ISO 26262 車輛功能安全發展淺談

李志升

工研院機械所 智慧車輛技術組 電能系統部

前言：ISO 26262 車輛功能安全標準於 2011 年發佈至今已被公認為國際間最為尖端(state-of-the-art)，特別針對車輛系統制訂之功能安全規範，此標準適用於安裝於量產型 3500 公斤以下客車內之電機電子系統，範疇涵蓋整個產品生命週期，包含初期安全概念、系統開發階段，一直到後端生產，販售於市場運作，至除役退出市場。本文將簡介 ISO 26262 標準並針對其中三個核心元素：V 型系統發展流程、車輛安全完整性等級(automotive safety integrity level, ASIL)，以及安全需求進行說明，最後簡述取得 ISO26262 認可必需執行之確認措施相關事宜。

ISO 26262 車輛功能安全標準由十個部分(parts)構成，除了第一與第十部分外，第二至第九部分皆包含整個生命週期必須被滿足的需求與規範，依序為功能安全管理(management of functional safety)、概念階段(concept phase)、系統階層產品發展(product development at the system level)、硬體階層產品發展(product development at the hardware level)、軟體階層產品發展(product development at the software level)、生產與操作(production and operation)、支援程序(supporting processes)，以及 ASIL 與安全相關分析(ASIL-oriented and safety-oriented analyses)。第一部分(vocabulary)為詞彙定義，第十部分(guideline on ISO 26262)則為輔助性指南，以範例說明標準內重要概念與解讀方法，讓使用者對各項需求能夠有更精確的理解與認知。

ISO 26262 標準的發佈對全球車輛產業有著的相當顯著的影響，不只是負責設計、整合與生產車輛的車廠，系統、零組件供應商，以及各種工具發展商皆於產品的生命週期間被賦於確保車輛功能安全責任，由其是現在車載系統愈趨複雜，車輛功能安全議題更是不容忽視的重要一環。原則上此標準以人員人身安全為核心訴求，包含駕駛者、車上乘客、其他用路人、路上行人乃至於保養維修人員，並聚焦於原自於車輛電力電子系統之故障與功能失效，標準內以工作產出物(work product)的形式管理與檢驗各項需求條文的符合性，工作產出物可視為相關細部需求條文的執行結果證明，第二部分至第九部分總共包含約 800 項詳細需求條文，對應約 130 項工作產出物，為了達成 ISO 26262 的符合性，需把相關適用的工作產出物完成，並通過標準內規範的確認措施(confirmation measure)的審核。由此可見想要達成 ISO 26262 完全的符合性(full compliance)不是一件容易的事。

雖然 ISO 26262 的內容涵蓋範圍廣闊，細節展開繁雜冗瑣，我們還是可從以下三個標準內重要的元素一窺其核心理念與精神：V 型系統發展流程、車輛安全完整性等級(ASIL)，以及安全需求。首先，產品發展流程必需嚴格遵循系統工程 V 型發展流程，並導入國際間認可的品質管理，此為 ISO 26262 最基本的要求。依據 V 型發展流程，產品發展必須以由上往下(top-down)的方式先從整車端建立系統需求，並逐步展開系統、硬

體、軟體設計，然後再由下往上(bottom-up)依序進行整合與測試驗證，整個過程亦需留下相關紀錄與佐證資料。

另一方面，ASIL 堪稱 ISO 26262 最重要的指標之一，標準定義有四個等級：A、B、C 和 D，分別代表車輛發生故障後導致人身危害的風險程度，D 為最高，ASIL 的分析定義必須依據第三部分的規範進行，主要是針對潛在之危害事件(hazardous event)進行嚴重度(severity)、暴露機率(probability of exposure)，及控制度(controllability)定義，之後自該危害事件所展開之安全需求則會繼承相關 ASIL，其效應在於產品安全生命週期各階段的需求會因等級而異，原則上，等級越高表示潛在性的風險越高，ISO 26262 則會要各階段求採取更多、更嚴謹的措施以確保風險降至可承受水平，換句話說，ASIL 基本上就是安全風險降低措施幅度的度量：風險越高，需做的努力越大。

最後 ISO 26262 要求執行嚴謹的需求工程(requirement engineering)，其中安全相關之需求必須透過標準內規範的方式推導展開，其中必須以階層性結構(hierarchical structure)由上往下展開逐步推導：安全目標(safety goal)、功能安全需求(functional safety requirement)、技術安全需求(technical safety requirement)、硬體安全需求(hardware safety requirement)，以及軟體安全需求(software safety requirement)，且所有安全需求必須具備雙向追溯性且被驗證。安全目標為所有安全需求的源頭，其目的為制定產品避免危害事件的發生所需滿足的系統發展需求，因此會繼承相關危害事件中最高的 ASIL，之後為了確保系統可實現安全目標會逐步往下展開各階層之安全需求，且所有安全需求將會繼承此 ASIL，若一個安全需求同時對應多個上一階的安全需求，則取最高 ASIL 為原則。ISO 26262 規定每一條安全需求皆需被分配(allocation of safety requirements)至特定系統、硬體或軟體元素，以確保所有安全需求被系統設計滿足，同時於測試階段必需進行安全需求的驗證。

前面有提到想要通過 ISO 26262 認證必需透過執行標準第二部分所規範的確認措施(confirmation measure)相關活動，主要由三個環節組成—確認審查(confirmation review)、功能安全稽查(functional safety audit)，以及功能安全考核(functional safety assessment)。確認審查的目的在於檢查一些特定、較重要的工作產出物內容是否確實地符合相關 ISO 26262 的規範要求，功能安全稽查著重於評估產品發展流程是否確實符合 ISO 26262 的要求，由其是功能安全相關活動的規劃、執行與管理，最後功能安全考核則綜觀地審查與評量產品是否確實地確保功能安全已被達成，其中包含所有工作產出物的審核、功能安全稽查的符合性，以及實施於產品中的安全措施(safety measure)的有效性，主要透過安全分析與安全機制(safety mechanism)的測試結果做為評估與判斷依據。ISO 26262 對執行確認措施的人員獨立性亦有規定並定義四個獨立性要求等級，包含 I0、I1、I2 以及 I3，各別簡述如下：

- I0：確認措施不強制執行，若執行則執行者需與工作產出物負責人非同一人
- I1：確認措施強制執行，執行者需與工作產出物負責人非同一人
- I2：確認措施強制執行，執行者需與工作產出物負責人隸屬於不同直屬主管
- I3：確認措施強制執行，執行者需與工作產出物負責人隸屬於獨立管理單位

每一項確認措施的獨立性要求會取決於相關的 ASIL 定義，原則上 ASIL 越高，獨立性的要求也就越高。

自 2011 年第一版發佈以來 ISO 26262 已經逐漸被全球車輛產業重視，實際上市場上已漸漸可發現標榜著符合 ISO 26262 的產品出現，國際間各大車廠也積極地導入並要求供應商提供符合 ISO 26262 的產品，台灣車輛產業勢必無法置身事外，積極布局導入提升產品安全性方能保持競爭力。 ■