



Sicurezza funzionale in Sistemi elettronici: Principi e Applicazioni

Alessandro Bastoni

Esperto in sicurezza funzionale
STMicroelectronics

Lezione n. 7

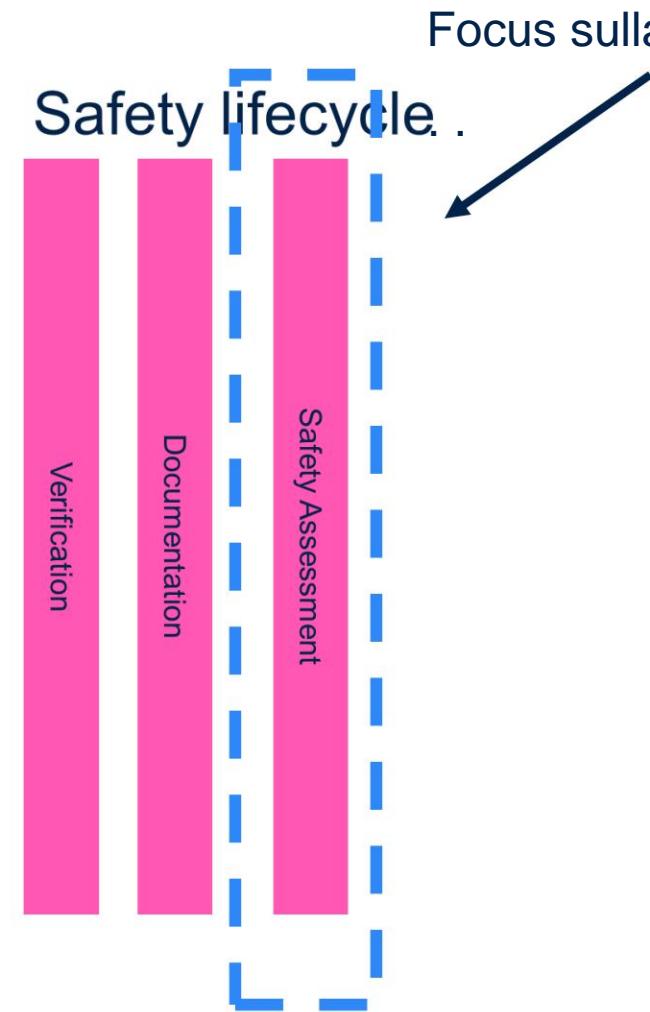
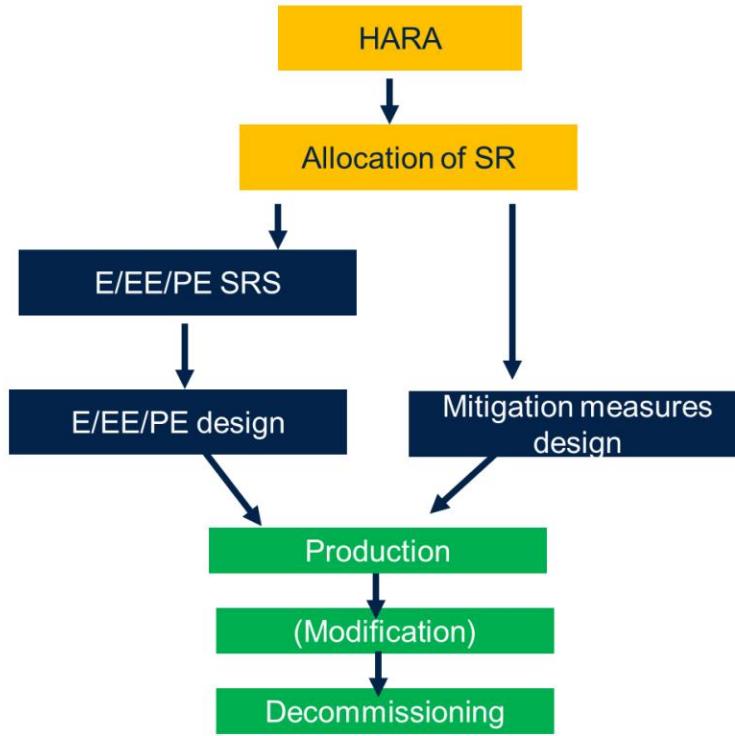
Varie nel processo di sicurezza



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.

