Gloria Mirabella, Davide Marano

Analisi della Sicurezza Funzionale di un autoveicolo

La normativa ISO 26262, introdotta nel 2011 e aggiornata nel 2018, costituisce lo standard internazionale per la functional safety (sicurezza funzionale) nell'ambito dell'industria automobilistica. La normativa si applica ai sistemi elettrici ed elettronici costituiti da componenti hardware e software presenti a bordo degli autoveicoli destinati alla produzione in serie. Tale standard definisce requisiti, processi e strumenti da utilizzare nell'iter di sviluppo del prodotto, al fine di garantire il mantenimento di elevati livelli di sicurezza per l'intero ciclo di vita del veicolo. In questo articolo è presentata una introduzione ai principali concetti della functional safety, con particolare riguardo alla fase di Hazard Analysis e Risk Assessment di un autoveicolo

Nell'ultimo decennio, l'aumento del numero di sistemi elettronici e funzionalità avanzate a bordo degli autoveicoli, ha rivoluzionato il comfort e la sicurezza di guida (si pensi ad esempio ai sistemi di frenata assistita, al controllo elettronico di stabilità ESP, ecc.). Allo stesso tempo ci si è resi conto di come questi possano determinare problemi per la sicurezza dell'utente finale a causa di interazioni errate tra sistemi elettronici, malfunzionamento degli stessi oppure usi errati delle funzionalità da parte dell'utente.

Per tale motivo nel 2011 è stato pubblicato lo standard internazionale ISO 26262, che introduce il concetto di "sicurezza funzionale" (Functional Safety) per i veicoli destinati alla produzione in serie. La sicurezza funzionale si propone di:

- ridurre il numero delle perdite umane dovuto a possibili malfunzionamenti dei sistemi elettrici/elettronici presenti a bordo del veicolo;
- ridurre il numero e l'entità delle azioni legali nei confronti delle case automobilistiche;
- ridurre il numero di campagne di richiamo di autoveicoli;
- evitare "overdesign" di componenti che non hanno impatto sulla sicurezza funzionale;
- garantire l'accesso semplificato ai mercati globali, mediante la conformità a normative internazionali unificate.

Lo standard di sicurezza ISO 26262 nell'industria automotive

La normativa ISO 26262 [1] è applicabile nell'ambito automotive, in particolare ai sistemi elettrici ed elettronici installati in autoveicoli destinati alla produzione in serie, aventi massa fino a 3500 kg. Impone un processo e una serie di procedure, volte ad analizzare, evitare o mitigare i possibili rischi causati da malfunzionamenti di sistemi elettrici/elettronici (E/E) e dall'interazione di tali sistemi. Tale standard non si occupa dei rischi legati a shock elettrici, rilascio di gas, radiazioni, tossicità, infiammabilità, reattività, corrosione, se non direttamente causati dal malfunzionamento di sistemi E/E. Per l'analisi di tali rischi esistono appositi standard dedicati.

Ad oggi, le aziende automobilistiche non sono obbligate a rispettare uno specifico standard, ma sono tenute a garantire lo sviluppo del prodotto secondo lo stato dell'arte nell'ambito della sicurezza funzionale. La normativa ISO 26262 costituisce lo stato dell'arte per la sicurezza funzionale, ed è ad oggi universalmente utilizzata da tutti i produttori di autoveicoli.

Il Ciclo a V e la "Safety Culture"

La sicurezza funzionale coinvolge trasversalmente tutte le fasi del processo di sviluppo prodotto che costituiscono il cosiddetto "ciclo di sviluppo a V" (Figura 1); interviene quindi durante le fasi di design e sviluppo, verifica e validazione, produzione, operazione e dismissione del prodotto. Il produttore deve, per l'intero ciclo del prodotto, dare evidenza di aver seguito un processo che permetta di evitare o mitigare i possibili rischi dovuti a malfunzionamenti dei sistemi elettrici/elettronici presenti a bordo del veicolo.

L'Analisi e Valutazione dei Rischi (Hazard and Risk Assessment – HARA)

Obiettivo della fase di design in ottica functional safety è progettare dei sistemi che siano fail-safe, ovvero sistemi che in caso di guasto possano raggiungere un predefinito "stato sicuro" denominato safe-state. I sistemi E/E devono dunque essere in grado di rilevare possibili guasti che possano compromettere la sicurezza degli utenti e, nel caso in cui tali guasti si verifichino, devono garantire il raggiungimento di uno stato sicuro.

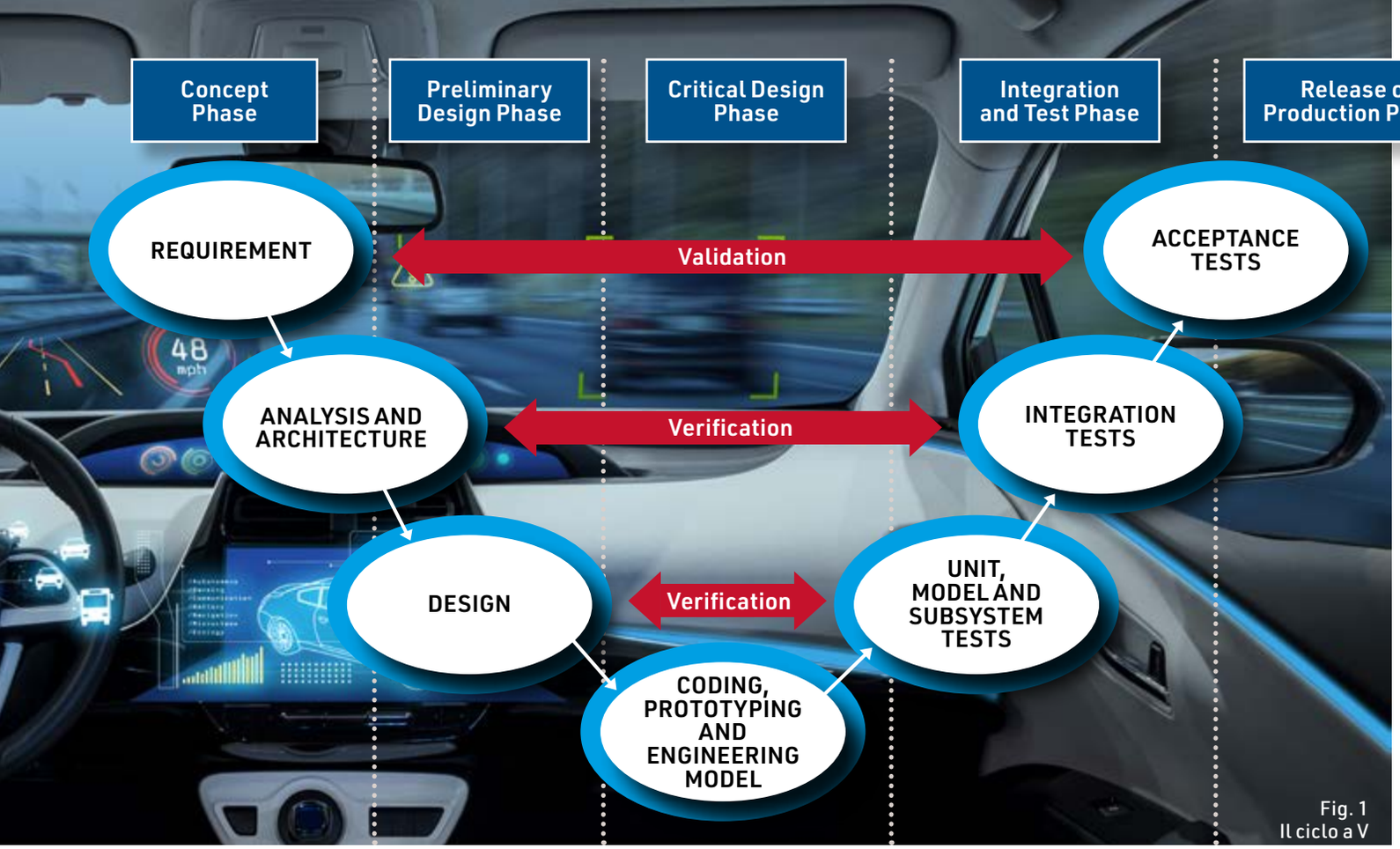

Fig. 1
Il ciclo a V

Ad esempio, in caso di fault del sensore di posizione del pedale acceleratore, il Safe State potrebbe consistere nell'attuare la strategia di Limp-Home o strategia di efficienza ridotta, che consiste nel limitare le performance del veicolo e avvisare l'utente tramite adeguate spie sul quadro.

Durante la fase di design, si redige l'Analisi e Valutazione dei Rischi (Hazard and Risk Assessment – HARA). Ogni funzionalità del veicolo viene analizzata e i possibili rischi, nel caso di malfunzionamento, vengono identificati in differenti condizioni operative del veicolo.

Un esempio di funzionalità di veicolo è la "Funzionalità di gestione della coppia" che ha lo scopo di fornire la coppia desiderata, tenendo conto delle richieste dell'utente e di altri sistemi (i.e. cruise control), tramite il controllo e l'attuazione del sistema di propulsione.

Nell'HARA, uno dei metodi più frequentemente utilizzati per l'identificazione dei rischi è l'HAZOP (Hazard and Operability study) secondo cui si applicano delle parole chiavi alla funzione, in modo da analizzare e coprire tutte i possibili malfunzionamenti. Tra le parole guida si possono menzionare, a titolo d'esempio, "non voluta" ovvero la funzione interviene quando non richiesto; "insufficiente" o "mancante" ovvero la funzione viene performata in maniera insufficiente rispetto a ciò che ci si aspetta o non viene performata del tutto. Alcuni esempi sono riportati in Tabella 1 e in [2].

Nel caso della funzionalità della gestione della coppia, applicando le parole chiave, si ottengono i malfunzionamenti di mancata attuazione (perdita di propulsione), eccessiva attuazione (accelerazione indesiderata), e così via. Una volta definiti i possibili malfunzionamenti (malfunctions) associati alla data funzionalità, si valutano i possibili scenari (rettilineo/curva, alta aderenza/bassa aderenza, ecc.) e i possibili rischi che tali malfunzionamenti comportano nei possibili scenari.

Il rischio viene quantificato tramite un parametro, chiamato ASIL (Automotive Safety Integrity Level), determinato dalla combinazione di tre parametri:

- Exposure (E): è una misura della frequenza di esposizione al rischio, intesa sia come probabilità di accadimento della condizione d'uso nel tempo di missione, sia come quantità di tempo sul totale (frequenza);
- Controllability (C): è una misura della probabilità che il guidatore o gli altri partecipanti allo scenario di guida (pedoni, ciclisti, o altri guidatori di veicoli coinvolti nel possibile incidente) siano in grado di evitare le conseguenze dell'hazard (mitigazione);
- Severity (S): è una misura della gravità del danno inflitto al guidatore, ai passeggeri o ad altri partecipanti allo scenario di guida se le misure di controllabilità fallissero (danno).

TAB. 1 - HAZOP KEYWORDS

Mancante	La funzione non interviene quando dovrebbe
Insufficiente	La funzione viene performata in maniera insufficiente rispetto a quanto atteso
Eccessiva	La funzione viene performata in maniera eccessiva rispetto a quanto atteso
Opposta	La funzione interviene in maniera opposta rispetto a quanto atteso
Anticipata	La funzione interviene anticipatamente rispetto a quanto atteso
Posticipata	La funzione interviene con ritardo rispetto a quanto atteso
Intermittente	La funzione viene performata in maniera intermittente
Non voluta	La funzione interviene quando non dovrebbe

Lo standard ISO 26262 definisce 3 classi per la severity, 4 classi per l'exposure e 3 classi per la controllability, riportate nella ISO 26262-3:2018. Uno strumento utile per la determinazione dell'exposure è il catalogo VDA 702 [3], realizzato dall'associazione VDA, composta da 620 aziende tedesche nell'ambito della produzione automobilistica. Nel catalogo sono riportati possibili scenari ed exposure associata (Tabella 2).

TAB. 2 - STANDARD ISO 26262 PER SEVERITÀ, ESPOSIZIONE AND CONTROLLO

Table 1 – Classes of Severity				
	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 2 – Classes of probability of exposure regarding operational situations					
	Class				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Table 3 – Classes of controllability				
	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Nella Tabella 3 si riportano i valori indicati nella ISO 26262, per la determinazione del valore di ASIL

TAB. 3 - DETERMINAZIONE DEL VALORE DI ASIL SECONDO ISO 26262

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	Aa
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
a See 6.4.3.11				

L'Automotive Safety Integrity Level (ASIL) è quindi una lettera, da A a D in ordine di importanza crescente, che rappresenta:

- il livello di rischio associato a ciascun hazard;
- Il grado di robustezza (integrità) che le parti di sistema interessate dall'hazard devono avere affinché il rischio risulti accettabile.

Nel caso in cui il rischio risulti accettabile, si attribuisce invece il parametro "QM" («Quality Management"), ciò implica l'assenza di requisiti specifici di sicurezza per il caso individuato.

Esempio: valutazione del malfunzionamento "Sudden Unintended Acceleration"

Si consideri il malfunzionamento denominato "Sudden Unintended Acceleration", ossia una accelerazione involontaria, inaspettata e incontrollata di un autoveicolo. Il malfunzionamento potrebbe essere imputabile, a titolo di esempio, ad un fault del pedale acceleratore o della centralina che gestisce la funzionalità di attuazione della coppia. Tuttavia, nell'HARA si analizza la funzionalità nel suo complesso senza entrare nel merito del componente che ha provocato il fault. Solo successivamente, a conclusione dell'Hara, seguirà l'allocazione dei requisiti ai componenti. Assumendo che il veicolo stia viaggiando in autostrada, con traffico medio, ad una velocità di 120 km/h, il malfunzionamento porterebbe ad una valutazione di exposure pari ad E4, dato che tale situazione di guida potrebbe potenzialmente presentarsi ogni volta che il veicolo viene guidato. L'evento può essere considerato normalmente controllabile dal 90% degli utenti portando ad una valutazione di controllability pari a C2. Il driver, avvertendo l'accelerazione e notando che la distanza rispetto al veicolo che segue diminuisce, sarà in grado di reagire tramite il pedale del freno. La stima della controllabilità dovrà essere confermata tramite simulazioni e test su veicolo. Nel caso in cui il guidatore non riuscisse a controllare l'evento, si avrebbe un impatto frontale/posteriore tra il veicolo in questione e il veicolo che segue. Considerando che la differenza di velocità tra due veicoli in autostrada è presumibilmente non superiore ai 50Km/h, è possibile assegnare una severity di S2 (possibili lesioni gravi, che mettono a rischio la vita dei passeggeri). Dalla Tabella 4 si evince che in tal caso l'ASIL risultante è B. Dopo il risk assessment ed a conclusione del medesimo, si assegnano i safety goal ed i safe state del sistema. I safety goal sono gli obiettivi che, se soddisfatti, garantiscono la sicurezza del veicolo. I safety goal sono derivati negando gli effetti dei malfunzionamenti sul veicolo e costituiscono la base di partenza per la formulazione delle specifiche di Safety (che avverrà in fase di system development). Nel caso dell'esempio citato, in cui l'effetto indesiderato del malfunzionamento è l'accelerazione non voluta, il Safety Goal sarà "Evitare una non voluta accelerazione del veicolo", assegnandogli l'ASIL massimo ottenuto dai possibili scenari presi in considerazione. I safe state del sistema, come già detto, sono modi operativi nei quali il veicolo deve portarsi in caso di fault (e.g. strategia di Limp-Home). Ogni Safety Goal viene classificato in termini di ASIL, determinandone la rilevanza. Ad ogni ASIL sono associate una serie di interventi di irrobustimento da attribuire all'intera catena di componenti (HW e SW) che concorrono al potenziale rischio.

BIBLIOGRAFIA

[1] ISO, ISO26262. "26262: Road vehicles-Functional safety." International Standard ISO/FDIS 26262 (2018).
[2] Kumar, R., "ISO 26262 Hazard and Risk Assessment for Hybrid Powertrain," SAE Technical Paper 2019-26-0107, 2019
[3] VDA 702 Situationskatalog E-Parameter nach ISO 26262-3