ISO 26262國際安全規範與應用介紹-以車輛中心開發AEB為例

◎財團法人車輛研究測試中心 褚政怡

壹、車輛中心研發流程通過ISO 26262認證

在自駕車普及之前，先進駕駛輔助系統(Advanced Driver Assistance System, ADAS)包括盲點偵測、前方碰撞預警、後方碰撞警示、夜視系統、停車輔助、適應性巡航控制、車道偏離警示與駕駛狀態偵測等，已成為最新車款之標準配備，並且由高階豪華車種普及到平價車款，以因應日漸高漲之安全意識與逐步完善之安全法規；根據產調資料顯示，由於民眾需求與各國陸續訂定法規強制安裝ADAS產品，帶動相關市場快速成長，例如2018年美國法規強制安裝倒車顯影以及歐盟法規規定安裝緊急求救系統等，預估ADAS商機將由2015年30億歐元，至2020年將倍增為72億歐元。

為協助我國車輛產業與電子產業參與ADAS市值躍升之趨勢，車輛中心開發多項車電系統，以緊急煞車輔助系統(Advanced Emergency Braking System, AEB)為例，該研發雛型性能優異，並具國內業者技術移轉實績，為確保符合消費市場注重之安全議題，其研發品質管理流程皆符合ISO 9001與CMMI-DEV ML3，並專案再導入ISO 26262且通過流程認證(圖1)，使研發技術同步符合最新之功能安全標準。

圖1. ARTC獲頒ISO 26262功能安全流程認證證書

貳、ISO 26262車電系統的功能安全標準

ISO 26262是國際標準組織(ISO)2011年公告最新之車電系統功能安全國際標準，本標準是調合自IEC 61508（1998年公告），將功能安全聚焦在車電系統。IEC 61508為最初電氣產品功能安全國際標準，係針對一般工業領域電機/電子/可程式電子系統之功能安全評估與管控方法加以規範，而車電系統與一般工業用系統是有相當差異，例如安全性、成本或可靠度要求等；因此，2011年就公告專屬於車輛領域之ISO 26262，其適用於小客車（M類）所裝載之車電系統，使得研發專案有清楚定義功能安全相關系統、硬體與軟體所應遵循之共同目標，並明確標示系統達成之安全門檻，以作為保安設計之產品開發資料。

為擴大適用機車（L類）/貨車（N類），並因應車電系統之半導體元件（例如微控制單元）之認證需求，或是ADAS系統防止駭客入侵之保全(cyber security)等議題，該標準也參考ISO/PAS 19695、ISO/PAS 19451與SAE J3061等標準，於2018年公告第二版ISO 26262標準，以滿足車電系統功能安全之最新需求。

一、ISO 26262標準概述

ISO 26262涵蓋車輛整個生命週期，稱為安全生命週期(Safety lifecycle)，由管理、開發、生產、經營、維修至報廢皆有相應之要求，本標準包含12章節：

Part 1 名詞解釋
Part 2 功能安全管理
Part 3 概念階段
Part 4 產品開發在系統層級
Part 5 產品開發在硬體層級
Part 6 產品開發在軟體層級
Part 7 生產與操作
Part 8 支援流程
Part 9 車輛安全完整性等級導向與安全導向分析
Part 10 ISO 26262指南
Part 11 ISO 26262半導體應用
Part 12 ISO 26262機車適用。

ISO 26262採行車輛安全完整性等級(AutomotiveSafety Integrity Level, ASIL)，以評估車電系統符合功能安全程度，使得研發專案清楚定義功能安全相關系統、硬體與軟體所應遵循之共同目標，明確標示ASIL為產品開發之安全目標。ASIL由嚴重度(Severity)、暴露機率(Probability of Exposure)與可控度(Controllability)決定，等級分為QM(Quality Management)與ASIL A至D等5種，QM等級無需適用ISO 26262，比照一般車輛產業品質管理系統ISO/TS 16949要求，而ASIL等級愈高，系統功能安全要求愈多，故ASIL D設計開發屬最嚴之安全考量；新版標準增訂機車安全完整性等級(Motorcycle SIL, MSIL)，等級亦為QM與MSIL由A至D共5種，MSIL QM與MSIL A兩種等級等同ASIL QM，而MSIL B等同ASIL A，MSIL C等同ASIL B，MSIL D等同ASIL C。

二、車輛安全生命週期

ISO 26262提供車輛安全生命週期各階段重要活動，例如車輛專屬風險基礎之整合水準、避免不合理風險之應用需求、確保合適安全水準之驗證與確認以及與供應商之關係需求等。

車電系統安全議題包含功能導向與品質導向之開發活動與工作產品，ISO 26262清楚定義研發專案之功能安全相關系統、硬體與軟體所應完成之開發活動與工作產品，形成產品之安全生命週期之各個階段，分為概念階段、產品開發與生產交付後等三階段，由綜合說明之功能安全管理起始，往下就是開始之概念階段，接續是產品開發在系統層級、產品開發在硬體層級、產品開發在軟體層級與結束之生產與操作，其間產品開發在系統層級包含產品開發在硬體層級與產品開發在軟體層級兩章，形成系統、子系統之階層架構，而軟、硬體開發互有關聯，確保系統開發是軟硬兼顧。

參、ISO 26262功能安全設計與CMMI流程整合

ISO 26262只專注於功能安全規範，與適用於發展之能力成熟度整合模式(CMMI-DEV)的等級3(ML3)流程相當，兩者搭配可形成完整之路線圖(Road Map)，才能有效導入組織運作。CMMI-DEV係美國軟體工程學院(SEI)自1984年起所發展的一套組織品質管理標準，以確保軟/硬體產品之研發品質，已廣為世界各研發組織流程改善以落實系統工程所遵循。

功能安全技術搭配系統工程之路線圖可形成完整機制，可作為研發流程融入功能安全之可行方案，滿足車電系統安全又可靠之需求；CMMI-DEV V1.3與ISO 26262關聯如表1所示，車輛中心比對ML3之18項流程與安全生命週期，將兩者融合建立一研發機制，藉由CMMI-DEV ML3建立之流程、生命週期與系統工程手法，再融入ISO 26262功能安全要求，使車電系統兼顧功能安全與產品可靠度。

表1. CMMI-DEV與ISO 26262關聯

CMMI-DEV ML3 流程	ISO 26262 細項
1.一般執行方法	2-5安全管理, 6-5展開軟體階段產品開發, 8-10文件化
2.組織流程專注	無相關
3.組織流程定義	2-5安全管理, 2-6概念階段與產品開發之安全管理, 3-6展開安全生命週期
4.組織訓練	2-5安全管理
5.需求發展	2-5安全管理, 3-5項目定義, 3-6展開安全生命週期, 3-7危害分析與風險評估, 3-8功能安全概念, 4-6技術安全需求規範, 5-6硬體安全需求規範
6.需求管理	8-6 安全需求規範與管理
7.計畫規劃+整合式計畫管理	2-5安全管理, 2-6概念階段與產品開發之安全管理, 3-5項目定義, 3-6展開安全生命週期, 4-5展開系統階段產品開發, 5-5展開硬體階段產品開發, 6-5展開軟體階段產品開發, 8-12軟體元件資格認可, 8-13硬體元件資格認可, 8-14使用證明
8.計畫監控+整合式計畫管理	2-6概念階段與產品開發之安全管理, 4-10 功能安全評估
9.供應商協議管理	8-5分散式開發介面, 8-12軟體元件資格認可, 8-13硬體元件資格認可
10.風險管理	3-7危害分析與風險評估
11.技術解決方案	2-6概念階段與產品開發之安全管理, 2-7量產後之安全管理, 3-6展開安全生命週期, 4-6技術安全需求規範, 4-7系統設計, 5-6硬體安全需求規範, 5-7硬體設計, 6-6軟體安全需求規範, 6-7軟體結構設計, 6-8 軟體單元設計與完成, 6-11軟體安全需求驗證, 7-5量產, 7-6操作、服務與報廢, 8-12軟體元件資格認可, 8-13硬體元件資格認可, 8-14使用證明, 9-5ASIL調適之需求分解, 9-6 共存元件, 9-7 共因失效分析, 9-8安全分析
12.產品整合	2-6概念階段與產品開發之安全管理, 4-5展開系統階段產品開發, 4-6技術安全需求規範, 4-8項目整合與測試, 5-6硬體安全需求規範, 5-10硬體整合與測試, 6-10 軟體整合與測試, 6-11軟體安全需求驗證, 8-13硬體元件資格認可, 8-14使用證明
13.查證	2-6概念階段與產品開發之安全管理, 3-7危害分析與風險評估, 3-8功能安全概念, 4-6技術安全需求規範, 4-7系統設計, 5-6硬體安全需求規範, 5-7硬體設計, 6-6軟體安全需求規範, 6-7軟體結構設計, 6-8 軟體單元設計與完成, 6-9 軟體單元測試, 6-10 軟體整合與測試, 6-11軟體安全需求驗證, 8-9驗證
14.確認	2-6概念階段與產品開發之安全管理, 4-5展開系統階段產品開發, 4-6技術安全需求規範, 4-9安全確認
15.度量與分析	5-8評價硬體結構度量, 5-9評價因硬體隨機失效造成之安全目標破壞
16.流程與產品品質保證	2-6概念階段與產品開發之安全管理
17.建構管理	8-7建構管理, 8-8變更管理, 8-11軟體工具使用信賴度, 8-12軟體元件資格認可, 8-13硬體元件資格認可, 8-14使用證明
18.決策分析與解決方案	無相關

肆、通過ISO 26262流程認證－以自動緊急剎車系統AEB為案例

車輛中心研發品質管理流程已符合ISO 9001與CMMI-DEV ML3，也融入ISO 26262功能安全流程，使研發專案形成由組織之機制來支持專業分工的系統工程團隊，並具備車電產業最新功能安全要求，車輛中心即運用開發AEB流程為標的，順利通過ISO 26262流程認證。

一、功能安全標準訓練與落差分析

ISO 26262為車電系統功能安全之流程/產品認證標準，車輛中心為服務車電產業需求，透過獲得國際ISO 26262流程之認證，移轉科研研發成果予廠商，並協助廠商接續商品化推進。車輛中心透過與台灣檢驗科技股份有限公司(SGS)合作專案，研發單位已有多位獲得車輛功能安全專業人員(Automotive Functional Safety Professional, AFSP)專業證照，可完善執行研發流程之落差分析、功能安全管理、功能安全概念與技術安全概念等作業。

車輛中心因應功能安全流程認證需求，採用AEB開發流程做為認證標的，透過組成安全小組，並呼應第三方(I3)認證單位要求，安全經理(Safety Manager)係由非AEB開發計畫成員擔任，其主要負責選擇計畫成員、建立並維護專案安全計畫(Safety Plan)、管理內部與外部介面。完整團隊組成與分工說明如下：

- 第三方負責流程認證(含輔導與諮詢)；
- 工作產品審核由計畫之部門主管負責；
- 安全經理負責安全計畫；
- 計畫主持人負責計畫執行規劃書；
- 系統工程師負責系統規劃，包含項目定義、危害分析與風險評估(Hazard analysis and risk assessment, HARA)、安全目標(Safety goals)、技術安全需求(Technical Safety Requirements, TSR)；
- 軟/硬體工程師負責硬體規劃，承接系統層級之功能安全需求(Functional Safety Requirements, FSR)，轉為軟/硬體層級之設計文件；
- 測試工程師負責測試規劃，承接系統層級之FSR，轉為測試文件。

落差分析(Gap Analysis)作業係由SGS-TÜV稽核員（主評）對車輛中心之研發流程、AEB計畫資料與ISO 26262標準要求之122項工作產品加以比對，評比分為四類成熟等級(Maturity Level)，包含符合(OK)、部分符合(Conditionally OK, COK)、尚未符合(Not OK, NOK)與無需符合(Tailored)等，以提供下階段文件準備之參考。

二、功能安全文件準備與融入流程

先準備功能安全系統、硬體與軟體層級之設計與測試文件，來進行功能安全管理、功能安全概念與技術安全概念等階段，由安全小組依專業分工完成各項工作產品，並與輔導顧問專家討論相關產出，以對應落差分析之主評建議，也以AEB試行計畫制定功能安全融入研發流程之可行方案。

首先，是功能安全管理階段，由安全經理完成安全計畫並定期更新，故此項工作產品會在資料紀錄表各個章節重複出現，以呈現安全計畫之最新進度或內容修訂。安全計畫包含項次、標準章節、內容、輸入文件、輸出文件、負責人、起/迄時間與備註等，這些項目同樣與ISO 26262標準要求之工作產品一致，如此逐項檢討安全計畫，就可完成功能安全要求，並納為計畫執行規劃書(Integrated Project Execution Plan, IPEP)之附件。計畫主持人也須在IPEP新增安全經理之專業分工，因需由非計畫成員擔任，故列在計畫成員之上以顯示其獨立性，又因為ISO 26262針對工作產品之

確認措施，皆不可由該工作產品之相關人員執行，所以需依Part2車電系統之ASIL執行分級作業。

再來是功能安全概念階段，應在項目定義說明文件目的、AEB之功能與目的、功能方塊圖、邊界條件與內/外部介面、安全與可靠度之潛在衝擊來源、其他需求（含環境條件）、法規與標準、外部措施與最小風險等，這些內容與IPEP之計畫目標與範圍，產品規格需求書(System Requirements Specifications, SRS)之產品介紹與用戶、客戶的期望、限制與介面、系統架構等重複，由系統工程師整理為英文資料，相關流程維持原訂之IPEP與SRS等工作產品。

危害分析與風險評估(HARA)是指車輛因電子電機系統故障所產生之風險，如非預期加速、非預期減速或燃燒/爆炸等，透過故障所生風險之嚴重度(S)、暴露機率(E)與可控度(C)三項參數，分析車輛安全完整性等級(ASIL)，得到QM、A、B、C、D等五種整車層級安全目標(Safety Goal)。

以AEB計畫所得HARA為例，因不同的操作情境、潛在危害、可能失效與外部減輕等，依據Part3決定ASIL，如某一項危害是非預期加速，其嚴重性為S3、發生機率為E4與可控性為C2，所以ASIL為C，所有ASIL取最高者，代表AEB的ASIL就是C。HARA需經第三方查證，SGS專家多次檢討各種AEB危害情境之S/E/C三項參數的想定，確認AEB之ASIL為C。

功能安全概念是依據HARA所得高層之安全目標（安全目標可能與數個危害相關，也可能數個安全目標與一個危害相關），規範系統之功能安全需求(FSR)，並推導功能安全參數（包含安全狀態、容許故障時間等），加以配置至相關元件的活動；另外，因應車電系統的成本考量，ISO 26262制定ASIL分解(decomposition)作法，將ASIL需求分配到數個元件中，使得單一需求可以降低，這只在專案架構中，被分解元件存在足夠獨立性條件下才能施行，可以透過相依性故障分析，確認其獨立性。

以AEB計畫所得FSR為例，如第1項安全目標(SG1)與FSR1、FSR2、FSR3、FSR15、FSR16相關，而單一FSR也與多個安全目標相關，所以功能安全需求(FSR1)與SG1、SG3、SG4與SG5相關，SG與FSR非屬直線關係，而是交互關聯（如表2所示）。技術安全概念階段是延續系統之功能安全需求展開為軟/硬體之功能安全需求規格，由系統工程師完成技術安全需求(TSR)，再交開發工程師制定軟/硬體技術安全需求之規格，進入設計與整合測試階段，系統工程師也訂定容許故障時間、分配元件與軟/硬體單元，以利後續開發工程師加以設計，再輔以測試工程師進行整合測試，確認AEB功能安全需求已經實現。

表2. 功能安全需求範例

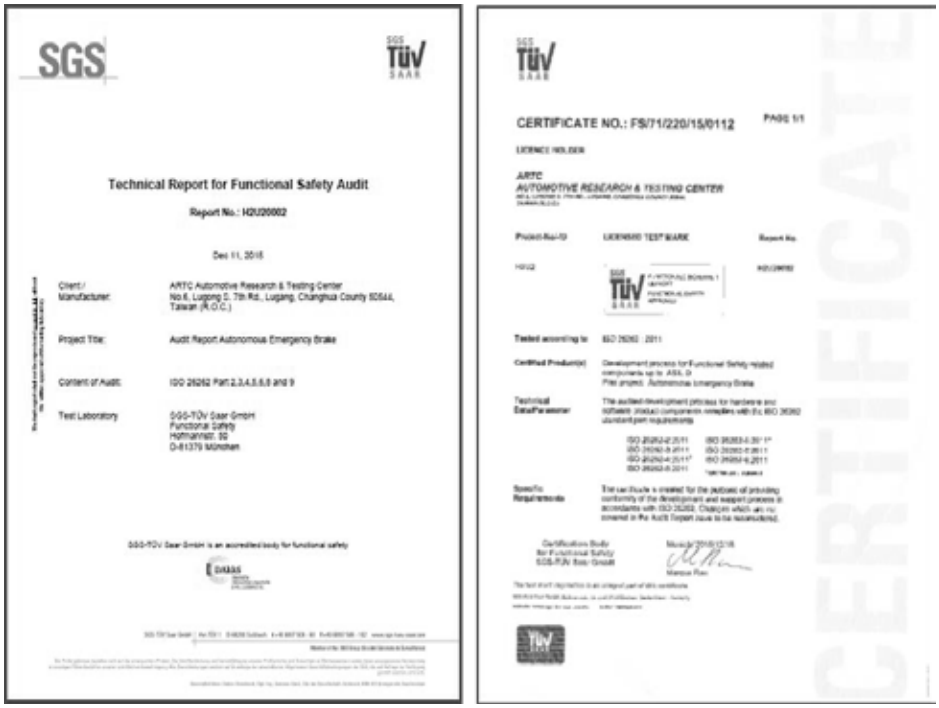
FSR ID	Functional Safety Requirement	From Safety Goal	Fault Tolerance Time	Allocated to element	ASIL
FSR 1	Invalid CAN message from EMS must be detected by AEB.	SG1,SG3,SG4,SG5	100ms	AEB ECU CAN Interface 1	C

三、功能安全流程認證

為確保車輛中心進行ISO 26262功能安全流程認證順利，採以事先會議進行預評，主要檢討安全經理所提報資料，包含詢問中心安全文化與建構管理機制，由於預評對安全小組執行狀況評價良好，僅有補充計畫訓練規劃與修正工具信賴度評價(Tool Confidence Level, TCL)檔案。

流程稽核(Process Audit)作業，係由安全經理以流程稽核簡報，逐項說明工作產品之執行狀況；最終，車輛中心取得ISO 26262功能安全流程認證，此證書係依稽核報告發行，兩項文件如圖2所示。該稽核報告需經德國認證單位(Deutsche Akkreditierungss- telle GmbH, DAkkS)授權才能發行，如同國內各檢測實驗室需獲全國認證基金會(TAF)認證，其所發行之檢測報告方能追溯至國際系統。

圖2. 稽核報告與流程認證證書



車輛中心獲頒認證，不僅展現在研發上之專業，更是對國內車電系統技術水準的肯定，因為各項研發系統雛型均具備初步功能安全設計與測試資料，再透過技術移轉予廠商，可縮短其產品認證時程，讓車電系統更接近世界需求，在開發的前端協助廠商完成了最後一里路之規劃，將可加速技術商品化進程，符合車廠對功能安全要求，進而快速加入供應鏈。