瞭解安全事項應用筆記——第 2 部分：

失效模式分配

■作者：Bryan Angelo Borres / ADI 資深產品應用工程師

本系列文章的第一部分針對元件失效率及可靠性預測方法展開了討論。本文 (第二部分) 則將進一步介紹失效模式、影響及診斷分析 (FMEDA)。作為系統整合商可採用的安全分析工具之一，FMEDA 能依據 IEC 61508 等功能安全標準的要求對安全相關系統的設計進行評估。開展 FMEDA 分析需要獲取多項元件資訊，其中包括失效率資料和失效模式分佈 (FMD)。本文即將闡述 FMD 等因素如何影響 FMEDA 評估，並介紹 ADI 的安全應用筆記如何提供此類資訊。

什麼是 FMEA ？

失效模式和影響分析 (FMEA) 是一種安全分析工具或方法，主要用於評估系統或流程，明確指出可能出現的失效形式，並瞭解這些失效模式對相關專案的性能和周邊環境造成的影響。通常，FMEA 會透過反覆運算方式來進行，目的在於為降低失效發生概率及減輕失效影響的決策提供支援，進而促進提升系統和流程的穩健性與可靠性。[1]

圖 1：FMEA 及其變體。

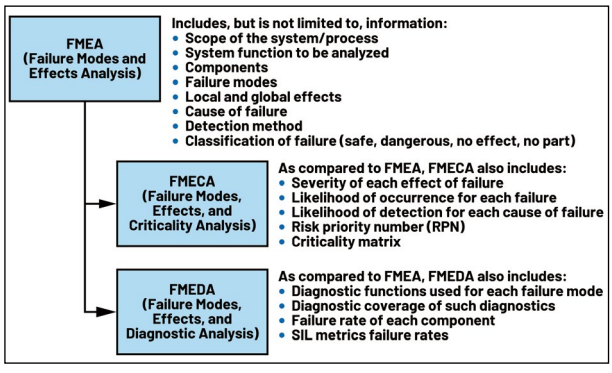

圖 1 展示了典型 FMEA 的構成要素及其一些廣為人知的變體：FMECA 和 FMEDA。FMEA 通常基於以下資訊：系統或流程的相關資訊、待分析的功能、組成系統的元件、每個元件的失效模式、局部及全域影響等。當 FMEA 根據失效模式的重要性對其進行優先順序排序時，稱為失效模式、影響及危害性分析。當 FMEA 採用某種度量方式來體現診斷功能的有效性時，則稱為失效模式、影響及診斷分析。[1,2]

在安全相關系統的設計中，FMEDA 通常用於以下方面：提供與每種失效模式對應的元件級失效率、衡量自動診斷功能的有效性、在設計決策中應用定量可靠性分析、證明最終設計優於其他備選方案，以及顯示硬體設計符合 IEC 61508 標準的要求。[2]

示例 FMEDA

表 1 呈現了一個源自 IEC 60812:2018 標準的 FMEDA 示例。儘管該示例並不完整 [1]，但仍展示了電源電路主要部分的評估方法。該電源電路採用線性穩壓器為元件內部提供電源電壓。

此 FMEDA 示例包含多種失效率數值，具體有安全失效率 (λS)、無影響失效率 (λNE)、危險可檢測失效率 (λDD) 和危險不可檢測失效率 (λDU)，這些都是計算安全失效比率 (SFF) 的重要參數。[1]

計算 SFF3：

$$SFF = \frac{\sum\lambda_S + \sum\lambda_{DD}}{\sum\lambda_S + \sum\lambda_{DD} + \sum\lambda_{DU}} \times 100\% \quad (1)$$

現有診斷功能對 R100 短路失效的診斷覆蓋率僅為 60%，對 IC18 的危險失效的診斷覆蓋率為 0%，據此計算得出 SFF 為 76.94%。若該電源電路僅設計用於單通道系統，則其僅

表 1：電源電路的 FMEDA 分析 (基於 IEC 60812:2018 標準表 F.12)

名稱	元件	功能	失效率 (FIT)	失效模式	FMD	影響	失效分類	診斷覆蓋率	λS (FIT)	λNE (FIT)	λDD (FIT)	λDU (FIT)
F50	保險絲	短路保護 (輸入端)	25	無法開路	50%	正常運行時無	無影響	—	0	12.5	0	0
				過早開路	10%	輸出斷電	安全	—	2.5	0	0	0
				開路緩慢	40%	對安全功能無影響	無影響	—	0	10	0	0
D12	抑制二極體	過壓保護 (EMC)	7	短路	95%	F50 熔斷	安全	—	6.65	0	0	0
				開路	5%	對安全功能無影響	無影響	—	0	0.35	0	0
R100	電阻，SMD	電流限制 (EMC)	0.2	短路	5%	無電流限制	危險	60%	0	0	0.006	0.004
				開路	65%	輸出斷電	安全	—	0.13	0	0	0
				參數	30% 變化	功能仍正常	無影響	—	0	0.06	0	0
C13	陶瓷電容，	EMC HDC/MDC	2	短路	50%	F50 熔斷	安全	—	1	0	0	0
				開路	30%	正常運行時無 (無保護)	影響	—	0	0.6	0	0
				值變化	20%	功能仍正常	無影響	—	0	0.4	0	0
D25	小訊號二極體 <0.1 W	電橋整流器	1	短路	50%	F50 熔斷	安全	—	0.5	0	0	0
				開路	35%	在交流供電情況下無法正常整流	安全	—	0.35	0	0	0
				參數變化	15%	功能仍正常	無影響	—	0	0.15	0	0
C2	電解電容，鋁電解電容，非固體電解質	濾波電容	5	短路	53%	F50 熔斷	安全	—	2.65	0	0	0
				開路	35%	直流供電下無正常運行時	無影響	—	0	1.75	0	0
				電解液洩漏	10%	對安全功能無影響	無影響	—	0	0.5	0	0
				電容減少	2%	仍正常	無影響	—	0	0.1	0	0
IC18	穩壓器，功率 > 1 W, > 1W，低複雜度	與 R100 配合使用的穩壓器，用於電流源	25	高位準鎖定	30%	無調節功能 -> 輸出開關	危險	0%	0	0	0	7.5
				低位準鎖定	30%	輸出斷電	安全	—	7.5	0	0	0
				短路	15%	無調節功能 -> 繼電器過電流 (多樣)	無影響	—	0	3.75	0	0
				開路	15%	輸出斷電	安全	—	3.75	0	0	0
				漂移	5%	功能仍正常	無影響	—	0	1.25	0	0
				功能	5%	功能仍正常	無影響	—	0	1.25	0	0
小計									25.03	32.66	0.006	7.504

能達到 SIL 1。[3] 若增加針對 IC18 危險失效的診斷功能，此設計可進一步改進，以達到更高的 SIL 等級。當新增的診斷功能對 IC18 危險失效的診斷覆蓋率達到 99% 時，其對應的 λDU 將從 7.5 FIT 降至 0.075 FIT，而 λDD 將從 0.006 FIT 增至 7.431 FIT，新的總 λDU 為 0.079 FIT，因此 SFF 為 99.76%。

計算 PFH4：

$$PFH = \sum \lambda_{DU} \quad (2)$$

圖 2：基於 LTC2933 安全應用筆記的 FMD。

System Function

- Monitor if a power supply is above the OV threshold or below the UV threshold and assert GPIO1, GPIO2 output signals LOW and GPIO3 output signal HIGH.

Table 3-1 Failure Mode Distribution (CF = 1.053)

Failure Modes	Failure Mode Distribution
At least one of the GPIO indicates a trip when it should not	48%
At least one of the GPIO doesn't indicate a trip when it should	52%

同時，該電源電路的總 λDU 需符合 IEC 615083 標準中關於危險失效概率的要求。降低與安全相關的系統總 λDU(包括電源電路及其診斷功能)，將對應降低每小時危險失效的平均頻率 (PFH)，進而更易滿足更高的安全完整性等級 (SIL) 要求。[4]

值得注意的是，有三列資料會影響失效模式、影響及診斷分析的失效率結果，如表 1 所示。這些列分別涉及：元件的失效率、失效模式分佈以及診斷覆蓋率。元件失效率通常來自元元件製造商，也可透過可靠性預測方法進行計算。而失效模式分佈是指元元件總失效率中可分配至每種失效模式的比例，該分佈通常也由元件製造商所提供。最後，診斷覆蓋率是指所用診斷功能對失效的檢測能力，這是系統整合商在設計中唯一可優化的因素，可透過增加診斷功能或採用更好的診斷方法來實現。

運用 ADI 的安全應用筆記加快系統的 FMEDA 進程

本系列的第一部分展示了 LTC2933 的安全應用筆記如何基於不同的可靠性預測方法提供基礎失效率資料。運用此類積體電路 (IC) 的失效率資料，並結合同一份檔案中如圖 2 所示的現成失效模式分佈資訊，可顯著加快基於此類 IC 的系統 FMEDA 進程。此類安全應用筆記還會說明假設的系統功能及 IC 使用的應用電路。

借助 ADI 的安全應用筆記，安全分析將變得更加準確，因為相關資訊是直接來自元件製造商，而非簡單地將全部失效率歸為危險失效率，或基於特定假設來設定某種 FMD。

結語

本文首先概述了一種名為 FMEA (失效模式與影響分析) 的安全分析工具，並介紹其衍生形式 FMECA (失效模式、影響及危害性分析) 和 FMEDA (失效模式、影響及診斷分析)。隨後，本文深入剖析了一個 FMEDA 實例，解釋整合診斷功能及其診斷覆蓋率對於提升電源電路的安全失效比率的作用。文章更進一步強調，在考慮診斷功能的前提下，降低未檢測到的危險失效率所具有的重要意義。最後，本文展示了系統整合商如何運用 ADI 安全應用筆記中提供的元件 FMD 資訊，以此提高系統 FMEDA 和安全分析的技術準確性。

參考文獻

1 “IEC 60812:2018.Failure Modes and Effects Analysis (FMEA and FMECA)”，國際電子電機委員會，2018 年。

2 Paddy Healy，“What Is a FMEDA?”，Exida，2023 年 4 月。

3“IEC 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”，國際電子電機委員會，2010 年。

4 Loren Stewart，“Back to Basics 17 - PFH”，Exida，2019 年 11 月。CTA