



Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale
STMicroelectronics

Lezione n. 1

Introduzione generale sulla sicurezza, incluso HARA



Riepilogo:

- Concetti generali: rischio, funzioni di sicurezza, Hazard e analisi del rischio, riduzione del rischio
- Standard di sicurezza
- Guasti, guasti, HRF vs sistematico

Perché la sicurezza funzionale è importante nella vita di tutti i giorni

Protegge la vita e la salute umana prevenendo incidenti e guasti pericolosi

Riduce il rischio di danni alla proprietà e danni ambientali causati da malfunzionamenti del sistema

Garantisce il funzionamento affidabile dei sistemi critici nei veicoli, nei dispositivi medici e nelle apparecchiature industriali

Crea fiducia nell'utente nella tecnologia attraverso prestazioni coerenti e sicure

Riduce al minimo i tempi di inattività e i costi associati a guasti e richiami

Abilita l'innovazione fornendo un quadro di sicurezza per le nuove tecnologie e l'automazione

Alcune definizioni utili

Evento/pericolo pericoloso: un evento che ha intrinsecamente la capacità di causare un danno (lesioni fisiche/morte di persone o danni a cose)

Rischio: è associato a un pericolo e combina la possibilità che si verifichi un danno e le conseguenze che ne derivano (quanto è grave il danno)

Rischio tollerabile/accettabile: rischio che può essere ragionevolmente considerato accettato in un determinato contesto o situazione. Dipende chiaramente dal sistema di valori corrente adottato nella società.

Sicurezza: assenza di rischi considerati inaccettabili.

Acronimo E/E/PE: Elettrico/elettronico/elettronico programmabile

Che cosa è la sicurezza funzionale (definizione IEC61508)

È parte della sicurezza complessiva (Sicurezza complessiva >> sicurezza funzionale; contribuisce a raggiungere un rischio tollerabile)

Dipende dal corretto funzionamento del sistema di controllo (nel nostro caso, E/EE/PE)

Potrebbe dipendere da misure aggiuntive in grado di ridurre il rischio

A proposito del concetto di “rischio”

Il concetto di rischio si basa solitamente su tre parametri:

Gravità: quante persone saranno coinvolte e in che modo (feriti/morti...)

Esposizione: quanto spesso corriamo il rischio dato

Controllabilità: esiste la possibilità per le persone coinvolte di controllare in qualche modo l'effetto del guasto del sistema

I tre parametri vengono combinati in una sorta di matrice incrociata per ricavare il rischio risultante.



Il “paradosso” dell’airbag

Un esempio significativo di classificazione del rischio è dato dal noto airbag per auto. Negli airbag abbiamo due distinte funzioni di sicurezza: a) Attivazione: attivare l’airbag quando necessario (incidente stradale) e b) Sicurezza: non attivare l’airbag quando non necessario (nessun incidente stradale).

Parametro	Mancato azionamento (l’airbag non si attiva quando l’auto ha un incidente)	Guasto di sicurezza (airbag in fiamme senza incidente stradale)	Confronto
Gravità	Medio: solo il conducente saranno interessati	Alto: perdere il controllo della propria auto (conseguenza di uno sparo inaspettato) può coinvolgere pedoni o altri conducenti di auto	Salvataggio > Cottura
Esposizione	Basso! Quando in realtà hai un incidente, almeno una o due volte nella vita, si spera ѕ	Alto! Ogni volta che guidi la tua auto, anche nel parcheggio	Salvataggio >> Licenziamento
Controllabilità Nessuna		Basso o nessuno	Salvataggio = Licenziamento

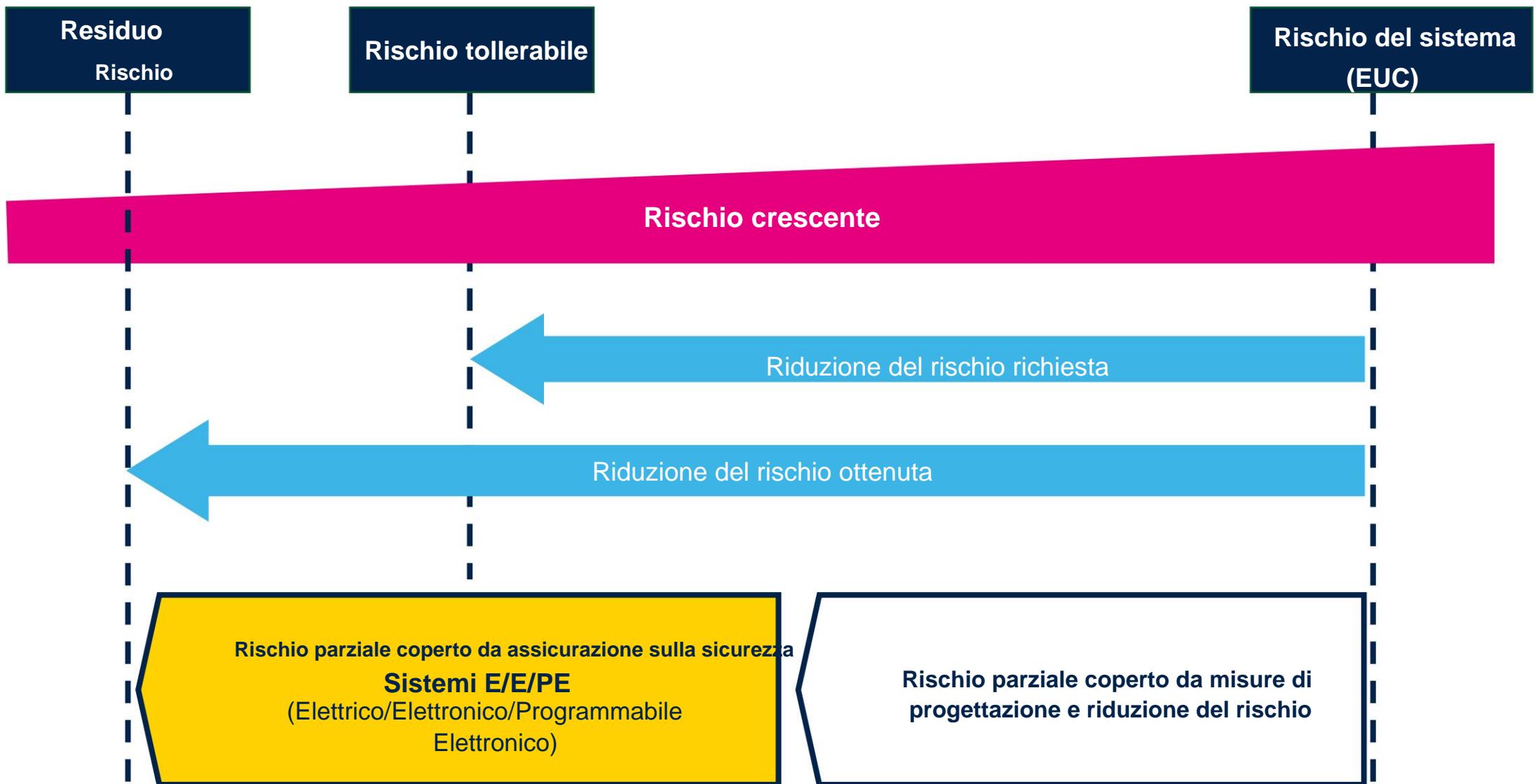
A proposito del concetto di “rischio”

ÿNon stiamo parlando di “eliminazione del rischio” (impossibile!) ma di “mitigazione del rischio” quindi evitare rischi inaccettabili

ÿIl concetto di “rischio tollerabile” è in continua evoluzione:

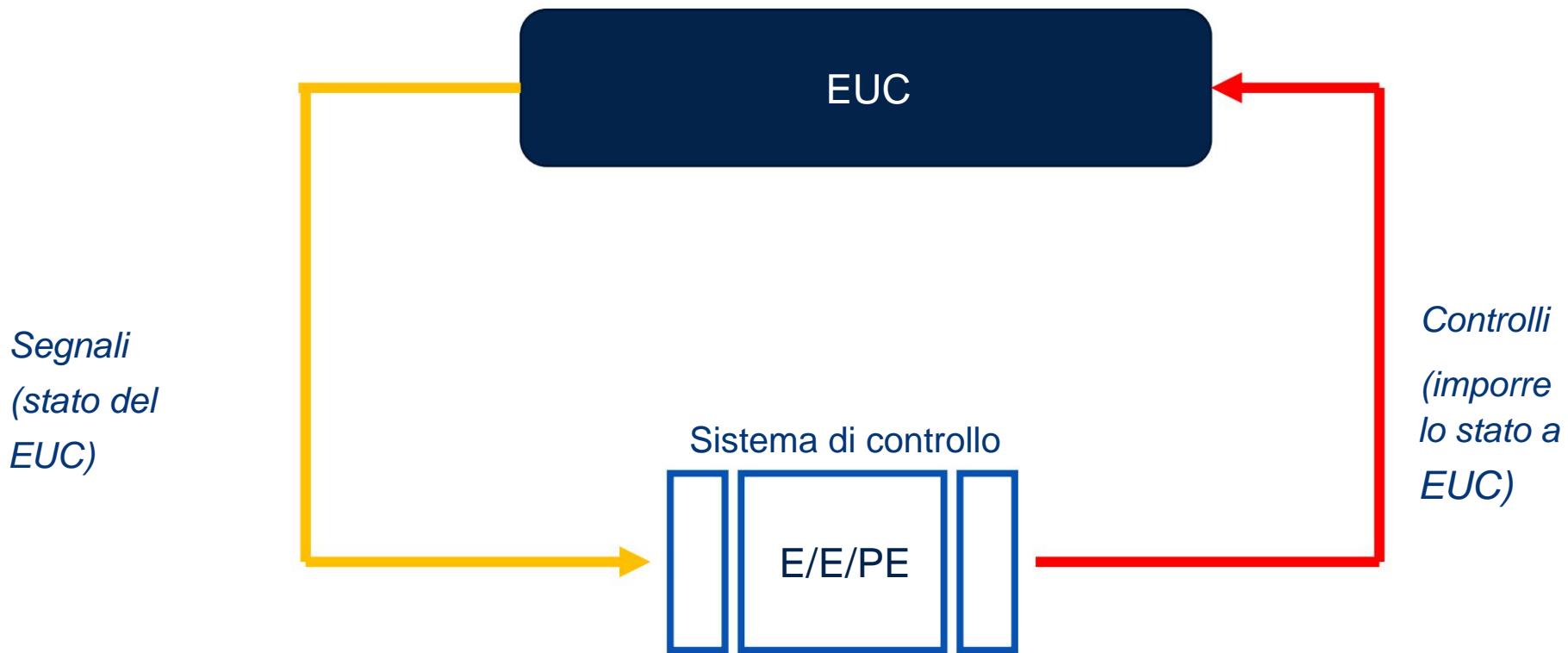
- ÿ Una volta che una nuova tecnologia si è diffusa ampiamente, le aspettative delle persone per l'assenza del rischio correlato tende ad aumentare (vedi ad esempio l'aviazione civile)
- ÿ Dipendenza dal mercato/settore, correlata alla percezione generale del pubblico (ad esempio, si ritiene ragionevolmente che le missioni spaziali siano più pericolose dei voli commerciali) e anche all'approccio legale (vedere ad esempio il mercato automobilistico, dove la probabilità di azioni collettive ad alto costo spinge per una maggiore sicurezza)

Riduzione del rischio



Il dualismo EUC/sistema di controllo

La norma IEC61508 si basa sul concetto che il sistema finale ("l'impianto") può essere descritto come una struttura duale: sistema controllato (EUC, Equipment Under Control) / sistema di controllo (ovvero un tipo di schema di controllo a feedback).



Il protagonista: la funzione di sicurezza

Funzione di sicurezza: funzione implementata da un sistema di sicurezza E/EE/PE (eventualmente anche con la partecipazione di misure aggiuntive per ridurre il rischio), ovvero

- destinato a raggiungere o mantenere la sicurezza (quindi, nessun rischio inaccettabile) per l'EUC,
- definito in dipendenza di uno specifico evento pericoloso

Esempi di funzioni di sicurezza:

- *Funzioni che devono essere eseguite come azione positiva per evitare pericoli (ad esempio arresto del motore di un braccio robotico)*
- *Funzioni che impediscono l'esecuzione di azioni (ad esempio impedire l'apertura di una porta quando un treno è in arrivo in movimento)*

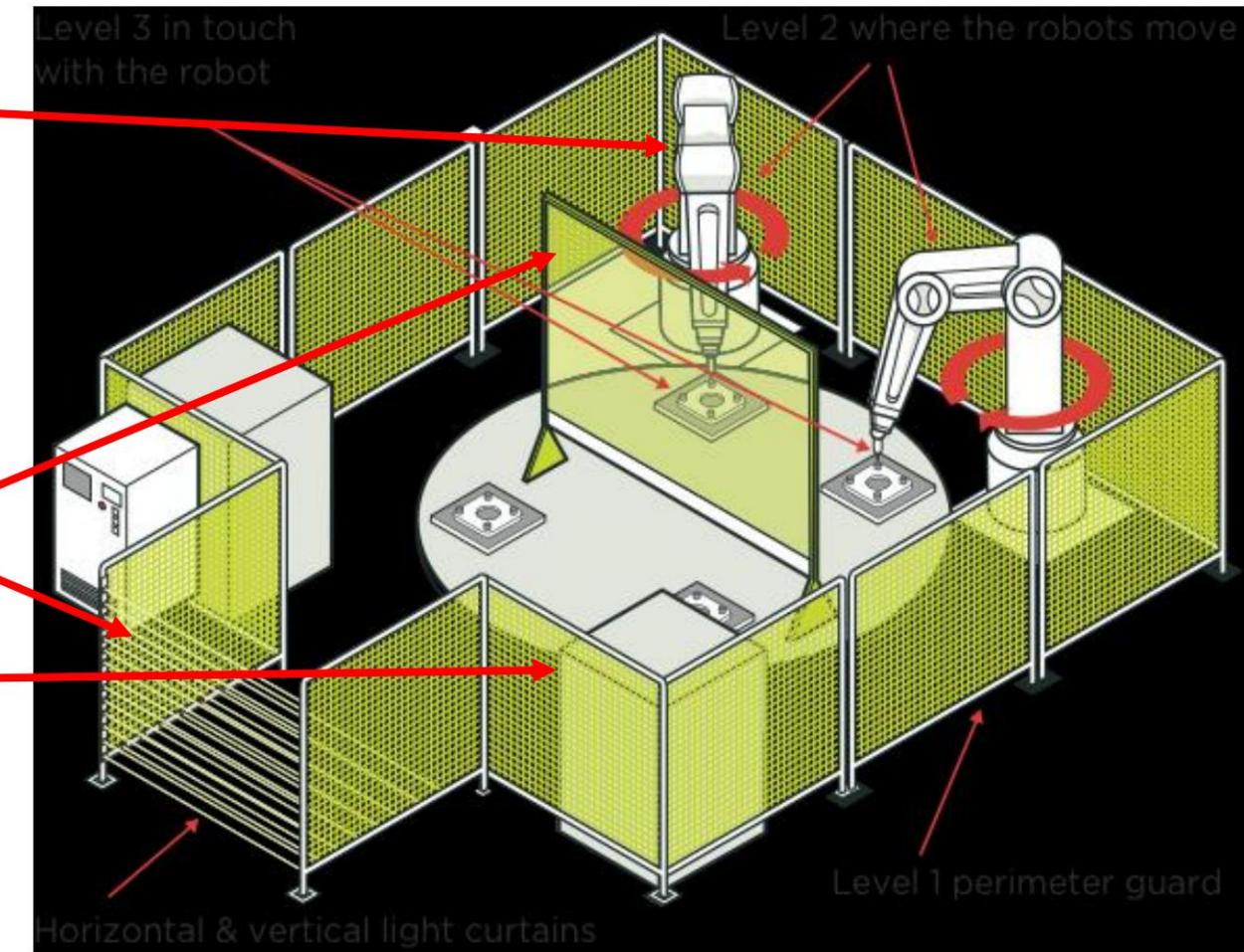
Esempio di mappatura: gabbia del braccio robotico

parte della sicurezza complessiva

EUC e sistema di controllo
EUC

che dipende dal corretto
funzionamento dei sistemi
di sicurezza E/E/PE

misure di riduzione del rischio.



Analisi dei pericoli e dei rischi

L'analisi dei rischi e dei pericoli è il processo volto a determinare il "livello di integrità della sicurezza" target (vale a dire "quanta sicurezza dobbiamo aggiungere al sistema") in base alla valutazione di diversi fattori quali l'esposizione al pericolo, la gravità delle conseguenze, la controllabilità e/o la possibilità di evitare il pericolo.

Gli standard di sicurezza forniscono solo linee guida e non procedure obbligatorie. Ad esempio, l'approccio basato sul grafico dei rischi.

Esempio HARA – ISO26262

Gravità (S)	Esposizione (E)	Controllabilità (C) Risultato ASIL
S3	E4	C3 ASIL D
S3	E4	C2 ASIL C
S3	E4	C1 ASIL B
S3	E3	C3 ASIL C
S3	E3	C2 ASIL B
S3	E3	C1 ASIL A
S2	E4	C3 ASIL C
S2	E4	C2 ASIL B
S2	E4	C1 ASIL A
S1	Qualunque	QM

Gravità (S) — Gli esempi vanno da S0 (nessun ferito) a S3 (ferite potenzialmente letali o fatali).

Esposizione (E) — Varia da E0 (incredibile) a E4 (alta probabilità).

Controllabilità (C) — Varia da C0 (controllabile in generale) a C3 (difficile da controllare)

Come misurare la sicurezza: livelli di integrità della sicurezza

Integrità della sicurezza: è un modo per misurare la probabilità che un sistema di sicurezza E/E/PE esegua correttamente una determinata funzione di sicurezza in determinate condizioni e tempi. Di conseguenza, esistono Livelli di Integrità della Sicurezza (SIL).



Livelli simili compaiono in altri standard di sicurezza (ASIL A->D in ISO26262, PL a->e in IEC13849, ecc.)



Ecosistema degli standard di sicurezza



IEC 61508-4

Edition 2.0 2010-04

**INTERNATIONAL
STANDARD****NORME
INTERNAZIONALE**

IEC61508 è il meta-standard

Ogni standard di sicurezza “legacy” definiva la sua proprietà:

- Ambito di applicazione (affinato)
- Criteri di valutazione del rischio (adattati all'applicazione)
- Livelli di integrità della sicurezza

I concetti e le definizioni generali sono generalmente ereditati dalla norma IEC61508.

Standard di sicurezza: approccio prescrittivo vs. basato sul rischio

Caratteristica	Basato sul rischio	Prescrittivo
Approccio	Basato sul rischio Ciclo di vita della sicurezza	Risolto, in base a requisiti dettagliati
Applicazione	Ampi sistemi di sicurezza industriale	Linee di prodotti specifici
Valutazione del rischio	Centrale e obbligatorio	Minimo o nessuno
Ciclo di vita della sicurezza	Definito e applicato	Spesso non definito
Verifica	Verifica e convalida formale	Test prescritti
Flessibilità	Alto	Basso
Focus sulla certificazione	Sicurezza funzionale e integrità della sicurezza Livello raggiunto	Conformità del prodotto

Basato sul rischio: IEC 61508 e tutti i suoi derivati, ISO 13849

Difetti e guasti

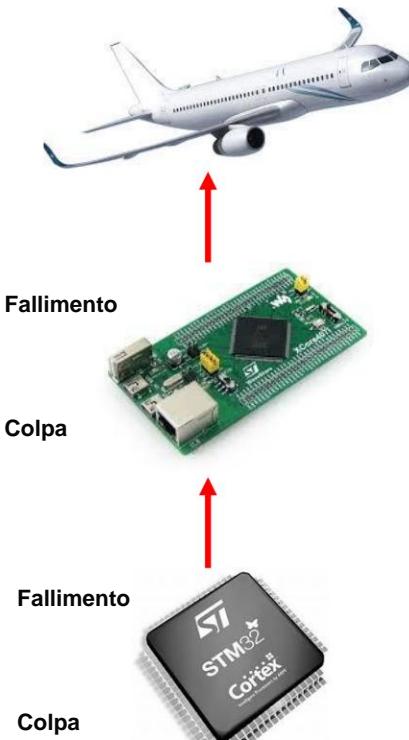
Guasto: condizione anomala che può causare una riduzione/perdita della capacità di un'unità funzionale di eseguire una specifica funzione richiesta

Guasto: cessazione della capacità di un'unità funzionale di fornire una funzione/operazione richiesta in un modo diverso da quello richiesto

La definizione è generica e include qualsiasi tipo di guasto o avaria.

I guasti sono la causa dei fallimenti.

Colpa → Fallimento



Nei sistemi "modulari" i guasti si propagano dagli strati inferiori a quelli superiori.

Perché ci concentriamo sui fallimenti

I guasti sono sempre la causa principale. MA se non causano un guasto, non vi è alcun rischio associato.

I guasti “emergono”, si osservano solo attraverso i guasti causati.

Un singolo guasto può essere la causa di molteplici guasti.

La sicurezza **dipende dal**
corretto funzionamento del
Sistemi di sicurezza E/E/
PE

e ad altre possibili misure di
riduzione del rischio.



Ci concentriamo sui guasti in
quanto rappresentano la
cessazione della capacità del
sistema di eseguire una
funzione e quindi potenzialmente
impediscono che la sicurezza venga raggiunta.

Il danno è causato da un
funzionamento errato o mancante
del sistema, quindi causato da
guasti e non da errori.

Il bivio della sicurezza funzionale



guasto hardware casuale: guasto che si verifica in un momento casuale e che deriva da uno o più possibili meccanismi di degradazione nell'hardware

guasto sistematico: guasto, correlato in modo deterministico a una certa causa, che può essere eliminato solo mediante una modifica della progettazione o del processo di fabbricazione, delle procedure operative, della documentazione o di altri fattori rilevanti

ATTENZIONE: questo concetto chiave è fonte di continui fuorvianti

Due tipi di fallimenti: RHF vs Sistematico

Guasti hardware casuali: il

il sistema è fisicamente danneggiato (in modo permanente o transitorio) che porta a il fallimento della funzionalità prevista



- Basato sull'analisi della probabilità (imprevedibile)
- Principalmente quantitativo (numeri!)
- Contromisure basate sul rilevamento e controllo dei guasti

Fallimenti sistematici: il sistema è sbagliato

progettato e quindi sotto una certa combinazione delle condizioni esterne/interne, o input, esso si discosterà dalla funzionalità prevista ("insetti")



- Basato sull'analisi del processo/ metodo (deterministico)
- Principalmente qualitativo (orientamento)
- Contromisure basate sulla prevenzione dei guasti (qualità del processo)

Che cosa (NON) è la sicurezza

La sicurezza funzionale NON è sicurezza

Sicurezza: si occupa di guasti su dispositivi/software (sistema non funzionante a causa di un guasto)

Sicurezza: si occupa di violazioni/attacchi intenzionali su dispositivi/hardware (le informazioni e/o il controllo del sistema vengono violati da un aggressore esterno)

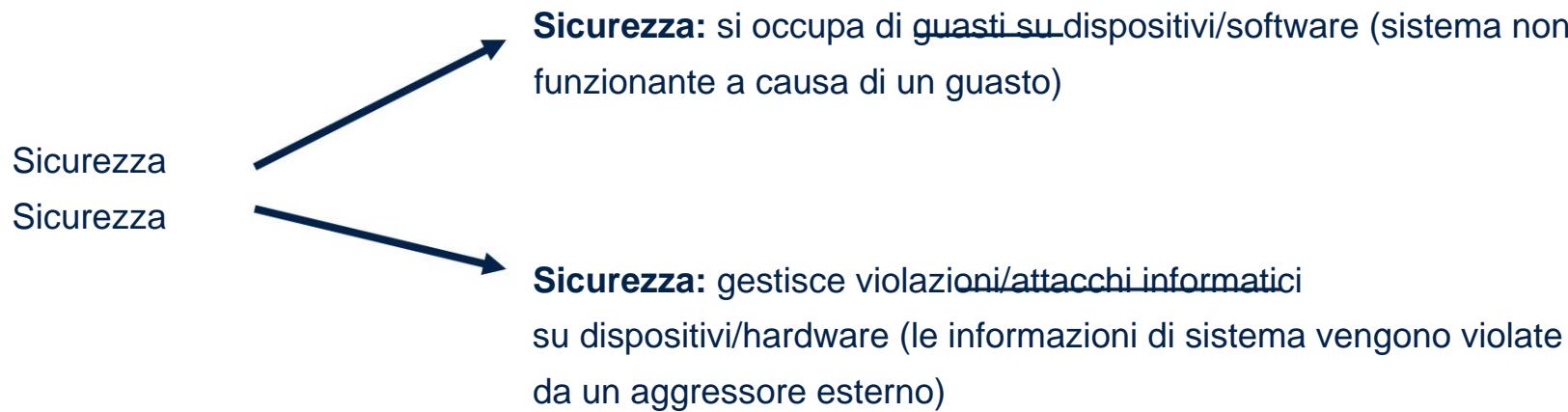
(Nota: solitamente la sicurezza funzionale considera come potenziale pericolo un uso improprio ragionevolmente prevedibile da parte dell'utente finale e non un uso improprio volontario).

La sicurezza funzionale NON è affidabilità

La sicurezza riguarda la capacità di un sistema di rilevare situazioni anomale e di raggiungere uno specifico stato sicuro. L'affidabilità riguarda la durata di vita dei sistemi perfettamente funzionanti (tutti quelli non funzionanti i sistemi sono considerati uguali: non esistono concetti di mitigazione/rilevamento, solo ridondanza se il caso)

Testo inglese: senza frantendimenti (?)

... in questa formazione utilizzeremo ampiamente la terminologia inglese perché, sfortunatamente, le altre lingue europee sono un po' fuorvianti:



Inoltre, nonostante la norma IEC61508 sia stata pubblicata in inglese e francese, la formulazione in inglese è ben nota alla comunità industriale e della sicurezza, quindi quest'ultima consente una maggiore comprensione/lettura dei documenti.

... ma nella terminologia inglese permangono ancora delle discrepanze...

Lezione n. 2

Teoria dei guasti casuali dell'hardware



Riepilogo:

- Guasti e guasti (hardware casuali)
- Tasso di fallimento
- Classificazione dei guasti
- Metriche di sicurezza: assolute e relative

Guasti casuali hardware: MODELLI DI GUASTO

Per i componenti semiconduttori, esistono due modelli di guasto principali: •

- Guasti permanenti
- Guasti transitori

Difetti permanenti

- Il guasto è irreversibile (ad esempio, transistor rotto, cella di memoria sicuramente aperta o in cortocircuito)
- Fonti: invecchiamento, stress termico

guasti transitori

- L'errore non è permanente (può essere un'inversione di bit in un registro o un problema nella logica) • Le inversioni di bit (note anche come "errori soft") possono essere corrette (o cancellate, ad esempio aggiornando per un FF)
- Fonti: EMI, radiazioni del pacco (particelle alfa), Radiazione solare (particelle di neutroni)

Difetti permanenti

Gli standard di sicurezza come IEC 61508 o ISO 26262 specificano il set minimo di guasti permanenti da considerare (principalmente come "guida"):

- ÿ Bloccato a 0/1
- ÿ Circuito aperto
- ÿ Cortocircuito
- ÿ Collegamento
- ÿ Alta impedenza
- ÿ Deriva
- ÿ Oscillazione

Nota: possono essere definiti come "fallimenti" generati da errori sottostanti, a seconda del livello di astrazione selezionato!

guasti transitori

Anche per i guasti transitori, gli standard di sicurezza come IEC 61508 o ISO 26262 specificano il set minimo di guasti da considerare (principalmente come "guida"):

- ÿ Inversioni di bit sui registri
- ÿ Inversioni di bit sulle celle di memoria volatile (RAM)
- ÿ Problemi su bus/connessioni/ingressi

Come stabilire guasti/guasti

Dato un determinato componente o tecnologia, sorgono dubbi su come stabilire un elenco ragionevole di potenziali guasti e conseguenti guasti. Alcuni schemi principali sono possibili:

- ÿDi solito, ogni standard di sicurezza elenca il set minimo di guasti/guasti da analizzare in base a al livello di integrità della sicurezza target (più alto è l'integrità, più grande sarà l'insieme di guasti/guasti)
- ÿDocumentazione collaterale che elenca potenziali guasti/avariamenti, vedere ad esempio il documento di riferimento della NASA [R1]. (cercare “modalità di guasto” per componenti discreti e analogici)
- ÿGli strumenti all'avanguardia per l'analisi della sicurezza (ad esempio gli strumenti FMEDA) di solito forniscono un elenco pratico di guasti/avariamenti per ogni tipo di componente.

Come affrontare i fallimenti casuali

I guasti casuali devono essere mitigati. Sono possibili due modi

- Prevenzione degli errori
- Rilevamento guasti

Prevenzione degli errori

- La probabilità di guasto è ridotta, ad esempio tramite la ridondanza di due funzioni indipendenti. Approccio ottimale per applicazioni mission-critical e per aumentare la disponibilità. Concetto associato di Hardware Fault Tolerance (HFT)

Rilevamento guasti

- Il sistema include nuove funzioni diagnostiche aggiuntive dedicate al rilevamento dei guasti. Di solito sono chiamati meccanismi di sicurezza
- Una volta rilevato un guasto, è possibile apportare una correzione (ad esempio vedere ECC) oppure (se non è possibile) il sistema viene informato del guasto e la sicurezza viene raggiunta con altri mezzi (il sistema viene guidato in stato sicuro)

Come gestire i guasti casuali - esempi

Esempio di prevenzione degli errori :

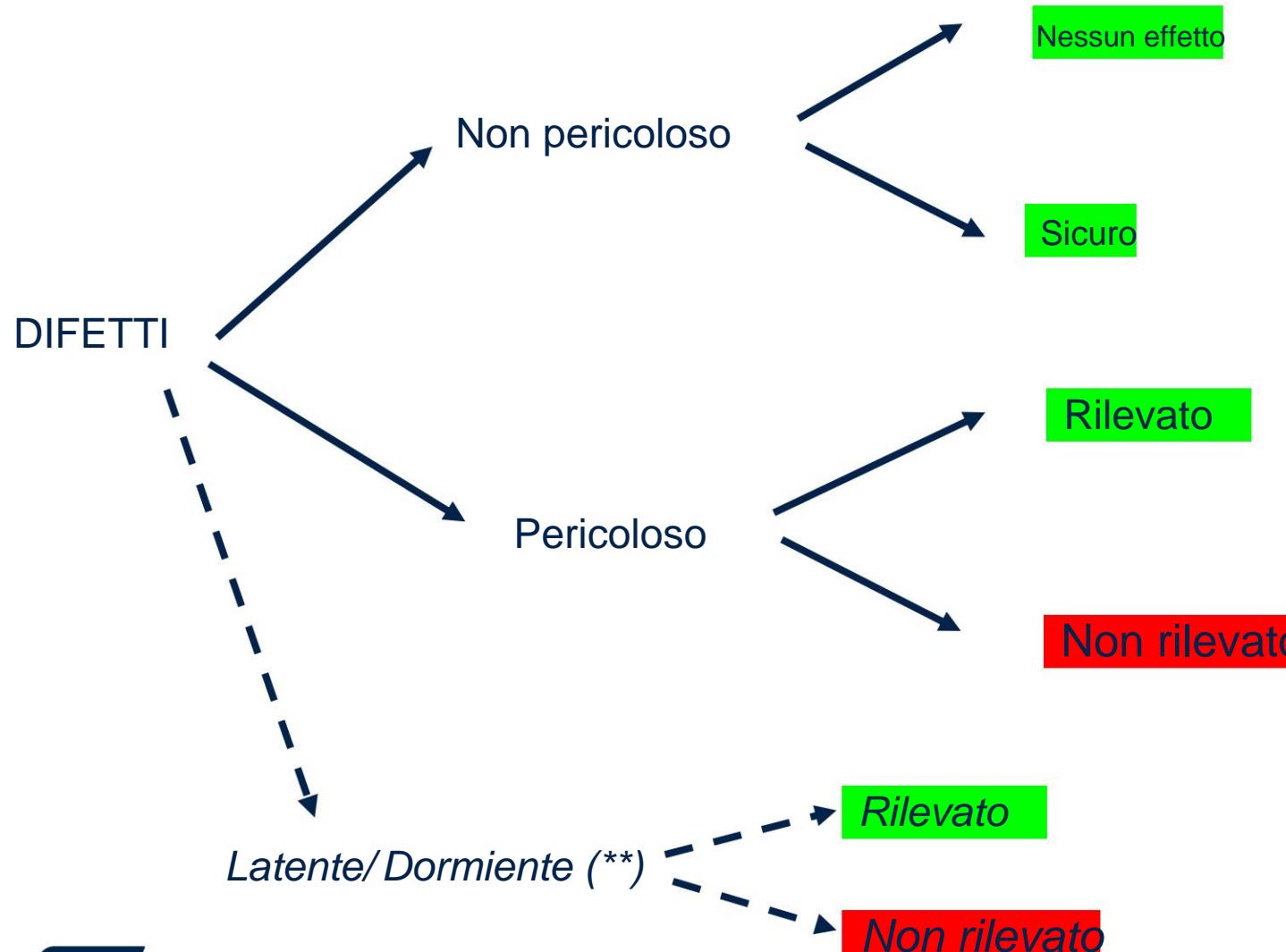
Blocco dei registri tramite chiave: l'accesso in scrittura ai registri di configurazione è protetto da una chiave (sequenza software di comandi da rispettare per sbloccare). Evita errori legati a scritture indesiderate sui registri.

Esempio di rilevamento guasti :

Parità: a ogni parola viene aggiunto un bit di parità (sono possibili più schemi), consentendo la scoperta di errori a livello di singolo bit durante la lettura dei dati (il bit di parità calcolato non corrisponde a quello memorizzato).

Rileva errori di inversione di singoli bit.

Classificazione dei guasti (*)



(*) Nota: questa terminologia può essere applicata anche ai guasti

(**) definito solo su alcuni standard di sicurezza

Classificazione delle faglie (definizioni)

I guasti/guasti possono essere classificati come:

Nessun effetto/nessuna parte/non correlato alla sicurezza: che interessa l'hardware non coinvolto nell'implementazione della funzione di sicurezza

Sicuro: guasto/guasto che guida (o aiuta a mantenere) il sistema in uno stato sicuro (in cui la sicurezza è raggiunta)

Pericoloso: in grado di interferire con la funzione di sicurezza

Rilevato: un guasto/guasto la cui presenza è rivelata da uno o più meccanismi di sicurezza

Non rilevato: il contrario del precedente

Latente/dormiente: un guasto che non può interferire direttamente con la funzione di sicurezza, ma che può farlo in presenza di un'altra.

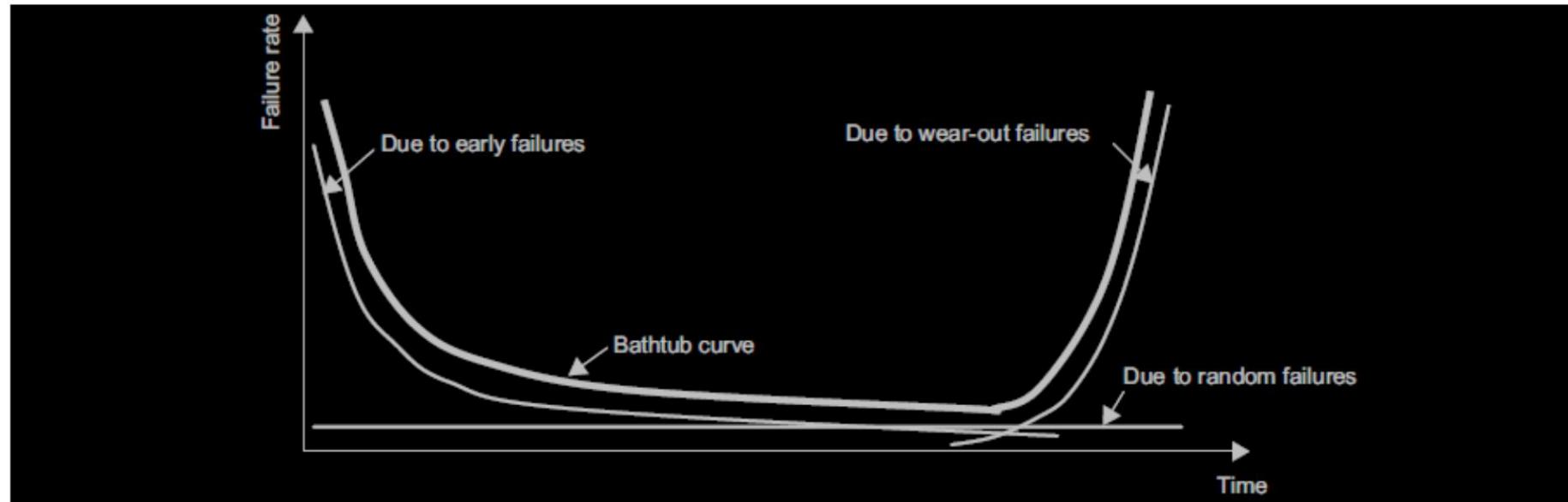
Nota: definizioni generali, un mix tra le definizioni IEC 61508 e ISO 26262

Guasti dei semiconduttori

Guasti Precoci: nel processo di produzione, i dispositivi a semiconduttore possono presentare difetti dovuti alla presenza di minuscole particelle, nonché a variazioni nelle attrezzature di produzione e nelle dimensioni. Questo fenomeno è noto come densità iniziale dei difetti.

Guasti casuali: i guasti derivanti da difetti di produzione si attenueranno con il tempo.

Guasti da usura: i semiconduttori si guastano quando raggiungono i limiti della loro durabilità di base. Questo periodo è chiamato "zona di usura". I guasti da usura variano a seconda delle differenze nelle sollecitazioni applicate al dispositivo durante l'uso.



Componenti discreti

I componenti discreti tendono a mostrare un tasso di guasto costante (resistori, induttori, condensatori ceramici), mentre pochi componenti specifici presentano una lieve curva a vasca da bagno (condensatori elettrolitici).

Le connessioni PCB e i connettori meccanici presentano un tasso di guasto costante con una fase di aumento dell'usura , che dipende principalmente dall'invecchiamento e dai cicli di sollecitazione meccanica.

I relè mostrano spesso una curva a vasca da bagno con una fase di usura evidente dovuta all'invecchiamento e ai cicli di commutazione/carico elettrico.

CONCLUSIONE: durante la ragionevole vita operativa di un sistema elettronico, tutti i guasti possono essere considerati nella loro fase di valore costante.

tasso di fallimento

tasso di guasto: parametro di affidabilità ($\dot{y}(t)$) di un singolo componente o sistema (entità) tale che $\dot{y}(t).dt$ è la probabilità di guasto di questa entità entro $[t, t+dt]$ nell'ipotesi che non si sia guastata durante $[0, t]$.

Il tasso di guasto \dot{y} è quindi una probabilità divisa per il tempo (importante!)

Si misura in FIT; 1 FIT equivale a 1 guasto ogni 10^{10} ore

Il tasso di guasto di una serie di componenti/sistemi è la somma dei tassi di guasto di ciascuno di essi. Il tasso di guasto dei sistemi ridondanti (parallel) è generalmente non costante.

Informazioni sui tassi di guasto di base

Il “tasso di guasto di base” per un dato componente semiconduttore è il tasso di guasto associato a un sottoinsieme specifico e individuale del componente stesso: ad esempio, porzione dell’area del silicio, transistor, bit di memoria ecc.

Il tasso di guasto di base è un argomento controverso, poiché nel settore esistono metodi diversi (ad esempio test accelerati e/o modelli matematici) con diversi livelli di confidenza. Il principale potenziale problema è la combinazione di dati provenienti da fonti diverse nel sistema FMEDA.

- Per i guasti permanenti, le fonti di dati più diffuse sono
 - IEC62380 (e il suo modello equivalente in ISO26262-11)
 - Norma Siemens SN29500-2:2010 (attualmente un po' obsoleta ma ancora ampiamente utilizzata)
- Per guasti transitori, forte dipendenza dalla tecnologia IC, dal pacchetto (LA vs ULA), dall’altitudine, schermatura. I dati provengono solitamente da test di irradiazione o tabelle ITRS

Metriche di sicurezza: assolute vs relative

Metriche assolute

ÿ espresso in FIT (1 guasto in 1 miliardo di ore)

Dipendono fortemente dalle ipotesi sulle condizioni operative (temperatura, cicli)

Forniscono una misura della probabilità di fallimento nel tempo

Metriche relative

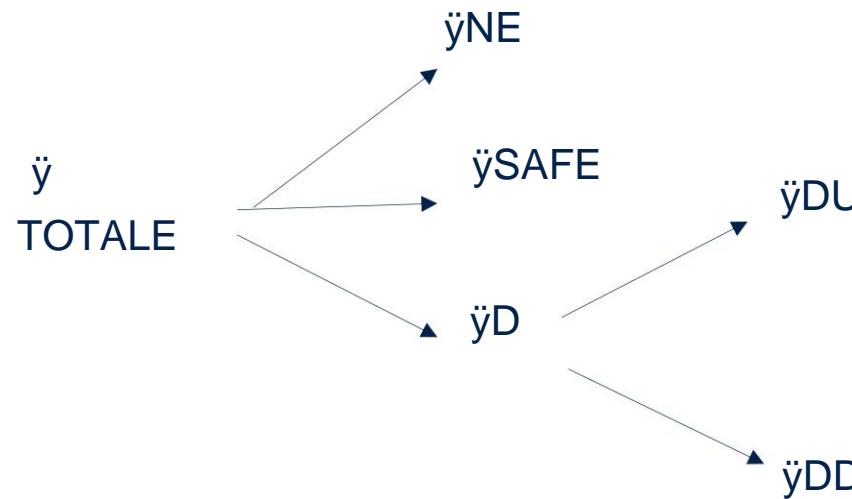
Espresso in percentuali dallo 0% al 100%

Sono il rapporto tra termini omogenei (ÿs) quindi dipendono solo dall'architettura

Esprimono una valutazione numerica della combinazione complessiva di tolleranza ai guasti, meccanismi di sicurezza e misure di mitigazione.

Informazioni sulle metriche di sicurezza – IEC 61508

Metriche assolute, \ddot{y} espresso in
FIT (1 guasto in 1 miliardo di ore)



Metriche relative
(percentuali dallo 0% al 100%)

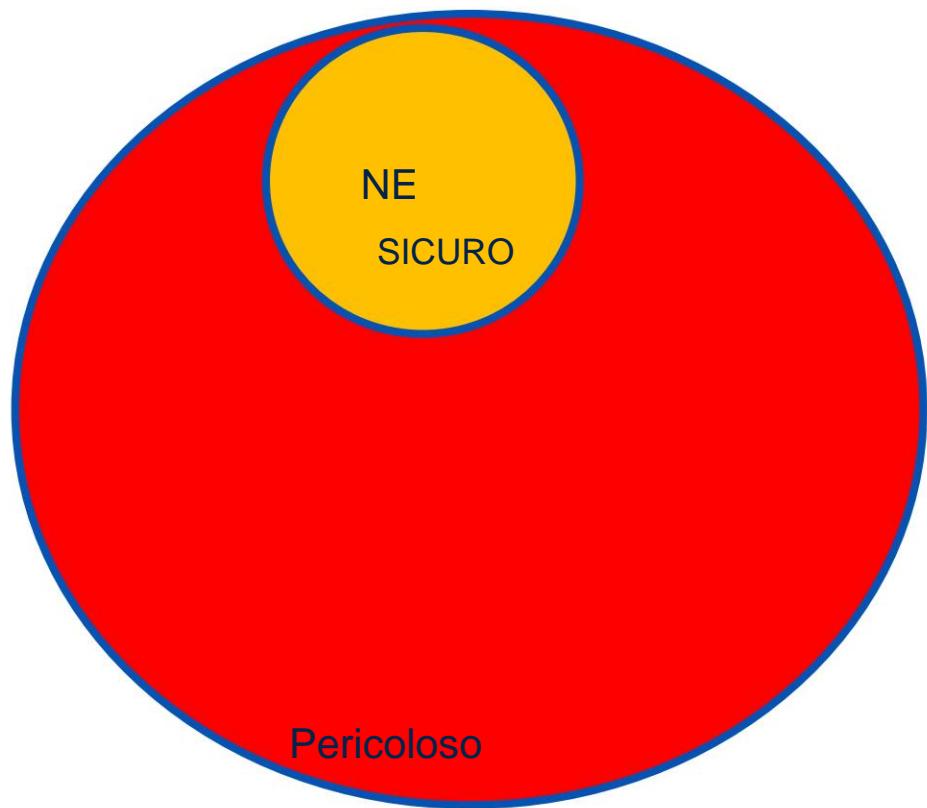
Copertura diagnostica

$$CC = \frac{\ddot{y}}{\ddot{y}}$$

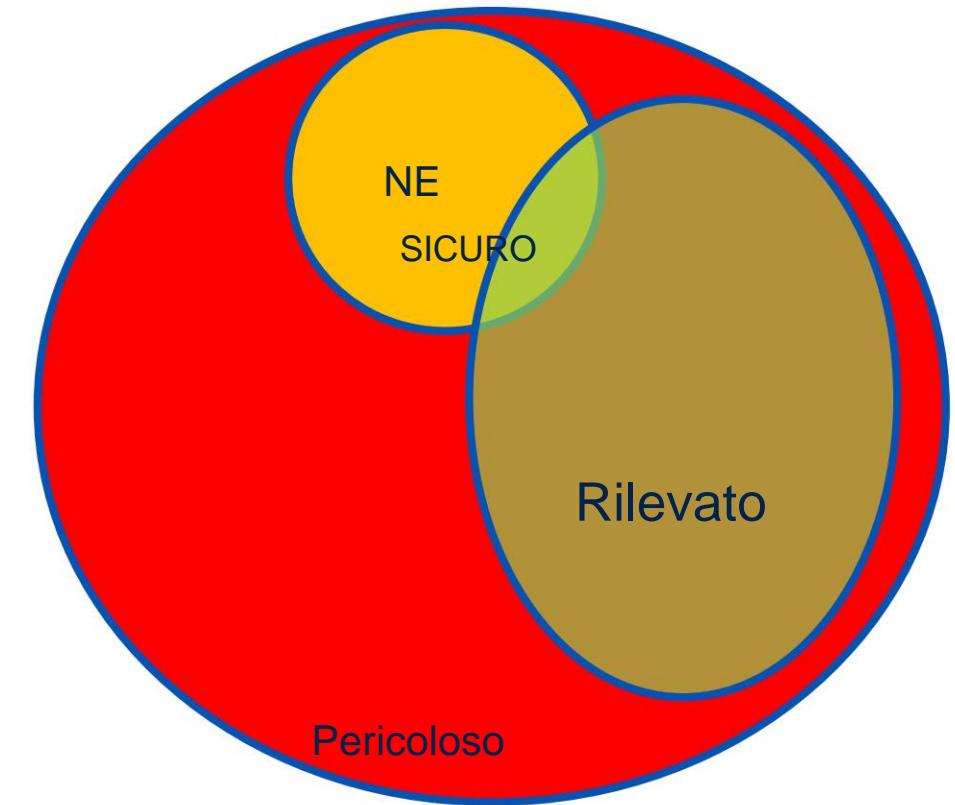
Frazione di guasti sicuri

$$SFF = \frac{\ddot{y} + \ddot{y}}{\ddot{y} + \ddot{y} + \ddot{y}}$$

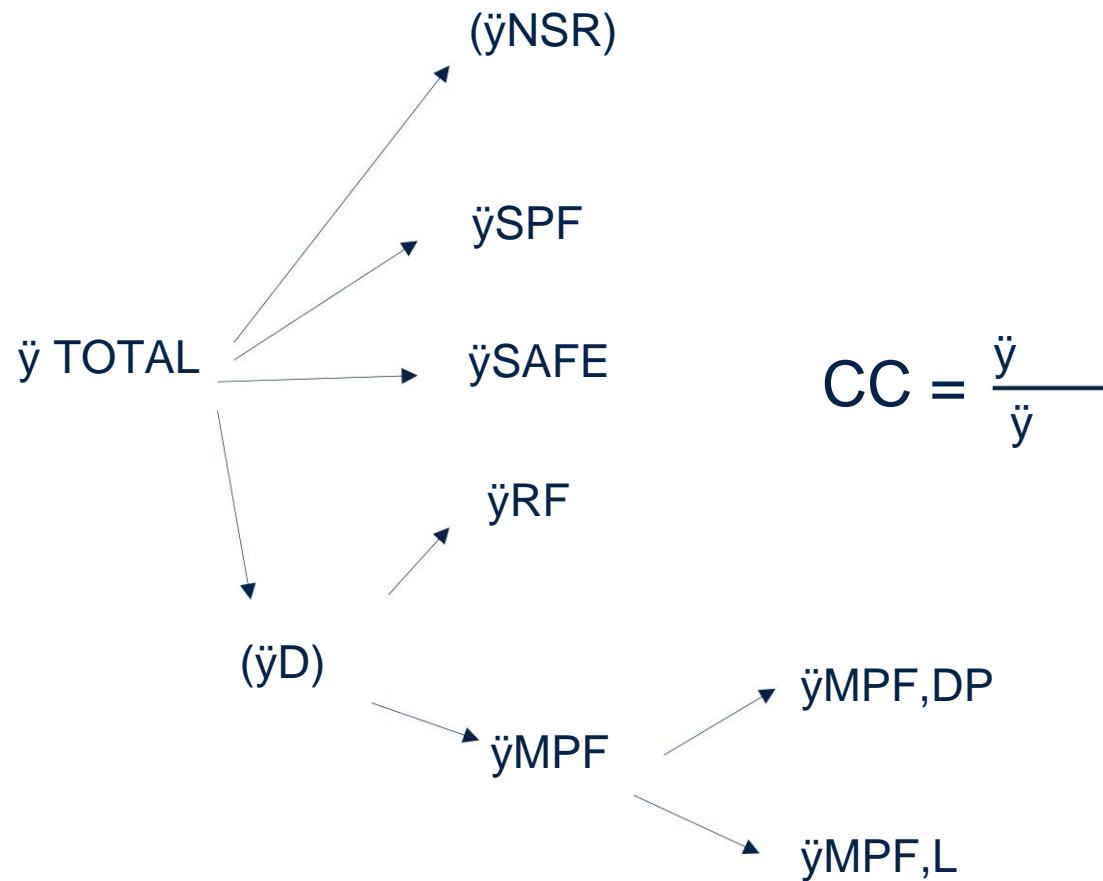
Rilevamento dei guasti



Aggiunta
di diagnostica



Informazioni sulle metriche di sicurezza – ISO 26262



$$CC = \frac{\ddot{y}}{\ddot{y}}$$

Metrica di guasto a punto singolo

$$SPFm = \frac{\ddot{y} + \ddot{y} + \ddot{y} +}{\ddot{y} + \ddot{y}}$$

Metrica di guasto latente

$$LFm = \frac{\ddot{y} + \ddot{y}}{\ddot{y} \ddot{y} \ddot{y} + \ddot{y} \ddot{y}}$$

Nota: la classificazione dei guasti ISO 26262 è piuttosto specifica a causa della sua classificazione esplicita per guasti doppi

Metriche di sicurezza relativa - obiettivi

Obiettivi delle metriche relative IEC 61508-2 (*)

SFF	HFT = 0	HFT = 1	HFT = 2
< 60%	Non consentito	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL 4

(*) Per un elemento di tipo B
SFF è il riferimento

Obiettivi delle metriche relative ISO 26262

SPFm	
90% - 97%	ASIL B
97% - 99%	ASIL C
>99%	ASIL D

LFm	ASIL
60% - 80%	ASIL B
80% - 99%	ASIL C
>90%	ASIL D

Metriche di sicurezza assoluta - obiettivi

SIL	Frequenza media dei guasti pericolosi (per HD/CM)
SIL 1	1E3 FIT < PFH < 1E4 FIT
SIL 2	100 FIT < PFH < 1000 FIT
SIL 3	10 FIT < PFH < 100 FIT
SIL 4	1 FIT < PFH < 10 FIT

Obiettivi delle metriche relative IEC 61508-2

ASIL	PMHF Metrica probabilistica per hardware casuale Fallimenti
ASIL B	PMFH < 100 FIT
ASIL C	PMFH < 100 FIT
ASIL D	PMFH < 10 FIT

Obiettivi delle metriche assolute ISO 26262

Nota: il calcolo di PHF/PMHF è collegato ai valori di $\bar{y}DU/\bar{y}RF$. I dettagli saranno forniti nella lezione relativa alle architetture di sicurezza.

Quanti guasti ci sono nel sistema?

In linea di principio, da 1 a N guasti possono interessare contemporaneamente il sistema. Se i guasti sono indipendenti, la probabilità di guasti multipli è bassa e comunque dipende dal tempo.

Ogni norma di sicurezza fornisce indicazioni esplicite sul numero minimo di guasti *simultanei* da considerare nell'analisi del sistema:

La norma IEC 61508 richiede guasti singoli, ma non chiede di "considerare" scenari di guasti multipli

ISO 26262 richiede guasti singoli + un secondo guasto solo sulla diagnostica (latente) $N>2$ è fuori dall'ambito

ISO 13849 richiede un solo errore, ad eccezione di PL/architettura specifici in cui è richiesto HFT=1

Guasti non indipendenti

Guasto dipendente: guasti causati da eventi non indipendenti, ovvero $P(A \text{ e } B) > P(A) \times P(B)$.

Guasto di causa comune: guasto che causa più guasti simultanei in un sistema multicanale

(esempio: guasti dell'alimentazione comune per un sistema multicanale)

Colpa → Fallimento



Problemi correlati

- Non possono essere inclusi nei calcoli DC, ѕ "standard"
- Possono potenzialmente compromettere la tolleranza ai guasti del sistema

Bibliografia



Documenti di riferimento

[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

Grazie

© STMicroelectronics - Tutti i diritti riservati.

Il logo ST è un marchio commerciale o un marchio registrato di STMicroelectronics International NV o delle sue affiliate nell'UE e/o in altri paesi.

Per ulteriori informazioni sui marchi ST, consultare www.st.com/trademarks.

Tutti gli altri nomi di prodotti o servizi appartengono ai rispettivi proprietari.





Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale
STMicroelectronics

Lezione n. 3

**Teoria della capacità sistematica, incluso il modello V e i preliminari su
Software e strumenti**



Riepilogo:

- Ciclo di vita della sicurezza
- **Modello V**
- **Note sui requisiti**
- **Sviluppo software**
- **Valutazione degli strumenti**

Come affrontare i fallimenti sistematici

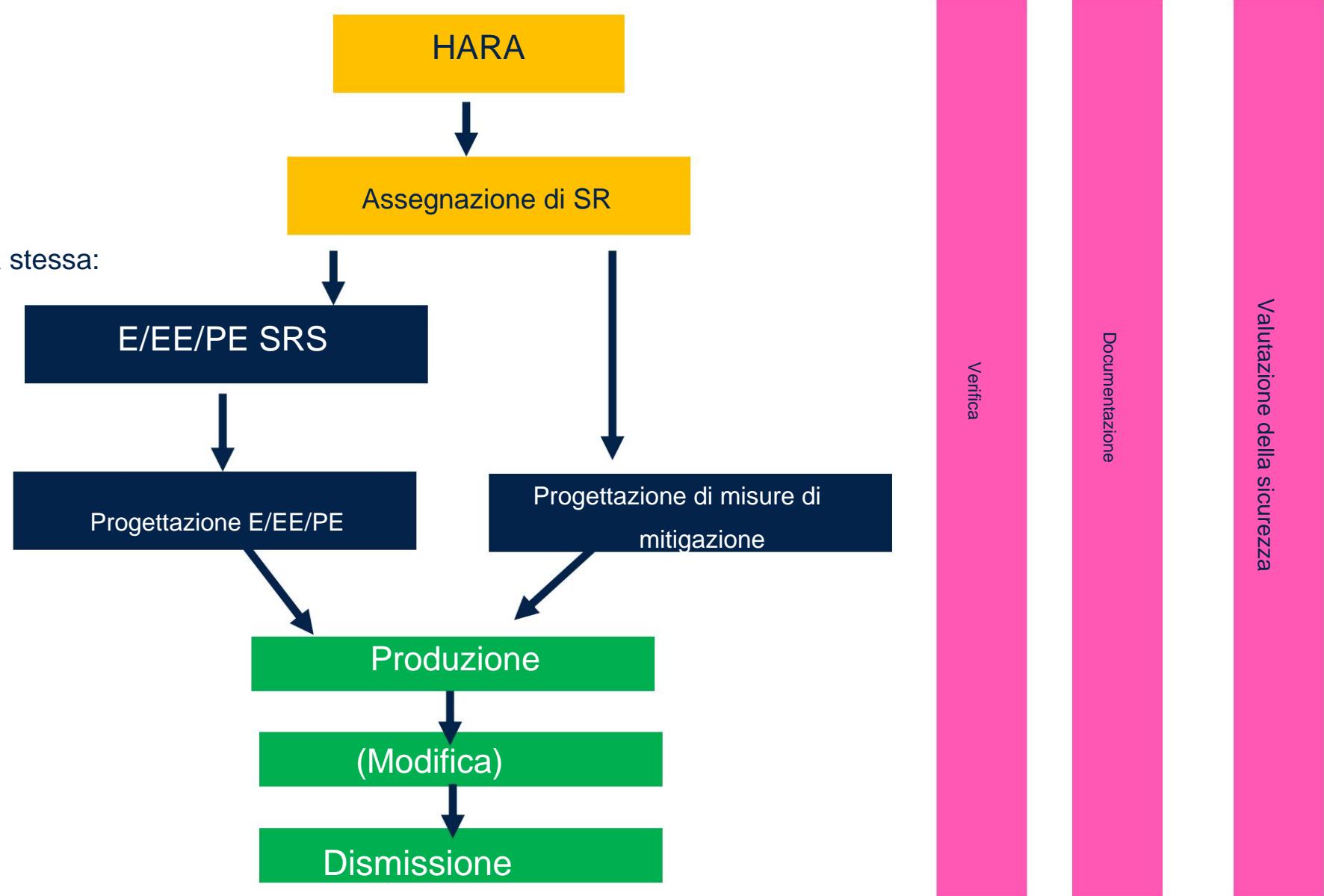
Mentre la maggior parte degli standard di sicurezza richiede di mitigare/considerare i guasti sistematici, la questione correlata è più complessa per gli standard basati sul rischio che stabiliscono un livello specifico di integrità della sicurezza anche per i guasti sistematici.

Esistono due modelli principali:

- **Ciclo di vita della sicurezza** formale (basato sulla rigorosa applicazione di regole di sviluppo personalizzate in base al livello di integrità della sicurezza)
- **Argomentazione comprovata in uso**, basata su prove di stabilità/assenza di difetti sistematici nel corso tempo
- I due modelli possono essere applicati anche al software incorporato e agli strumenti software.

Ciclo di vita della sicurezza

Ogni norma di sicurezza definisce il proprio specifico ciclo di vita della sicurezza; la struttura generale è sostanzialmente la stessa:



Verifica e convalida

La verifica è il processo di conferma, attraverso l'esame e l'evidenza oggettiva, che un prodotto, un sistema o un componente soddisfa i requisiti specificati. Risponde alla domanda: "Stiamo costruendo il prodotto correttamente?".

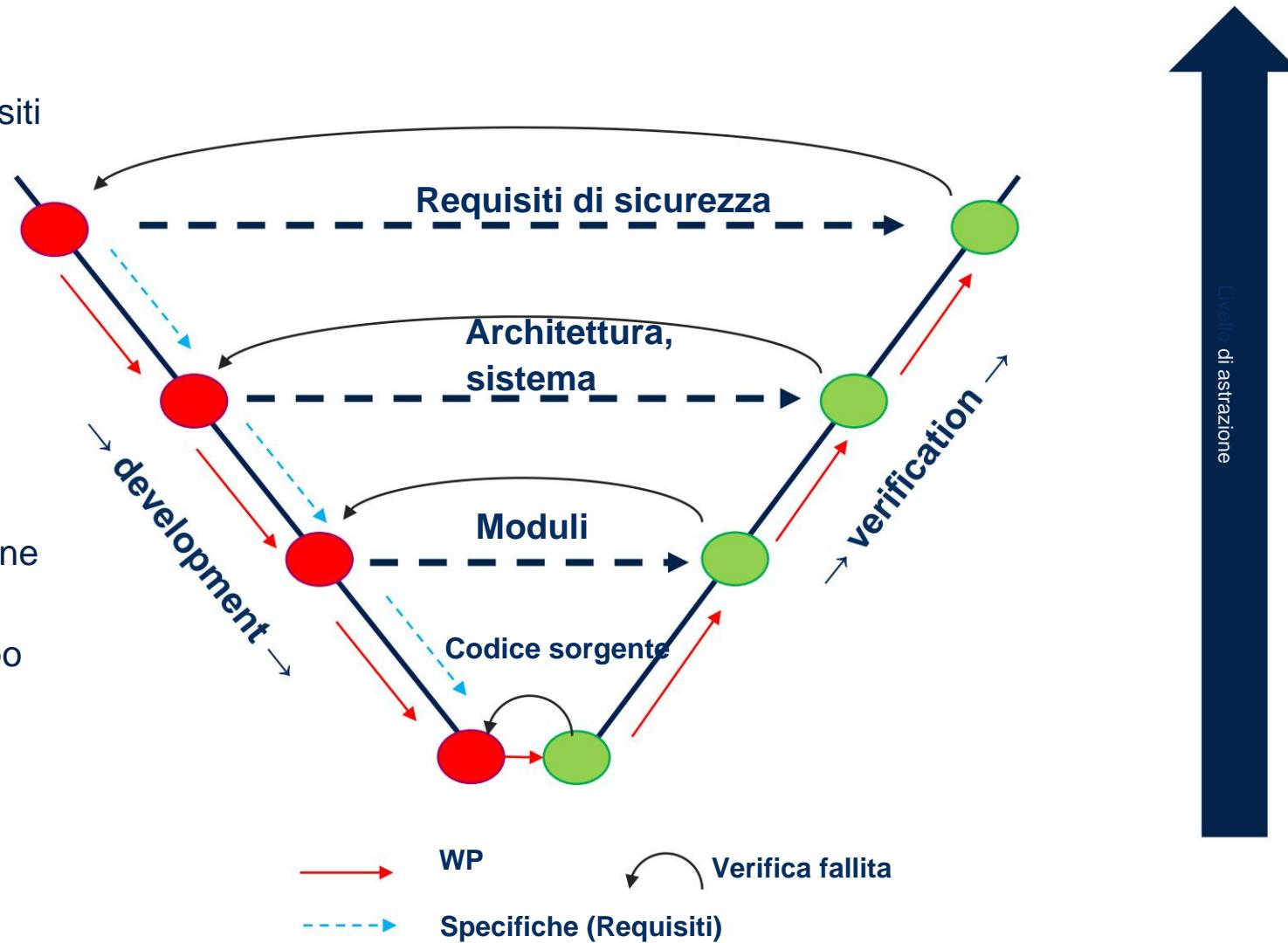
La convalida è il processo di conferma, attraverso l'esame e l'evidenza oggettiva, che il prodotto soddisfa i requisiti per l'uso specifico previsto nel mondo reale. Risponde alla domanda: "Stiamo costruendo il prodotto giusto?"

Aspetto	Verifica	Validazione
Scopo	Confermare che i requisiti siano implementati correttamente	Confermare che il prodotto soddisfa le esigenze dell'utente e l'uso previsto
Messa a fuoco	Conformità alle specifiche	Idoneità allo scopo
Attività tipiche	Revisioni, ispezioni, test di unità/componenti	Test a livello di sistema, test di accettazione dell'utente

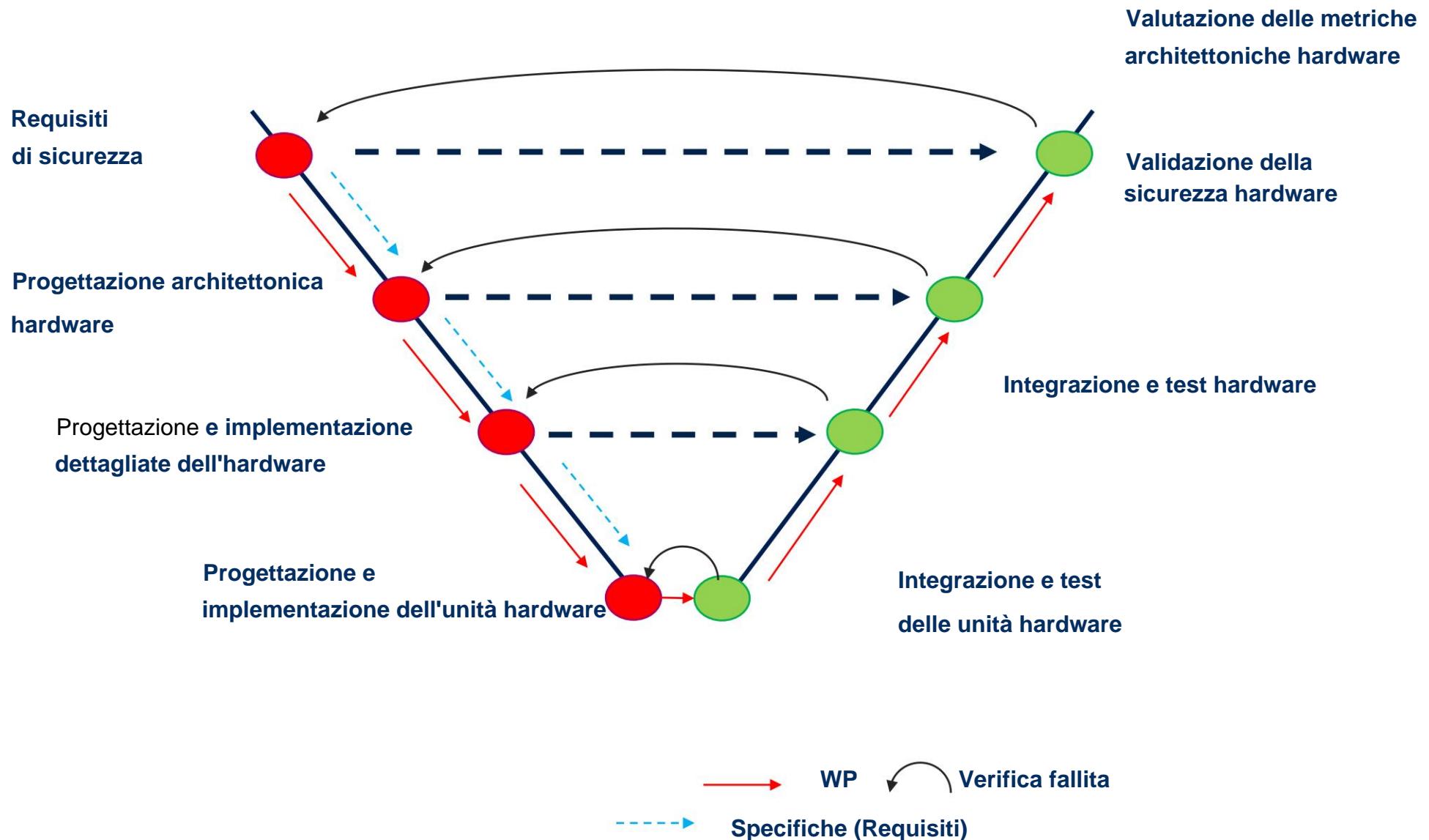
Caratteristiche del modello V (IEC 61508-3, ISO 26262-6)

Vantaggi

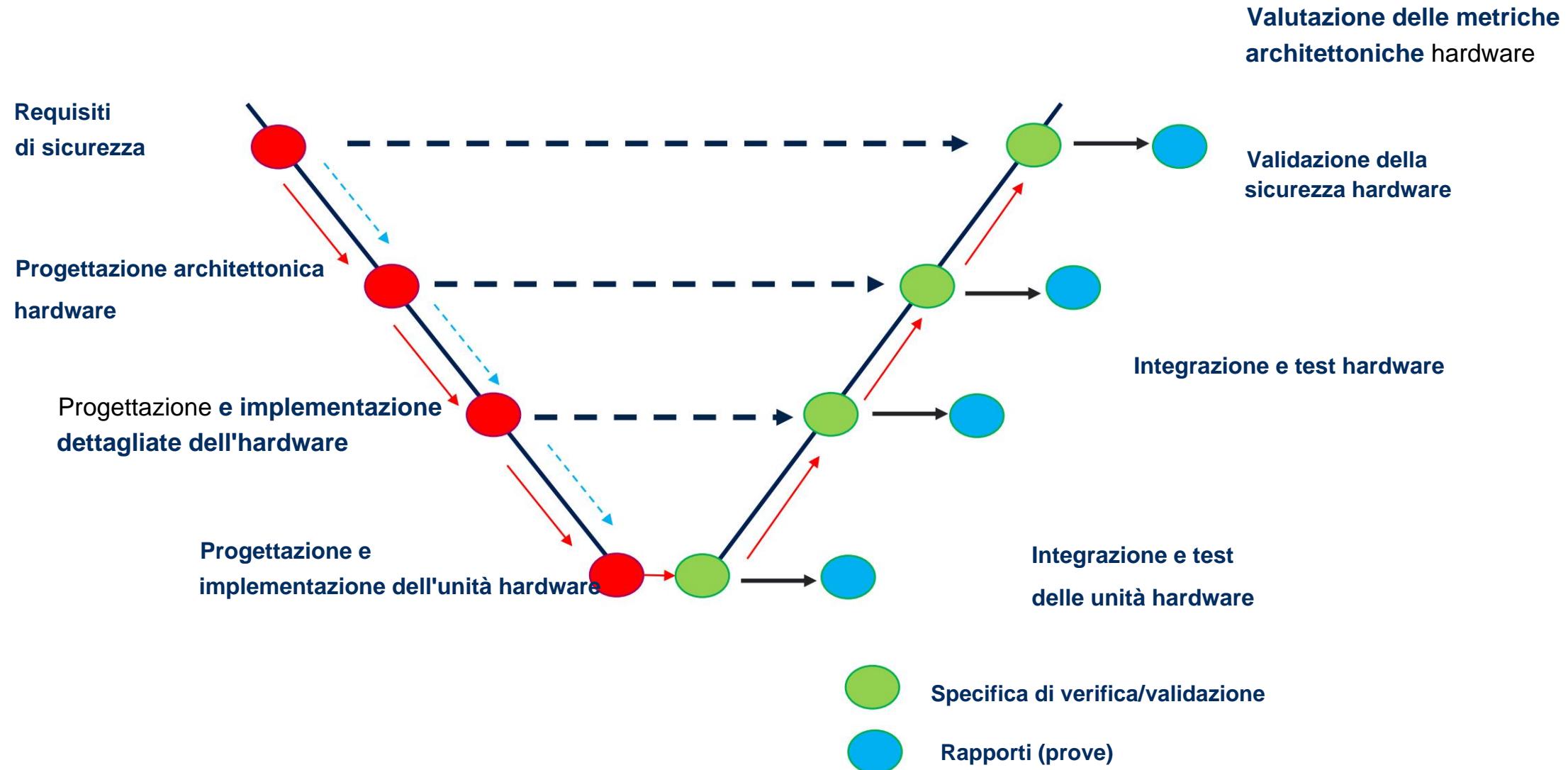
- L'approccio top-down è forzato
- Modello client/server basato sui requisiti tra le fasi
- Ingressi/uscite tra le fasi (WP) ben definito
- Test specificati allo stesso livello di astrazione dello sviluppo
- La non conformità dopo la verifica viene gestita gerarchicamente (potrebbe avere un impatto sulle fasi di sviluppo correlate)
- Tracciabilità garantita all'interno



Modello V per lo sviluppo hardware (ISO 26262-5) - fasi



Modello V per lo sviluppo hardware (ISO 26262-5) - documenti



Informazioni sulla tracciabilità

Il modello V della IEC61508 richiede la tracciabilità in avanti e all'indietro tra diversi set di requisiti di specifica e verifica. HR per SIL3/4, solo R per SIL1/2. Tra le altre tecniche, la tracciabilità è un'ottima risorsa per la sicurezza e la qualità nello sviluppo del software:

Tracciabilità futura: verifica che un
requisito venga adeguatamente affrontato
nelle fasi successive del ciclo di vita.



Pro: risorsa chiave per valutare
correttamente l'impatto di un cambiamento
in base all'aggiornamento/modifica dei
requisiti di alto livello

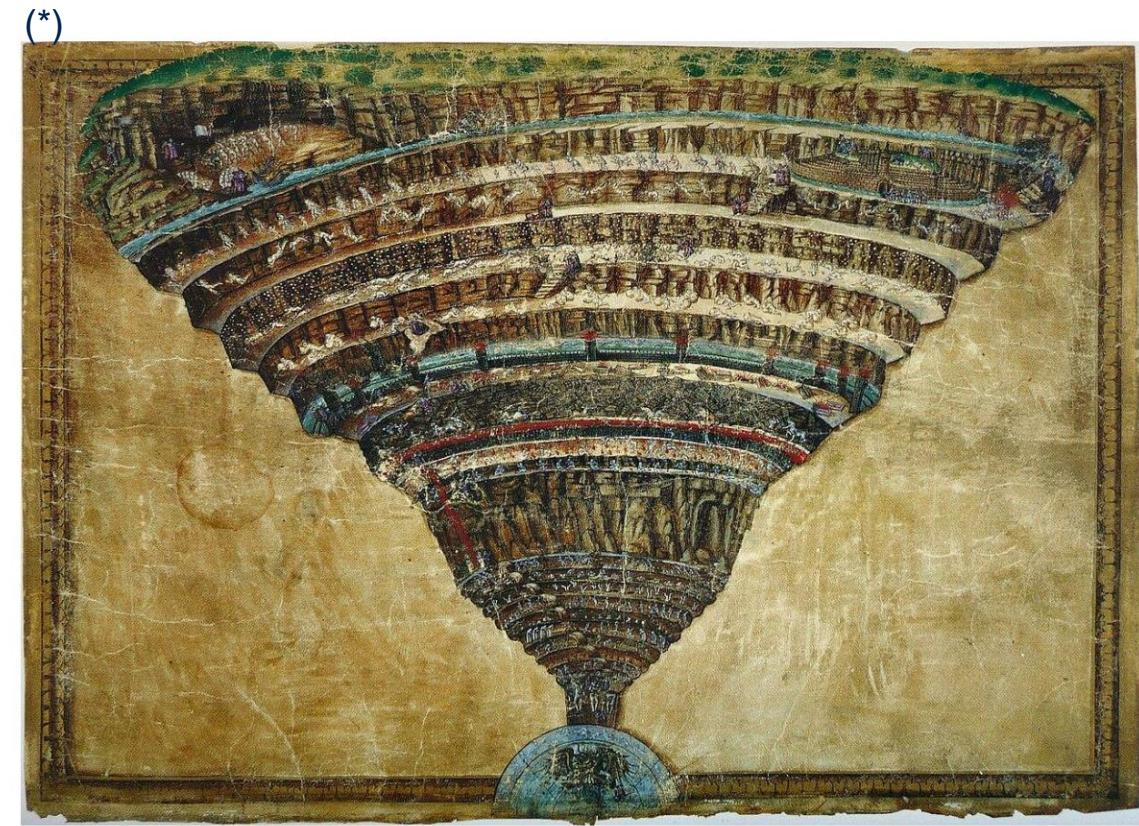
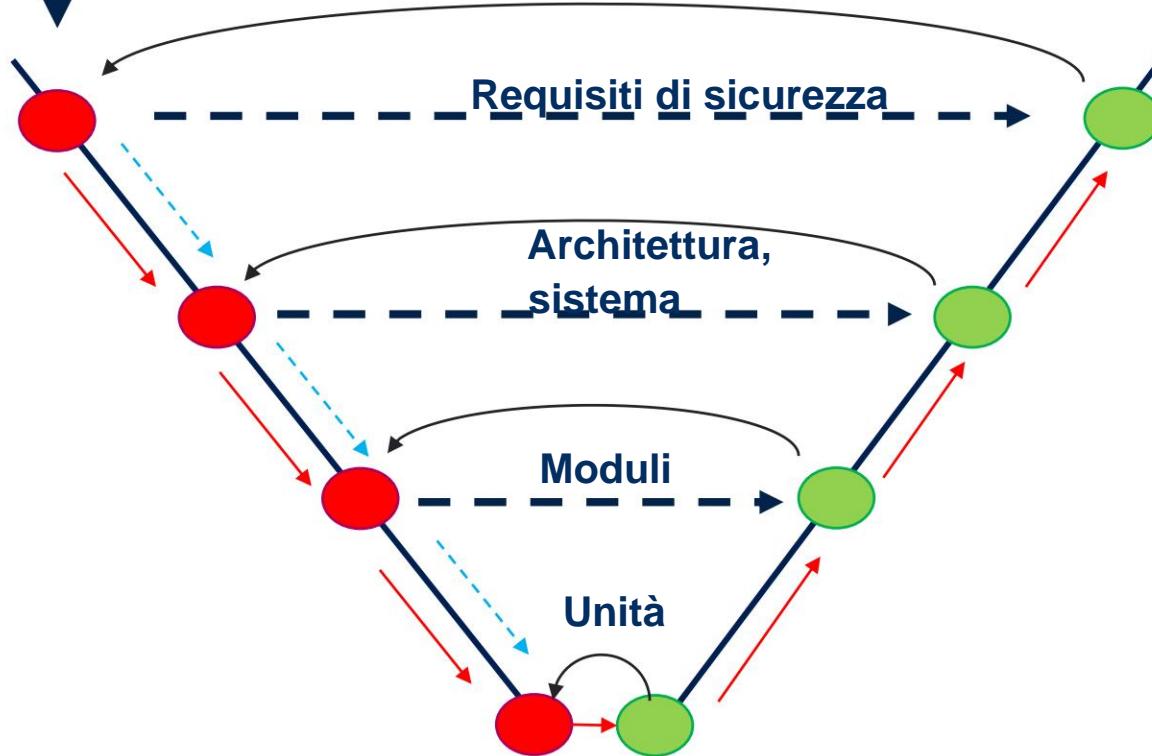
Rintracciabilità a ritroso: verifica che ogni
decisione di implementazione sia
chiaramente giustificata da qualche
requisito.



Pro: diminuisce la probabilità di funzioni/
parti hw inutilizzate e ingiustificate

La trappola del modello V

Il diavolo del modello V è qui – vedi riferimento [R3]



Il diavolo di Dante è qui

SOTIF (Sicurezza della funzionalità prevista)

ISO/PAS 21448: fornisce linee guida per garantire la sicurezza nei sistemi avanzati di assistenza alla guida (ADAS) e nei veicoli autonomi. SOTIF (Safety Of The Intended Functionality)

SOTIF affronta i rischi per la sicurezza derivanti dalle funzionalità previste di un sistema, soprattutto quando non sono presenti guasti o anomalie.

SOTIF si concentra sui pericoli causati da limitazioni prestazionali, condizioni ambientali o uso improprio, andando oltre la tradizionale sicurezza basata sui guasti. Sposta l'attenzione sulle specifiche di sistema incomplete, che per loro natura non vengono intercettate dal modello V.

Lo scopo della norma SOTIF è identificare e mitigare i rischi correlati al corretto comportamento del sistema che possono comunque portare a situazioni non sicure. Integra la norma ISO 26262, coprendo scenari in cui il sistema si comporta come progettato ma presenta comunque rischi per la sicurezza.

Adattamento dei metodi nel modello V

Il modello formale V prescrive per ogni fase elenchi di metodi consigliati.

Le raccomandazioni sono inserite in tabelle e classificate in questo modo:

HR/++ la tecnica o la misura è altamente raccomandata per il livello di integrità della sicurezza correlato; se non utilizzata, la motivazione alla base del suo mancato utilizzo deve essere dettagliata e concordata con il valutatore.

R/+: la tecnica o la misura è consigliata per questo livello di integrità della sicurezza come inferiore raccomandazione a una raccomandazione HR/++ o come misura aggiuntiva del margine di sicurezza.

NR: la tecnica o la misura non è assolutamente raccomandata per questo livello di integrità della sicurezza.

Adattamento dei metodi nel modello V

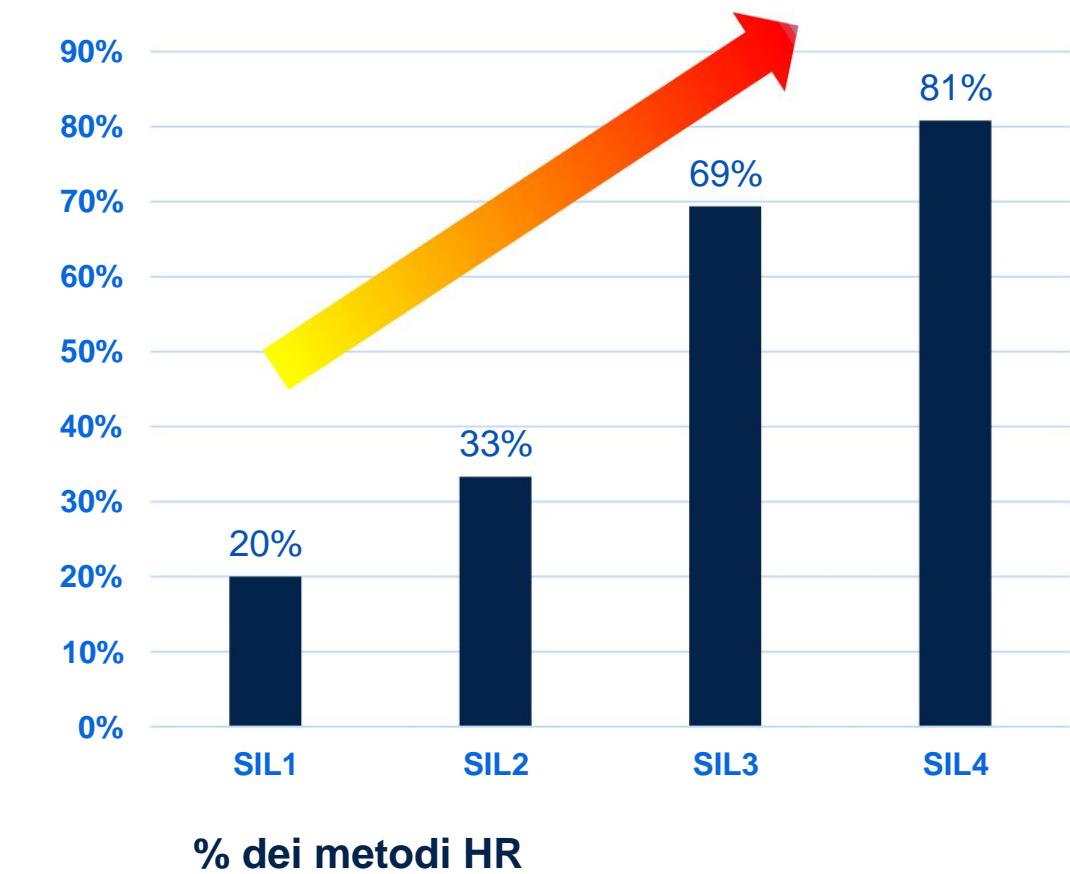
Esempio nozionale di tabella.

		SIL 1	SIL 2	SIL 3	SIL 4
1	Misure contro la rottura della tensione, variazioni di tensione, sovratensione, bassa voltaggio	R	Risorse umane	Risorse umane	Risorse umane
2	Aumento dell'immunità alle interferenze	R	Risorse umane	Risorse umane	Risorse umane
3	Separazione spaziale di più linee	Risorse umane	Risorse umane	Risorse umane	Risorse umane
4
5

Contenuto delle tabelle IEC 61508-3 vs SIL/SC

La richiesta di applicazione del metodo dipende fortemente dal livello SIL:

Le “raccomandazioni generiche” si trasformano in “prescrizioni dettagliate” sul lato inferiore della V (ad esempio coperture delle metriche software, approccio numerico)



Requisiti

Un requisito è formalmente definito come:

una dichiarazione documentata

descrivere una condizione o una capacità

che un sistema, un prodotto o un servizio deve soddisfare

per soddisfare le esigenze o i vincoli delle parti interessate.

Questa definizione è coerente con i principali standard di ingegneria dei sistemi e del software.

I requisiti costituiscono il pilastro fondamentale del modello formale a V.



Cosa è realmente necessario?



Requisiti qualità

La norma ISO/IEC/IEEE 29148:2018 (Requirements Engineering) descrive esplicitamente gli attributi di qualità che i requisiti devono soddisfare, tra cui:

Atomicità: il requisito esprime una singola esigenza o capacità (per evitare ambiguità e complessità).

Univocità: il requisito ha una sola interpretazione.

Completezza: il requisito include tutte le informazioni necessarie.

Coerenza: il requisito non è in conflitto con gli altri.

Verificabilità: il requisito può essere verificato tramite ispezione, analisi, test o dimostrazione.

Modificabilità: il requisito può essere modificato senza introdurre errori.

Tracciabilità: il requisito può essere ricondotto alla sua origine e ai relativi artefatti.

Correttezza: il requisito riflette accuratamente le esigenze delle parti interessate.



Come scrivere (buoni) requisiti

Metodi semi-formali:

- Linguaggio naturale strutturato (SNL) – ("Il sistema deve [azione] [oggetto] [sotto condizioni].")
- Diagrammi di stato
- Tabelle decisionali
- Casi d'uso UML,

Metodi formali:

- Reti di Petri
- Lega
- ...

Linguaggio naturale strutturato (SNL) - esempio

Basato su un modello coerente, ad esempio: [l'attore] deve [azione] [oggetto] [sotto condizioni].

Linee guida:

- Utilizzare un linguaggio chiaro e preciso
- Usa la forma attiva
- Utilizzare una terminologia coerente (glossario)
- Evitare affermazioni negative
- Utilizzare nomi singolari e numerazione coerente
- Limitare l'uso dei pronomi

Argomento dimostrato in uso (*)

Sulla base della dimostrazione, supportata dall'esperienza operativa in un periodo di tempo specifico e prolungato, che la probabilità di guasti sistematici sconosciuti è sufficientemente bassa per il livello di integrità della sicurezza target.

Le principali problematiche legate a questo approccio sono:

- ÿRichiede la presenza di una procedura di monitoraggio credibile per i guasti sul campo
- ÿIn alcuni casi, difficilmente collegabile a specifici livelli di integrità sistematica
- ÿDi solito, adatto solo per componenti molto semplici, perché le modifiche alla configurazione possono invalidare l'argomento
- ÿDipendenza da molteplici fattori, incluso il processo di produzione dei componenti

() si possono trovare nomi diversi sull'ecosistema degli standard di sicurezza*

Valutazione degli strumenti

Le norme IEC 61508 e ISO 26262 definiscono un approccio strutturato per valutare l'affidabilità degli strumenti software utilizzati nello sviluppo e nella verifica dei sistemi di sicurezza. Ciò garantisce che gli strumenti non introducano o non rilevino errori che potrebbero compromettere la sicurezza funzionale.

La struttura è simile: gli strumenti vengono valutati in base alla loro capacità di influenzare (negativamente) l'implementazione o la verifica della funzione di sicurezza. Successivamente, si valuta la possibilità di identificare in un secondo momento i problemi introdotti.

Il risultato della valutazione è la prescrizione di requisiti specifici sugli utensili, che possono prevedere:

- Adozione di strumenti “certificati” sviluppati esplicitamente secondo un ciclo di vita di sicurezza
- Adozione di misure di mitigazione aggiuntive (ad esempio confronto degli output degli strumenti, comprovato nell'uso) discussione, ecc.)

Valutazione degli strumenti – IEC61508

Uno strumento di supporto software offline è un'applicazione software che supporta una o più fasi del ciclo di vita dello sviluppo del software, ma non ha alcuna influenza diretta sul sistema di sicurezza durante il suo runtime. Questi strumenti sono classificati in tre classi in base alla loro interazione con il sistema di sicurezza:

Strumenti T1: questi strumenti non producono output che influiscano direttamente o indirettamente sul codice eseguibile (inclusi i dati) del sistema di sicurezza.

Strumenti T2: questi strumenti supportano il test o la verifica del progetto o del codice eseguibile. Sebbene errori in questi strumenti possano far sì che i difetti passino inosservati, non possono introdurre errori nel software eseguibile stesso.

Strumenti T3: questi strumenti generano output che contribuiscono direttamente o indirettamente al codice eseguibile del sistema correlato alla sicurezza.

Valutazione degli strumenti – IEC61508

La scelta degli strumenti deve essere giustificata. Si applicano quindi i seguenti requisiti:

ÿ. Documentazione:

Tutti gli strumenti T2 e T3 devono avere specifiche o documentazione chiare che ne descrivano dettagliatamente il comportamento e i vincoli di utilizzo.

ÿValutazione:

Valutare gli strumenti T2 e T3 per comprendere quanto siano affidabili e identificare possibili modalità di errore che potrebbero avere un impatto sul software eseguibile. Applicare misure di mitigazione se necessario.

ÿProva di conformità (solo T3):

Fornire la prova che gli strumenti T3 soddisfano le specifiche, sulla base di un utilizzo positivo in passato e/o di una convalida formale.

Lezione n. 4

Metodi di analisi della sicurezza (FMEDA/FTA/DFA/ETA/Markov)



Riepilogo:

- FMEA
- FMEDA
- DFA
- Analisi di Markov

Principi di FMEA (Analisi delle modalità e degli effetti dei guasti)

Identificare in modo proattivo le potenziali modalità di guasto nei prodotti, nei processi o nei sistemi per migliorare l'affidabilità e la sicurezza.

Elementi chiave:

- ÿ Modalità di guasto: modo specifico in cui una parte o un processo può guastarsi (ad esempio, crepa, cortocircuito).
- ÿ Effetto: impatto del guasto sul sistema o sull'utente (ad esempio, perdita di funzionalità, pericolo per la sicurezza).
- ÿ Causa: causa principale o fattore scatenante della modalità di guasto (ad esempio, difetto del materiale, errore umano).

Utilizzare il Risk Priority Number (RPN) o metriche simili basate su:

- ÿ Gravità (S): quanto è grave l'effetto.
- ÿ Occorrenza (O): probabilità che si verifichi un guasto.
- ÿ Rilevamento (D): probabilità di rilevare il guasto prima che raggiunga il cliente

Processo iterativo: aggiornare regolarmente la FMEA durante le modifiche alla progettazione, la produzione e il feedback sul campo per mantenere l'efficacia.

Esempio di FMEA

Esempio nozionale (processo)

Processo <small>Fare un passo</small>	Potenziale Modalità di errore	Effetti potenziali	Cause potenziali (S) (O) (D)	Azioni consigliate dall'RPN			
Componenti di saldatura	Giunto di saldatura scadente	Malfunzionamento del dispositivo o guasto	Saldatura insufficiente errore dell'operatore	9 4		3 108	Addestrare gli operatori, migliorare i controlli del processo di saldatura
Posizionamento dei componenti	Componenti disallineati	Cortocircuito o circuito aperto il circuito	Disallineamento durante posizionamento	8	3	4 96	Utilizzare macchine di posizionamento automatizzate, aggiungere l'ispezione visiva
Test di assemblaggio finale	Test funzionali incompleti	Dispositivi difettosi spedita al cliente	Procedura di prova incompleto	10 2		5 100	Standardizzare le procedure di test, aggiungere una checklist di test

- **Gravità (S):** Impatto sul sistema o sull'utente (scala da 1 a 10, 10 = più grave).
- **Occorrenza (O):** Probabilità di fallimento (scala da 1 a 10, 10 = più frequente).
- **Rilevamento (D):** probabilità che il guasto venga rilevato prima del rilascio (scala da 1 a 10, 1 = altamente rilevato).
- **RPN:** $RPN=S \times O \times D$; valori più alti indicano una priorità più alta

Principi di FMEDA (Modalità di guasto, effetti e Analisi diagnostica)

Simile alla FMEA con le seguenti specifiche:

- ÿ Include l'indicazione della diagnostica (mirata a mitigare/rilevare i guasti)
- ÿ Quantitativo: eliminare l'RPN a favore dei calcoli dei tassi di errore.
- ÿ Fornisce un risultato complessivo in termini di DC e SFF (SPF)
- ÿ Per ogni riga della modalità di guasto, include informazioni sul modello di guasto associato (per calcolare correttamente la distribuzione del guasto)
- ÿ Solo Hw: non può essere applicato a processi e software

L'argomento chiave è il problema della distribuzione dei guasti (come associare la modalità di guasto individuale al tasso di guasto del sistema)

Principi dell'analisi dell'albero dei guasti (FTA)

L'FTA è un metodo analitico deduttivo top-down utilizzato per identificare le cause dei guasti a livello di sistema.

Scopo: analizzare sistematicamente come le combinazioni di guasti di base possano portare a un evento critico indesiderato (l'evento principale).

Caratteristiche principali:

- ÿ Inizia con un evento principale definito (guasto o pericolo del sistema). ÿ
- Utilizza porte logiche (AND, OR) per mappare le relazioni tra guasti. ÿ L'analisi top-down scorre verso il basso fino a quando non viene trovato un evento di base (causa principale). ÿ Aiuta a visualizzare i percorsi di guasto e le loro interdipendenze.

Principi dell'analisi dell'albero dei guasti (FTA)

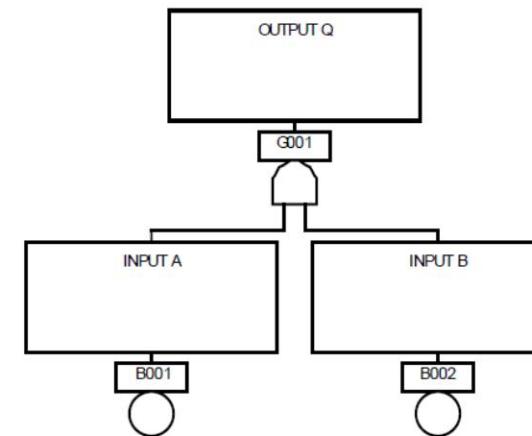
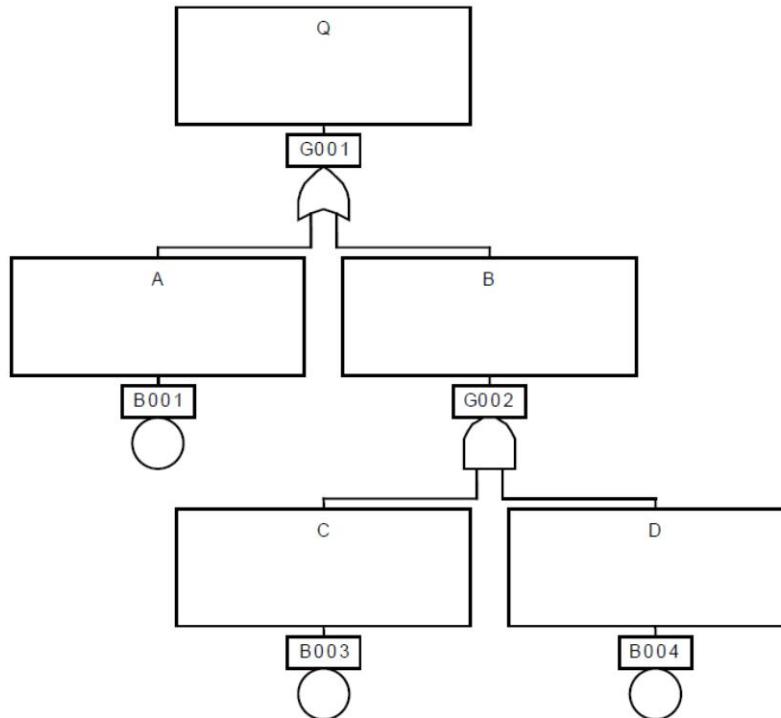


Figure 4-5. The AND-Gate

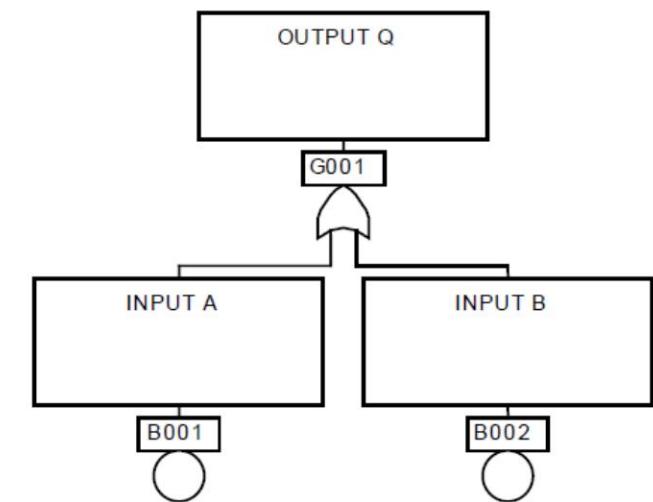


Figure 4-2. The OR-Gate

Per spiegazioni complete fare riferimento al documento di riferimento [R4], sezione 4.1 Simbologia: i componenti fondamentali dell'albero dei guasti

Principi dell'analisi dell'albero dei guasti (FTA)

Breve riepilogo delle principali regole/specificità dell'FTA

Regola del completamento del gate: tutti gli input di un particolare gate devono essere completamente definiti prima di intraprendere un'ulteriore analisi di uno qualsiasi di essi.

Nessuna regola gate-to-gate: gli ingressi dei gate devono essere eventi di guasto correttamente definiti e i gate non devono essere collegati direttamente ad altri gate.

Minimum Cut Set: è la più piccola combinazione di guasti di base che può causare il guasto di livello superiore (evento principale). Rappresenta un insieme minimo di guasti dei componenti che portano al guasto del sistema e uno dei principali vantaggi dell'esecuzione di un'analisi FTA nel sistema.

Analisi dei guasti dipendenti (DFA)

Lo scopo è identificare e analizzare i guasti che non sono indipendenti ma si verificano a causa di una causa comune o di una dipendenza tra i componenti...

Viene esplorato in dettaglio principalmente in ISO26262

Si avvale di altre tecniche di analisi della sicurezza (principalmente FTA e talvolta FMEA), concentrandosi sulla rilevazione di guasti dipendenti.

Gli standard di sicurezza aiutano la ricerca con tabelle guida specifiche (argomenti tipici da analizzare nella ricerca di tali DFA)

Bibliografia



Documenti di riferimento

[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

Grazie

© STMicroelectronics - Tutti i diritti riservati.

Il logo ST è un marchio commerciale o un marchio registrato di STMicroelectronics International NV o delle sue affiliate nell'UE e/o in altri paesi.

Per ulteriori informazioni sui marchi ST, consultare www.st.com/trademarks.

Tutti gli altri nomi di prodotti o servizi appartengono ai rispettivi proprietari.





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

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".

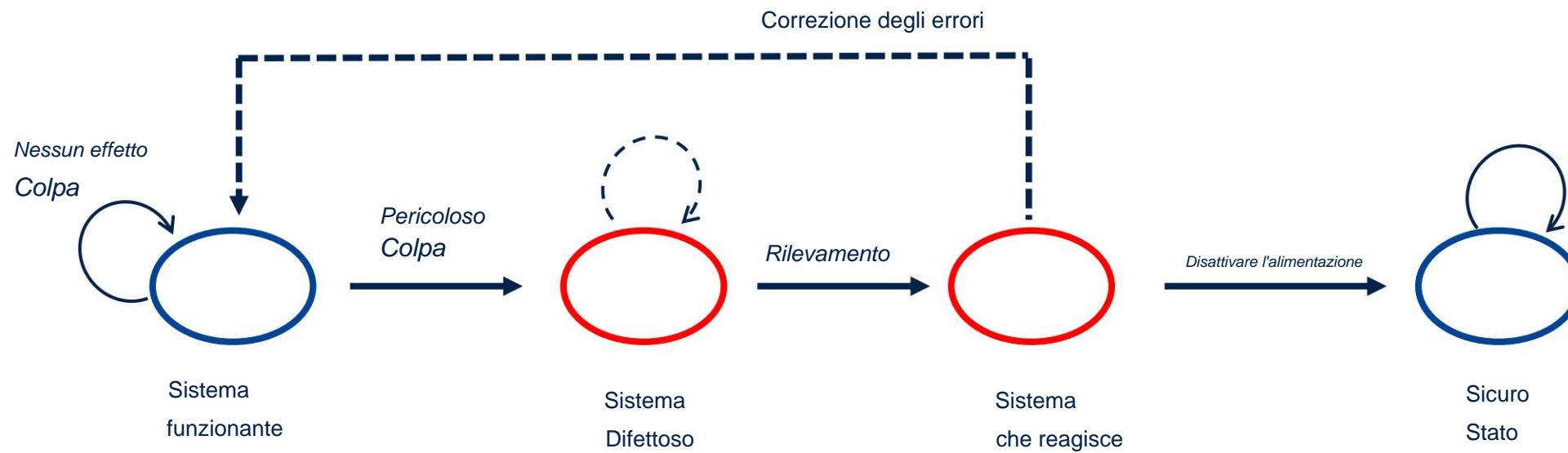
Stato sicuro

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).

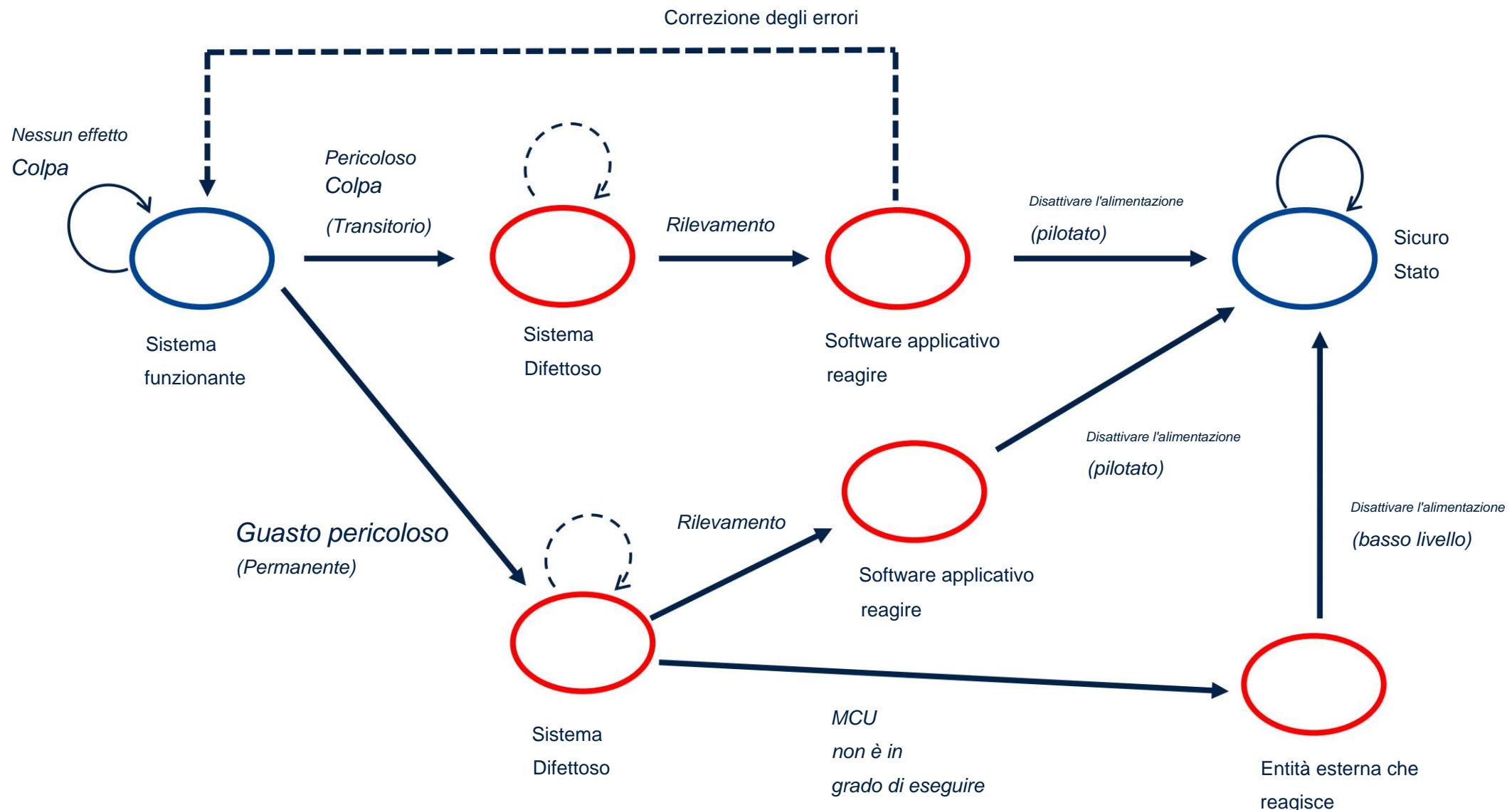


Stato sicuro ed evoluzione del sistema (generale)

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

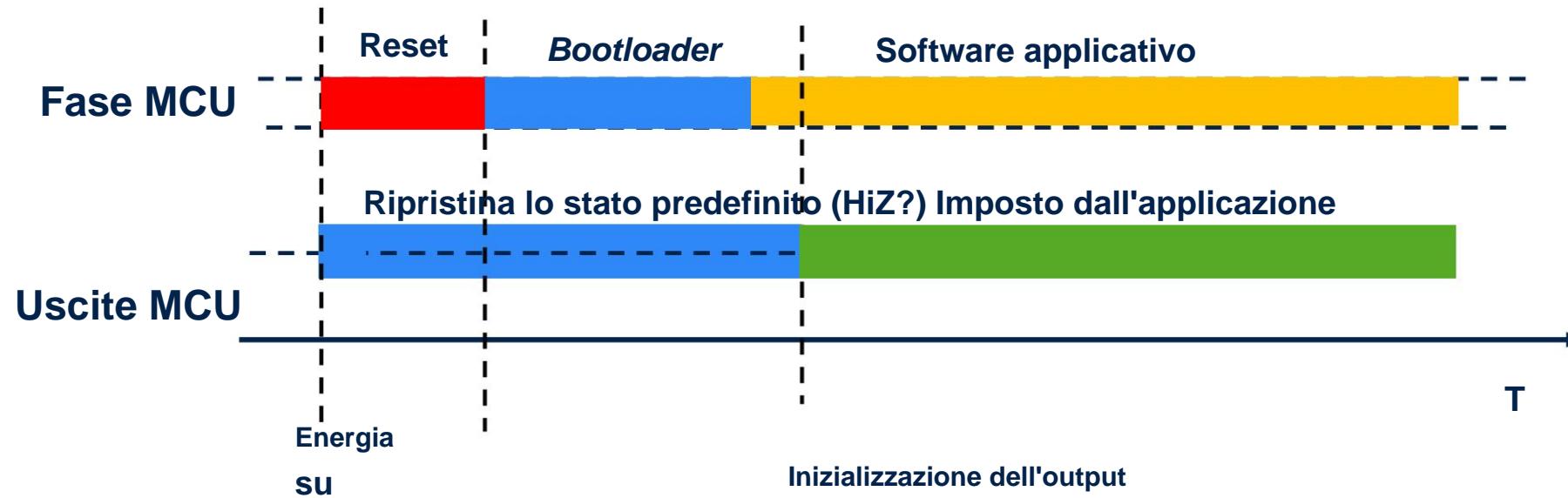


Stato sicuro ed evoluzione del sistema (aggiunta di modelli MCU e di guasto)



Stato sicuro e avvio del sistema

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

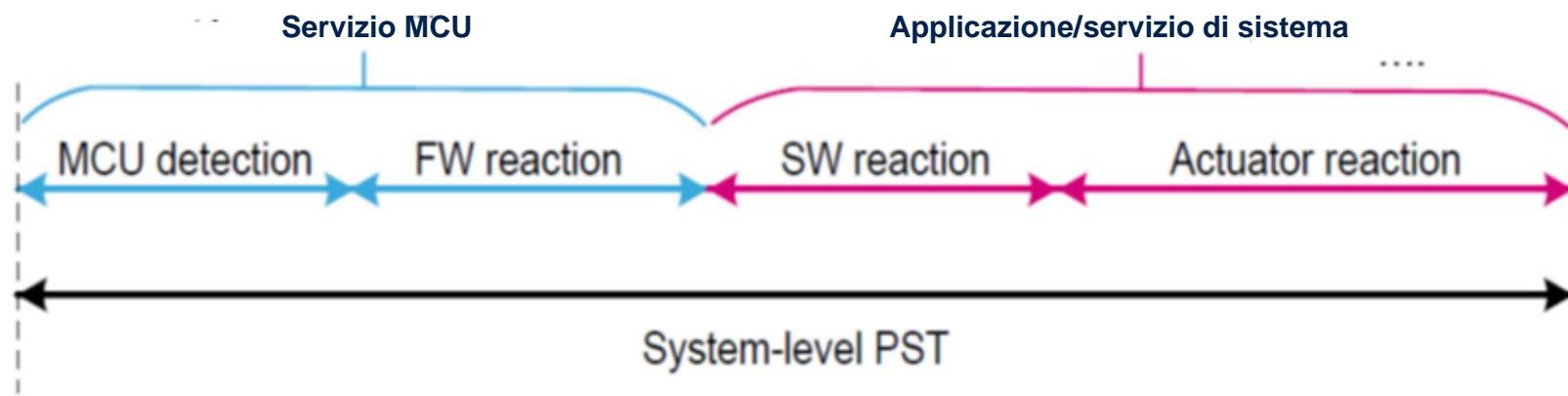


La fase di avvio (inclusa la possibile esecuzione del bootloader, più lunga per i dispositivi senza flash) richiede misure aggiuntive esterne all'MCU per garantire lo stato sicuro

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

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 ѕ PFD Probabilità di guasto su richiesta: probabilità

HD/CM ѕ 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.

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

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

¶I sistemi CM richiedono che ogni diagnostica periodica venga eseguita almeno una volta per PST (Processo 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)

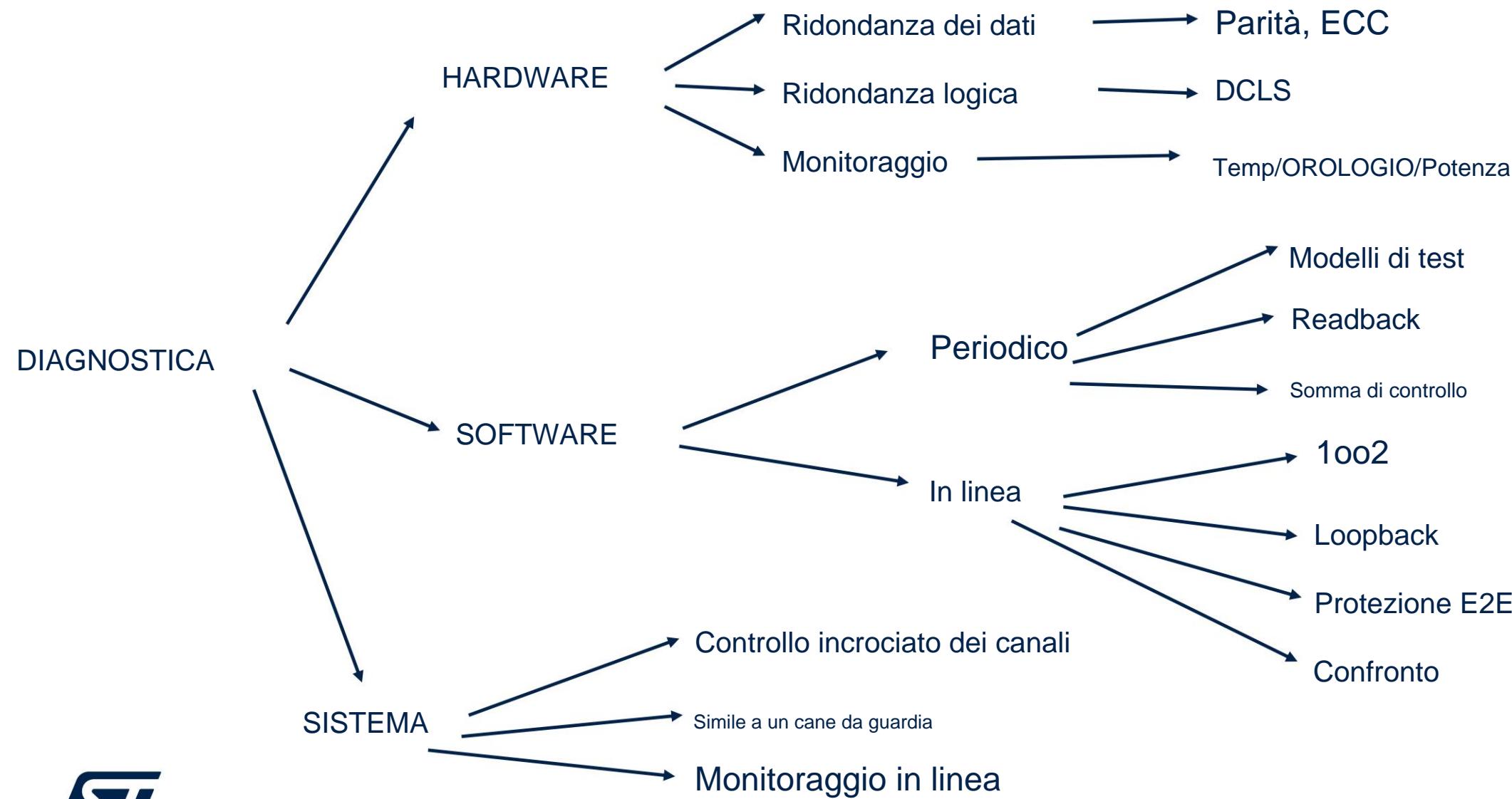
Il concetto di test di prova

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 $\bar{y}DU$, 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

- ÿ Modello di guasto affrontato (permanente/transitorio/entrambi?)
- ÿ Periodicità (continua/su richiesta/periodica)
- ÿ Reazione all'errore (messaggio(flag/interruzione))
- ÿ Correzione degli errori (sì/no/parziale)
- ÿ Protezione da test/guasti multipli (elenco delle diagnosi alternative per i guasti che impediscono il corretto funzionamento dei meccanismi di sicurezza stessi)
- ÿ Inizializzazione/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

• Tabelle 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%)

• Iniezione/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)

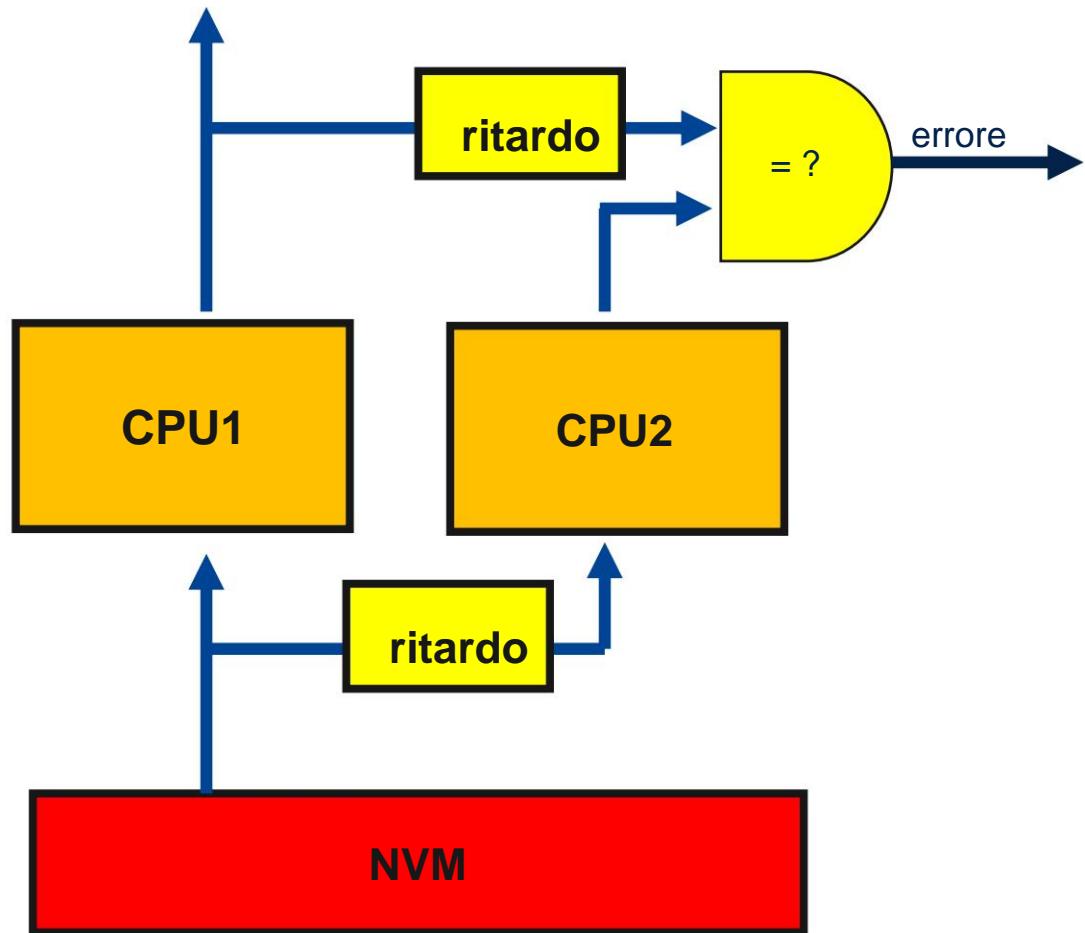
PRO

- 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
- ÿ che impediscono l'esecuzione del software

Risultati funzionali



Bit di parità

A ogni parola viene aggiunto un bit di parità (più **CONS**

sono possibili schemi), consentendo l'errore di un singolo bit
bit quando i dati vengono letti.

ÿ 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

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

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

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

Cane da guardia interno

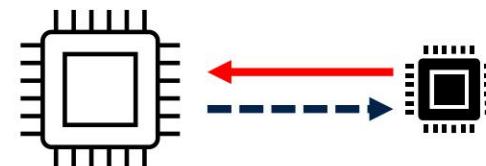
Forza un reset della CPU quando l'azione richiesta dal software (ad esempio, la scrittura del registro con una chiave) non viene eseguita entro il periodo programmato. La politica di temporizzazione può essere applicata tramite requisiti di finestra.

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.

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



Riferimenti utili sui meccanismi di sicurezza

Il riferimento [6] elenca nella sezione "7 Breve descrizione dei meccanismi di 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](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

© STMicroelectronics - Tutti i diritti riservati.

Il logo ST è un marchio commerciale o un marchio registrato di STMicroelectronics International NV o delle sue affiliate nell'UE e/o in altri paesi.

Per ulteriori informazioni sui marchi ST, consultare www.st.com/trademarks.

Tutti gli altri nomi di prodotti o servizi appartengono ai rispettivi proprietari.





Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale
STMicroelectronics

Lezione n. 6

**Architetture di sicurezza formali (IEC61508, ISO13849) + metodi ISO26262
(decomposizione ASIL). Mappatura su casi d'uso automotive e robotica**

Riepilogo:

- Concetti generali (HFT)
- Architetture IEC 61508 (1oo1,1oo2,2oo2)
- Decomposizione ASIL, teoria ed esempi
- Considerazioni sul ruolo del software



A proposito del concetto di “diversità”

La diversità è definita nella norma IEC61508-4 “diversi mezzi per eseguire una funzione richiesta”

In alcune circostanze può essere richiesta la diversità (ad esempio per utilizzare la regola di composizione SC+1 con canali ridondanti)

La diversità è la risorsa chiave per combattere i fallimenti delle cause comuni (e per far fronte alla loro potenziale analisi incompleta)

La diversità è possibile sia nell'hardware che nel software.

Per il software, è possibile ottenere anche la diversità temporale (lo stesso calcolo viene eseguito in momenti diversi) fornendo protezione contro gli errori software che hanno un impatto sulla CPU

La diversità è un vantaggio ma anche un costo (tempo di progettazione, risorse hardware, spazio di memoria, complessità, maggiore verifica, potenziali problemi di disponibilità).

La diversità può essere utilizzata come fattore di mitigazione per i guasti degli utensili (procedura di valutazione degli utensili per utensili T3)

Tolleranza ai guasti hardware (HFT)

La tolleranza ai guasti hardware di N significa che $N+1$ è il numero minimo di guasti che potrebbero causare una perdita della funzione di sicurezza.

Per determinare l'HFT non è possibile prendere in considerazione altre misure che controllano l'effetto dei guasti (come la diagnostica)

Alcuni guasti possono essere esclusi dalle considerazioni, sulla base di motivazioni specifiche basate sulla loro probabilità.

↳ HFT è fondamentalmente una proprietà dei sottosistemi, non dei componenti.

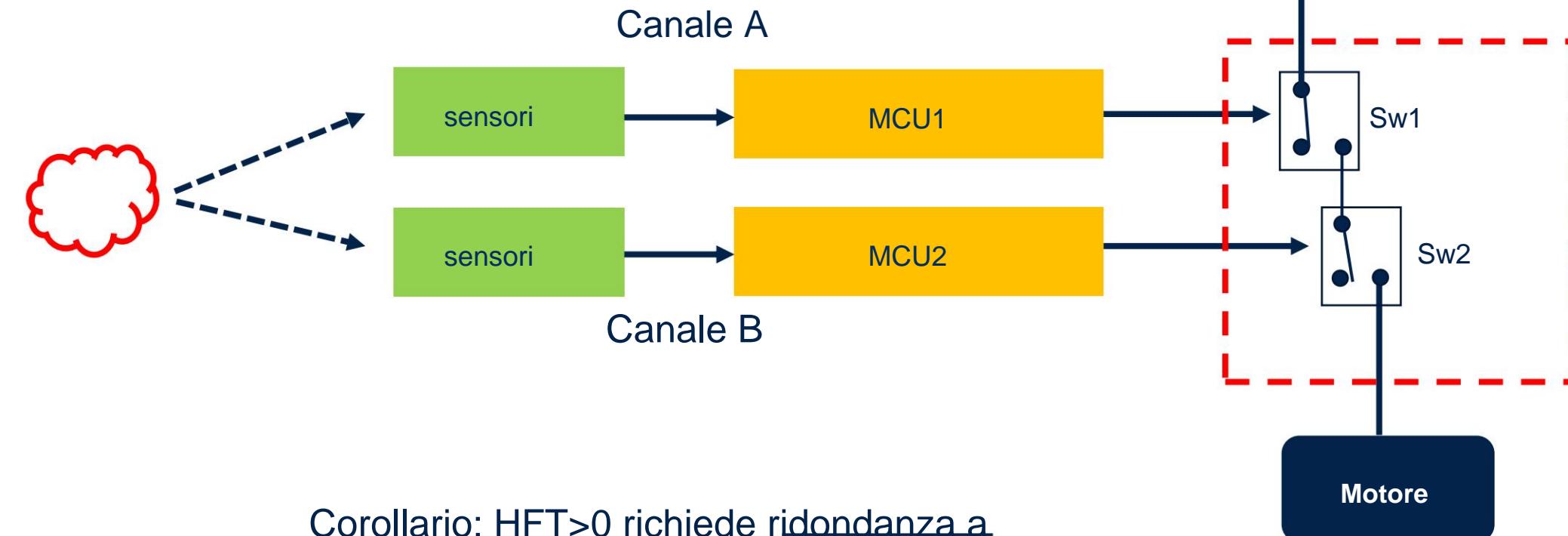
Ricorda: HFT è una delle voci per stabilire gli obiettivi SFF per i sistemi hw

Nota: IEC 61508 include requisiti di architettura speciali per circuiti integrati con ridondanza on-chip

Tolleranza ai guasti hardware (HFT)

Esempio nozionale del sistema HFT=1

SF: Per interrompere l'alimentazione del motore tramite un interruttore in base a condizioni specifiche sui sensori



Corollario: $HFT>0$ richiede ridondanza a un certo livello

Che cosa è un'architettura di sicurezza

In generale, una buona definizione di **architettura** è "la rappresentazione della struttura di un sistema che consente l'identificazione dei componenti fondamentali, dei loro confini e delle loro interfacce, e include l'allocazione dei requisiti a questi componenti". Questa è una sorta di definizione generale.

Non esiste una definizione esatta di "architettura di sicurezza" negli attuali standard di sicurezza. Questo può essere dedotto, analizzando il framework IEC 61508, in questo modo:

L'architettura di sicurezza definisce la struttura e l'organizzazione del sistema correlato alla sicurezza, comprese le funzioni di sicurezza, i meccanismi di sicurezza, gli stati sicuri e la loro allocazione agli elementi hardware e software per ottenere l'integrità di sicurezza richiesta.

IEC 61508: 1oo1

1oo1 è l'architettura a canale singolo (PE = Processing Element)

È lo schema architettonico più semplice ma anche il più impegnativo / NESSUN vantaggio!
Tutto si risolve all'interno della struttura semplice.

La corrente continua deve essere garantita dalla diagnostica intrinseca (HW/SW)

HFT = 0



La transizione di stato sicura potrebbe essere complessa

Non è possibile alcuna diversità nell'hardware ÿ SC hardware da raggiungere a livello di componente

Diversità nel software difficilmente possibile ÿ SC del software da raggiungere a livello di componente

IEC 61508: 1oo1 - formule

Modalità a bassa richiesta:

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Modalità continua/alta richiesta:

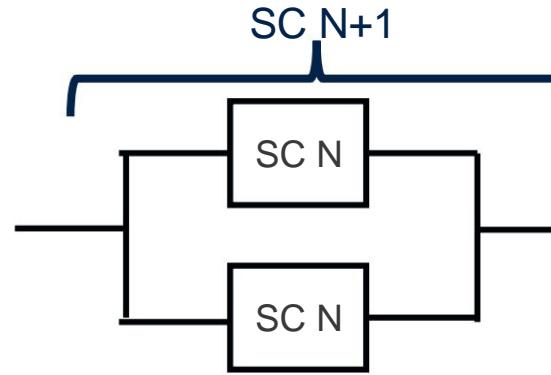
Se si presume che il sistema di sicurezza metta l'EUC in uno stato sicuro al rilevamento di qualsiasi fallimento, per un'architettura 1oo1 si ottiene quanto segue

$$PFH_G = \lambda_{DU}$$

IEC 61508: 1oo2

Sono possibili molteplici tipi di diversità nell'hardware ÿ l'hardware SC può essere più semplice grazie a Regola $N+N = N+1$

La diversità nel software è possibile ÿ il software SC è più semplice grazie alla regola $N+N = N+1$



Attenzione: ÿ

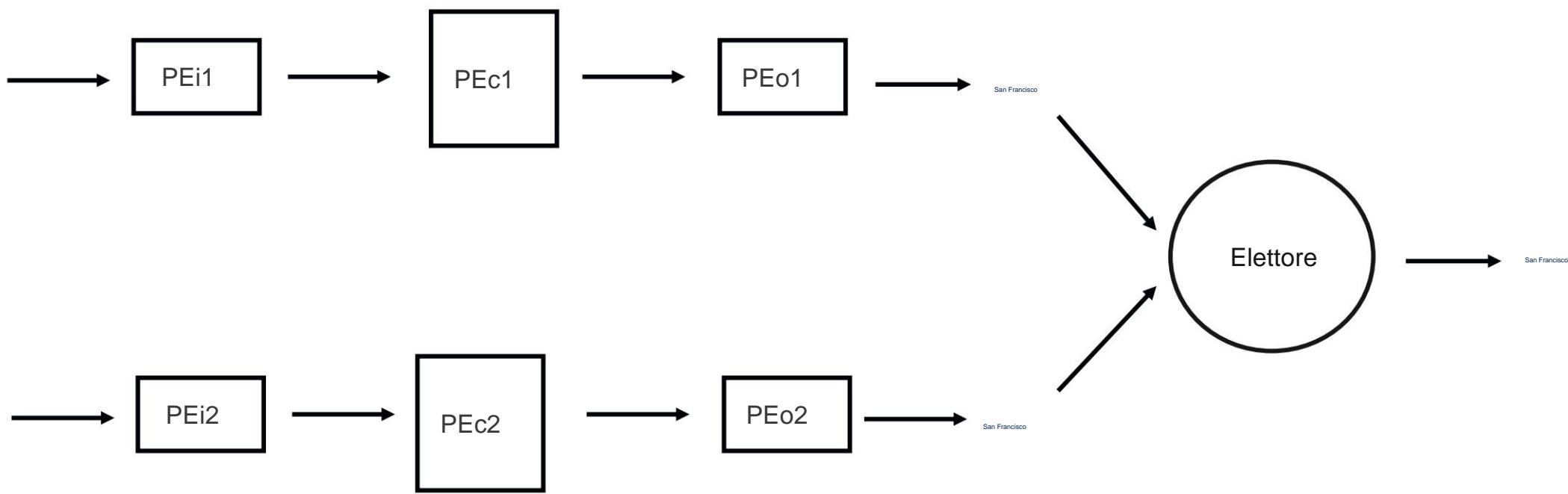
È richiesta l'indipendenza tra gli elementi ÿ Consentita solo una volta (non più composizioni a cascata)

MA ancora alcune complicazioni

Cause comuni di guasti da esplorare (metriche di impatto sulla sicurezza!)

L'elettore deve essere HFT = 1 intrinsecamente

IEC 61508: 1oo2



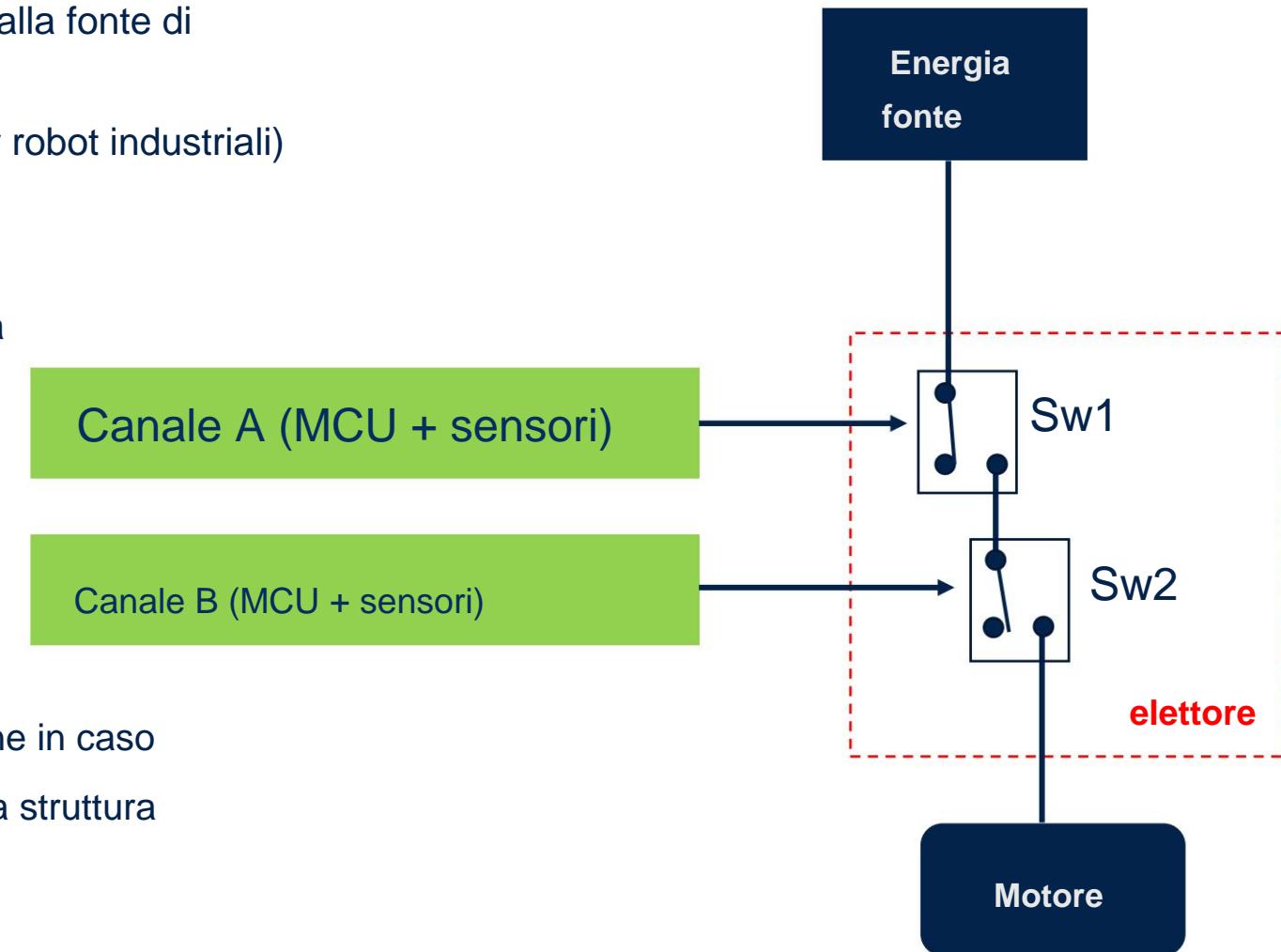
Nota: tenere presente che la collaborazione incrociata tra i due MCU può portare ad un aumento dei fattori di penalità \bar{y} e $\bar{y}D$ (causa comune di guasti tra MCU)

Esempio nozionale 1oo2

Funzione di sicurezza: "Collegamento motore aperto alla fonte di alimentazione in condizioni di segnali di ingresso specifici" (applicazione ad esempio barriera attiva per robot industriali)

Stato sicuro: collegamento elettrico APERTO

La natura di questa funzione di sicurezza consente una facile implementazione per gli elettori



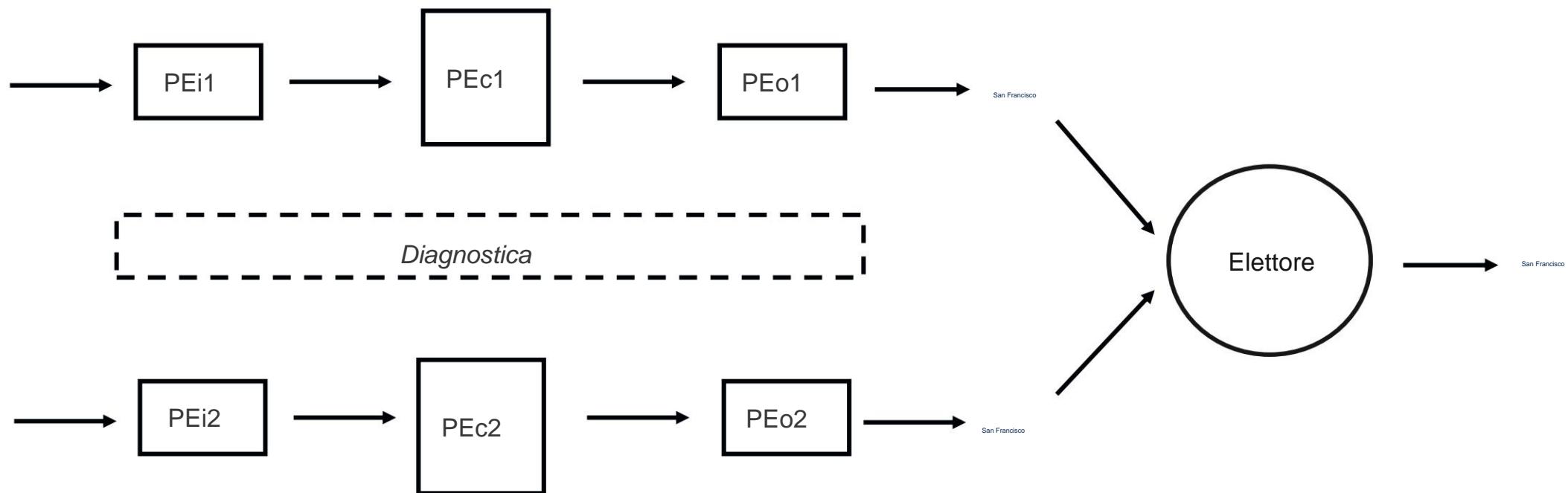
Nota: la struttura dell'interruttore forza la disconnessione in caso di guasto dell'alimentazione locale dell'elettore. Per una struttura HFT=1 reale dell'elettore, gli interruttori devono essere implementati in modo ridondante.

IEC 61508: 2oo2

2oo2 è costituito da due canali collegati in parallelo, in modo che entrambi i canali debbano richiedere la funzione di sicurezza prima che questa possa aver luogo.

La corrente continua deve essere garantita da una diagnostica intrinseca per ciascun canale. La diagnostica segnalerebbe guasti ma non modificherebbe il voto.

Lo schema è HFT = 0. PFH = 2 \bar{y} DU

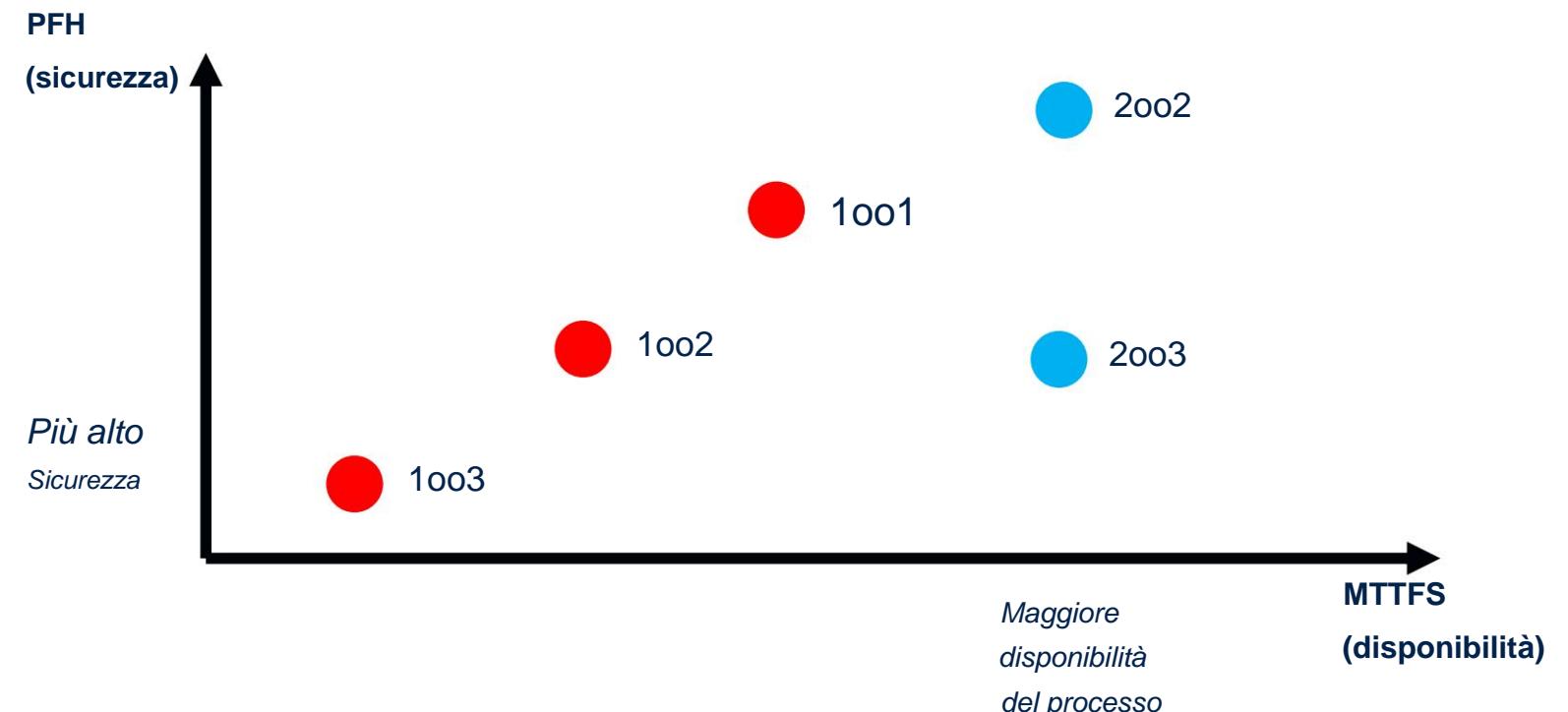


1oo2 contro 2oo2 contro 2oo3

1oo2: la priorità è la sicurezza (PFH inferiore)

2oo2: la priorità è sulla disponibilità (PFH più elevato ma meno transizioni di stato sicuro false positive)

2oo3: mantiene i vantaggi dei due schemi precedenti, a un costo più elevato



Decomposizione ASIL

La decomposizione ASIL è descritta nella clausola 5 della norma ISO 26262-9:2018.

Lo scopo principale dell'implementazione della decomposizione ASIL è quello di abbassare il livello ASIL.

Un requisito di sicurezza viene scomposto in requisiti di sicurezza ridondanti, che vengono poi assegnati a elementi sufficientemente indipendenti.

Il processo di decomposizione ASIL deve rispettare lo schema indicato nella Tabella 1 della norma ISO 26262-9:2018.

D	ASIL D(D) + QM(D)
D	ASIL C(D) + ASIL A(D)
D	ASIL B(D) + ASIL B(D)
C	ASIL C(C) + QM(C)
C	ASIL B(C) + ASIL A(C)
B	ASIL B(B) + QM(B)
B	ASIL A(B) + ASIL A(B)
A	ASIL A(A) + QM(A)

SR1: Requisito di sicurezza ASIL C

SR1.1: ASIL B(C)

SR1.2: ASIL A(C)

Decomposizione ASIL – regole generali

La ridondanza omogenea (ad esempio, tramite dispositivo o software duplicato) non è, in generale, sufficiente per ridurre l'ASIL a causa della mancanza di indipendenza tra gli elementi

Gli obiettivi di sicurezza non possono essere scomposti

I requisiti scomposti devono soddisfare in modo indipendente il requisito originale (definizione di ridondanza)

La decomposizione ASIL può essere applicata più di una volta (!) (grande differenza con la combinazione di elementi in IEC 61508)

Qual è la scommessa: i requisiti di sicurezza scomposti sono più semplici e/o più economici in termini di implementazione. Quindi: la scomposizione ASIL non è sempre una soluzione vincente...

Decomposizione ASIL – regole generali

(INVARIANTI)

L'ASIL decomposto risultante deve essere espanso con l'ASIL originale prima della decomposizione, ad esempio ASIL A(C)

La valutazione della sicurezza funzionale dell'articolo è definita dall'ASIL originale

L'indipendenza degli elementi composti deve essere valutata mediante l'analisi dei guasti dipendenti

I requisiti per il test e l'integrazione sono definiti dall'ASIL del livello di integrazione pertinente

I valori target per le metriche HW sono definiti dall'ASIL originale a livello di elemento

Software correlato alla sicurezza vs software non correlato alla sicurezza

Nelle architetture articolate, il software è spesso parte del concetto di sicurezza.

La coesistenza tra software correlato alla sicurezza e software non correlato alla sicurezza può verificarsi nei sistemi basati su microcontrollori (spesso per ragioni di costo, ad esempio riutilizzo di software open source per attività non correlate alla sicurezza).

Il problema principale è la separazione, ovvero garantire che il software non correlato alla sicurezza non possa interferire con la funzione di sicurezza:

- ÿ Interferenza spaziale: sovrascrittura della memoria, accesso alle periferiche ecc.
- ÿ Interferenza temporale: violazione del determinismo, occupazione delle risorse, jitter, mascheramento degli interrupt ecc.

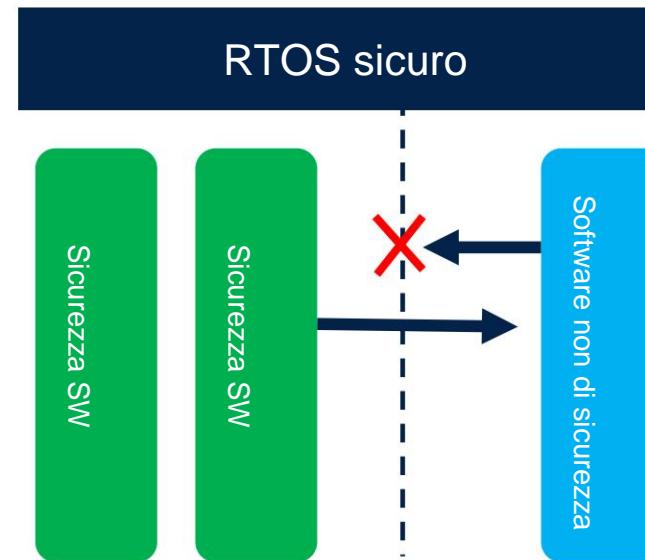
La segregazione dell'hardware può essere difficile poiché i tipici microcontrollori non hanno MMU complesse (spesso è disponibile solo una MPU di base)

Software correlato alla sicurezza vs software non correlato alla sicurezza

Possibili vettori per la soluzione del problema della coesistenza:

Il software non correlato alla sicurezza è semplice: potrebbe essere fattibile rimpatriarlo all'interno del modello V certificato per il software applicativo

Il software non di sicurezza è complesso: la segregazione del software tramite un RTOS sicuro potrebbe garantire a) l'isolamento delle potenziali interferenze spaziali b) il determinismo del software di sicurezza indipendentemente da quello non di sicurezza. I costi generali sono rappresentati dal costo e dalla disponibilità del RTOS sicuro.



Diapositive di backup



IEC 61508: 1oo2 - formule

Modalità a bassa richiesta:

$$PFD_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{T_1}{2} + MRT \right)$$

Modalità continua/alta richiesta:

$$PFH_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU} t_{CE} + \beta \lambda_{DU}$$

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](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

© STMicroelectronics - Tutti i diritti riservati.

Il logo ST è un marchio commerciale o un marchio registrato di STMicroelectronics International NV o delle sue affiliate nell'UE e/o in altri paesi.

Per ulteriori informazioni sui marchi ST, consultare www.st.com/trademarks.

Tutti gli altri nomi di prodotti o servizi appartengono ai rispettivi proprietari.





Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale
STMicroelectronics

Lezione n. 7

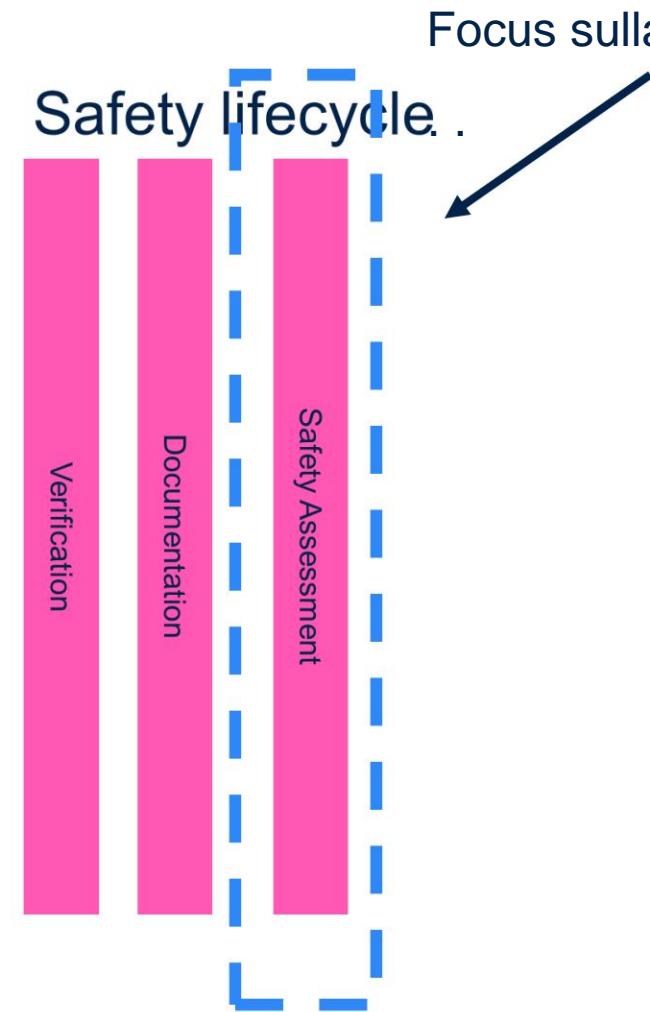
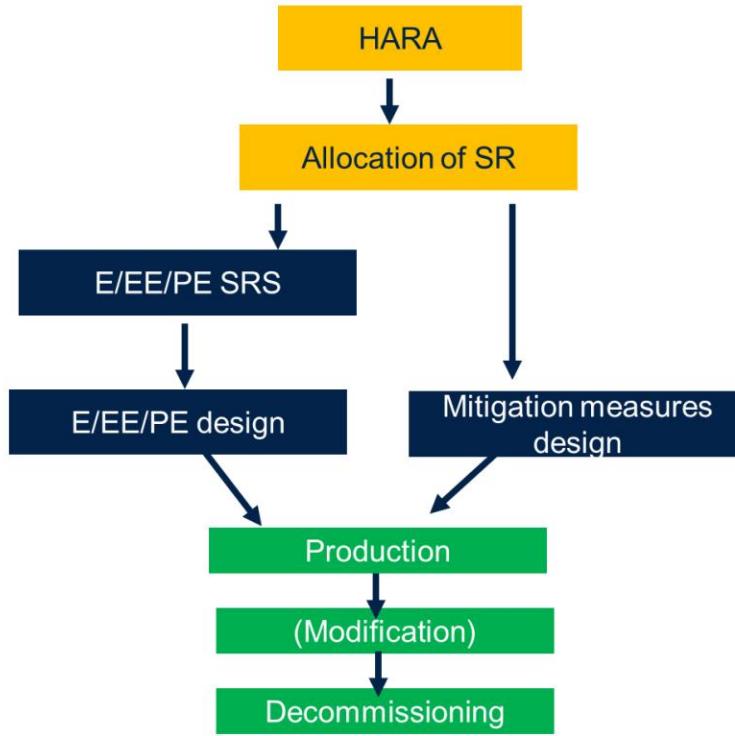
Varie nel processo di sicurezza



Riepilogo:

- Valutazione della sicurezza funzionale, indipendenza
- Valigetta di sicurezza
- Processo di certificazione

Riepilogo sul ciclo di vita della sicurezza



Focus sulla valutazione della sicurezza:

Valutazione della sicurezza funzionale

Cos'è: IEC61508-4: 3.8.3: "indagine, basata su prove, per valutare la sicurezza funzionale raggiunta da uno o più sistemi di sicurezza E/E/PE e/o altre misure di riduzione del rischio"

Chi lo farà: il valutatore (persona, persone o organizzazione che esegue la valutazione della sicurezza funzionale al fine di giungere a un giudizio sulla sicurezza funzionale raggiunta dai sistemi di sicurezza E/E/PE e da altre misure di riduzione del rischio) che deve essere indipendente come da tabella seguente.



Livello minimo di indipendenza	Livello di integrità della sicurezza / Capacità sistematica			
	1	2	3	4
Persona indipendente	Consentito	Consentito su progetti consolidati e semplici	Insufficiente	Insufficiente
Dipartimento indipendente		Consentito su progetti/tecnologie nuovi/complessi	Consentito su progetti consolidati e semplici	Insufficiente
Organizzazione indipendente			Consentito su progetti/tecnologie nuovi/complessi	Consentito

A proposito di indipendenza

I criteri di indipendenza sono specificati in IEC61508-4, 3.8.11-13:

• persona indipendente: persona separata e distinta dalle attività che vi si svolgono durante l'attività specifica, senza responsabilità diretta.

• dipartimento indipendente: dipartimento separato e distinto dai dipartimenti responsabili delle attività

• organizzazione indipendente: organizzazione separata e distinta, per gestione e altre risorse, provenienti dalle organizzazioni responsabili delle attività

Quando è richiesta un'organizzazione indipendente, anche per grandi organizzazioni come i produttori di semiconduttori è comune affidarsi a organismi competenti/agenzie di certificazione (ad esempio TÜEV, UL, ecc.) – in tal caso l'indipendenza è chiaramente raggiunta e accettata .

Il caso di sicurezza

Il Safety Case è perfettamente descritto in ISO26262:10, 5.3.1

Lo scopo di un safety case è quello di fornire un argomento chiaro, completo e difendibile, supportato da prove, che un articolo è esente da rischi irragionevoli quando utilizzato in un contesto previsto

Elementi principali:

gli obiettivi di sicurezza e i relativi requisiti di sicurezza

la raccolta di argomenti sulla sicurezza (relativi al prodotto o al processo)

i prodotti di lavoro della serie di standard ISO 26262 (le prove)

La descrizione è applicabile anche al framework IEC61508 (dove il caso di sicurezza non è formalmente definito)



Come costruire un Safety Case

Il modo migliore per creare un Safety Case è seguire la descrizione ISO26262 con un'implementazione formale (in altre parole, utilizzando linguaggi formali come ad esempio Goal Structured Network).

Il vantaggio maggiore sarebbe quello di collegare la descrizione allo strumento utilizzato per gestire formalmente i requisiti.

L'approccio è spesso ritenuto difficile, per cui nell'industria si tende a costruire il Safety Case tramite un "testo narrativo" (sotto forma di rapporto sulla sicurezza).

Il testo narrativo può creare confusione, poiché si rischia di perdere i confini tra affermazioni e motivazioni correlate. Pertanto, si raccomanda di mantenere formalmente la catena causale.

Affermazioni Argomenti Prove

Nota: la presenza di un approccio basato su testo narrativo nella documentazione di terze parti (manuali di sicurezza, ecc.) richiede solitamente uno sforzo aggiuntivo per consentire un'organizzazione più strutturata dei requisiti inclusi.

Certificazioni zoo in breve

Certificazione: è una delle espressioni più ambigue (e abusate) nell'ambito della sicurezza funzionale, poiché viene utilizzata per descrivere situazioni molteplici e diverse. Alcuni esempi:

· Pre-certificato: software sviluppato secondo un modello V certificato. La certificazione e le rivendicazioni correlate riguardano il flusso di sviluppo generico seguito dall'organizzazione e la conformità di ogni software specifico deve essere valutata sulla base degli artefatti/documenti forniti

· Pre-certificato: uno strumento T2 o T3 per il quale è richiesta un'analisi dello strumento di supporto offline secondo IEC61508-3m 7.4.4 è stato eseguito e revisionato in modo indipendente, ma esistono ancora azioni complesse sul lato dell'utente finale

· Pre-certificato: un elemento hardware o software formalmente certificato rispetto a specifiche affermazioni, utilizzato come parte di una soluzione completa che lo integra (e non in grado di estendere magicamente le affermazioni all'intero sistema)

Il certificato SIL

Il certificato SIL è una certificazione di sicurezza funzionale che dimostra che un prodotto o un processo soddisfa gli standard internazionali IEC 61508.

Viene rilasciato da una terza parte indipendente per garantire la conformità ai requisiti di indipendenza della norma IEC 61508-1, in particolare per il raggiungimento dei livelli SIL più elevati 3 e 4, che richiedono il coinvolgimento di una divisione separata o di un organismo indipendente.

Il certificato è autosufficiente e fornisce tutte le informazioni necessarie per l'integrazione in un sistema di sicurezza. Oltre al manuale di sicurezza dell'articolo certificato, include istruzioni per un corretto utilizzo al fine di garantire il mantenimento del livello SIL dichiarato.

Il certificato contiene anche un marchio registrato con l'ID identificativo del prodotto certificato, che deve essere apposto sul prodotto per consentirne la tracciabilità e una chiara distinzione tra prodotti SIL e non SIL. I certificati sono solitamente archiviati in un database pubblico disponibile sul web.

Diversi tipi di certificato SIL

I certificati possono essere rilasciati in uno dei seguenti 3 tipi:

• **Certificato di tipo SIL:** valido per un'intera tipologia di prodotto, il processo di certificazione si sviluppa a partire dall'analisi di un prototipo che, una volta certificato, sarà idoneo alla produzione in serie. Il certificato è quindi valido per un numero illimitato di prodotti, purché identici in ogni aspetto al prototipo convalidato. Il certificato di tipo SIL ha una durata definita dall'organismo di certificazione in base alla complessità dell'oggetto (ad esempio, limitato nel tempo o soggetto a conferma annuale). Esempio: microcontrollori di sicurezza.

• **Certificato SIL per singolo prodotto:** limitato al dispositivo espressamente coperto dal certificato, questa tipologia è frequente per produzioni non in serie, assemblaggi personalizzati e progetti. Il certificato riporta espressamente il numero di serie o un identificativo univoco del prodotto a cui si riferisce. Esempio: una fabbrica.

• **Certificato SIL di processo:** attesta la conformità allo standard internazionale IEC 61508 del processo di implementazione di una o più fasi del Safety Lifecycle/ Esempio: verifica della conformità dei processi e delle procedure ai requisiti normativi.

Informazioni principali in un certificato

IDENTIFICAZIONE DEL PRODOTTO CERTIFICATO Non è un passaggio banale. Prestate sempre attenzione a quale sia effettivamente il confine della certificazione (un singolo prodotto? Una linea di prodotti? ecc.)

NORMA DI RIFERIMENTO Questa è la base utilizzata per la certificazione, importante per la comprensione del campo di applicazione reale (ad esempio IEC61508:2010 ÿ IEC61508-3:2010)

RICHIESTA L'informazione più importante. Qual è la dichiarazione effettiva contenuta nel certificato? Prestare attenzione alle affermazioni generiche (ad esempio "conforme a IEC 61508"... davvero tutte e 7 le parti???) senza limiti chiari sulla capacità raggiunta. Ricordare sempre: HRF e SC hanno obiettivi deterministici.

INFORMAZIONI AGGIUNTIVE Molto diverse da un certificato all'altro. Possono raccomandare il rispetto di requisiti aggiuntivi inclusi in un Manuale di Sicurezza o in un Rapporto di Sicurezza. Prestare attenzione a frasi come "il Rapporto è parte integrante del presente certificato" - in tal caso, esaminare immediatamente il Rapporto.

Diapositive di backup



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](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

© STMicroelectronics - Tutti i diritti riservati.

Il logo ST è un marchio commerciale o un marchio registrato di STMicroelectronics International NV o delle sue affiliate nell'UE e/o in altri paesi.

Per ulteriori informazioni sui marchi ST, consultare www.st.com/trademarks.

Tutti gli altri nomi di prodotti o servizi appartengono ai rispettivi proprietari.

