ISO 26262 系統功能安全設計標準之研究

The Study of ISO 26262 System Functional Safety Design Standards

陳柏睿 副工程師
財團法人車輛研究測試中心 研發處 底盤與系統驗證工程專案

主要聯絡人：陳柏睿
電話：04-7811222#2426
E-mail:Bo-Ruei@artc.org.tw
地址：彰化縣鹿港鎮鹿工南七路 6 號

摘要

車輛產業是一個不允許失效發生的產業，為了防止系統失效的發生，必須有一套嚴謹且可靠的開發流程來讓開發工程師依循。ISO 26262 標準提供一套功能安全設計流程來讓開發工程師依循，且對於分析結果有一嚴謹的確認制度，因此未來 ISO 26262 將成為車輛產業系統功能安全設計分析手法的主流。本文針對 ISO 26262 標準進行研究及解析，內容主要包含(1)ISO 26262 簡介(2)ISO 26262 執行流程(3)ISO 26262 議題探討。

ABSTRACT

The occurrence of system failure is not allowed in vehicle industry. In order to prevent it, developers must have rigorous and reliable development processes. ISO 26262 standards provide a set of functional safety design processes to help developers to follow, and a strict accreditation criteria to ensure that analysis results are consistent with requirements. Consequently, ISO 26262 will become the main analysis techniques of a system function safety design for vehicle industry in the future. This paper elaborates on ISO 26262 standards, which includes (1) ISO 26262 introduction, (2) ISO 26262 implementation processes, and (3) ISO 26262 issues.

關鍵字：ISO 26262、功能安全、安全程度等級
Keywords: ISO 26262, Functional Safety, Automotive Safety Integrity Levels (ASILs)

一、前言

車輛產業是一個不允許系統失效發生的產業，因為一發生失效車輛廠商將面臨官司賠償與商譽受損的巨大風險，為了防止系統失效的發生，必須有一套嚴謹且可靠的開發流程來讓系統開發工程師依循，以往車輛產業大部分是採用失效模式效應分析(Failure Mode and Effects Analysis, FMEA)手法來進行失效分析與預防，FMEA 手法對於硬體失效有一定程度的預防效果，但對於軟體失效的預防效果就較為有限，除 FMEA 手法外，近期亦漸漸有車輛廠商將 ISO 26262 功能安全設計標準應用於失效分析與預防上，ISO 26262 標準可補足 FMEA 手法於軟體分析的不足，在軟硬體功能安全設計方面皆提供一套流程來讓開發工程師依循，且對於功能安全分析結果有一嚴謹的確認制度，因此未來 ISO 26262 將成為車輛產業系統功能安全設計分析手法的主流。本文針對 ISO 26262 標準進行研究及解析，內容主要包含(1)ISO 26262 簡介

(2)ISO 26262 執行流程(3)ISO 26262 議題探討。

二、ISO 26262 簡介

1、ISO 26262 發展歷程：

ISO 26262 大約於 2005 年開始發展，該標準主要係調和 IEC 61508 而來，並著重於車輛電子/電機系統的功能安全，ISO 26262 的適用範圍為 3.5 噸以下客車(passenger cars)上所搭載之電子/電機系統，目前 ISO 26262 處於草案階段，但成熟度已達 90%以上，預計 2011 年 10 月發佈正式版本，於 2015 年將可能成為歐洲法規(European regulation)，未來 ISO 26262 對於車輛產業的影響程度將不亞於 ISO/TS 16949。

為避免 ISO 26262 實施對車輛產業所造成的衝擊，目前全球之 OEM 廠、一階零組件廠、車用晶片商、開發工具商皆已開始著手於其產品開發過程中導入 ISO 26262，或使其販售之軟硬體開發工具符合 ISO 26262 之要求。

2、ISO 26262 組成架構：

ISO 26262 標準包含 10 個章節(Part)，分別為

(1) 名詞解釋(Vocabulary)
(2) 功能安全管理(Management of functional safety)
(3) 概念階段(Concept phase)
(4) 產品開發：系統層級(Product development: system level)
(5) 產品開發：硬體次系統層級(Product development: hardware level)
(6) 產品開發：軟體次系統層級(Product development: software level)
(7) 生產與操作使用(Production and operation)
(8) 支援流程(Supporting processes)
(9) ASIL 等級界定與安全達成度分析(ASIL-oriented and safety-oriented analyses)
(10) ISO 26262 指南(Guideline)

ISO 26262 涵蓋了整個安全生命週期，從管理、開發、生產、經營、服務維修至報廢回收皆有規定應執行的方法與步驟。ISO 26262 採用安全程度等級 ASILs(automotive safety integrity levels)來評斷系統需符合之功能安全程度，ASIL 等級程度由 ASIL A(最低)~ASIL D(最高)，ASIL 等級越高之系統功能安全考量需越嚴謹。

3、ISO 26262 執行效益：

ISO 26262 可使公司內部清楚定義專案展開流程與功能安全相關系統、硬體、軟體開發應共同遵循的目標，此有利於爭取加入大型跨國車輛系統開發專案，對外可清楚定義出系統所需達成之安全門檻，且因有依國際共同標準來進行系統保安設計，所以未來若發生系統失效造成消費者傷害時，所有開發過程文件皆可成為善盡產品責任之法律證明文件。

三、ISO 26262 安全生命週期

ISO 26262 之安全生命週期主要由 12 個階段所組成，其模型如圖 1 所示。

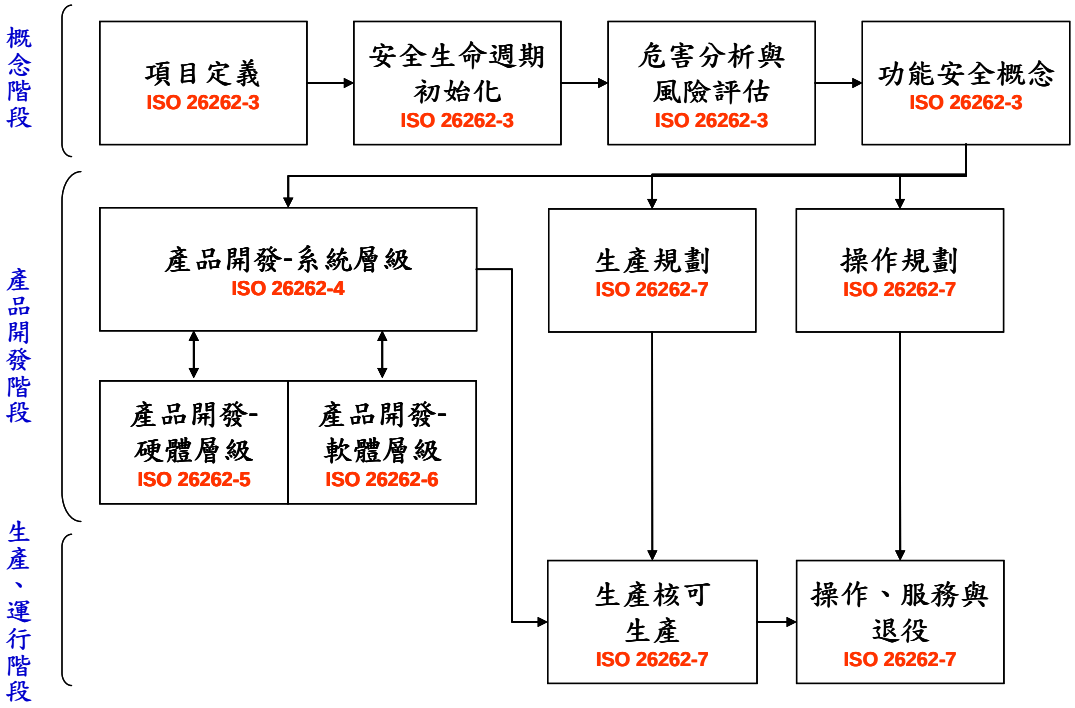


圖 1 ISO 26262 之安全生命週期模型

安全生命週期之 12 個階段分別為：

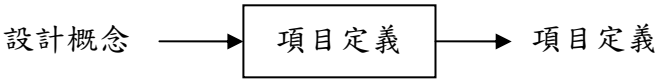
(1) 項目定義(Item definition)：定義相關功能、定義開發如何進行、是否使用或修改現有模組。
(2) 安全生命週期初始化(Initiation of the safety lifecycle)：評估每個小階段的實行必要性。
(3) 危害分析與風險評估(Hazard analysis & risk assessment)：依系統化方法進行危害與風險的界定及評估。
(4) 功能安全概念(Functional safety concept)：依安全目標發展功能安全需求並配置到系統架構上。
(5) 產品開發-系統層級(Product development - system level)：系統層級功能安全需求發展與執行。
(6) 產品開發-硬體層級(Product development - hardware level)：硬體層級功能安全需求發展與執行。
(7) 產品開發-軟體層級(Product development - software level)：軟體層級功能安全需求發展與執行。
(8) 生產規劃(Production planning)：產品生產規劃。
(9) 操作規劃(Operation planning)：產品操作規劃。
(10) 生產核可(Release for production)：生產前確認相關功能安全需求皆被設計與實行。
(11) 生產(Production)：關於組裝與製造之需求發展與執行。
(12) 操作、服務與退役(Operation, service, and decommissioning)：關於產品監控、控制與回饋之需求發展與執行。

四、ISO 26262 執行流程

ISO 26262 安全生命週期之 12 個階段下又可細分為 26 個小階段，其中 Phase 1~4 屬於安全生命週期之概念階段，Phase 5~7 與 Phase 21~24 屬於安全生命週期之產品開發階段-系統層級，Phase 8~13 屬於安全生命週期之產品開發階段-硬體層級，Phase 14~20 屬於安全生命週期

之產品開發階段-軟體層級，Phase 25~26 屬於安全生命週期之生產、運行階段，以下將針對 26 個小階段的執行重點與輸入、輸出項目來進行說明，下列說明中各小階段之輸入與輸出項目名稱若相同者，則輸出項目代表輸入項目之更新版本。

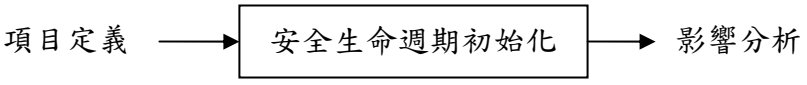
Phase 1：項目定義(Item definition)



本階段的重要任務為確認「項目(系統、系統陣列)」的相關功能，收集所有相關的資訊與設計準則，輸出與「項目」相呼應的資料與文件，資料的完整性是成功進行分析的基礎，有完整的資料將有更完整的安全工程被執行。相關資料與設計準則應包含如下：

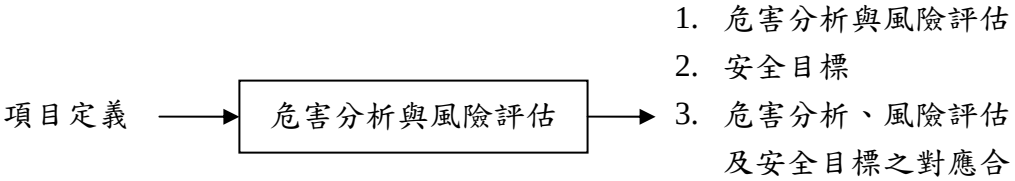
(1) 相關之法規(如：ECE…)
(2) 相關之地區/國家標準(如：SAE, IEC, ISO…)
(3) 功能/非功能需求
(4) 環境需求(使用地區、使用限制…)
(5) 已知的安全需求
(6) 與其他「項目」的關連性

Phase 2：安全生命週期初始化(Initiation of the safety lifecycle)



本階段的重要任務為評估每個小階段的實行必要性，之後進行影響分析，若是全新的產品開發必須遵循完整的安全生命週期，若是產品修改或再升級則部分小階段可不必執行。

Phase 3：危害分析與風險評估(Hazard analysis and risk assessment)



本階段的重要任務為針對「項目」進行傷害度、發生度、可控度之定義，再依傷害度、發生度、可控度來定義安全程度等級，之後依安全程度等級來發展安全目標，最後利用審查來檢視對應之合適性。傷害度、發生度、可控度與安全程度等級之定義表，如表 1~4 所示，其中安全程度等級定義表中之 A~D 分別代表 ASIL A~ASIL D，QM 代表 ASIL QM，ASIL QM 等級不需要提出安全目標，但必須審視定義為 ASIL QM 的合理性。

表 1 傷害度定義表[1]

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

表 2 發生度定義表[1]

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

表 3 可控度定義表[1]

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

表 4 安全程度等級定義表[1]

		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	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

註：QM→代表安全程度等級為 ASIL QM
A~D→代表安全程度等級為 ASIL A~D

Phase 4：功能安全概念(Functional safety concept)

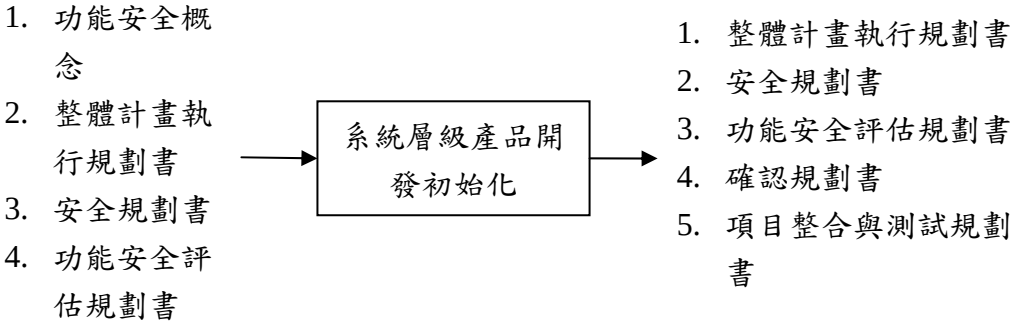
1. 項目定義
2. 危害分析與風險評估
3. 安全目標

→ 功能安全概念 →

1. 功能安全概念
2. 功能安全概念之合適性審查

本階段的重要任務為依循 ISO 26262 之規定，利用系統工程設計方法來發展功能安全概念，此功能安全概念必須符合安全目標，之後將功能安全概念配置到項目(系統、系統陣列)內的不同元素(軟體模組、硬體模組、軟體單元、硬體元件)，最後審查功能安全概念之完整性、合理性與吻合性。

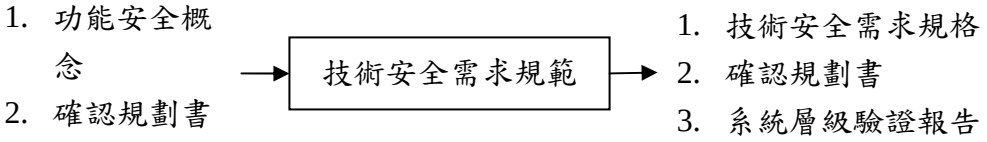
Phase 5：系統層級產品開發初始化(Initiation of product development at the system level)



在實行系統設計前相關活動需被明確規劃，為了滿足符合所需之安全生命週期，現有之規劃與執行流程需不斷的修改與維護，因為如果沒有相對應的規劃書將無法實現與證明達成功能安全概念，相關規劃書之負責人與主要內容描述如下：

(1) **整體計畫執行規劃書**：主要撰寫人為專案經理，主要內容為整體計畫執行的規劃及計畫執行規劃與安全規劃間的連結，並規劃合理的預算、能力、資源、時程與合格性檢查，來確保安全規劃可以被執行。
(2) **安全規劃書**：主要撰寫人為安全經理，主要內容為規劃與定義相關之安全活動，並確保安全活動能按時完成並產出正確的工作產品，規劃內容必須有(A)何時來執行安全活動(B)使用什麼關鍵方法來執行(C)多少時間內需完成安全活動。
(3) **功能安全評估規劃書**：主要撰寫人為安全經理或具足夠工程判斷能力之工程師，此規劃書需包含內部確認規劃，並標明哪個階段應插入內部確認，內部確認應邀請誰來執行。
(4) **確認規劃書**：主要撰寫人為驗證經理/驗證工程師，規劃書內需標示確認執行理由、誰執行確認、何時執行確認、何地執行確認、如何執行確認，與確認之準則、方法、環境、資源，及產出文件。
(5) **項目整合與測試規劃書**：主要撰寫人為驗證經理/驗證工程師，主要內容為何時執行整合測試與如何執行整合測試。

Phase 6：技術安全需求規範(Specification of the technical safety requirements)

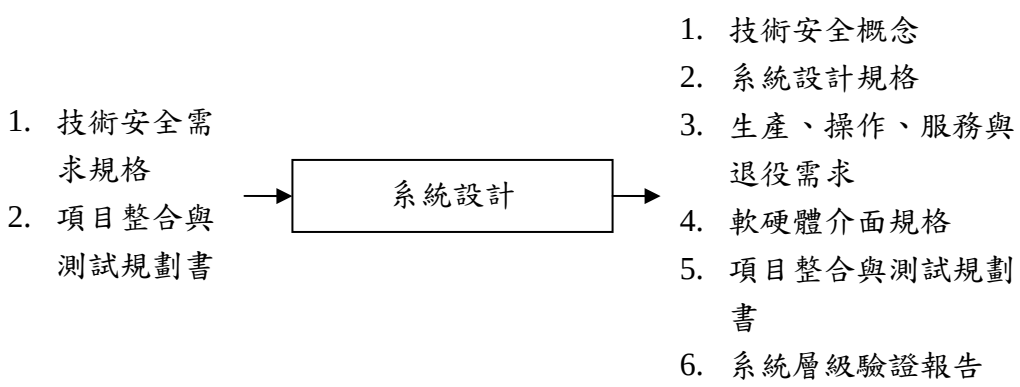


本階段的重要任務為依據「安全目標」與「功能安全需求」來發展更詳細的技術安全需求，技術安全需求要素包含：

(1) 系統屬性：包含外部介面(如：CAN…)、環境條件(如：車輛級距(大型房車、中型房車…)、溫度...)、功能上的限制(如：作動敏感度...)、系統建構要求(如：調校機電介面…)。
(2) 功能/非功能需求：功能/非功能需求之實現需靠哪些項目與元素來達成。
(3) 系統響應：執行技術安全需求的系統響應。
(4) 依賴性設計：鑑別與安全相關的依賴性與複雜度。
(5) 設計安全機制：透過什麼方法來執行安全機制，方法包含(A)偵測、識別與控制故障(B)驅動系統進入安全狀態(C)警告與進入能力降級模式。
(6) 設計安全狀態：每一個安全狀態處理一個或多個故障，一進入安全狀態，故障應立即被處理或轉移。
(7) 針對不同故障類型設計安全機制：安全機制應可處理單點、雙點與多點故障，亦必須具備

處理潛在故障(latent faults)的能力。

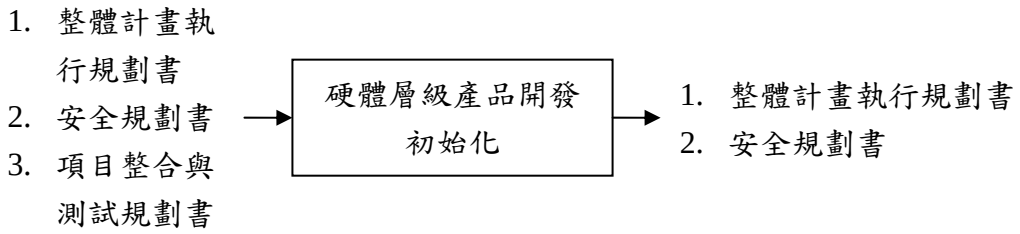
Phase 7：系統設計(System design)



本階段的重要任務為系統設計，系統設計執行流程與應考慮事項如下：

(1) 合理之初步架構假設。
(2) 修改或加入新元素來符合技術安全需求。
(3) 系統架構如何實施以符合技術安全需求。
(4) 在滿足技術安全需求下定義系統架構與內部元素配置。
(5) 分類為安全相關與非安全相關之元素。
(6) 設計系統介面。
(7) 執行安全分析(如：Design Failure Mode and Effects Analysis, DFMEA、Fault Tree Analysis, FTA…等)找出潛在失效原因，並給予因應設計。
(8) 確保系統設計符合(A)分層設計(B)無複雜設計(C)可維護性(D)可測性之設計目標。
(9) 設計控制硬體隨機故障的方法。
(10) 分配技術安全需求到硬體、軟體或軟體與硬體。
(11) 定義軟硬體之介面規格。
(12) 定義生產、操作、服務與退役的初始需求。
(13) 驗證系統設計的正確性。

Phase 8：硬體層級產品開發初始化(Initiation of product development at the hardware level)



本階段主要是由二階供應商(Tier 2)來執行，供應商負責涵蓋 Phase 9~13 之硬體層級安全規劃，所產出之安全規劃需整合至上一階之「整體計畫執行規劃書」與「安全規劃書」，並讓一階供應商(Tier 1)或車廠審查。

Phase 9：硬體安全需求規範(Specification of hardware safety requirements)

1. 整體計畫執行規劃書
2. 安全規劃書
3. 技術安全概念
4. 系統設計規格
5. 軟硬體介面規格

→ 硬體安全需求規範 →

1. 硬體安全需求規格
2. 硬體配置度量(metrics)需求
3. 硬體隨機失效需求
4. 軟硬體介面規格
5. 硬體安全需求驗證報

本階段的重要任務為設計硬體安全需求使之符合先前定義的技術安全需求，且所有硬體安全需求需被設定到元素中，設計硬體安全需求應考慮：

(1) 考慮先前設計的安全機制來進行硬體設計。
(2) 硬體應設計具對應外部錯誤(external error)的能力。
(3) 考慮將硬體安全需求對應到不同硬體元素，以防止失效的影響。
(4) 設計硬體元件特性需考慮安全功能。
(5) 依 ASIL 等級來設定失效率的設計目標值與失效可被偵測查知之機率。
(6) 硬體元件選用需遵循 ISO 26262 Part8 Clause 13 之規定。
(7) 界定故障並提出因應設計。
(8) 驗證硬體安全需求之正確性。
(9) 定義硬體實現和驗證的細節。

Phase 10：硬體設計(Hardware design)

1. 硬體安全需求規格
2. 軟硬體介面規格
3. 系統設計規格
4. 整體計畫執行規劃書
5. 安全規劃書

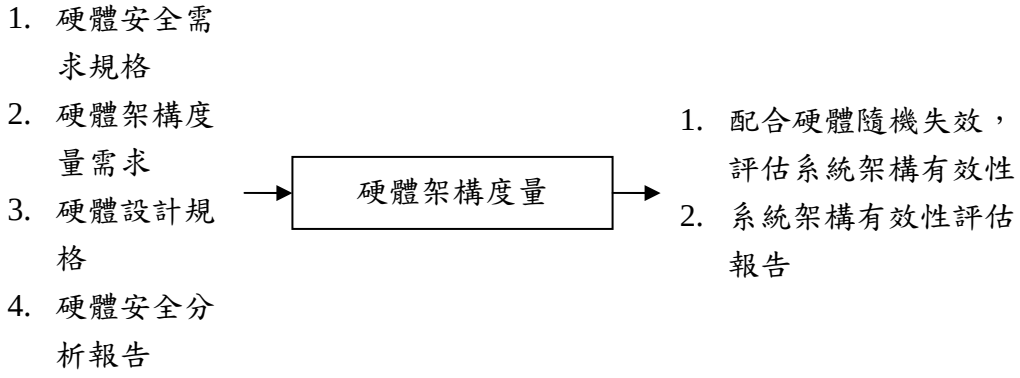
→ 硬體設計 →

1. 硬體設計規格
2. 硬體安全分析報告
3. 硬體設計驗證報告
4. 生產與操作需求

本階段的重要任務為依照「系統設計規格」與「硬體安全需求」來進行硬體設計，硬體的安全程度等級(ASIL)需與所對應系統的安全程度等級(ASIL)相呼應，除硬體設計外本階段還有下列事項需注意：

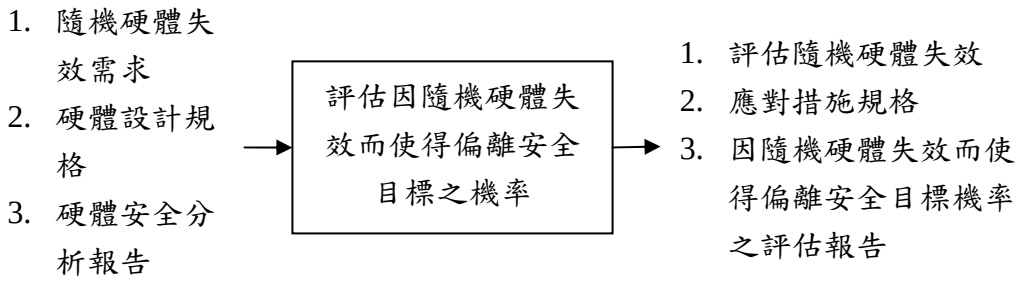
(1) 需維持「硬體設計」與「硬體安全需求」間的追溯性。
(2) 需考慮來自非功能性(Non-functional)行為的失效。
(3) 導入車廠經驗、國際標準…(如：design rule database)來進行硬體設計。
(4) 需確保硬體零件規格符合使用環境要求。
(5) 進行硬體架構安全分析，並產出硬體安全分析報告，報告需包含(A)錯誤分類與描述(B)改善措施證明(C)計算自我診斷涵蓋率(D)DFMEA(E)FTA。

Phase 11：硬體架構度量(Hardware architecture metrics)



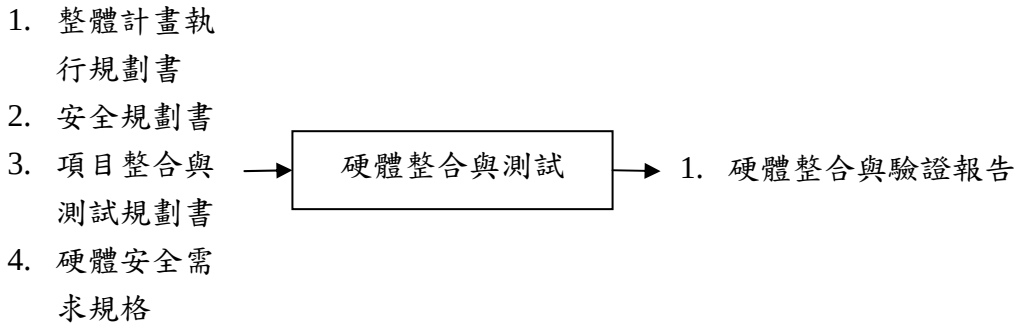
本階段的重要任務為評估硬體架構承接失效錯誤的能力，採用的方法為定量分析方法，定量分析內容包含(1)計算自我診斷率(%)(2)計算單點錯誤控制率(%)(3)計算潛在錯誤控制率(%)(4)計算失效率(FIT, 每 10^9 小時發生一個錯誤則 FIT 等於 1)(5)決定單點與潛在故障指標。

Phase 12：評估因隨機硬體失效而使得偏離安全目標之機率(Evaluation of violation of the safety goal due to random HW failures)



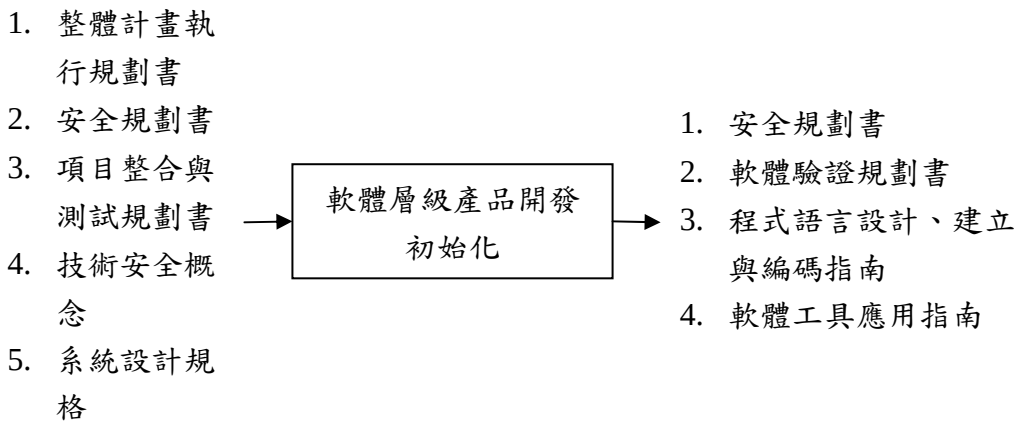
本階段的重要任務為(1)設定基準來評估隨機硬體失效的風險(2)證明應對措施設計已有效降低隨機硬體失效的風險，一般常使用之應對措施設計為(1)採取較大之安全係數(2)執行破壞測試來確認設計符合需求。

Phase 13：硬體整合與測試(Hardware integration and testing)



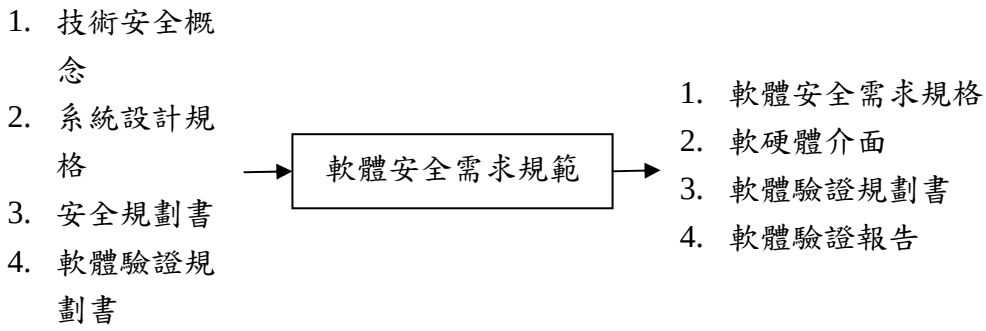
本階段的重要任務為(1)執行硬體整合與測試(2)確認硬體產品性能表現與硬體安全需求一致，測試規範需包含(1)測試案例如何設計(2)測試儀器之校正需求(3)確立必須執行之測試項目。

Phase 14：軟體層級產品開發初始化(Initiation of product development at the software level)



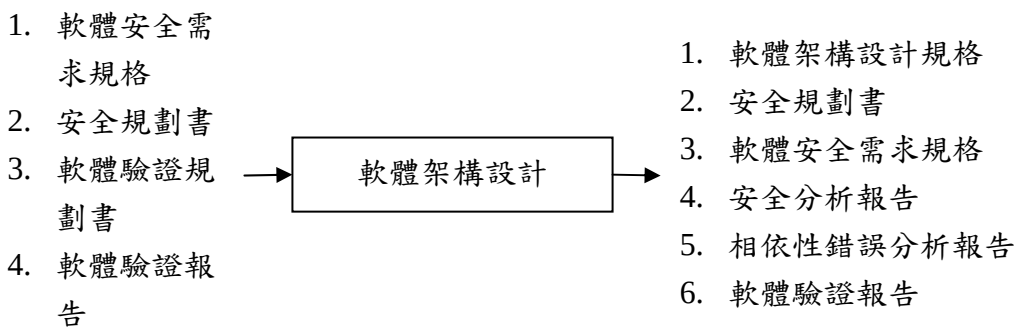
本階段的重要任務為進行涵蓋 Phase 15~20 之軟體層級安全規劃，並更新修改先前的相關規劃書。軟體層級安全規劃應包含(1)活動時程(2)活動執行方法(3)軟體開發應遵循的規則，規劃時應考慮(1)應該執行什麼活動(2)活動使用什麼方法來執行，如：審查…(3)用什麼策略來完成軟體開發(4)軟體開發過程之工具語言需一致。另軟體開發過程所使用之工具需符合 ISO 26262 之規定，且需符合本階段所定義之軟體工具應用指南。

Phase 15：軟體安全需求規範(Specification of software safety requirements)



本階段的重要任務為依據「技術安全概念」與「系統設計規格」來設計軟體安全需求規格，並將相關設計資料文件化。一般而言軟體的問題是很難處理的，所以必須針對每個安全相關的軟體單元來進行危害分析，並利用軟體安全需求規格之設計來產生預防失效故障發生的安全機制。

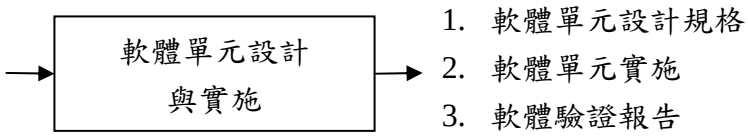
Phase 16：軟體架構設計(Software architectural design)



本階段的重要任務為依據「軟體安全需求規格」來發展軟體架構設計規格，此架構規格必須符合 ISO 26262 規範。安全分析報告內容必須有，軟體元件安全相關特性之查明與確認，及安全機制之支援規格。相依性錯誤分析報告主要是用來確保軟體安全需求已被成功的實行，有時軟體安全需求是否成功執行取決於軟體元件間有無互相干擾，所以軟體元件間的獨立性需先被分析與確認。

Phase 17：軟體單元設計與實施(Software unit design and implementation)

1. 安全規劃書
2. 軟體驗證規劃書
3. 軟體架構設計規格
4. 軟體安全需求規格
5. 軟體驗證報告

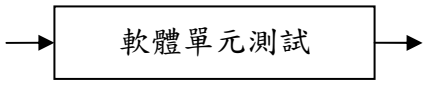


1. 軟體單元設計規格
2. 軟體單元實施
3. 軟體驗證報告

本階段的重要任務為依據完成確認之「軟體安全需求規格」與「軟體架構設計規格」來進行軟體單元設計與實施。軟體單元需依 ASIL 等級來選擇適當的撰寫語言(如：natural language, informal, semi-formal, formal…)，設計軟體單元時需考慮(1)功能行為(2)暫存器(register)的使用拘束條件(3)儲存空間(data storage)的使用拘束條件，並避免非必要的元素與維持可測性及可維護性。

Phase 18：軟體單元測試(Software unit testing)

1. 安全規劃書
2. 軟體驗證規劃書
3. 軟體單元設計規格
4. 軟體單元實施
5. 軟體驗證報告

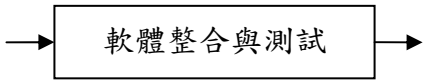


1. 軟體驗證規劃書
2. 軟體驗證規格
3. 軟體驗證報告

本階段的重要任務為確認(1)軟體程式碼與軟體單元設計規格是否吻合一致(2)軟體程式碼與對應功能間是否有非預期之功能存在。

Phase 19：軟體整合與測試(Software integration and testing)

1. 安全規劃書
2. 軟體驗證規劃書
3. 軟體架構設計規格
4. 軟體單元實施
5. 軟體驗證規格
6. 軟體驗證報告

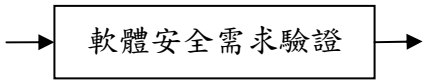


1. 軟體驗證規劃書
2. 軟體驗證規格
3. 軟體驗證報告
4. 嵌入式軟體

本階段的重要任務為(1)將完成確認之軟體單元整合為軟體元件，再將各軟體元件整合為嵌入式軟體(2)驗證嵌入式軟體是否與軟體架構設計規格吻合一致。在進行軟體整合時需先定義整合之順序與次序並考慮每個軟體單元/軟體元件間的依存關係，且需有文件證明軟體整合是有依據的而非隨意進行整合。在進行驗證時需注意(1)測試與分析已涵蓋所有軟體(2)分析結果必須文件化並保存(3)需進行目標環境與測試環境間的差異分析。

Phase 20：軟體安全需求驗證(Verification of software safety requirements)

1. 安全規劃書
2. 軟體驗證規劃書
3. 軟體安全需求規格
4. 軟體架構設計規格
5. 軟體驗證規格
6. 軟體驗證報告
7. 整合測試報告

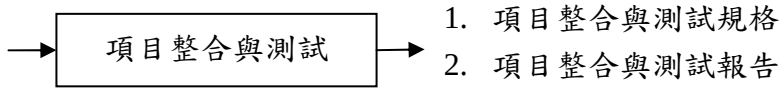


1. 軟體驗證規劃書
2. 軟體驗證規格
3. 軟體驗證報告

本階段的重要任務為驗證軟體是否與軟體安全需求吻合一致，驗證執行的測試環境(如：實車、平台、Hardware-in-the-loop…)需依照 ASIL 等級來進行選取且需與軟體驗證規劃書內之要求一致，並至少需於一個以上的不同環境內執行測試。另需對驗證結果進行評估，項目包含(1)是否依明確準則判定驗證結果為通過/失敗(2)檢查預期結果與實際結果的一致性(3)檢查測試是否涵蓋所有軟體安全需求。

Phase 21：項目整合與測試(Item integration and testing)

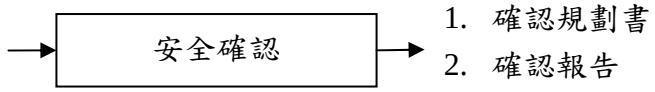
1. 系統設計規格
2. 安全目標
3. 功能安全概念
4. 技術安全概念
5. 軟硬體介面規格
6. 項目整合與測試規劃書



在完成 Phase 8~13 之硬體開發與 Phase 14~20 之軟體開發後，於本階段又回到系統層級產品開發階段，本階段的重要任務為(1)依相對應的整合策略將「項目」內的所有元素加以整合(2)驗證整合完成後之「項目」以確認它實現了所有相對應的安全需求。在「項目整合與測試規格」中需包含(1)整合的順序與次序以及整合測試方法，在整合測試過程中所有的功能安全需求與技術安全需求應至少被測試一次(2)測試項目應包含：安全機制執行性能、內部介面一致性、外部介面一致性、故障檢測有效性、故障診斷涵蓋率、系統強健程度(3)需有系統/實車整合測試。

Phase 22：安全確認(Safety validation)

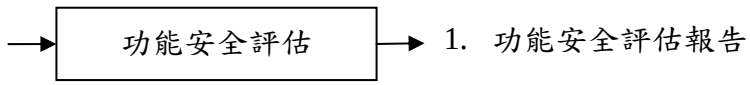
1. 確認規劃書
2. 安全目標
3. 功能安全概念
4. 危害分析與風險評估



本階段的重要任務為(1)確認「項目」與「安全目標」及「功能安全概念」吻合一致(2)「項目」搭載於實車上能全面實現「安全目標」。確認規劃書之撰寫需考慮(1)實車上需執行之測試項目(2)清楚定義測試程序、測試案例、駕駛條件、接受準則(3)測試所需之資源、工具與環境。確認報告內容需包含(1)相關測試結果，包含測試案例、測試方法與判定準則(2)FMEA/FTA/ETA/Simulation 分析結果(3)長期(long term)測試(4)實際使用情況測試，包含一般使用者與專家使用者(5)測試結果審查(review)。

Phase 23：功能安全評估(Functional safety assessment)

1. 安全案例
2. 安全規劃書
3. 功能安全評估規劃書



本階段之主要工作為針對「項目」進行最後階段的功能安全評估，一般而言 Phase 23 與 Phase24 應一起被執行。

Phase 24：生產核可(Release for production)

1. 功能安全評估報告
2. 安全案例

→ 生產核可 →

1. 生產核可報告

一般而言 Phase 23 與 Phase24 應一起被執行，此兩階段之主要工作為審視安全案例之相關證據(如：相關工作產品、分析報告、測試報告、驗證報告…)是否已可足夠證明符合安全需求與安全目標，若符合且已盡到該盡之產品責任就可以進行發佈生產。ISO 26262 標準主要是利用下列項目來確認是否善盡產品責任：(1)安全案例已被配置且可用(2)安全案例之相關工作產品與證據已被評估且接受(3)功能安全評估報告具有效性(4)功能安全評估報告的建議結論是什麼(5)功能安全評估報告的核准者是誰(6)是否依照功能安全評估報告的建議結論來進行生產。

Phase 25：生產(Production)

1. 生產、操作、服務與退役需求
2. 硬體元件失效應對措施規格
3. 生產核可報告

→ 生產 →

1. 生產規劃書
2. 生產控制規劃書
3. 量測控制執行文件
4. 可生產性需求
5. 生產流程能力評估報告

本階段之主要工作為生產規劃、試量產、生產。如果系統規格與技術安全需求已夠成熟，在釋出給軟、硬體供應商生產前即應開始進行生產規劃，生產規劃書內容需包含(1)從安全相關規格特性所發展之生產需求(2)元素儲存議題(3)依以往經驗來訂定所需之生產能量(4)適合的生產方法、流程、工具…(5)生產能力(6)依安全相關規格特性所發展之生產控制規劃，除生產規劃書外亦應發展適當的生產議題收集表，以收集生產過程中之相關問題。在試量產時期所設定的生產流程需與未來之實際生產流程一致，試量產亦應遵循相關規定，系統整合測試或實車整合測試需使用試量產所生產之樣品來執行。在生產時期需監控下列事項(1)確認實際生產流程是否與規劃流程一致(2)設計機制來分析生產失效(3)依分析結果來提出新的預防措施(4)生產流程與人員能力稽核(5)監控測試設備(6)確保生產項目配置正確之控制措施(7)上述措施的相關文件(如：控制結果、數據、項目編號…)。

Phase 26：操作、服務與退役(Operation, service, and decommissioning)

1. 生產、操作、服務與退役需求
2. 生產核可報告
3. 警告與能力降級模式概念

→ 操作、服務與退役 →

1. 維護規劃書
2. 維修說明書
3. 使用手冊
4. 現場調查說明
5. 退役說明
6. 操作、維護與退役需求

本階段之主要工作為操作、服務與退役之執行規劃並產出維護計畫書，另現場執行流程監控亦必須被設計與執行。維護計畫書內容主要為(1)操作、服務與退役之流程與操作需求(2)

警告與降級模式概念(3)現場調查資料之收集與監控方式(4)維護的次序、方法、時間、活動、重要工具與措施(5)維護工具與措施之應用指南…等。

五、ISO 26262 議題探討

以下將針對 ISO 26262 之相關議題來進行探討說明。

(1) ISO 26262 是針對產品來進行認證而非針對公司流程來進行認證，但進行認證之先決條件為公司具備流程管控的能力，因此公司需具備 ISO 9001 或 ISO/TS 16949 方能進行 ISO 26262 認證。

(2) ISO 26262 的執行關鍵人員為專案經理(Project manager)與安全經理(Safety manager)。專案經理之職責為(A)專案展開(B)確保安全活動被確實執行(C)確保安全活動與 ISO 26262 要求一致(D)於規劃階段估測所需之資源、經費與人力(E)確定公司提供認證所需之資源(F)任命安全經理，安全經理之能力要求為(A)清楚瞭解「項目」之定義(B)清楚瞭解安全生命週期模型(C)清楚瞭解每個階段必須產出之工作產品。安全經理之職責為(A)擔負功能機能安全之管理責任(B)依據安全事件指派合適人選來執行(C)即時與專業的產出安全分析結果(D)提出並維護安全規劃書(E)監控安全規劃書與實際執行狀況的差異。因專案經理著重計畫管理能力而安全經理則需具備系統整合能力與技術技能，因此不建議由一人同時擔任專案經理與安全經理，除非是小型計畫。

(3) 為確保每一階段的執行正確性，因此必須執行確認審查(Confirmation review)，此審查主要是來確認流程與產出物是否正確及完整，ISO 26262 針對不同之 ASIL 等級與審查類型有不同之審查獨立性要求，不同的獨立性要求因肩負不同的法律責任因此會有不同的審查形式，獨立性「-」因不需肩負法律責任所以可以不執行確認審查，獨立性「I0」則建議執行確認審查，獨立性「I1」必須由公司內部自行執行確認審查，獨立性「I2」最好由第三方公證單位執行確認審查，獨立性「I3」必須由第三方公證單位執行確認審查，除確認審查外，ASIL B~D 的項目還必須執行功能安全流程稽核與功能安全評估(確認技術面是否夠安全)。

(4) 若計畫採取分散式開發，則必需依 ISO 26262 之規定來進行供應商評選，需評定供應商之工程技術是否具備掌握不同 ASIL 的能力、是否具備品保系統、供應商之人力與設備是否符合要求、先前開發產品的安全評估結果…等。

(5) 安全需求必須具備(A)明確可理解(B)最小化(C)具一致性及與其他需求不衝突(D)具可行性(E)具可驗證性，每個安全需求亦必須有獨特項目編號與對應的 ASIL，並要將其狀態(提出、接受、承認、完成確認)加以顯示。

(6) ISO 26262 之所有工作產品皆須納入建構管理系統且於安全生命週期內必須持續維護。

(7) 若安全生命週期內有變更申請則需進行變更管控，每個變更申請都必須有一個獨特項目編號，該編號下必須記載申請日期、變更理由、變更內容與配置之建構項目位置，亦應針對變更項目進行影響評估，影響評估項目包含變更種類(調適、擴充、設變…)、影響的工作產品規模、影響的單位、所導致的功能安全改變範圍、變更所需時程…等，最後必須由具核定權限的人來核決變更申請結果。

(8) 在概念階段、設計與開發階段、測試階段、生產與運行階段皆須針對所對應的產出與工作產品進行驗證確認。

(9) ISO 26262 之工作產品與證據可以(A)書面文件(B)錄影資料(C)資料庫的形式呈現，相關文件需包含標題、作者、審核、文件編號、變更歷程與文件狀態(草案或發佈)。

(10) 軟體開發工具(設計輔助工具、模擬工具、驗證工具)必須取得合格證明後方可使用於車輛功能安全計畫上。

(11) 為減少開發時程與經費，現有已開發之軟體元件(圖形庫、參數庫、資料庫、操作系統、操作系統服務、設備驅動程式)可以被再使用(re-use)，但再使用之軟體元件必須取得合格證明。

(12) 硬體元件用於車輛功能安全計畫上之要求如下：

A. 基礎硬體零件(如：電阻、電晶體…)→需取得 ISO 16750, AEC Q100, AEC Q200…等認證。

B. 硬體零件(如：解碼器、CAN 收發器…)→需取得 ISO 16750, AEC Q100, AEC Q200…等認證，若有安全需求關聯性，則還必須遵守 ISO 26262 Part8 Clause 13 之規定。

C. 硬體元計(如：致動器、感知器、MCU…)→必須遵守 ISO 26262 Part8 Clause 13 之規定，若有安全需求關聯性，則還必須遵守 ISO 26262 Part4 與 ISO 26262 Part5 之規定。

D. 複合硬體元件(如：ECU…)→必須遵守 ISO 26262 Part4 與 ISO 26262 Part5 之規定。

(13) 除軟硬體元件外，項目(Item)、系統(System)、功能(Function)、硬體產品(Hardware product)、軟體產品(Software product)皆可被再使用於車輛功能安全計畫上，但都必須通過嚴謹的評估流程後方可再使用。

六、結論與建議

ISO 26262 為目前全球唯一針對車輛功能安全設計之標準，此標準因對安全生命週期與週期內之工作項目及產出物有詳細的定義，使得車輛系統功能安全之嚴謹與可靠度大幅提升，也因此國際車廠與零組件廠對於 ISO 26262 的重視程度相當高，於草案階段就開始逐步引進融入於原有之系統開發流程，國內亦有大廠為取得國際 OEM 廠的訂單，已開始進行 ISO 26262 之導入。

考量 ISO 26262 之國內外發展趨勢與提升產品嚴謹與可靠度並善盡產品責任，建議未來於車輛電子/電機相關保安系統開發上除使用目前之 FMEA 失效設計手法外，亦可逐步的將 ISO 26262 導入至系統開發流程內，如此之作法除可加強設計產品的穩健性外亦有利於產品之推廣與銷售。

參考文獻

[1] ISO/DIS 26262-1~10, “Road vehicles - Functional safety - Part 1~10”, International Organization for Standardization, 2009.

[2] 台灣德國萊因教育訓練中心，「ISO 26262 認證訓練課程講義」，民國 99 年。

[3] 台灣檢驗科技股份有限公司，「ISO-26262/DIS Safety Lifecycle Management 課程講義」，民國 100 年。