La sicurezza funzionale degli apparecchi a controllo elettronico

Ralf Hickl
Product sales manager microcontroller

Ileana Keges
Product sales manager microcontroller

Martin Motz
Product sales manager microcontroller

Rutronik Elektronische Bauelemente

Nel caso di applicazioni critiche è necessaria l'implementazione di una funzione di sicurezza in grado di rilevare gli errori in modo affidabile e una strategia atta a riportare il sistema in condizioni di sicurezza in un tempo prestabilito in caso di guasto

I meccanismi di controllo di natura elettronica sono sempre più diffusi – sia a bordo dell'auto, in produzione, in ambiente domestico, sia persino all'interno del corpo umano. Ciò che era in passato collegato tramite una connessione meccanica, oggi è regolato da sensori, dispositivi di controllo, bus di segnale, connessioni radio e azionamenti elettrici. In passato la sicurezza funzionale era garantita dal progetto e dal dimensionamento dei componenti meccanici. E oggi?

Per tutelare la vita e la salute umana, i dispositivi elettronici programmabili devono essere in grado di individuare in tempo reale e in modo affidabile eventuali errori e, in caso di guasto, ripristinare una condizione di sicurezza in un lasso di tempo prestabilito. Questo è ciò che richiedono le norme basate sullo standard IEC 61508. Tra le applicazioni tipiche, nelle quali la sicurezza rappresenta un aspetto critico, si possono segnalare montacarichi, controlli dei bruciatori nei sistemi di riscaldamento, airbag, sistemi X-by-wire e così via. Essi sono classificati secondo diverse classi di rischio, in base al potenziale danno provocato in caso di guasto, che sono denominate, in relazione alla norma di riferimento, ad esempio Livello di Integrità della Sicurezza (SIL – Safety Integrity Level) o Livello di Prestazioni.

Per tutte le norme vale il seguente concetto: per soddisfare i requisiti è necessaria l'implementazione di una funzione di sicurezza in grado di rilevare gli errori in modo affidabile e una strategia per riportare il sistema condizioni di sicurezza in un tempo prestabilito in caso di guasto.

Parallelamente a ciò, deve essere creato un modello matematico per l'affidabilità, con il quale calcolare la probabilità di guasto del sistema e l'affidabilità della funzione di sicurezza. Le normative di riferimento, come ad esempio IEC61508, o altre norme per un settore specifico derivate da queste ultime, come ISO 13849, definiscono un valore minimo ben preciso della funzione di sicurezza, affinchè possa definirsi affidabile. Il rispetto di questi valori deve essere dimostrato da un ente di certificazione, ad esempio il TUV.

Per il modello matematico dell'affidabilità sono necessari i valori dei tassi di guasto dei componenti del sistema (FIT – Guasti nel Tempo), oltre alla copertura del test di autodiagnosi, per garantire l'individuazione tempestiva dei guasti.

I valori empirici dei tassi di guasto sono ad esempio reperibili nella norma SN 29500 di Siemens e sono a disposizione dei produttori di componenti. Partendo da questi ultimi, il modello matematico dell'affidabilità del sistema fornisce

i dati che possono essere utilizzati per documentare gli aspetti della sicurezza richiesti dagli standard, da fornire all'Ente di certificazione. Una sfida per gli sviluppatori consiste nell'ottenere informazioni numeriche valide per ottenere i tassi di FIT richiesti e il grado di copertura ottimale della diagnosi. Ad esempio, è possibile eseguire numerosi test suulla memoria, ma è difficile stabilire quanti fra tutti i possibili guasti alla memoria vengono individuati attraverso la diagnosi e la corretta modalità di verifica di questi dati? I singoli produttori di microcontrollori hanno già affrontato questa sfida e offrono un prezioso supporto: di seguito alcuni esempi significativi.

Fig. 1 – Renesas offre un ricco ecosistema di sicurezza per la propria serie di prodotti RX

L'ecosistema per la sicurezza di Renesas

Renesas ha sviluppato una libreria di autotest per la serie di microcontrollori a 32 bit RX631/N, certificata dal TÜV Rheinland in base allo standard IEC 61508. Questa autodiagnosi copre la rilevazione di errori casuali e persistenti nel core della CPU, compresa l'unità in virgola mobile e l'estensione DSP, nella RAM utente e nella memoria Flash. Il grado di copertura della diagnosi di queste unità funzionali è quindi superiore al 90 %. I test possono essere condotti in modo ciclico, in blocco oppure a intervalli durante il funzionamento. È possibile raggiungere il livello SIL2 usando solo un dispositivo della serie RX631/N, mentre per ottenere un livello SIL3 è necessario un sistema costituito da due chip. Unitamente alla libreria, Renesas fornisce anche un manuale per la sicurezza e un manuale del software per la sicurezza. Una licenza gratuita di valutazione consente di visionare le funzioni presenti in libreria prima dell'acquisto.

L'ecosistema per la sicurezza della serie di dispositivi RX comprende inoltre un compilatore di IAR, EWRXFS, certificato secondo IEC 61508. Con quest'ultimo, Renesas ha anche sviluppato una libreria di autotest. Wittenstein, azienda specializzata nel settore dei sistemi di trasmissione, offre, con il proprio SAFERTOS, un sistema operativo in tempo reale certificato per i microcontrollori della serie RX di Renesas. La funzione di moduli software pre-certificati rappresenta una solida base per la certificazione degli apparecchi finali e riduce il tempo di sviluppo. Il manuale per la sicurezza individua i tassi di FIT e li suddivide nelle varie unità funzionali del chip. In questo modo è possibile migliorare la precisione il modello per l'affidabilità. Inoltre i componenti approvati contribuiscono a ridurre il numero degli argomenti di discussione con l'organismo di certificazione, con riflessi favorevoli sul time-to-market. I prodotti V850E/P e RH850/P, ampiamente utilizzati in campo automobilistico, utilizzano due core the elaborano lo stesso codice in modo sincronizzato (lockstep). I risultati delle operazioni vengono confrontati e le differenze sono identificate come errori.

Fig. 2 – L'immagine illustra la realizzazione e la certificazione di applicazioni critiche per la sicurezza: la famiglia AURIXTM di Infineon con il relativo software per la sicurezza e l'alimentazione

Infineon PRO-SILTM: sicurezza in campo automobilistico e 'industriale

Infineon offre, sotto il marchio PRO-SILTM, una gamma completa di prodotti che includono microcontrollori, IC per la gestione dell'alimentazione, sensori, driver trifase, unitamente al relativo software e alla documentazione (manuale per la sicurezza FMEDA = modalità di guasto, effetti e analisi diagnostica). Le fasi di sviluppo e i processi, a livello sia hardware, sia software, sono basati sullo standard ISO 26262. Il più recente membro della della famiglia di prodotti PRO-SIL è la famiglia AURIX, che include il software per la sicurezza e il relativo chip di alimentazione TLF35584. Questa famiglia di prodotti si propone come una soluzione a livello di sistema, con cui realizzare e certificare in modo più semplice le applicazioni critiche per la sicurezza. Il campo di impiego spazia dalle applicazioni classiche in campo automobilistico ai sistemi di trasporto – treni, autobus, o macchine utilizzate in campo agricolo o delle costruzioni – fino ad arrivare alle applicazioni critiche per la sicurezza.

La famiglia AURIX, perfettamente scalabile in termini di memoria, di potenza di calcolo e di package, è caratterizzata da un assorbimento di corrente modesto e da funzioni di sicurezza ottimizzate. Allo scopo di riconoscere tempestivamente eventuali errori, i core della CPU dispongono di un core di backup che gira in backgroud, che esegue i calcoli in parallelo

Fig. 3 – La famiglia di microcontrollori dual core SPC56 L di STMicroelectronics è adatta per applicazioni per la sicurezza funzionale nell'elettronica automotive

con uno sfasamento di due cicli di clock e confronta i risultati.
L'esecuzione hardware di un gran numero di funzioni di sicurezza permette a Infineon di ridurre sensibilmente l'onere di sviluppo soft-ware per gli uti-lizzatori. Attualmente è in corso una certificazione per la sicurezza basata sullo standard ISO 26262, a opera del TÜV SÜD. Sono previste ulteriori certificazioni relativamente sia a standard generici, come ad esempio IEC 61508 sia a standard specifici, come ad esempio ISO25119 per i veicoli agricoli.

STMicroelectronics: un microcontrollore dual-core per applicazioni ASIL D

STMicroelectronics ha sviluppato e certificato la famiglia di microcontrollori dual-core SPC56 L, ideata specificamente per applicazioni per la sicurezza dell'elettronica a bordo veicolo, , in conformità agli standard per la sicurezza IEC 61508 e ISO 26262. I membri della famiglia sono equipaggiati con due core ad alte prestazioni, con un massimo di 2 MB di memoria Flash, 192 KB di RAM interna, tre interfacce CAN e dispongono di periferiche ottimizzate per applicazioni nel campo della sicurezza e del controllo motore. Grazie all'architettura dual-core, il numero di componenti che devono essere duplicati è estremamente ridotto, con conseguente diminuzione dei costi di sistema. Inoltre l'architettura garantisce una notevole flessibilità, grazie alla possibilità di commutare tra la modalità operativa lockstep e quella parallela. L'esecuzione in tempo reale dello stesso codice in entrambi i core (lockstep) assicura i massimi livelli di sicurezza, mentre l'esecuzione utilizzando codici differenti (elaborazione parallela) consente di ottenere le migliori prestazioni.
Di conseguenza, non solo le funzioni della CPU risultano duplicate, ma vengono anche realizzate ulteriori ridondanze sul chip, conferendo ai prodotti della linea SPC56 L un elevato grado di sicurezza. Oltre alla diagnostica hardware automatizzata, sono disponibili altre funzioni di sicurezza tra cui l'unità CRC, risorse di memoria con ECC, un sensore di temperatura, unità centralizzata di rilevamento degli errori e di controllo e unità di rilevamento della tensione e di anomalie cicliche.
Grazie a ciò, la linea di dispositivi SPC56 L soddisfa i requisiti più stringenti dello standard ASIL-Livello ASIL D – come confermato da un ente indipendente di certificazione.
La linea di microcontrollori a 32 bit SPC56 L appartiene alla famiglia SPC56, utilizzata in ambito automobilistico – nella carrozzeria telaio in ambito automotive e sicurezza. Tutti i prodotti sono basati sul core e200, che sfrutta la Power Architecture a a 32 bit e dispongono di memoria flash embedded e periferie ottimizzate.

La libreria software per la sicurezza di Microchip

Microchip offre la libreria software per la sicurezza (Safety Software Library) di classe B per i microcontrollori a 8 bit, 16 bit e 32 bit. Essa comprende un certo numero di API, utilizzate per il riconoscimento di malfunzionamenti e per aumentare la sicurezza delle applicazioni; esse costituiscono e quindi aiutano lo sviluppatore a realizzare la propria applicazione in conformità allo standard IEC60730. È disponibile, in base ai requisiti di sicurezza dell'applicazione, una linea completa di test per l'implementazione: test dei registri della CPU, test dei

Fig. 4 – Microchip offre una libreria software per la sicurezza di classe B per i propri microcontrollori a 8 bit, 16 bit e 32 bit

contatori dei programmi, test di memorie volatili e non volatili (Flash/EEPROM), test di interrupt e test del segnale di clock.
Questi moduli pre-certificati, forniti dai diversi produttori, accelerano la fase di sviluppo e di certificazione della soluzione. Lo scopo è conseguire un certo tasso di copertura diagnostica per il microcontrollore con l'aiuto della libreria software o del monitoraggio mutuo delle CPU. La documentazione fornisce i parametri necessari per realizzare il modello per l'affidabilità. In ogni caso è necessario specificare i requisiti di sicurezza che si applicano al sistema. In ogni caso, occorre valutare in anticipo se il pacchetto di soluzioni proposte dai produttori soddisfa in modo ottimale i requisiti dell'applicazione. A questo proposito un distributore come Rutronik può fornire una consulenza indipendente e completa sulle offerte di diversi produttori. ■