life.augmented

Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale

STMicroelectronics

Lezione n. 5

Diagnostica (hw e sw), evoluzione del sistema, partizionamento hw/sw

Riepilogo:

- **Stato sicuro**
- **Evoluzione del sistema nel tempo**
- **Modalità di funzionamento, PST, frequenza dei test**
- **Elementi di diagnostica, hw, sw, sistema**

life.augmented

Declassamento

I componenti hardware devono essere utilizzati a livelli che, secondo la progettazione del sistema, devono essere ben al di sotto dei valori massimi delle specifiche.

Il derating è la pratica volta a garantire che, in tutte le normali circostanze operative, i componenti hardware funzionino ben al di sotto dei loro livelli di stress massimi: può essere definito come un margine di sicurezza.

IEC61508 raccomanda il derating (fattore 2/3) per i componenti hardware

IAO13849-1 menziona esplicitamente il derating come una delle tecniche aggiuntive economizzate per ridurre la possibilità di guasti sistematici (di nuovo fattore 2/3).

Il de-rating può svolgere un ruolo rilevante nel garantire che l'ipotesi "tasso di guasto = costante" sia ancora valido.

Stato sicuro

Lo stato sicuro è formalmente definito in entrambi gli standard principali:

IEC61508-4: stato dell'EUC quando la sicurezza è raggiunta

ISO26262-1: modalità operativa, in caso di guasto, di un elemento senza un livello di rischio irragionevole

Nella norma IEC61508 il sistema deve essere sempre in "stato sicuro", sia quando funziona perfettamente sia quando è difettoso.

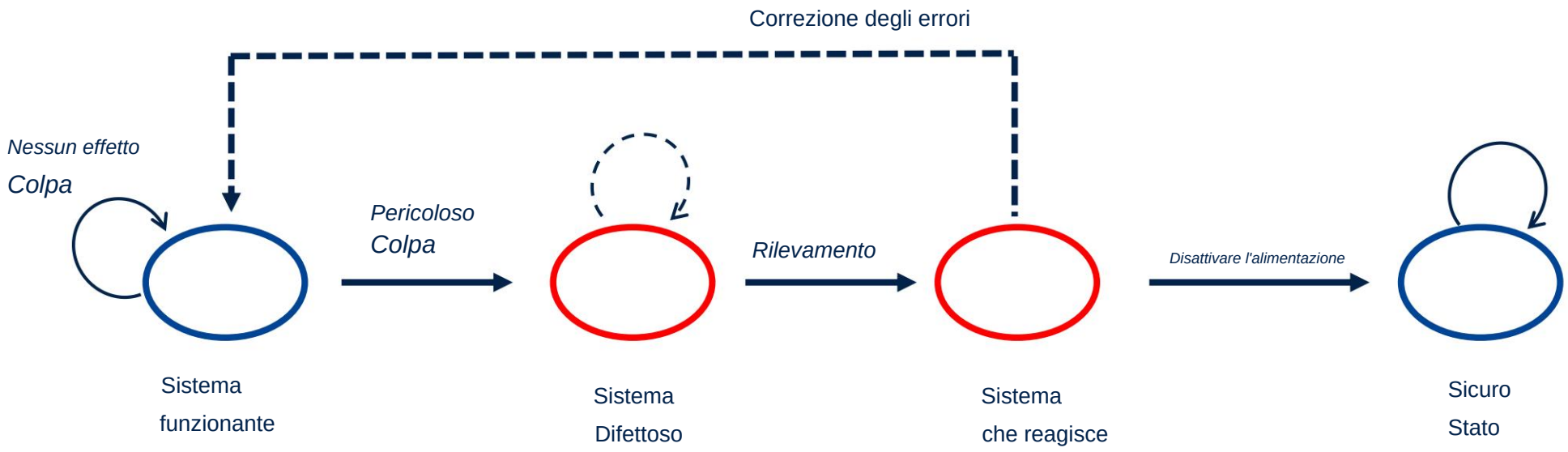
Nell'uso comune, "Safe State" indica lo stato specifico in cui il sistema garantisce la sicurezza in caso di guasto (bias ISO26262), solitamente in modalità "degradata".

Stato sicuro

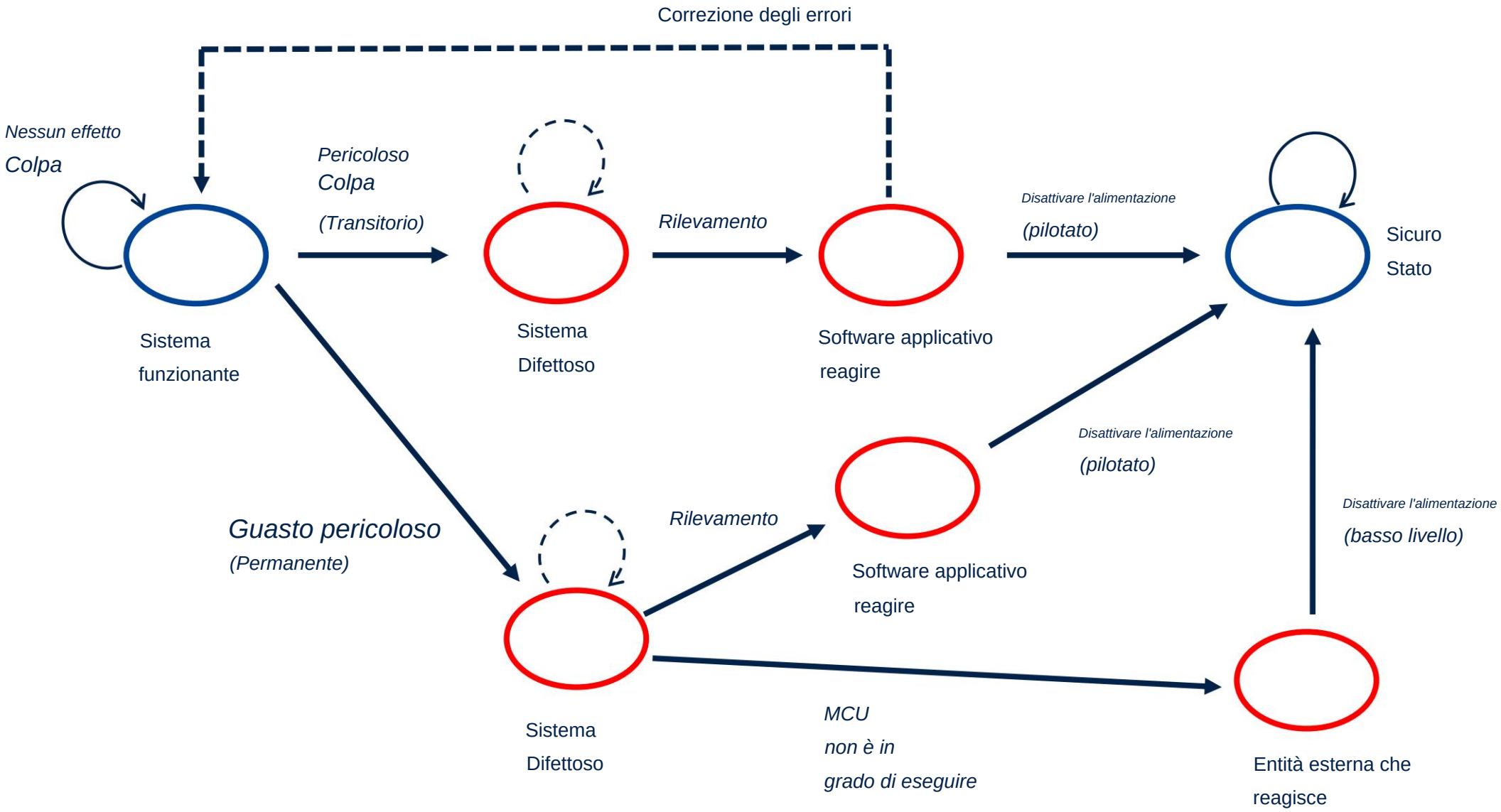
La definizione di stato sicuro non è mai generica, poiché è strettamente connessa all'applicazione finale, ovvero al modo in cui gli output/le decisioni vengono comunicati/attuati (la funzione di sicurezza). Come per la funzione di sicurezza, la definizione di stato sicuro avviene a livello di sistema (è possibile definire anche uno stato sicuro locale).

Stato sicuro ed evoluzione del sistema (generale)

Importante: lo Stato Sicuro deve essere sempre raggiungibile, indipendentemente dall'effettivo guasto che colpisce il sistema.

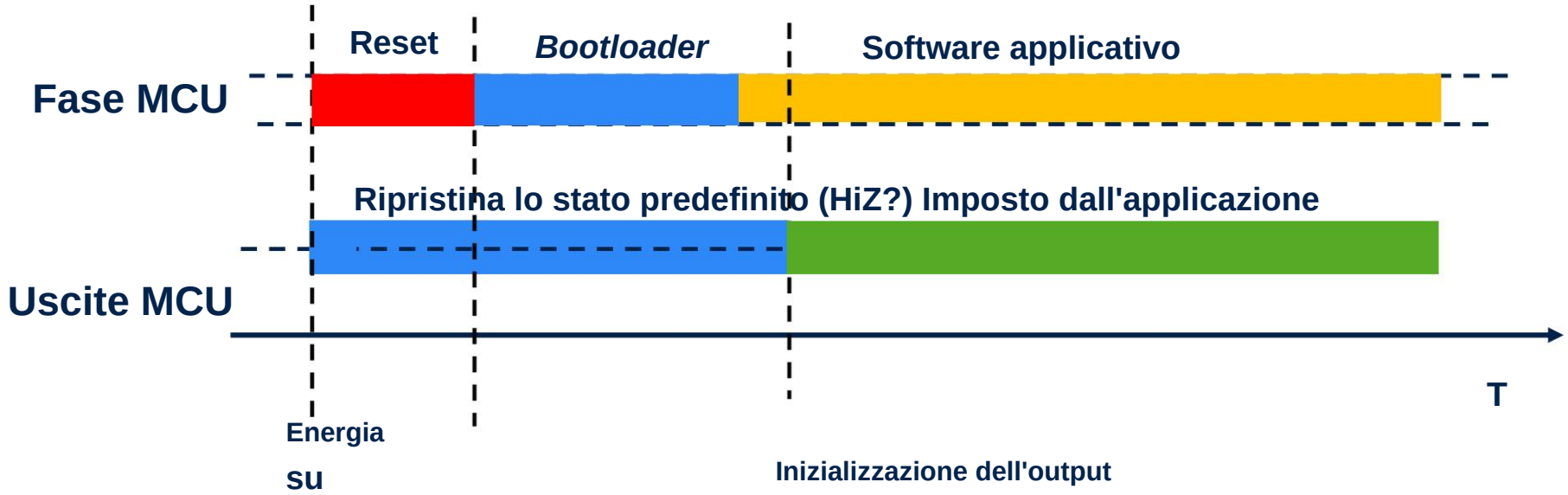


Stato sicuro ed evoluzione del sistema (aggiunta di modelli MCU e di guasto)



Stato sicuro e avvio del sistema

Importante: lo Stato Sicuro deve essere sempre garantito, anche quando non è possibile l'esecuzione del software



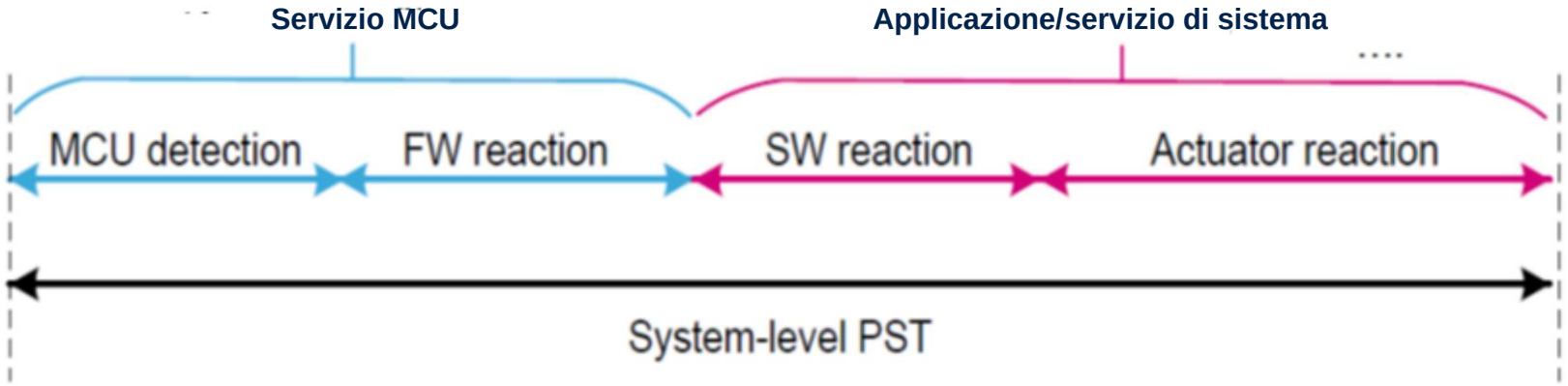
La fase di avvio (inclusa la possibile esecuzione del bootloader, più lunga per i dispositivi senza flash) richiede misure aggiuntive esterne all'MCU per garantire lo stato sicuro

I guasti che si verificano durante la fase di accensione possono causare il blocco del sistema in una delle fasi iniziali.

life.augmented

Sequenza temporale per la comprensione della limitazione PST

Questa è la tipica sequenza temporale/causale dal rilevamento di un guasto al raggiungimento dello stato sicuro.



Si noti che il tempo di sicurezza del processo PST è definito come il tempo che intercorre tra l'insorgenza di un guasto pericoloso e il momento in cui si verifica un pericolo reale. Nei sistemi CM, la diagnostica deve essere in grado di intervenire entro il PST.

Attenzione: non sono inclusi i casi limite relativi al blocco della CPU o all'impossibilità di eseguire correttamente le azioni software. Per questo motivo, è necessaria la transizione allo stato sicuro da parte di entità esterne (ad esempio un watchdog).

Modalità di funzionamento (IEC61508)

Nella norma IEC61508 la modalità di funzionamento è correlata alla frequenza con cui è richiesta la funzione di sicurezza; determina la metrica target (PFD/PFH) e la frequenza di prova:

Modalità a bassa richiesta: la funzione di sicurezza viene eseguita solo su richiesta, per trasferire l'EUC in uno stato di sicurezza specificato e dove la frequenza delle richieste non è superiore a una all'anno

Modalità ad alta richiesta: la funzione di sicurezza viene eseguita solo su richiesta, per trasferire l'EUC in uno stato sicuro specificato e quando la frequenza delle richieste è maggiore di una all'anno

Modalità continua: in cui la funzione di sicurezza mantiene l'EUC in uno stato sicuro come parte del normale funzionamento

LD ÿ PFD Probabilità di guasto su richiesta: probabilità

HD/CM ÿ PFH (Probabilità di guasto all'ora: probabilità/tempo)

Modalità di funzionamento (IEC61508)

La frequenza di esecuzione diagnostica periodica dipende dalla Modalità: DC può essere richiesta solo per i meccanismi di sicurezza eseguiti entro i limiti specificati di seguito.

ÿSui sistemi LD, si applica il concetto di test di prova (fare riferimento alla diapositiva correlata).

ÿSistemi HD: la frequenza dei test è legata alla frequenza delle richieste delle funzioni di sicurezza (100x più veloce). Ciò consente concetti basati sul software.

ÿI sistemi CM richiedono che ogni diagnostica periodica venga eseguita almeno una volta per PST (Process Tempo di sicurezza), introducendo un concetto correlato

Modalità di funzionamento (IEC61508)

Esempi di funzioni di sicurezza LD/HD/CM:

Modalità	Funzione di sicurezza	Descrizione
LD	Sistema di arresto di emergenza (ESD) Arresta il processo	in modo sicuro in caso di evento pericoloso (ad esempio, perdita di gas, incendio).
Alta definizione	Sistemi di interblocco di sicurezza	Spesso invocato per prevenire operazioni non sicure (ad esempio, l'apertura di una valvola solo in condizioni di sicurezza)
CM	Sistema di rilevamento incendi e gas (monitoraggio continuo)	Monitora costantemente la presenza di fuoco o gas e attiva immediatamente allarmi o arresti in caso di rilevamento

Si noti che nello stesso sistema di sicurezza è possibile avere funzioni di sicurezza coesistenti con diverse modalità di funzionamento (ad esempio in un sistema antincendio, un CM SF per il rilevamento di incendi/ fumo e un LD SF per l'installazione degli sprinkler)

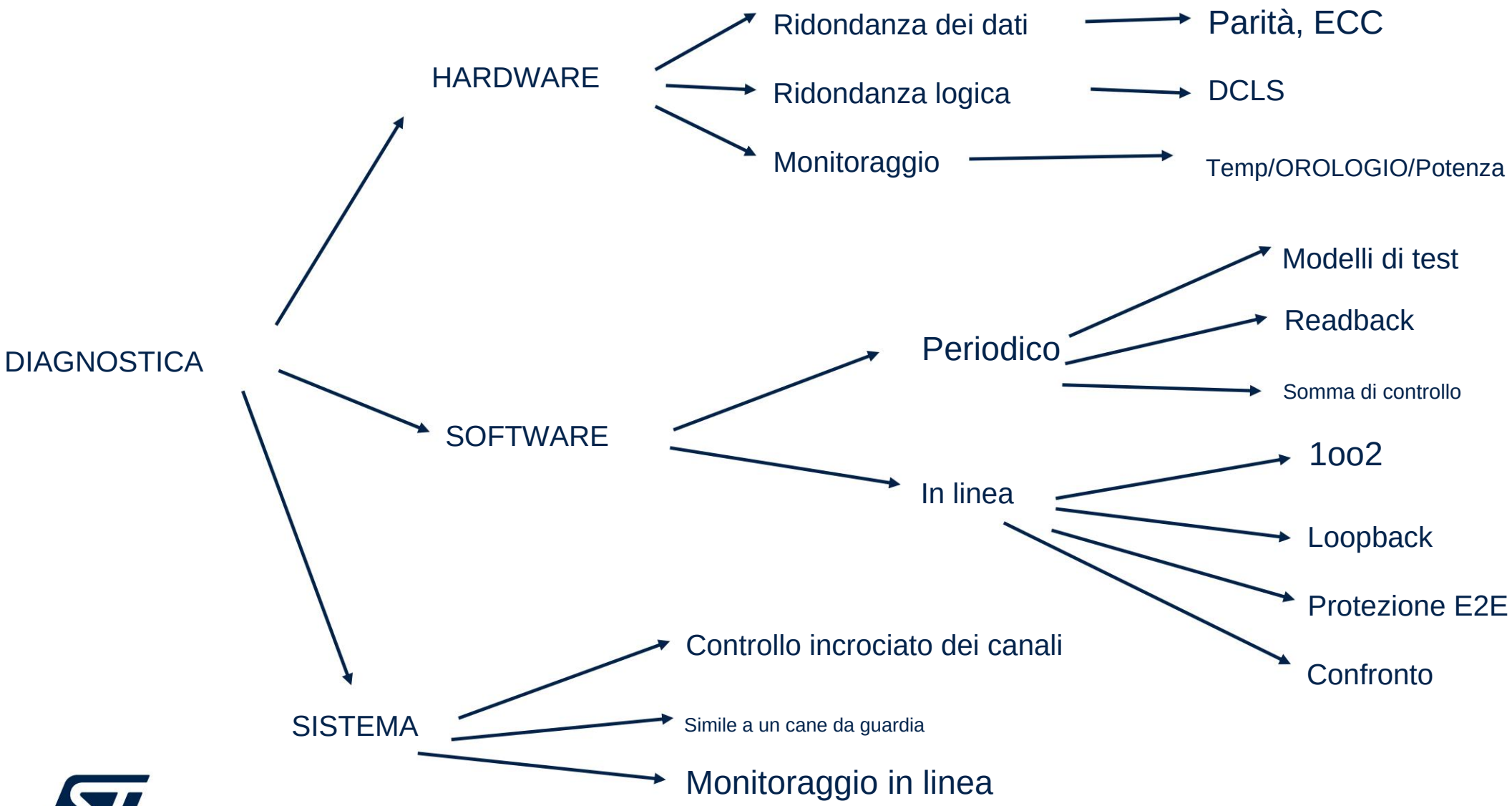
Il concetto di test di prova

Il test di prova è definito come un test periodico eseguito per rilevare guasti nascosti pericolosi in un sistema di sicurezza, per rallentare (se necessario) una riparazione che possa ripristinare il sistema a una condizione "come nuova" o il più vicino possibile a tale condizione.

Il test di prova è il metodo principale per garantire la sicurezza nei sistemi a bassa domanda, dove il PFD è la metrica dominante. La periodicità del test è imposta dal livello SIL target e dal tasso di guasto del dispositivo (più alto è ÿDU, più breve è l'intervallo)

I test di prova possono essere applicati anche ai sistemi HD/CM con l'intento di affrontare guasti "nascosti" relativi a strutture difficili da testare durante il funzionamento, come funzioni diagnostiche, catena di errori (segnalazione e reazione), guasti parzialmente corretti. Solitamente, l'effetto sul PFH è trascurabile.

Classificazione dei meccanismi di sicurezza



Pro/Contro per categorie

Caratteristiche dei meccanismi di sicurezza

Ci sono caratteristiche comuni da definire quando si parla di meccanismi diagnostici/di sicurezza

ÿModello di guasto affrontato (permanente/transitorio/entrambi?)

ÿPeriodicità (continua/su richiesta/periodica)

ÿReazione all'errore (messaggio/flag/interruzione)

ÿCorrezione degli errori (sì/no/parziale)

ÿProtezione da test/guasti multipli (elenco delle diagnosi alternative per i guasti che impediscono il corretto funzionamento dei meccanismi di sicurezza stessi)

ÿInizializzazione/configurazione (alcune diagnostiche sono sempre attive, altre potrebbero richiedere una configurazione da sw, ecc.)

DC raggiunto: come stabilirlo

Esistono molteplici modelli per stabilire la copertura diagnostica raggiunta per un dato meccanismo di sicurezza

ÿTabelle di riferimento degli standard di sicurezza: molti standard di sicurezza includono una tabella di riferimento dove per un insieme di diagnosi di alto livello specificate viene fornito un intervallo/indicazione per la DC raggiungibile (*). Solitamente, valori enumerati (Alto=99%, Medio-90%, Basso=60%)

ÿIniezione/simulazione di guasti: il componente viene modellato all'interno di uno strumento in grado di emulare i guasti che interessano l'hardware e la capacità di reazione della diagnostica. La DC viene calcolata in modo statistico

(*) Attenzione: “raggiungibile” non significa “raggiunto”. Di conseguenza, tali valori sono considerati il massimo DC ottenibile per tale diagnosi (!).

Blocco Dual Core Step (DCLS)

PRO

ÿ Rilevamento rapido dei guasti

ÿ Rileva guasti sia permanenti che transitori

ÿ DC altamente raggiunto

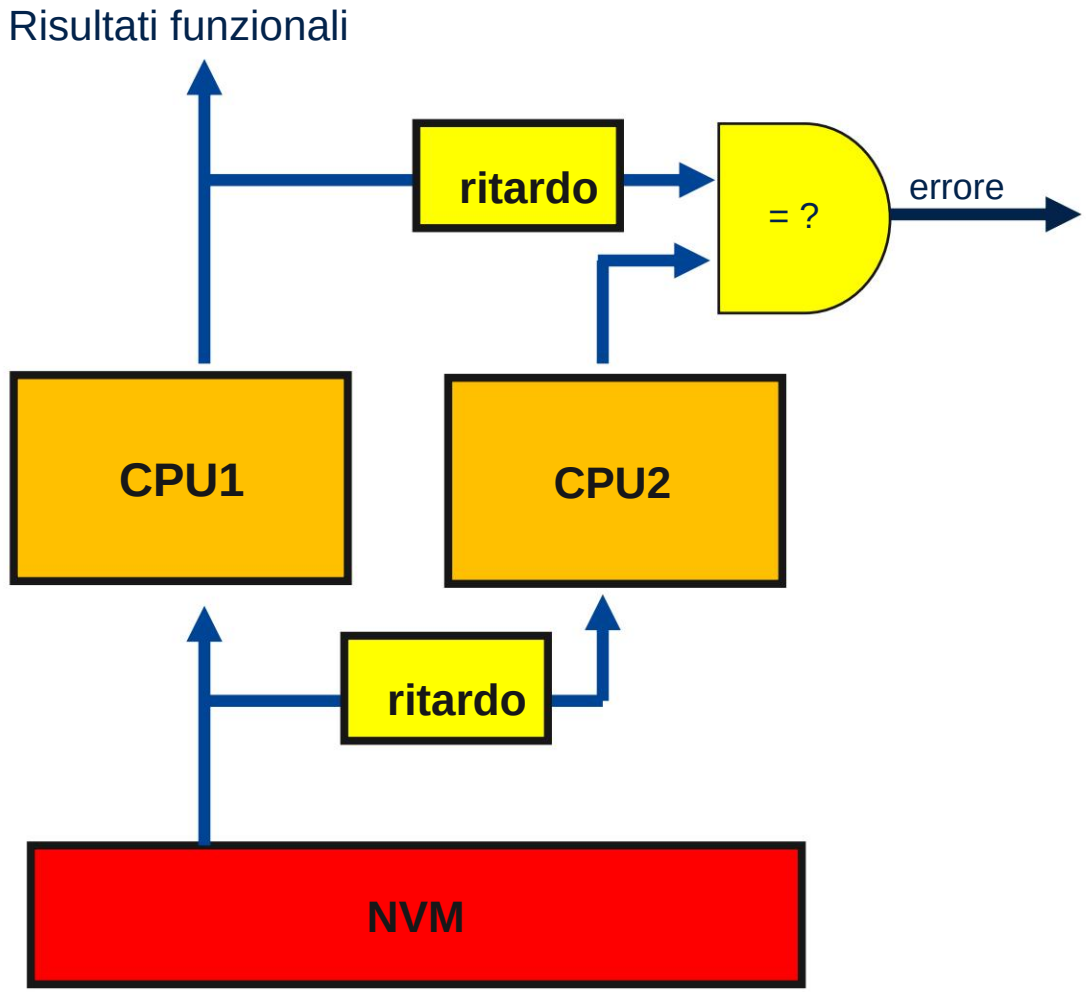
ÿ Indipendente dall'applicazione

CONTRO

ÿ Costo e complessità quindi disponibili solo su
dispositivi pronti per la sicurezza

ÿ La seconda CPU è solo per il monitoraggio, quindi HFT=0

ÿ Sono ancora necessarie entità aggiuntive per gestire i guasti
che impediscono l'esecuzione del software



Bit di parità

A ogni parola viene aggiunto un bit di parità (più **CONS**
sono possibili schemi), consentendo l'errore di un singolo bit ÿ
bit quando i dati vengono letti.

PRO

ÿ Rilevamento rapido dei guasti

ÿ Rileva guasti sia permanenti che transitori

ÿ Il miglior compromesso tra costo del dispositivo e
DC medio raggiunto

ÿ Indipendente dall'applicazione

ÿ Nessuna penalità di tempo dal punto di vista dell'utente finale

Copertura garantita solo sul rilevamento di un singolo
guasti (50% su doppio, ecc…)

ÿ La copertura raggiunta è discutibile a causa delle differenze
tra le linee guida degli standard di sicurezza

ÿ Di solito, il controllo viene eseguito in lettura ÿ errore
l'accumulo deve essere gestito (lavaggio)

ÿ Se le linee di indirizzo non sono incluse, sono necessari
test aggiuntivi per il decodificatore di indirizzo

ECC

A ogni parola viene aggiunto un codice ridondante multi-bit (sono possibili diversi schemi), consentendo la correzione di un singolo errore e il rilevamento di un doppio errore durante la lettura dei dati.

PRO

ÿ Rilevamento rapido dei guasti

ÿ Consente la correzione di singoli errori, aumentando così la disponibilità del sistema

ÿ Rileva guasti sia permanenti che transitori

ÿ DC altamente raggiunto

ÿ Indipendente dall'applicazione

ÿ Nessuna penalità di tempo dal punto di vista dell'utente finale

CONTRO

ÿ Di solito, il controllo viene eseguito in lettura ÿ errore l'accumulo deve essere gestito (lavaggio)

ÿ Di solito, la correzione viene eseguita solo sui dati inviati alla CPU e non sulle celle ÿ l'errore persiste

ÿ Se le linee di indirizzo non sono incluse, sono necessari test aggiuntivi per il decodificatore di indirizzo

life.augmented

Cane da guardia interno

Forza un reset della CPU quando l'azione richiesta dal software (ad esempio, la scrittura del registro con una chiave) non viene eseguita entro il periodo programmato. La politica di temporizzazione può essere applicata tramite requisiti di finestra.

PRO

ÿ Gestisce guasti permanenti o transitori influenzando la corretta capacità di esecuzione del software

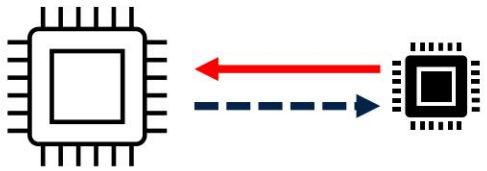
ÿ Contribuisce alla capacità sistematica del software intercettando un flusso di controllo o una temporizzazione errati

CONTRO

ÿ Mancanza di diversità hardware poiché condivide con il CPU lo stesso substrato di silicio e spesso anche potenza/clock

ÿ Impossibile gestire completamente i guasti che portano all'impossibilità di esecuzione del software

ÿ Spesso sovrapposto da un watchdog esterno come richiesto da IEC61508-2, Tabella A.1/Tabella A.14.



life.augmented

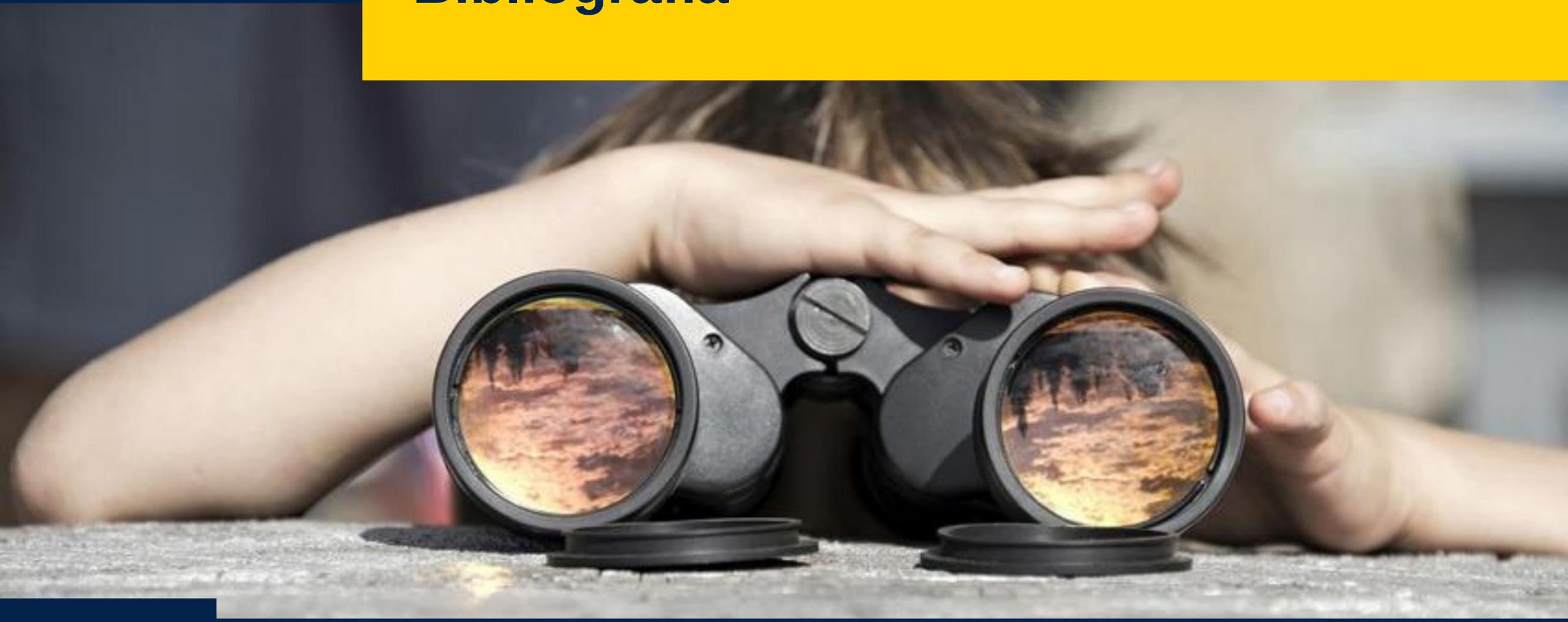
Riferimenti utili sui meccanismi di sicurezza

Il riferimento [6] elenca nella sezione "7 Breve descrizione dei meccanismi di “ più di 100 diverse misure di sicurezza diagnostica definiti in un microcontrollore ASIL D di sicurezza automobilistica (TI). Consultare anche "Appendice A Riepilogo dell'utilizzo consigliato delle funzionalità di sicurezza" dove una tabella esaustiva fornisce una vista sinottica di tutte le caratteristiche per le diagnostiche elencate.

Il riferimento [7] fornisce descrizioni simili nella sezione “3.6 Diagnostica hardware e software”, in questo caso viene adottata una formulazione IEC 61508 in tutto il documento. Anche in questo caso, l'obiettivo è un MCU con livello di sicurezza intermedio SIL 2.

Il riferimento [8] offre una prospettiva diversa su un dispositivo “più semplice”, un PMIC. Fare riferimento alla sezione “5 Meccanismi di sicurezza dell'architettura TPS65919-Q1 e ipotesi di utilizzo” per una visione del set molto diverso di diagnostica dedicata.

Bibliografia



Documenti di riferimento 1/2

[R1]: Affidabilità della microelettronica: modellazione basata sulla fisica dei guasti e valutazione della durata di vita - Jet Propulsion LaboratoryCalifornia Institute of Technology Pasadena, California

[R2]: : Manuale di affidabilità dei semiconduttori – Renesas Electronics, Rev.2.50 gennaio 2017

[R3]: ExoMars 2016 - Schiaparelli Anomaly Inquiry (ESA) scaricato da https://exploration.esa.int/web/mars/-/59176-exomars-2016-schiaparelli-anomaly-inquiry

[R4]: Manuale dell'albero dei guasti con applicazioni aerospaziali - Ufficio di sicurezza e garanzia della missione della NASA, V 1.1 2002 ,

[R5]: il software FTA aperto può essere trovato sul web, ad esempio https://www.fault-tree-analysis.com/free-fault-tree-analysis-software, oppure verifica il download di OpenFTA

Documenti di riferimento 2/2

[R6]: Manuale di sicurezza per TMS570LS31x e TMS570LS21x Hercules™ ARM®-Based Safety Microcontrollori critici

[R7]: Manuale di sicurezza della serie singlecore UM2331-STM32H7 STMicroelectronics – da https://www.st.com/en/embedded-software/x-cube-stl.html#documentation

[R8]: Manuale di sicurezza per l'unità di gestione dell'alimentazione (PMU) TPS65919-Q1

Grazie

life.augmented