Skytechnology
GRUPPO SKYTEAM

ESPERIENZE DI ESECUZIONE DI GAP ANALYSIS E RELATIVI PIANI DI ADEGUAMENTO ALLA ISO 26262

9° Automotive Software Workshop

Ernesto Viale

1 Dicembre 2011

Skytechnology srl

Skytechnology è una società di ingegneria, con sedi a Milano, Torino e Roma, che opera nell'area dei sistemi embedded aiutando i propri Clienti:

- a sviluppare e testare dispositivi elettronici
- ad applicare a processi e prodotti le normative sulla Functional Safety (IEC 61508, ISO 26262, CENELEC 50126/8/9, RTCA DO-178B) e sul Miglioramento (CMMI e SPICE).

Contenuti del documento

- Illustrare alcuni aspetti caratteristici riscontrati nell'assessment e nell'adeguamento alla ISO 26262:
  - Qualità e miglioramento.
  - Organizzazione.
  - Integrazione fra il ciclo di vita del prodotto e il ciclo di vita dell'elettronica.
  - HA&RA.
  - Test e collaudi.
  - Metodi e tecniche
- Descrivere la roadmap di adeguamento e gli strumenti usati per la Gap Analysis e la definizione delle azioni.

Qualità e miglioramento

- **ISO 9001 e ISO/TS 16949**.
  - La ISO/TS è la norma più restrittiva e rigorosa fra tutte quelle derivate dalla ISO 9001 e specifiche di un settore.
  - Se l'organizzazione ha già in essere un QMS, è opportuno condividere con l'ente Qualità l'integrazione del QMS con le clausole applicabili della ISO 26262.
  - Altrimenti, è opportuno definire un insieme minimo di procedure che regolino gli aspetti fondamentali dell'organizzazione della sicurezza.
- **CMMI e (A)SPICE**.
  - Se l'organizzazione usa all'interno o verso i propri fornitori uno dei modelli di miglioramento, i processi di gestione (e.g. change management) e quelli relativi al ciclo di vita, possono essere definiti e poi auditati utilizzando le indicazioni dei modelli di miglioramento.
  - CMMI-DEV +SAFE.
  - ISO/IEC 15504-10.

Qualità e miglioramento

- Insieme minimo di procedure:
  - Gestione del system safety lifecycle e template dei work product.
  - Gestione delle anomalie di sicurezza funzionale.
  - Gestione della documentazione di sicurezza funzionale.
  - Gestione delle risorse.
  - Gestione delle azioni correttive/preventive e delle misure dei processi.
  - Approvvigionamento e qualificazione dei fornitori.
  - Gestione dei SW e HW safety lifecycle e template dei work product.
  - Identificazione e tracciabilità degli item e degli elements.
  - Gestione delle modifiche.
  - Review, audit e assessment dei progetti e processi di sicurezza.

Organizzazione

- Profili e job description:
  - Project Manager, Safety Manager e mutue responsabilità.
  - Sistemisti.
  - HW e SW Project Manager.
  - Collaudatori.
  - Reviewer, Auditor e Assessor
- Vincoli di indipendenza delle confirmation review.
- Ciclo di Emissione, Verifica, Approvazione e Distribuzione per ogni work product.
- La classe QM nella determinazione dell'ASIL dovrebbe avere definite le relative responsabilità.

Cicli di vita

- Il ciclo di vita dell'item, come definito dalla ISO 26262, deve essere integrato con il ciclo di vita del prodotto, considerando i seguenti aspetti:
  - Coinvolgimento della funzione Sicurezza Funzionale in punti critici del product lifecycle (e.g. anomalia di sicurezza segnalata dal campo).
  - Sincronizzazione delle attività di definizione dei requisiti di sicurezza e dell'esecuzione dei test ai vari livelli, con le corrispondenti milestone a livello prodotto.
  - Gestione delle modifiche, ad esempio, durante le fasi di produzione.

- Le attività specifiche di safety analyses sono tipicamente eseguite all'interno dell'organizzazione e con il supplier con modalità conformi alle clausole della ISO 26262.
- L'intervento di adeguamento dovrebbe essere più sul Sistema di Gestione della sicurezza funzionale (i.e. organizzazione, istituzionalizzazione dei processi, tracciabilità dei requisiti, formalizzazione dei collaudi, uso di metodi di supporto).
- Un punto di attenzione è l'attribuzione dell'ASIL in funzione delle classi di severità, exposure e controllabilità.
- Attenzione dovrebbe essere posta alla definizione dei criteri che definiscono ciascuna classe, in modo da ridurre la soggettività del giudizio e garantire l'omogeneità dell'assegnazione del livello di ASIL.

Test e collaudi

- Largo uso di strumenti di controllo della Tracciabilità, che presuppone l'ingegnerizzazione dei requisiti.
- Applicazione di strategie di integrazione a livello software, hardware e sistema, che presuppongono, ad esempio:
  - un controllo puntuale del rispetto delle milestone, in particolare di release.
  - efficienza e flessibilità nella risoluzione delle anomalie (di sicurezza).
  - Efficacia nella root cause analysis di valutazione di impatto delle anomalie e delle relative modifiche.
- Integrazione della metodologia di test in uso, con i metodi previsti dalla ISO 26262 (e.g. classi di equivalenza) e uso sistematico di tool di supporto e testbench.

Metodi e tecniche

- Classificare le pratiche in uso nell'organizzazione per la progettazione e collaudo, etichettandole con il metodo, tra quelli previsti dalla ISO 26262, che più si avvicina, come scopo e modalità di esecuzione.
- Per gli ASIL più alti, l'uso di un metodo può comportare, all'inizio della sua applicazione, vincoli e rigidità nel progetto.
- L'uso di un tool di supporto, specie se genera un output che possa costituire, in tutto o in parte, uno o più dei work product, può garantire, nel tempo, la sistematicità di applicazione del metodo.

Gap Analysis e Adeguamento

- Compilazione di una Checklist di dettaglio, per ogni Parte della ISO 26262, che mappa nel dettaglio le sub-clauses della Parte.
- Ogni Checklist è costituita dai seguenti fogli di lavoro:
  - Work product, che permette di assegnare un punteggio sulla compliance della singola sub-clause.
  - Methods, che traccia le evidenze di applicazione dei metodi sulle Parti che li prevedono.
  - Gaps, che traccia le deviazioni rispetto a quanto previsto dalla Parte, sia per i processi, che i work product, che i metodi.
  - Corrective Actions, che elenca le azioni correttive, relative a uno o più Gap individuati.
- Aggiornamento periodico di un cruscotto, che riporta i semafori di compliance per ogni clausola di ogni Parte e permette la caratterizzazione dei Gap e l'assegnazione delle priorità alle azioni correttive.

Checklist di dettaglio

WP	Req.	Subclause	Keyword	Guide	Score
Item definition		e) functionality required from other items, elements and the environment; f) the allocation and distribution of functions among the involved systems and elements; and g) the operating scenarios which impact the functionality of the item.	Content	e) Does it consider functionality required by other items, elements and the environment?	100
Item definition			Content	f) Does it consider the allocation and distribution of functions among the involved systems and elements?	100
Item definition			Content	g) Does it consider the operating scenarios which impact the functionality of the item?	100
Item definition	5.5	Work products Item definition resulting from the requirements of 5.4.	WP	a) Is Item definition issued and approved?	75

Work products | Tables | Gaps | x-ref Corrective actions | Gap-Corrective actions

Score	Evidences	Notes
100	Procedure XXXX, Item Definition template	
100	Procedure XXXX, Item Definition template	The template includes specific sections for criteria and constraints to be applied for the activities of requirements decomposition and allocation (i.e. section 3 Item Description).
100	Procedure XXXX, Item Definition template	
75	Procedure XXXX, Item Definition template	Item definition is also an input for the Initiation of the safety lifecycle (6.3.1), Hazard analysis and risk assessment (7.3.1)

Criteri di scoring

- Possible values: N/A, 0, 25, 50, 75, 100 as following:
  - **N/A**: the subclause is not applicable in the context of the project subject of the assessment. The reason of non applicability must be defined.
  - **0**: the subclause has not been satisfied in the project subject of the assessment
  - **25**: the subclause has not been satisfied but there are some aspects or matters that demonstrate that the subject of the subclause should be addressed with relevant work
  - **50**: the subclause has not been satisfied but there are some aspects or matters that demonstrate that the subject of the subclause should be addressed with an effort sustainable by the organization that owns the process
  - **75**: the subclause has not been fully satisfied but all the main requirements have been addressed by the project
  - **100**: the subclause has been fully satisfied

Dashboard

CLAUSES PANEL

	Part 2	Part 3	Part 4	Part 5	Part 6	Part 7	Part 8	Part 9
Clause 5								
Clause 6								
Clause 7								
Clause 8								
Clause 9								
Clause 10								
Clause 11								
Clause 12								
Clause 13								
Clause 14								

	Score	Criteria
	100	Fully implemented
	75	Largely implemented
	50	Partially implemented
	0-25	Not implemented
		Not rated

SUB-CLAUSES PANELS

PART 2 – MANAGEMENT OF FUNCTIONAL SAFETY

safety management	5.3.1	5.3.2	5.4.2	5.4.3	5.4.4	5.4.5	5.5.1	5.5.2	5.5.3						
management during the concept phase and the product	6.3.1	6.3.2	6.4.2	6.4.3	6.4.4	6.4.5	6.4.6	6.4.7	6.4.8	6.4.9	6.5.1	6.5.2	6.5.3	6.5.4	6.5.5
Clause 7 Safety management after the item's release for production	7.3.1	7.3.2	7.4.2	7.5.1											

PART 3 – CONCEPT PHASE

Clause 5 Item

Gaps Synoptics | Gaps Metrics | Processes | Work Products | Methods | Metrics Database

Pronto

Dashboard

	ISO/FDIS 26262 CLAUSES		Score	GAP ANALYSIS ON SAFETY LIFECYCLE PROCESSES Gaps			GAPS CHARACTERIZATION Gap Type	Gap Criticality
4	PART 2	MANAGEMENT OF FUNCTIONAL SAFETY						
92	PART 3	CONCEPT PHASE						
93	Clause 5	Item definition						
94							a. -	-
95	5.3.1	Prerequisites	-1	n.a.			b. -	-
96							c. -	-
97				a. To be defined the minimum set of infomation necessary for item definition			a. Documentation	Low
98	5.3.2	Further supporting information	75				b. -	-
99							c. -	-
100							a. -	-
101	5.4	Requirements and recommendations	100				b. -	-
102							c. -	-
103							a. Documentation	edium Low
104	5.5	Item definition	75	a. Item Definition to be formally reviewed and approved			b.	
105							c.	
106	Clause 6	Initiation of the safety lifecycle						
107							a.	
108	6.3.1	Prerequisites	100				b.	
109							c. -	-
110							a.	
111	6.3.2	Further supporting information	100				b. -	-
112							c. -	-
113				Improvement opportunity:			a. -	-
114	6.4.1	Determination of the development category	100	maintain the official list of			b. -	-
115				Items Definitions			c. -	-

Documentation
Measures
Modification
Organization
Planning
Process
QMS
Verification

Gaps Synoptics | Gaps Metrics | Processes | Work Products | Methods | Metrics Database

Skytechnology
GRUPPO SKYTEAM

Via Francesco Gonin, 55

20147 Milano

Tel. +39 02 370511

Fax. +39 02 37051226

Via Adolfo Ravà, 124

00100 Roma

Tel.: +39 06 45439361

Fax: +39 06 45439237

Corso Svizzera, 185

10149 Torino

Tel.: +39 011 7715774

Fax: +39 011 7419448