車用電子系統的功能安全需求-ISO 26262國際安全規範簡介及其應用

Safety Requirements of Vehicular Electronics – An Introduction of ISO-26262 and Its Application

呂昆龍　張國樑　黃立仁　紀坤明　張雍昌　楊智仁
Kuen-Long Lu, Kuo-Liang Chang, Li-Ren Huang, Kung-Ming Ji, Yung-Chang Chang, Chih-Jen Yang

中文摘要

近年來，汽車電子產業開始發現系統失效的問題，一旦發生失效，就有可能導致乘客生命安全受到威脅，而車輛廠商也將面臨官司賠償與商譽受損之巨大風險。為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，因此車輛領域專家們開始著手發展車輛領域之功能安全標準，ISO-26262便在此環境與需求下應運而生。在ISO-26262標準中，以功能安全管理(Management of functional safety)、汽車產品設計開發的安全生命週期(Safety lifecycle)及分析定義汽車安全完整性等級(Automotive Safety Integrity Level, ASIL)為主要規範。此標準以項目定義及風險分析來評估系統所需達到之ASIL安全等級目標。本文將介紹ISO-26262標準所規範的系統功能安全發展概念，並以一個微控制器分析案例來展示ISO-26262在實際設計上的應用。

Abstract

Nowadays, failures due to design flaws are more and more significant for the vehicular electronic system. Effect of such failures could cause pedestrians injured or even life-threatened. Hence vehicular electronic system vendors would face the risks such as huge amount of recall and compensation. The business reputation could also be negatively affected. Therefore, a rigorously formalized system development flow becomes necessary so that developers can follow for failure avoidance and that's why experts in automotive filed establish the functional safety standards specialized for vehicular electronics, termed ISO-26262. In ISO-26262 standard, three primary topics, Management of Functional Safety, Safety Lifecycle, Automotive Safety Integrity Level, ASIL, are involved. The ASIL is determined by system developers according to the Hazard Analysis and Risk Assessment (HARA) results. In this article, we will try to give the sketch of ISO-26262 standard, and explain how to develop a system with functional safety consideration. Lastly, we will take a MCU as the case study to demonstrate the application of ISO-26262 standard.

關鍵詞(Key Words)

汽車電子；功能安全；安全生命週期 (Vehicular Electronics; Functional Safety; ISO-26262)

1．前言

ISO 26262:(Road vehicles - Functional Safety)[1]是在IEC 61508 標準的基礎上，以道路車輛電子及電氣系統應用產業的角度，具體規範車用電子安全系統開發到使用的安全生命週期之技術與管理要求。此標準特色如下：

- 提供一個車輛安全生命週期 (設計、生產、運轉、維修、退役)，並根據電子/電氣系統的發展類別(新開發、衍生、修改、再使用)在各生命週期階段內支持必要的活動;
- 提供汽車的具體風險基礎評估，以確定風險等級(車輛安全完整性等級，ASIL)，如圖1;
- 利用車輛安全完整性等級(ASIL)規範具體項目的必要安全設計要求，以達到可接受的安全等級;
- 提供所需的確認措施，以確保足夠和可以接受的安全程度能夠被達成。

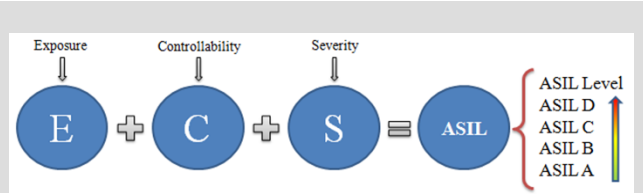

圖 1　ASIL車輛安全完整性等級規範

ISO-26262 涵蓋了從管理、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至ASIL D，其中以等級A為最低D為最高，ASIL等級越高的系統功能安全要求及目標就越需要嚴謹。此規範由IEC 61508[2]為基底，針對車輛電子及電機系統的功能安全來進行修改，而規範的產品設計開發流程以V-model設計驗證模型來呈現。

下列為ISO-26262安全流程之各章節名稱[1]：

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

而在這些章節中，又以三大階段為主要重點，如圖2所示：

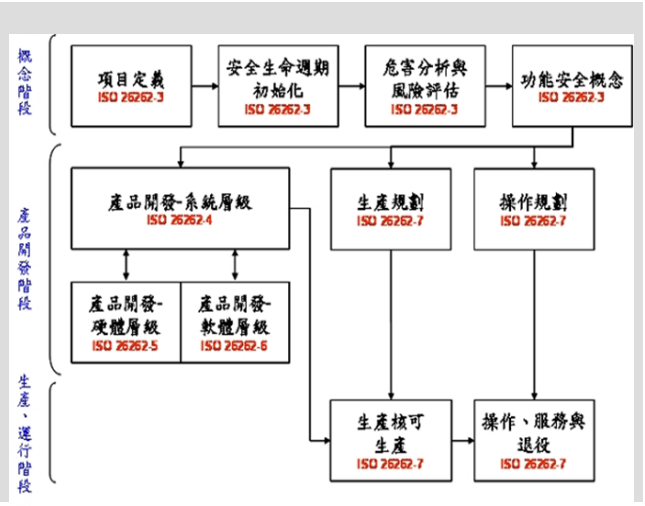

圖 2　ISO-26262 安全生命週期流程

1. 概念階段：以Part 3為主，其中包括項目定義(Item definition)、安全生命週期初始化(Initiation of the safety lifecycle)、危害分析與風險評估(Hazard analysis & risk assessment)和功能安全概念(Functional safety concept)。建立初步系統架構及功能，並對其以安全分解(Safety decomposition)[3]的觀念來進行車輛層級(Vehicle level)、系統層級(System level)及子系統層級(Sub-System level)的風險分析，借此定義系統所需達到的安全目標(Safety goal)，最後需列出有效的安全機制(Safety mechanism)，若此系統分析結果沒有達到該有的安全目標，則需要加入安全機制來進行安全等級的改善。

2. 產品開發階段：以Part 4、Part 5和Part 6為主，分為系統層級(System level)、硬體層級(Hardware level)和軟體層級(Software level)。透過上階段之架構分析及安全機制來進行系統的設計與驗證。在測試驗證的部分，規範中列舉出各ASIL等級所需的測試方法。

3. 生產、運作階段：以Part 7、Part 8為主，在於規範產品生產、操作規劃、生產前確認相關功能安全需求皆被設計與實行、關於組裝與製造之需求發展與執行與產品銷售後續服務的SOP(Start Of Production)流程。

2 · SEooC 概念介紹與車用微控制器硬體設計

ISO-26262 車用安全標準無疑是台灣欲發產車用微控制器必須要拿到的入場卷，而此標準也提供了台灣相關產業可依循的方針。欲導入ISO-26262安全規範，首先必須先清楚了解欲開發產品的定位。台灣IC產業的基礎雄厚，最有可能朝微控制器晶片(Micro-Controller Unit，MCU)發展，在車用電子產業中，屬於第二級供應商(Tier 2)。在ISO 26262的規範中，微控制器晶片的安全性需求(Safety Requirement)是由第一級供應商(Tier 1)根據其應用的風險評估來制定並提供給晶片開發商，後者再依照安全性需求來研發微控制器晶片。然而目前台灣車用電子產業中缺乏第一級供應商，微控制器晶片開發商若不想依靠國外第一級供應商提供安全性需求的相關規格，ISO-26262還提供了另外一條可行的開發流程，稱之為SEooC (Safety Element out of Context)，其流程圖如下圖3所示[4]：

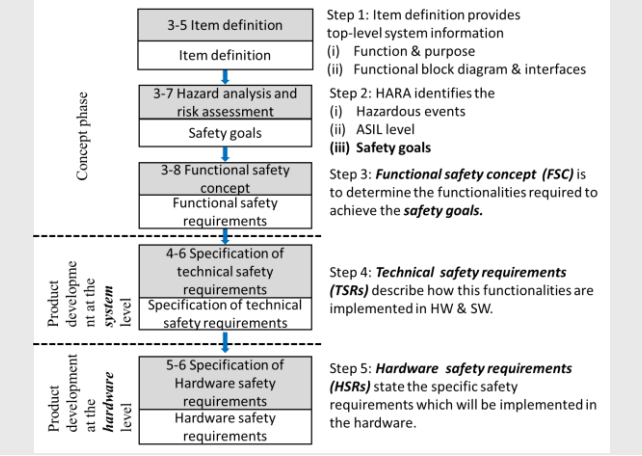

圖 3　針對微控制器硬體的SEooC開發流程

在缺乏第一級供應商的情況下，ISO 26262規範允許第二級供應商自行假設其應用，並扮演第一級供應商的角色：包括產品定義、透過執行風險評估(Hazard Analysis and Risk Assessment，HARA)來決定其應用的車輛安全完整性等級(ASIL)、制定系統層級的安全目標(Safety Goal)以及功能安全需求(Functional Safety Requirement，FSR)以及功能安全技術實現需求(Technical Safety Requirement，TSR)等。根據TSR就可以再進一步制定出的硬體安全需求(Hardware Safety Requirement，HSR)，工程師就可以依據HSR來開發微控制器晶片。(但需特別注意的是制定的所有安全目標以及安全需求都須經過第三方單位的認證。)

3 · ISO-26262 安全性驗證方法

為了實現具有高可靠度/安全性的車用電子系統，勢必要在系統的設計中加入安全機制(Safety Mechanism)來避免系統失效時造成危害。然而加入什麼樣的安全機制，如何才能讓安全機制發揮最大的效用，不能僅憑研發工程師的主觀認定，必須透過一套有系統的分析方法來制定安全機制的設計方針。故安全性分析(Safety Analysis)也是ISO 26262規範中非常重要的一項要求，而當微控制器晶片的ASIL要求在等級B以上時，也必須透過安全性分析來驗證是否能夠達成預期的ASIL要求。

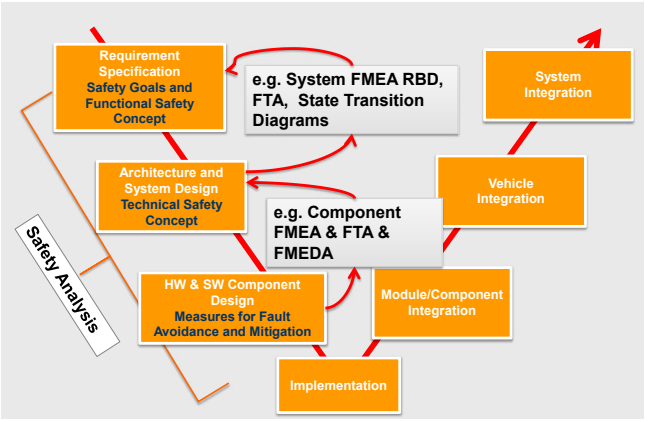

圖 4　將安全性分析導入至V-model示意圖

上圖4為常見的車用電子產品的V-model開發流程，由圖4可知安全分析主要從晶片研發初期時就必須進行，才能為安全機制的設計提供最好的依據。在ISO 26262規範中建議的安全分析方法主要有FMEA(Failure Mode and Effect Analysis)、FTA(Fault Tree Analysis)以及FMEDA(Failure Mode Effect and Diagnostic Analysis)三種。三種分析方法都有其不同的目的，FMEA主要是用於列出MCU內元件有哪些可能的失效模式，以及這些失效模組對MCU的影響；FTA則是列出導致MCU失效的原因主要是由於哪個/些元件出錯所導致；而FMEDA主

要是用來分析不同的安全機制對於各種不同的元件失效模式的有效性。針對MCU硬體設計的開發商來說，FMEDA尤其重要，因為在ISO 26262規範中，FMEDA是用來評判MCU硬體能否達到ASIL要求的主要依據之一。第4章將會有MCU FMEDA的實例展示。

3.1 ISO-26262 軟體安全性驗證方法

ISO-26262標準對軟體的設計與測試驗證於Part6單元有詳細描述。因為汽車領域有其特殊之發展需求，如控制系統的Model based design與規格驗證等。汽車電子發展流程常用V-Model流程來敘述，如圖5所示。從系統的需求透過模型建立分析來產生系統設計規格並透過工具如CarSim或dSPACE來驗證確認設計規格是否滿足需求。進而再配置安全功能到硬體或軟體的設計上。

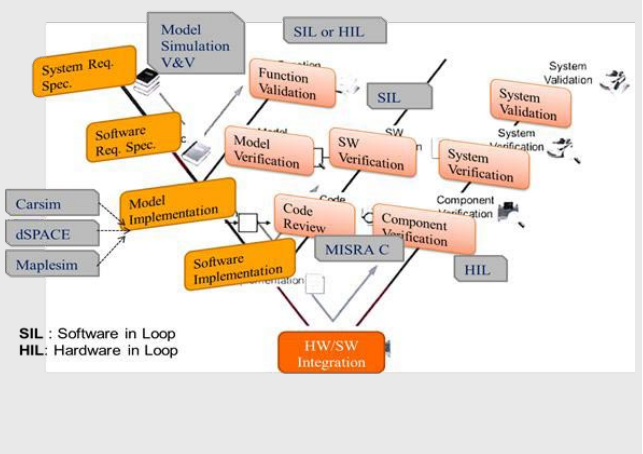

圖 5　V模型軟體發展與測試流程

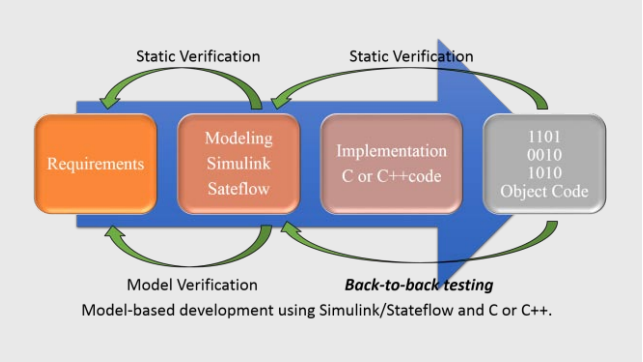

圖 6　軟體測試驗證流程

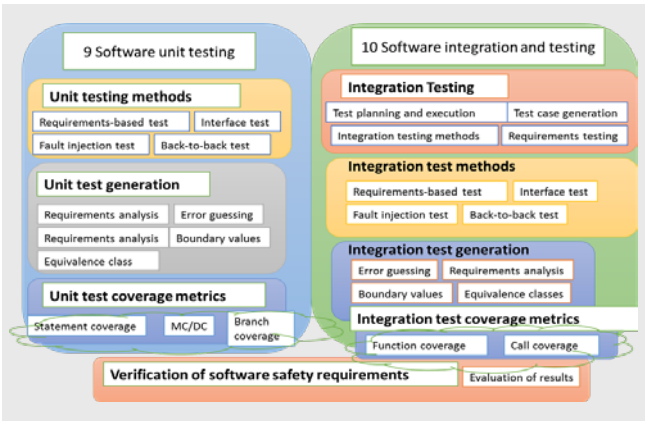

圖 7　軟體測試度量依據ISO-26262標準要求

軟體的驗證從Model Based Software 驗證到原始程式碼的靜態分析(Static Analysis) 以及動態分析(Dynamic Analysis)來驗證軟體設計的安全性。靜態分析常用MISRA C or C++來檢查是否違背安全設計法則，常見的動態分析包括白箱測試(white box testing)以及Back-to-Back 測試，如圖6所示。軟體的測試度量(metrics)標準要求須符合單元測試涵蓋(Coverage) 如語句(Statement)、分支(Branch)、MC/DC(Modified Condition/Decision Coverage 以及整合測試(Integration Test)，如功能涵蓋率(Function Coverage)、呼叫功能涵蓋率(Call Coverage)，如圖7所示。

圖8是資通所自主研發的車用微控制器架構圖，其主要應用為電動車馬達的控制，故此微控制器須能符合高安全性的要求。在此我們

4．車用微控制器實例展示

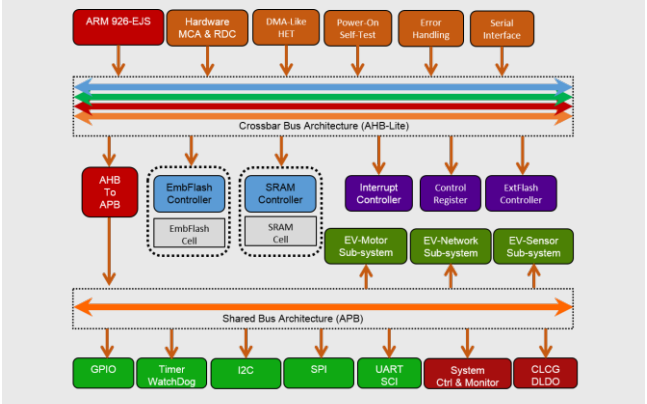

圖 8　車用微控制器架構(未加入安全機制)

表 1　ISO 26262 ASIL量化標準

	ASIL B	ASIL C	ASIL D
SPFM	> 90%	> 97%	> 99%
LFM	> 60%	> 80%	> 90%
PMHF	< 100 FITs	<100 FITs	< 10FITs

將此微控制器的安全性要求設為ASIL D。而根據表1可知其各項相關參數的量化標準。

表1中SPFM是Single Point Fault Metrics的縮寫，代表的是對於單點錯誤的容忍能力。而LFM則是Latent-multiple-point Fault Metrics的縮寫，代表的則是對於多點錯誤的容忍能力。最後PMHF則是Probabilistic Metrics for Hardware Failure的縮寫，及所謂的硬體失效率，單位為FIT(Failure In Time)。

下表2是圖8車用微控制器在未加入安全機制前的硬體失效率。

表 2　MCU Failure Rate

Subsystem	Component	Base Failure rate (FITs)
Microprocessor	ARM926-EJS	80
Memory	Control register	30
	Flash controller	50
	SRAM controller	25
Communication	AHB-Lite	25
	APB	25
	AHB-APB bridge	50
Controller	External flash controller	50
	Interrupt controller	30
Peripherals	GPIO	30
	Timer watchdog	30
	I2C	30
	SPI	30
	UART SCI	30
Other IPs	MCA & RDC	50
	DMA	50
	Power-on self-test	30
	Error handler	50
	Serial interface	30
Total		725

由表2可知，其硬體失效率高達725，與ASIL D的要求還有很大的落差。分析此差距是加入安全機制時非常必要的事前工作，可以讓設計者在決定採用何種安全機制時能夠有所依據，盡量避免不適當設計的產生。

為了達成ASIL D的要求，勢必須加入安全機制(Safety Mechanism)來提升微控制器的安全性，而ISO 26262對於ASIL-D的硬體設計有非常

表 3　MCU Failure Rate

Element	Safety mechanism
Processing units	Software diversified redundancy (one hardware channel)
	Reciprocal comparison by software
	HW redundancy
	Configuration register test
Non-volatile memory	Memory monitoring using error-detection-correction codes (EDC)
	Memory signature
	Block replication
Volatile memory	RAM march test
	Memory monitoring using error-detection-correction codes (EDC)
	Block replication
	Running checksum/CRC
Analogue and digital I/O	Test pattern
	Multi-channel parallel output
	Monitored outputs
	Input comparison/voting
Communication bus (serial, parallel)	Complete hardware redundancy
	Inspection using test patterns
	Combination of information redundancy, frame counter and timeout monitoring
Power supply	Voltage or current control
Program sequence monitoring/Clock	Combination of temporal and logical monitoring of program sequence
	Combination of temporal and logical monitoring of program sequences with time dependency
Combinatorial and sequential logic	Self-test supported by hardware
On-chip communication	Complete hardware redundancy
	Test pattern

高的要求(如表1)，任何克服故障的方法都必須有賴於故障的偵測與診斷機制。一般來說，診斷機制的故障診斷率越高，也代表微控制器的安全性越高。因此高安全性反映在硬體設計上即代表安全機制需要非常高的故障診斷率(Diagnostic Coverage，DC)。DC值在ISO-26262中可分為high(99%)、medium(90%)、與low(60%)三種等級，表3列出ISO-26262 part 5 所提供的微控制器安全機制參考設計，這些安全機制都具有99%的DC值，欲達成ASIL D的要求，建議加入這些具有高故障診斷率的安全機制至微控制器設計中。

下圖9是參考上表3之後，將圖8微控制器進一步改良之後的架構圖，比較圖8與圖9可以發現加入安全機制後整體架構圖的改變。為了驗證加入的安全機制可以使微控制器的整體故障率達到ASIL D的要求，在此我們採用了FMEDA方法來分析，下表4是針對此架構所進行的FMEDA的部分結果展示[4]。根據FMEDA的分析結果，改良後的微控制器的硬體失效率可降至9.45FITs，已符合ASIL D的< 10 FITs的要求。

由上述實例展示可知，為了要達成高安全性微控制器的設計，在架構設計時就必須將安全性的議題納入考量。這無疑會使本來的設計週期所需花費的時間變長，也會增加額外的人力與軟硬體投資，然而因為車用微控制器晶片與人身生命安全有重大關聯，這些投資是不可避免的。若將來台灣的IC設計產業想擴大車用電子產品的市場，勢必要將以往只考慮成本與出貨時間的觀念加以調整。

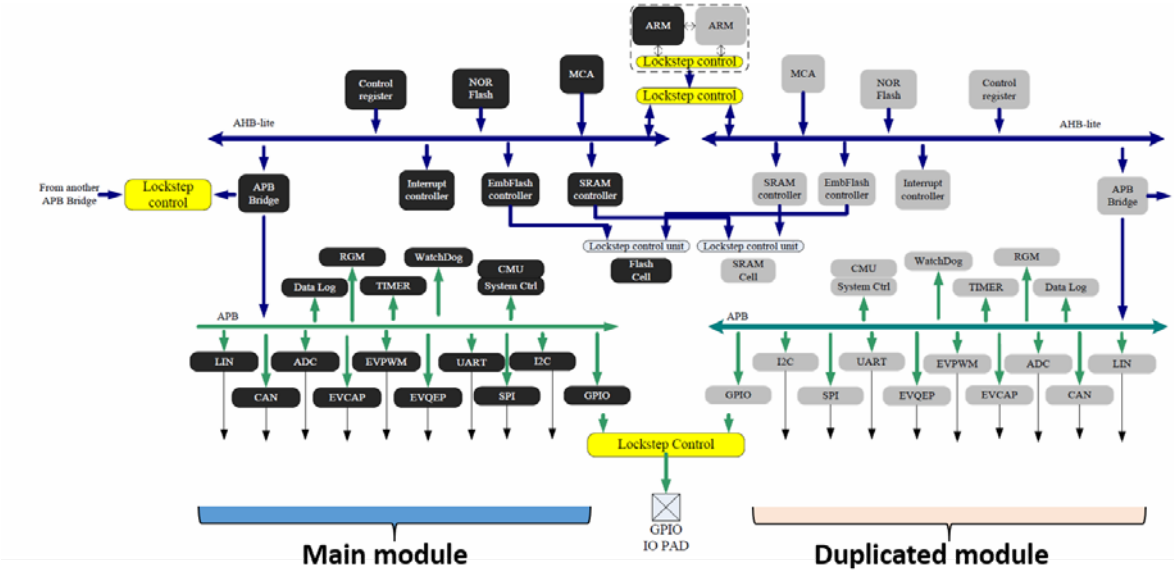

圖 9 車用微控制器架構(加入安全機制)

表 4 微控制器晶片的FMEDA部分結果

System: Bison-2 MCU
Subsystem:
Component:
Design Lead: Kung-Ming Ji
Core Team: ITRI ICL R400

Failure Mode, Effect, and Diagnostics Analysis

FMEDA Number:
Prepared By: Kuen-Long Lu
FMEDA Date: 2014/11/6
Revision Date:
Page:

							Single Point Fault / Residue Fault				Latent Mutiple Point Fault			
HW Block	Failure rate / FIT	Component name	Safety-related component to be considered in the calculations ?	Failure Mode	Failure mode distribution	Component Failure rate / FIT	Failure mode that has the pontential to violate the safety goal in absence of safety mechanism?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal?	Failure mode coverage wrt. violation of safety goal	Residual or Single-Point-Fault failure rate / FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component?	Detection means? Safety mechanism(s) allowin to prevent the failure from being latent?	Failure mode coverage wrt. Latent failure	Latent Multiple-Point Fault failure rate / FIT
Micro-processor	110	ARM9 CPU CORE	Yes	Output incorrect result	73%	80	x	Dual-Core Lock Step	100%		x	CPU Lock-Step Comparison	99%	0.8
		LSCU	Yes	Output incorrect comparing result	27%	30	x	Second-staged Comparison	100%		x	Second-staged Comparison	99%	0.3
Memory Unit	265	Control register	Yes	Content is corrupted	11.3%	30	x	Dual-Module Redundancy	100%		x	Lock-Step Comparison	99%	0.3
		Flash controller	Yes	Output incorrect control signal	18.9%	50	x	Dual-Module Redundancy	100%		x	Lock-Step Comparison	99%	0.5
		Flash (ECC + Cell)	Yes	Content is corrupted	30.2%	80	x	Error Correction Code	100%		x	Lock-Step Comparison + Data ECC	99%	0.8
		SRAM controller	Yes	Output incorrect control signal	9.4%	25	x	Dual-Module Redundancy	100%		x	Lock-Step Comparison	99%	0.25
		SRAM (ECC + Cell)	Yes	Content is corrupted	30.2%	80	x	Error Correction Code	100%		x	Lock-Step Comparison + Data ECC	99%	0.8

5 · 結論

在本文中，針對汽車電子產業目前主要依循的功能安全規範，ISO-26262，提供整體概念與其核心精神的介紹。另外針對ISO-26262中較為特別的SEooC設計概念也有所著墨。針對軟體安全性設計的部分，則是介紹了其測試項目以及與V-model發展流程之間的整合關係。最後則是利用資通所本身所開發的微控制器作為展示案例，說明ISO-26262安全標準的實際應用。

本文最主要的目的是讓國內相關產業界能夠對ISO-26262有一初步認識，並且分享作者針對功能安全設計的研究成果與心得，期望能對國內汽車電子產業提供有用的參考資料。

參考文獻

[1] "ISO 26262 Road vehicles - Function Safety," ed: International Organization for Standardization, 2011.

[2] “International Standard IEC 61508: Functional Safety of Electrical/Electronic/ Programmable Electronic Safety Related Systems”. IEC, Geneva. www.iec.ch

[3] Andrea Piovesan, John Favaro, “Experience with ISO 26262 ASIL Decomposition”, Automotive SPIN, Milano, 2011.

[4] 呂昆龍, “遵循ISO 26262規範 車用MCU可靠度/安全性達標”, 新通訊 2015 年 4 月號 170 期

作者簡介

呂昆龍

資訊與通訊研究所/生醫與工業積體電路技術組/車用電子設計應用部/工程師。AFSP(Automotive Functional Safety Professional) Certification from SGS-TÜV。專長為容錯架構設計、可靠度模型、錯誤注入與可靠度驗證、功能安全性分析與設計。
E-mail: sone@itri.org.tw

張國樑

SGS功能安全主任及台灣區負責人，AFSE(Automotive Functional Safety Expert) Certification from SGS-TÜV，專長為醫療與汽車電子軟體功能安全分析驗證。
E-mail: Jeff-tw.Chang@sgs.com

黃立仁

資訊與通訊研究所/生醫與工業積體電路技術組/組長。AFSP(Automotive Functional Safety Professional) Certification from SGS-TÜV。專長為類比/混和訊號IC設計、車規IC設計、功能安全性分析與設計、超大型積電電路測試。
E-mail: lrhuang@itri.org.tw

紀坤明

資訊與通訊研究所/生醫與工業積體電路技術組/車用電子設計應用部/資深工程師兼副經理。專長為數位VLSI設計、EDA設計流程整合、功能安全性分析與設計。
E-mail: digo@itri.org.tw

張雍昌

資訊與通訊研究所/生醫與工業積體電路技術組/車用電子設計應用部/工程師。AFSP(Automotive Functional Safety Professional) Certification from SGS-TÜV。專長為晶片網路容錯架構設計、功能安全性分析與設計。
E-mail: ycchangs@itri.org.tw

楊智仁

資訊與通訊研究所/生醫與工業積體電路技術組/車用電子設計應用部/工程師。AFSP(Automotive Functional Safety Professional) Certification from SGS-TÜV。專長為微控制器容錯架構設計、功能安全性分析與設計、軟硬體協同驗證。
E-mail: Jeff.Yang@itri.org.tw