVE
PER SETTORE DI RIFERIMENTO

Sicurezza Funzionale nell'Automazione Industriale

ISO 13849-1: sicurezza del macchinario

IEC 62061: sicurezza del macchinario

IEC 61496: apparecchi elettrosensibili di protezione

IEC 61800-5-2: azionamenti elettrici a velocità variabile

IEC 50156: equipaggiamento elettrico per forni e apparecchiature ausiliarie

ISO 15998: sistemi di controllo macchina (MCS) che utilizzano componenti elettronici

ISO 22201: ascensori

ISO 25119: trattori e macchine per l'agricoltura

Sicurezza Funzionale nel rischio Esplosione

EN 15233: metodologia per la valutazione della sicurezza funzionale di sistemi di protezione autonomi

EN 13463-6: apparecchi non elettrici destinati a essere utilizzati in atmosfere potenzialmente esplosive

EN 50495: dispositivi di sicurezza

EN 50402: apparecchiature elettriche per la rilevazione e la misura di gas o vapori combustibili o tossici, o di ossigeno

Sicurezza Funzionale nel settore Aerospaziale

US RTCA DO-178B: North American Avionics Software

US RTCA DO-254: North American Avionics Hardware

EUROCAE ED-12B: European Airborne Flight Safety Systems

Sicurezza Funzionale nel settore Automotive

ISO 26262: veicoli stradali

Sicurezza Funzionale nel settore Rail

EN 50126 (IEC 62278): RAMS

EN 50128 (IEC 62279): telecomunicazioni, segnalamento ed elaborazione – Software per sistemi di comando e protezione

EN 50129 (IEC 62425): sistemi elettronici di sicurezza per il segnalamento

Sicurezza Funzionale nel settore Medicale

IEC 60601-1: apparecchi elettromedicali

Sicurezza Funzionale dei prodotti di consumo

IEC 60730: standard di sicurezza per gli elettrodomestici

Legenda

FMEA Failure Mode and Effect Analysis
FTA Fault Tree Analysis
SIL Safety Integrity Level
PL Performance Level