SETTORE INDUSTRIA

Corso avanzato su Sicurezza Funzionale e Safety Integrity Level (SIL) dei Sistemi Elettrici, Elettronici ed Elettronici Programmabili per applicazioni di sicurezza in accordo allo standard IEC/EN 61508 (2010)

Italia

Scegli la certezza.
Aggiungi valore.

Cod. PSIL

Durata
32 ore. Orario: 9:00 - 18:00

Obiettivo
L'obiettivo del corso è di qualificare il personale tecnico ed i progettisti di componenti, macchine e impianti che includono sistemi di sicurezza di tipo E/E/EP (Elettrico, Elettronico, Elettronico Programmabile) al fine di:

- conoscere i concetti fondamentali legati alla Sicurezza Funzionale e i contenuti della norma IEC/EN 61508, le definizioni e la struttura dell'approccio metodologico alla verifica della sicurezza dei sistemi integrati (hardware/software),
- acquisire pratica con il Safety Life-Cycle previsto dalla norma IEC/EN 61508,
- attuare un'analisi dei rischi per l'assegnazione dei requisiti SIL alle funzioni di sicurezza,
- acquisire familiarità con i principali metodi di analisi RAMS (tecniche qualitative e quantitative quali FMECA, alberi dei guasti, schemi a blocchi, ecc.) per la verifica dei requisiti SIL dei sistemi di protezione realizzati con tecnologie E/E/EP,
- inquadrare l'approccio per la progettazione e realizzazione di software di sicurezza ai sensi della IEC/EN 61508,
- Acquisire le competenze per interagire con fornitori e clienti con riferimento alla Sicurezza Funzionale.

Programma
Durante il corso verranno trattati i seguenti argomenti.

1° giorno: La Sicurezza Funzionale – Aspetti generali, definizioni, struttura, contenuti e requisiti della norma [IEC/EN 61508-1, IEC/EN 61508-4]

- Introduzione e contesto,
- Principali definizioni,
- Struttura della norma (contenuti e applicabilità delle diverse sezioni; requisiti tecnici, gestionali e di supporto),
- Il Ciclo di Vita in Sicurezza Complessivo (*Overall Safety Life-Cycle*) e i requisiti generali delle singole fasi specifiche:
  - concezione e definizione degli scopi e ambiti complessivi,
  - analisi dei pericoli e dei rischi, requisiti di sicurezza complessivi (definizione e allocazione), specifica dei requisiti di sicurezza per i sistemi di protezione E/E/EP,
  - progetto e sviluppo dei sistemi di protezione E/E/EP e cicli di vita in sicurezza specifici per Hardware e Software,
  - planning per installazione e commissioning, validazione, operazione e manutenzione dei sistemi di protezione E/E/EP,

- installazione e commissioning,
- validazione del sistema,
- operazione e manutenzione,
- gestione delle modifiche,
- decommissioning e smantellamento,
- attività trasversali di verifica,

- Il *Functional Safety Management*: processi e requisiti,
- Gestione della Documentazione: requisiti e struttura,
- Il *Functional Safety Assessment* e i relativi requisiti di indipendenza.

***2° giorno*: La Sicurezza Funzionale – Analisi dei Rischi e dei Pericoli, Allocazione dei Requisiti di Integrità della Sicurezza Funzionale [IEC/EN 61508-5]**

- L'analisi di Sicurezza e di Rischio: concetti fondamentali,
- Richiami di Teoria delle Probabilità,
- Introduzione alle tecniche per l'identificazione dei pericoli e per la valutazione del rischio:
  - richiami al processo di identificazione dei pericoli,
  - richiami alle tecniche HAZID e HAZOP,
  - matrici di rischio e criteri di accettabilità del rischio,
  - analisi di criticità mediante la valutazione del rischio.
- Definizione e allocazione dei requisiti di sicurezza funzionale:
  - identificazione degli scenari di rischio,
  - identificazione delle funzioni di sicurezza e allocazione delle tecnologie applicative (sistemi di protezione E/E/EP o altre misure di riduzione del rischio),
  - assegnazione dei requisiti di integrità funzionale alle funzioni di sicurezza identificate e allocazione dei livelli di integrità della sicurezza (*Safety Integrity Level* – SIL) per le funzioni da implementare con tecnologie E/E/EP,
  - i concetti di Salvaguardia e di Barriere di Protezione Indipendenti (*Independent Protection Layer* – IPL),
  - le modalità operative delle funzioni di sicurezza (*Low Demand*, *High Demand*, *Continuous*),
- Le tecniche per l'allocazione dei requisiti di integrità funzionale:
  - tecniche qualitative semplificate (HAZOP & matrici di rischio parametriche),
  - tecniche qualitative di base (Grafi Calibrati di Rischio),
  - tecniche semi-quantitative (*Layer of Protection Analysis* – LOPA),
- Specificazione dei Requisiti di Sicurezza per le funzioni di protezione a supporto della progettazione dei sistemi di sicurezza con tecnologia E/E/EP.

***3° giorno*: La Sicurezza Funzionale – Progetto e Sviluppo di Sistemi di Protezione di tipo E/E/EP secondo i Requisiti di Integrità di Sicurezza, Attività di Verifica dei Requisiti SIL di Sistema per gli aspetti Hardware [IEC/EN 61508-2, IEC/EN 61508-6]**

- Introduzione alle attività di progetto e sviluppo di sistemi di protezione di tipo E/E/EP,
- Il Ciclo-Vita in Sicurezza specifico per la fase di progetto e sviluppo dei sistemi di protezione di tipo E/E/EP:
  - la specifica dei requisiti di design per sistemi di protezione E/E/EP,
  - la fase di planning delle attività di validazione,
  - la fase di progetto e sviluppo: requisiti legati alla progettazione dell'Hardware e all'interazione con lo sviluppo del Software,
  - la fase di integrazione del sistema,

- requisiti per le fasi di operazione e manutenzione, validazione e gestione delle modifiche,
- attività trasversali di verifica,

- Richiami di Teoria dell'Affidabilità e cenni all'Analisi RAMS di sistemi complessi:
  - introduzione all'Analisi di Affidabilità,
  - caratterizzazione dei componenti dal punto di vista affidabilistico e manutentivo, modelli di manutenibilità (componenti riparabili al guasto, riparabili quando testati, non riparabili, ecc.),
  - analisi FMECA e Analisi di Manutenibilità,
  - sorgenti di dati affidabilistici (banche dati commerciali, analisi dei dati da campo),
  - calcolo dell'affidabilità e disponibilità dei componenti,
  - analisi di affidabilità e disponibilità dei sistemi e relative tecniche quantitative: *Fault Tree Analysis* (FTA), *Reliability Block Diagrams* (RBD)
  - indici di criticità quantitativi,
  - le cause comuni di guasto (*Common Cause Failure* – CCF),
- I requisiti di Sicurezza Funzionale alla base del progetto di sistemi di protezione di tipo E/E/EP,
- Requisiti relativi all'*Hardware Safety Integrity*:
  - requisiti architettonico/funzionali (Route 1_H & Route 2_H), definizione e valutazione dei relativi parametri di riferimento (*Hardware Fault Tolerance* – HFT, *Safe Failure Fraction* – SFF, *Diagnostic Coverage* - DC),
  - requisiti probabilistici relativi ai guasti di tipo random dell'Hardware, definizione e valutazione dei relativi parametri di riferimento (*Probability of Failure per Demand* – PFD e *Probability of Failure per Hour* – PFH),
- Requisiti relativi alla *Systematic Safety Integrity*:
  - i concetti di *Systematic Failure* e di *Systematic Capability*,
  - requisiti per la prevenzione e il controllo dei guasti sistematici (Route 1_S),
  - requisiti per la classificazione di componenti come *proven in use* (Route 2_S),
  - requisiti per la dimostrazione di adeguatezza di software pre-esistente (Route 3_S),
- Requisiti per il comportamento del sistema a seguito di detezione di guasti pericolosi,
- Requisiti per gli aspetti di comunicazione e trasferimento di dati,
- Cenni ai requisiti relativi al progetto di Circuiti Integrati per Applicazioni Specifiche (*Application Specific Integrated Circuits* - ASIC) e per Circuiti Integrati con "*on-chip redundancy*".

***4° giorno*: La Sicurezza Funzionale – Cenni allo sviluppo di Software di Sicurezza secondo i requisiti di Sicurezza Funzionale [IEC/EN 61508-3] – Casi applicativi di Allocazione e Verifica di requisiti SIL per funzioni di sicurezza e sistemi di protezione di tipo E/E/EP**

- Introduzione, scopo e ambito di applicazione,
- Requisiti aggiuntivi per la Gestione della Sicurezza Funzionale del Software di Sicurezza (Management of Safety-Related Software) e Software Configuration Management,
- Cenni al Ciclo-Vita in Sicurezza specifico per lo sviluppo del Software e ai requisiti relativi a ciascuna fase:
  - specifica dei requisiti di sicurezza per il Software,
  - pianificazione delle attività di Validazione,
  - progetto e sviluppo del Software,
  - integrazione dei sottosistemi di tipo EP (Hardware & Software),
  - validazione del sistema di protezione per gli aspetti Software,
  - procedure per l'operazione e la manutenzione del Software,
- Relazione tra le fasi di progetto e sviluppo dell'Hardware e del Software,
- Cenni al V-Model per lo sviluppo del Software,

- Cenni ai requisiti per l'utilizzo di Software pre-esistente: Route 1_S (*compliant development*), Route 2_S (*proven in use*), Route 3_S (*assessment of non-compliant development*),
- Cenni ai requisiti per tool di supporto on-line e off-line per lo sviluppo del Software di sicurezza,
- Cenni ai requisiti specifici per Software "*data-driven*" (*fixed program*, *limited variability*, *full variability*) e alla non interferenza tra elementi Software implementati su un singolo computer.

- Esercitazione finale in aula e discussione:
  - caso applicativo di allocazione di requisito SIL per una funzione di protezione da realizzare con tecnologie E/E/EP nell'ambito di una unità di processo,
  - caso applicativo di verifica dei requisiti SIL per gli aspetti Hardware per un sistema di protezione di tipo E/E/EP da realizzare nell'ambito di una unità di processo.

Destinatari

Progettisti di componenti, macchine e impianti, responsabili e coordinatori di progetto, responsabili di manutenzione e personale tecnico.

Prerequisiti

Nessuno.

Docente

Il corso viene svolto da docenti qualificati TÜV Italia Akademie.

Materiale didattico

Dispensa, contenente le slides proiettate durante il corso.

Attestati

Attestato di Frequenza.