life.augmented

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, Hzard e analisi del rischio, riduzione del rischio**
- **Standard di sicurezza**
- **Guasti, guasti, HRF vs sistematico**

life.augmented

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

life.augmented

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 ÿ	Alto! Ogni volta che guidi la tua auto, anche nel parcheggio	Salvataggio >> Licenziamento
Controllabilità Nessuna		Basso o nessuno	Salvataggio = Licenziamento

Conclusione: il rischio associato al fallimento del salvataggio è maggiore rispetto al fallimento del salvataggio. Anche questo non era ovvio.

life.augmented

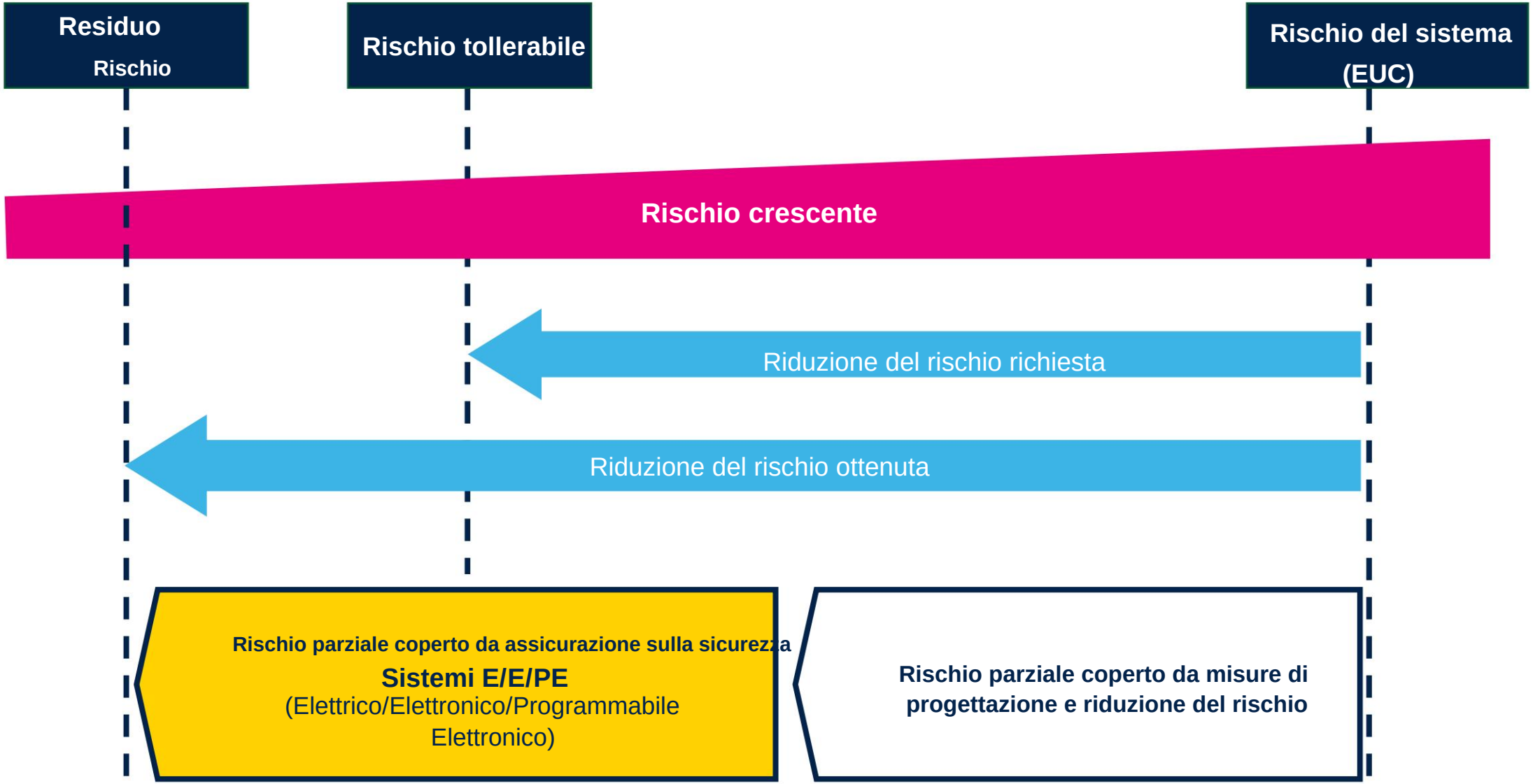
A proposito del concetto di “rischio”

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:

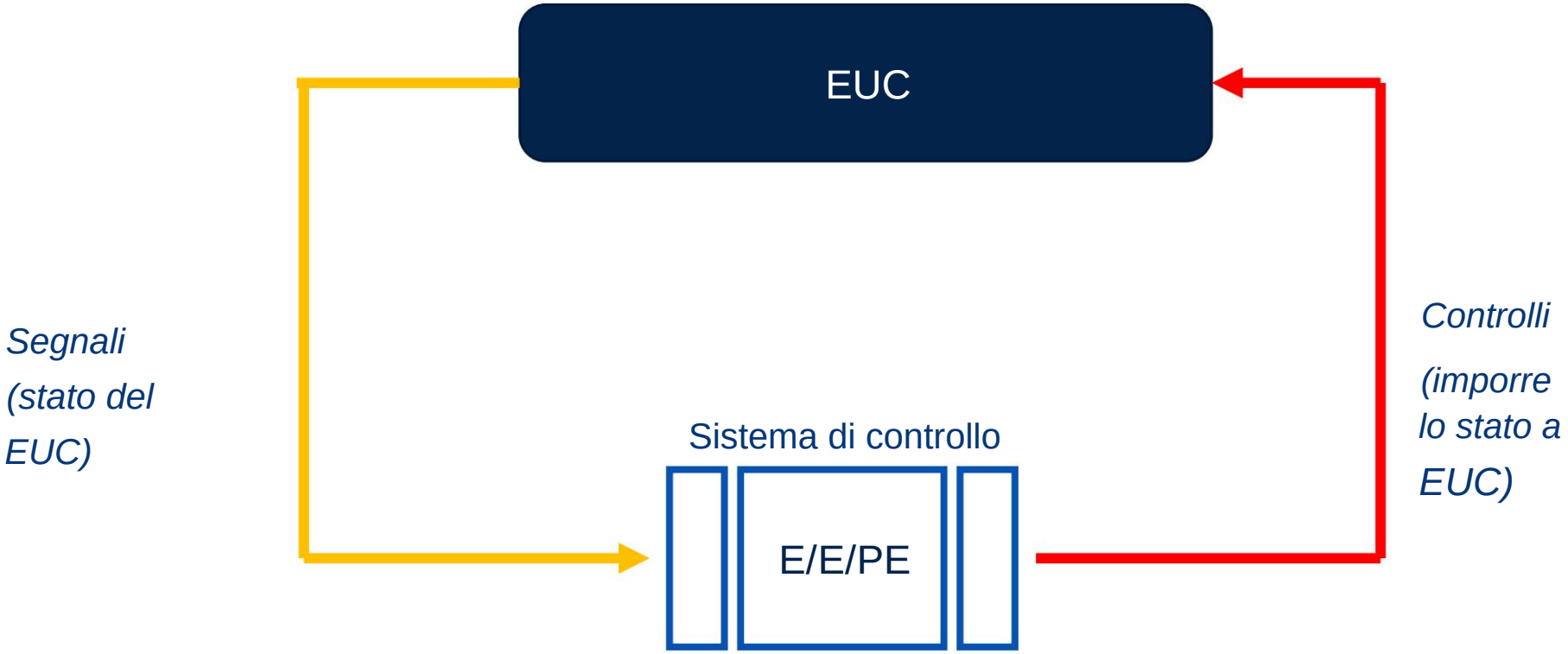
- ÿ Una volta che una nuova tecnologia si è diffusa ampiamente, le aspettative delle persone per l'assenza del rischio correlato tende ad aumentare (vedi ad esempio l'aviazione civile)
- ÿ Dipendenza dal mercato/settore, correlata alla percezione generale del pubblico (ad esempio, si ritiene ragionevolmente 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

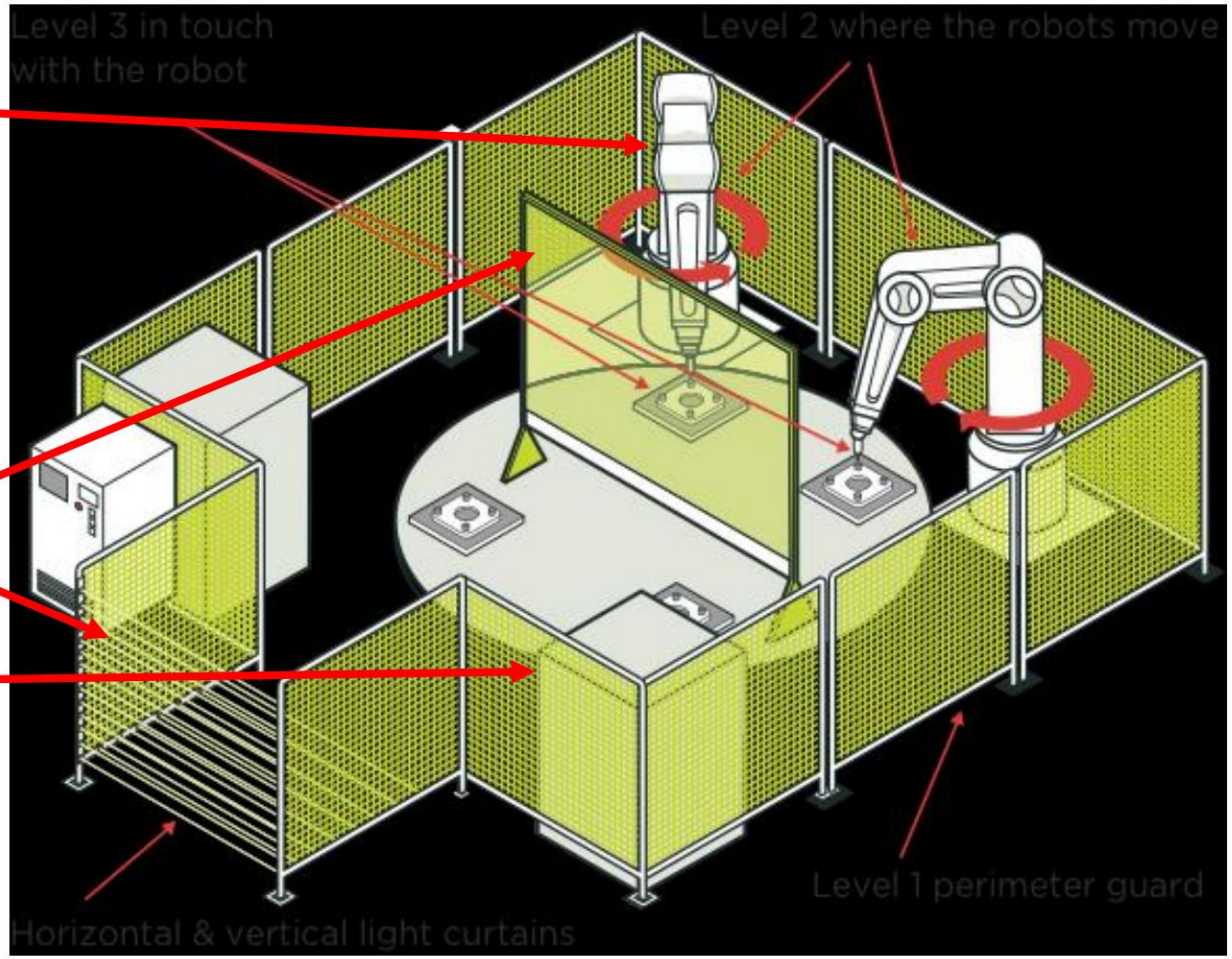
parte della sicurezza complessiva

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	Qualunque	QM

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

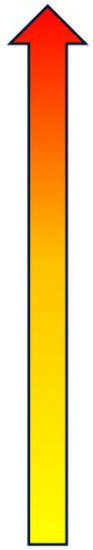
Esposizione (E) — Varia da E0 (incredibile) a E4 (alta probabilità).

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

life.augmented

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).



SIL 4 (Impianto nucleare, ferrovie)

SIL 3 (Controllo motore, industria pesante)

SIL 2 (Robot industriali, piccoli macchinari, medicale)

SIL 1 (E-bike, piccoli elettrodomestici)

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

life.augmented

Ecosistema degli standard di sicurezza

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.

life.augmented

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

Prescrittivo: IEC 60730/60335, UL 1998

life.augmented

Difetti e guasti

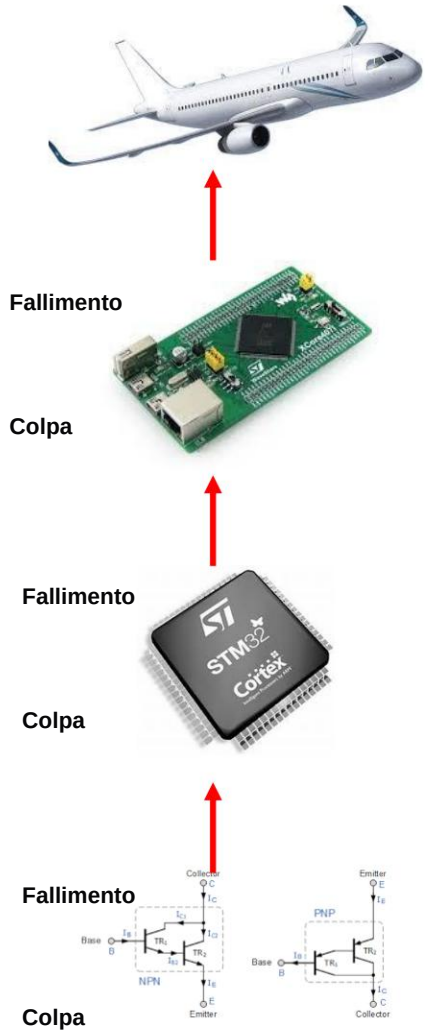
Guasto: condizione anomala che può causare una riduzione/perdita della capacità di un'unità funzionale di eseguire una specifica funzione richiesta

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.

life.augmented

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 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)

life.augmented

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 fraintendimenti (?)

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

Sicurezza

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

Sicurezza

Sicurezza: gestisce violazi~~oni/attacchi informatic~~i su dispositivi/hardware (le informazioni di sistema vengono violate da un aggressore esterno)

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…

life.augmented

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)

life.augmented

Come gestire i guasti casuali - esempi

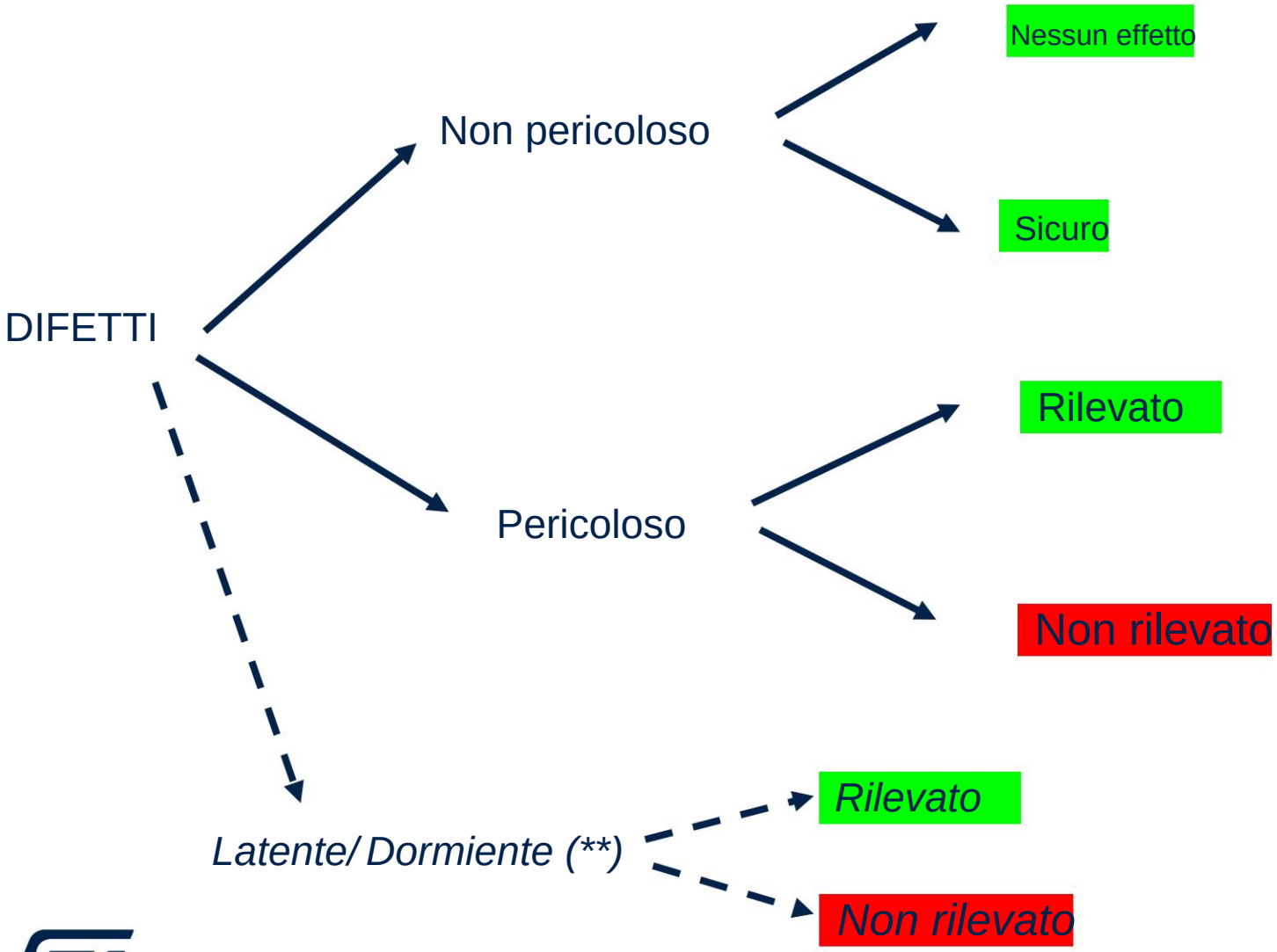
Esempio **di prevenzione degli errori :**

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.

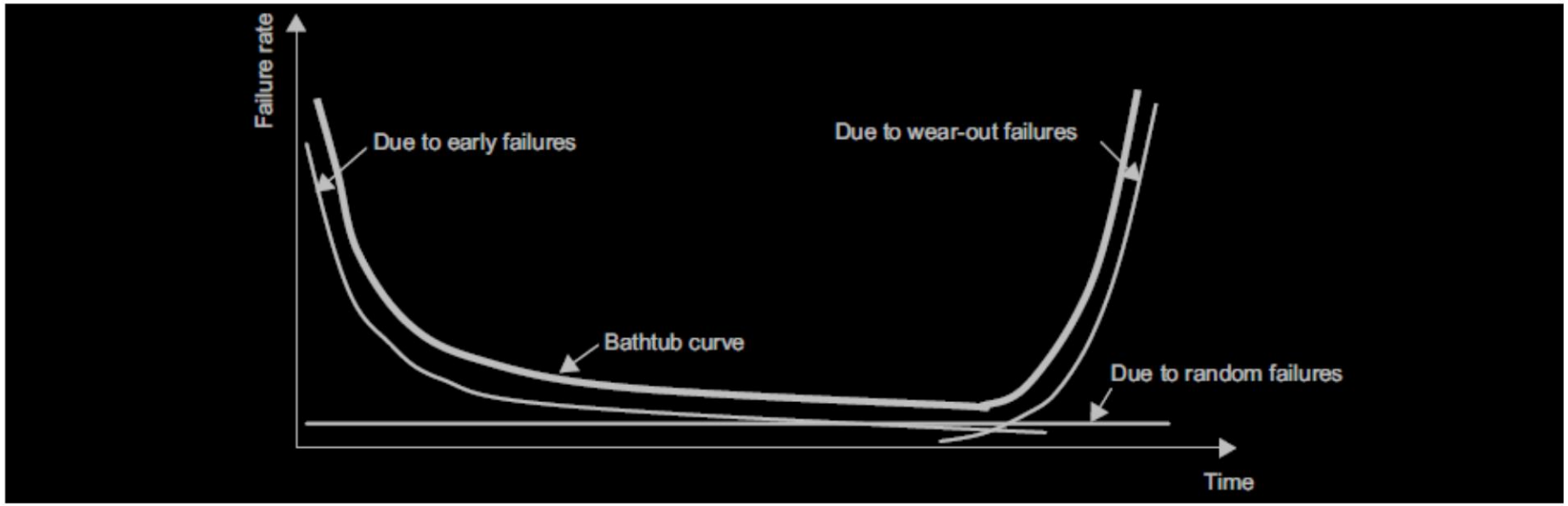
Nota: definizioni generali, un mix tra le definizioni IEC 61508 e ISO 26262

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 (ÿ(t)) di un singolo componente o sistema (entità) tale che ÿ(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 ÿ è quindi una probabilità divisa per il tempo (importante!)

Si misura in FIT; 1 FIT equivale a 1 guasto ogni 10E+9 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 (paralleli) 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

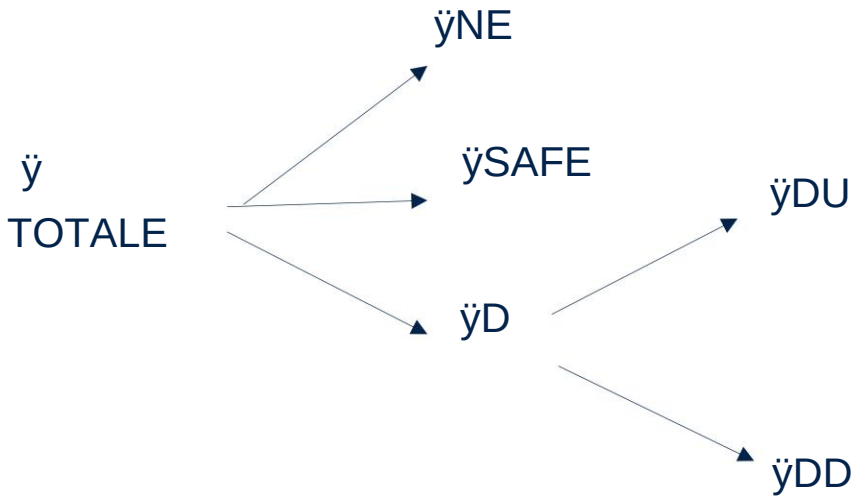
Espresso in percentuali dallo 0% al 100%

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



Metriche relative

(percentuali dallo 0% al 100%)

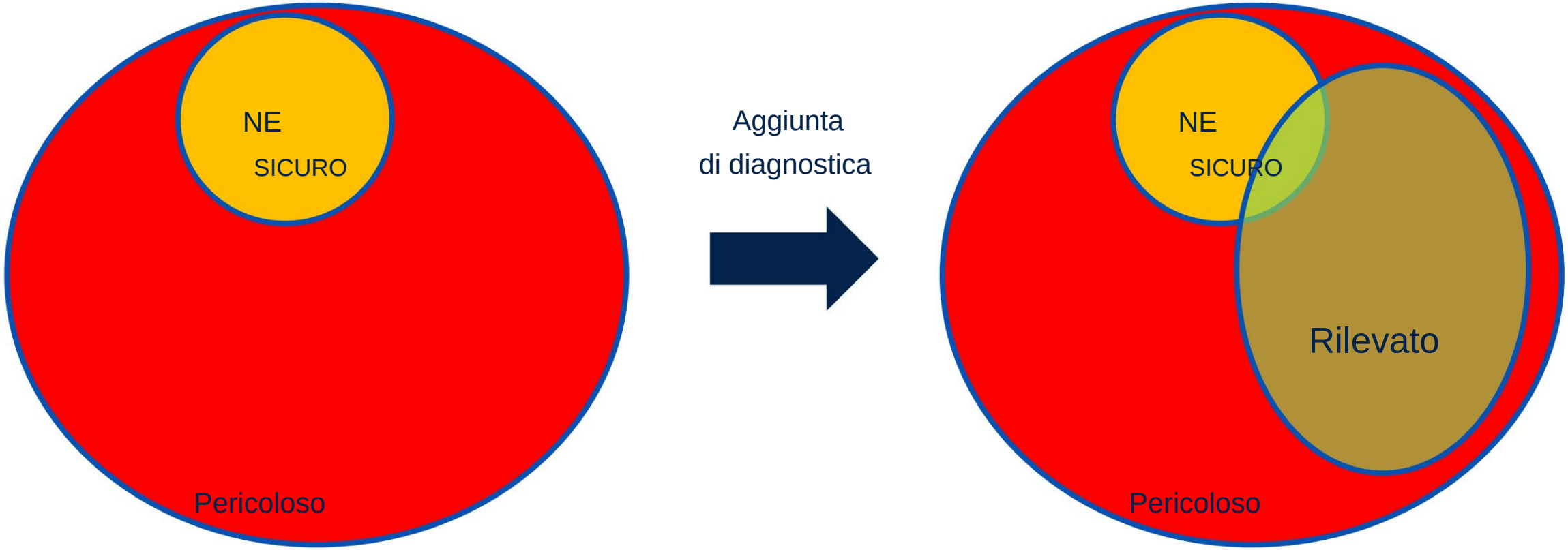
Copertura diagnostica

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

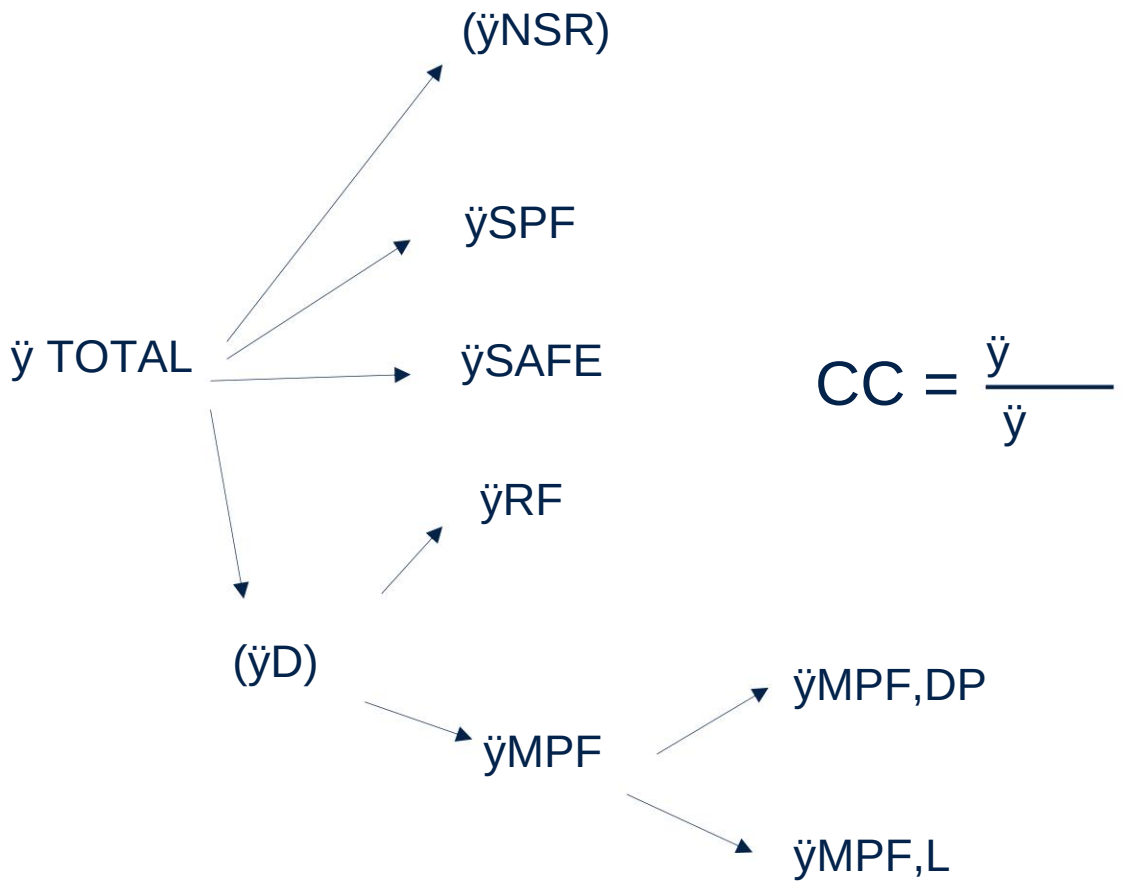
Frazione di guasti sicuri

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

Rilevamento dei guasti



Informazioni sulle metriche di sicurezza – ISO 26262



$$CC = \frac{ÿ}{ÿ}$$

Metrica di guasto a punto singolo

$$SPFm = \frac{ÿ + ÿ + ÿ +}{ÿ \qquad ÿ + ÿ}$$

Metrica di guasto latente

$$LFm = \frac{ÿ \qquad\qquad + ÿ}{ÿ\ ÿ\ ÿ \qquad\qquad ÿ\ ÿ}$$

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

life.augmented

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 ÿDU/ ÿRF. I dettagli saranno forniti nella lezione relativa alle architetture di sicurezza.

life.augmented

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

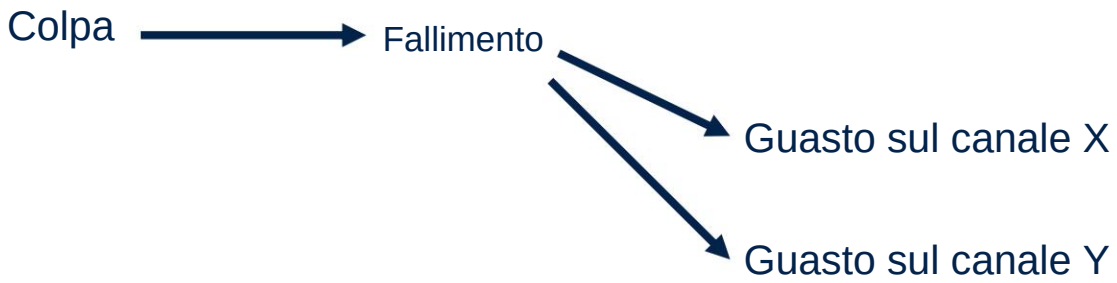
ISO 13849 richiede un solo errore, ad eccezione di PL/architettura specifici in cui è richiesto HFT=1

Guasti non indipendenti

Guasto dipendente: guasti causati da eventi non indipendenti, ovvero P(A e B) > P(A) × 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)

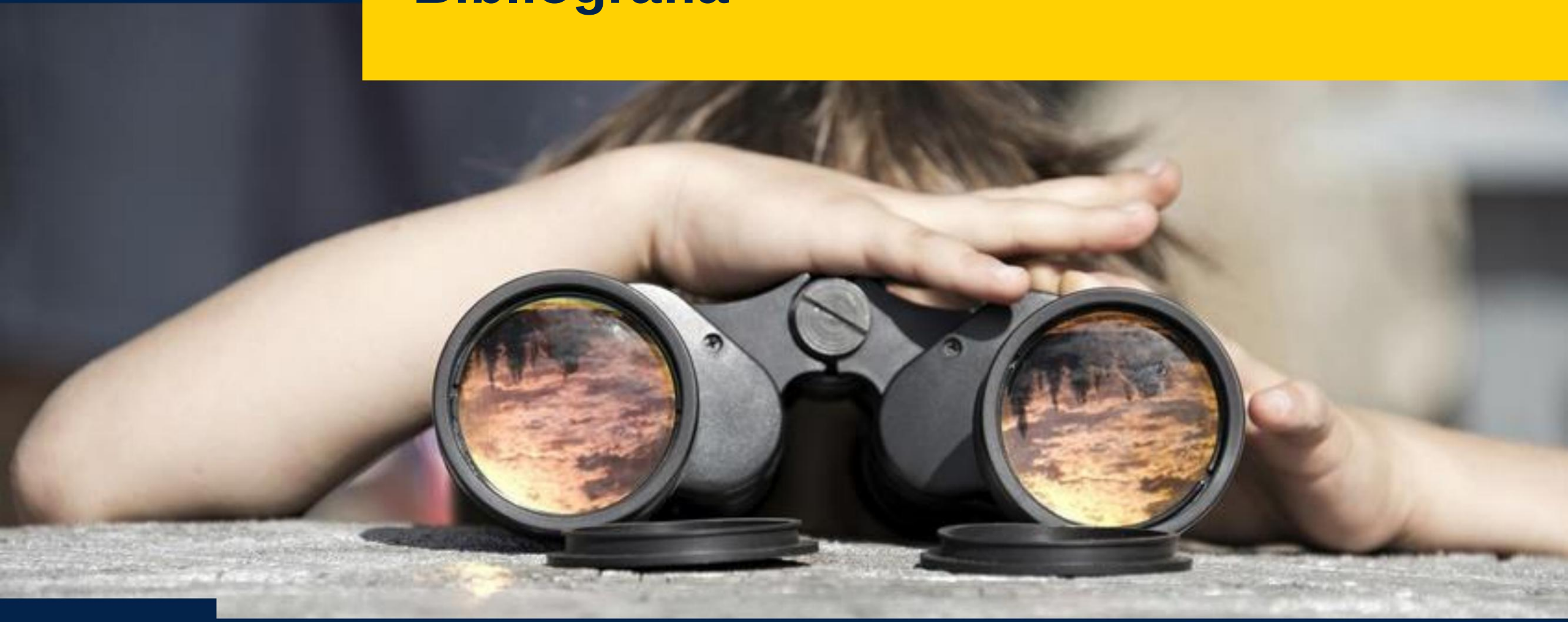


Problemi correlati

- Non possono essere inclusi nei calcoli DC, ÿ "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

life.augmented