SYNOPSYS®

技術白皮書

應用於半導體的 FMEDA 安全驗證方法論

SGS

作者

Alessandra Nardi
新思科技
功能安全與安全性傑出架構師

Teo Cupaiuolo
新思科技
主任應用工程師

Liu Min
SGS-TÜV Saar
功能安全專案經理

簡介

當今汽車所需的系統與晶片日益繁複，因此在設計開發階段中遵循功能安全(functional safety)程序變得至關重要。應用於汽車的半導體複雜性及精密度，正在推動整個供應鏈對功能安全的需求，影響到的不僅是汽車製造商，還涉及半導體設計公司與 EDA 工具供應商。而對於參與這些繁複半導體分析過程的功能安全工程師，其任務是要在數以千計的模式中，識別可能會出現設計故障的模式 (亦稱為故障模式 (failure modes, FMs))，以及可能導致該類故障的原因。

針對繁複設計，要以手動方式達成高效能又高效率的功能安全分析極為費時，且實際上非常容易出錯。在整個晶片設計流程中，先進功能安全方法需要涵蓋多個層面的自動化，並得以無縫接軌整合故障模式影響與診斷分析 (Failure Modes Effects and Diagnostic Analysis, FMEDA)。FMEDA 先進分析工具至少應能夠：

- 採用經認證工具的安全方法，為 SoC 提供可擴展性
- 讓工程師可以同時執行任務，實現相似的安全目標
- 能夠在整個 RTL 到 GDS (圖形設計系統，graphic design system) 流程循序追蹤 FMEDA
- 從 Jama Connect® 等管理工具匯入安全需求
- 擷取架構設計資料
- 連接設計流程每個部分的完整控制艙艙 (cockpit)，包括擷取設計資料、選擇正確安全機制、驗證功能安全以及實作

手動方法以試算表 (例如：Excel) 為基礎，容易出錯，而且不符合上述需求。

對於以能通過 ISO 26262 認證為目標的汽車設計而言，在安全規劃階段就必須有經認證的功能安全評估人員參與。功能安全評估人員會針對 FMEDA 所採取的整體安全方法以及在設計開發週期期間使用的工具提供指導。

本篇技術白皮書將探討新思科技 VC 功能安全管理器 (Synopsys VC Functional Safety Manager, FSM) 在晶片開發過程中，如何啟用 FMEDA 全方位整合式分析，幫助加速 IP 與 SoC 功能安全認證的速度。

此外，本篇內容也包括了新思科技與 SGS-TÜV Saar GmbH (ISO 26262 功能安全評估的全球領導者) 合作，如何協助制定新思科技 VC FSM 中的 FMEDA 分析技術，進而加速 ISO 26262 認證，並縮短上市時程 (time-to-market)。

功能安全基本原理

微電子學應用遵循兩大安全標準：IEC 61508 係由國際電工委員會 (International Electrotechnical Commission, IEC) 制定，適用於一般電子用品市場的功能安全標準；而 ISO 26262 則是國際公認功能安全標準，適用於安裝在道路交通工具的電氣和/或電子系統。ISO 26262 提出的標準化系統生命週期需要實施諸多程序和方法，才能實現系統性安全功能目標。這種標準化生命週期建議使用經認證的先進 EDA 技術，進行需求工程、架構建模、驗證、實作，並運用此流程所產生的見解(insight)做為未來發展的基礎。

這些流程在功能安全生命週期中的關鍵作用是定義安全分析目標，接著驗證系統架構，並提供相關佐證，以確保設計是根據汽車安全完整性等級 (Automotive Safety Integrity Level, ASIL) 目標執行安全相關功能。除此之外，安全分析旨在調查系統性故障與隨機硬體故障的可能原因，以及這些故障對其功能產生的後續影響。驗證安全機制至關重要，目的是要偵測硬體生命週期期間發生的隨機故障，並確保在故障發生時達到安全狀態。

而 ISO 26262 所要求的故障模式與影響(Failure Mode and Effect Analysis, FMEA) 質化分析以及 FMEDA 量化安全分析，對於評估單點故障指標 (Single Point Fault Metric, SPFM) 和潛在故障指標 (Latent Fault Metric, LFM) 等硬體架構指標而言，是不可或缺的一環。

應用於半導體的 FMEDA 安全分析

圖 1 顯示半導體生命週期期間可能會發生的故障類型，以及相關的關鍵安全分析指標。

為了解決系統性故障 (請參照圖 1)，使用質化系統設計 FMEA (D-FMEA) 來調查原因，像是選擇錯誤材料、錯誤尺寸、應用元件不適合、耐久性不足、演算法不可採納，以及未考慮時間限制等。

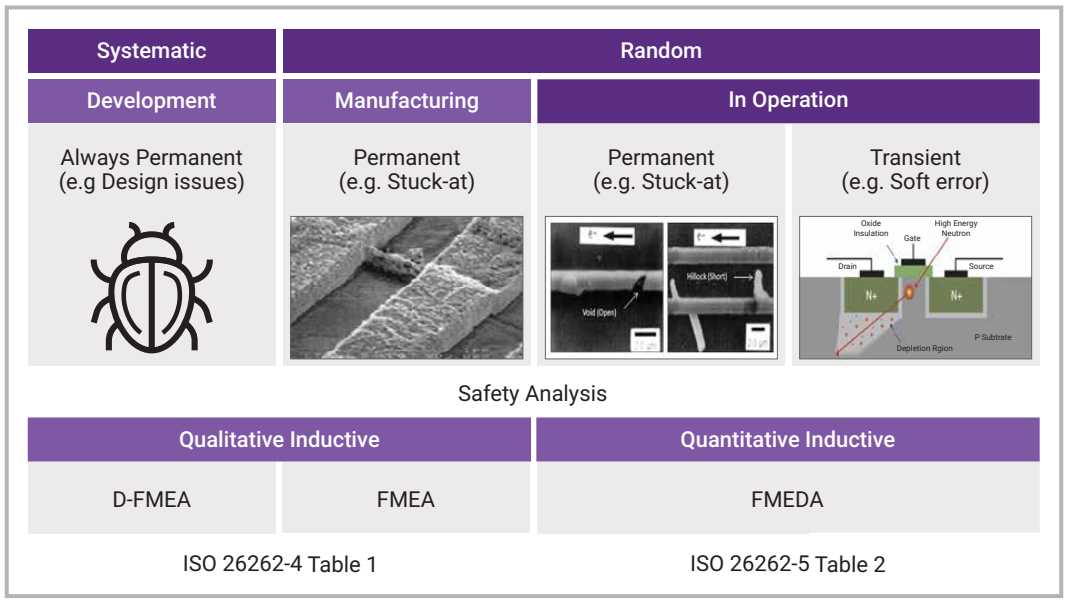


圖1 : 系統性故障和隨機故障以及對應的安全分析

為了解決隨機故障問題，FMEA 質化分析 和 FMEDA 量化分析皆會依據在功能安全開發生命週期中獲得的可用增量設計 (increment design) 資訊，在該週期中 (請參照圖 1) 逐步執行並更臻完善。

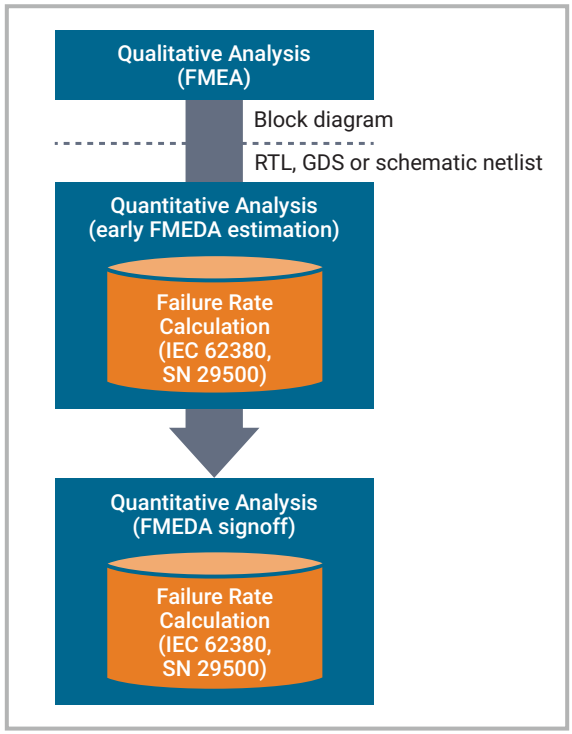


圖2 : 質化分析與量化分析

圖 2所示，在功能安全生命週期初期，通常會執行隨機故障的質化分析 (FMEA)，其中包括得以識別設計可能發生故障的方法。在此階段，僅提供方塊圖 (block diagram)，而功能安全專家則以此為基礎，根據功能描述將設計分成零件、子零件與 FM 三個安全等級。

隨著功能安全生命週期推進並生成 RTL 設計時，功能安全專家會執行初期量化分析以估算設計面積 (請參照圖 2)。此評估分析採用對應的穩定性標準 (SN 29500、IEC 62380、MIL-HDBK-217，或甚至是以操作經驗為基礎的企業資料庫)，對基本故障率 (設計故障概率) 進行初步估算。在此階段，故障模式分佈 (Failure Mode Distribution, FMD)，即故障模式的相對權重，也是基於著重在分析電路最重要的部分來計算的。

到了功能安全生命週期的最終階段，設計資訊已穩定，而且可以使用邏輯閘層網表(gate level netlist)。在這個階段，功能安全專家針對最終設計反覆進行量化分析(簽核)，進而在基本面積與計算基本故障率方面達到更高精準度。最後，將根據最終設計層級來劃分設計，並定義故障模式。

總結而言，功能安全專家會執行前述的三個階段分析，每個階段皆包含針對特定故障模式以及其與相應設計元件(故障根本原因)「關聯性」的分析。若要藉由加乘設計元件面積與基本故障率來計算故障概率，則必需這類分析。基本上，概率值的連接與計算過程會以佔用面積和技術類型為基礎，很大程度是手動且繁複的工作，且通常基於各種啟發式(heuristics)方法進行推論。此外，此類操作的複雜度會隨著設計繁複程度增加而擴展。而 EDA 工具對映射(mapping)自動化的支援，對於減少手動工作以及避免忽略錯誤等層面有著重要的作用。故障模式被定義之後，為了達到預期的穩健度，會將安全機制插入設計中，接著需要依據 ISO 26262 或專家判斷來推估診斷覆蓋率 (diagnostic coverage, DC)，然後採用專門的功能安全 (Functional Safety, FS) 驗證來證實有效性。功能安全專家會在更高的抽象層級(abstraction level) 定義 SoC 或 IP FMEA 與 FMEDA 所需考量的故障模式。在此更高的抽象層級中，無法透過概率假設或推斷「設計或實作期間可能發生錯誤的原因」直接得出故障模式。

有鑑於 SoC 設計複雜度持續增加，同時整體專案時程縮短，需要有效地利用晶片設計中獲得的見解，從編碼、程式碼分析和各種故障回應功能分析開始，藉由使用效能模擬將其作為進一步的安全分析輸入(input) 來源。

新思科技功能安全分析與功能驗證結合使用

上一章節強調，採用 Excel 試算表等傳統方法實現與追蹤 FMEDA，並不能有效擴展以符合現代 SoC 的繁複需求。而且，功能安全分析流程與 IC 設計流程無縫接軌的相容性，對縮短認證時間至關重要。最後，功能安全工程師還需要一個 FMEDA 持久性資料庫，以實現可追溯性分析、存取管理、稽核選項與版本控制。

新思科技 VC 功能安全管理器 (Synopsys VC Functional Safety Manager, FSM) 可實現功能安全管理自動化，取代與功能安全驗證流程不相容的試算表及 FMEDA 分析解決方案等傳統手動方式。VC FSM 扮演 FMEDA 分析的控制艙(cockpit)，推動整個半導體設計開發以實現功能安全，包括設計探索與分析、驗證和實作階段。

ISO 26262	RMS integration

• Native support of **IEC 62380** and **SN 29500** standards
• Compliant **Safety Reports**
• **Native tracking**:
  • Analysis
  • Safety Verification Plan
  • Linking with FI results
	• **Requirements importing** from RMS to keep track of safety requirements

System Complexity	**Automation**
• **Design extraction** in the analysis • Integration of **multiple FMEDAs** • **Design Data** information • **Server/Client** architecture • Analysis **Versioning**	• **SFF** allows integration with **Verification** tools • **SSF** allows integration with **Implementation** tools

圖3 : 新思科技 VC 功能安全管理器提供的關鍵區別

新思科技 VC FSM 在下列所述四大關鍵領域 (請參見圖 3) 為功能安全專家與工程師提供協助。

- ISO 26262 要求驗證與實作所使用的工具皆需經過認證。而新思科技 VC FSM TCL 1 已通過 ISO 26262-8 第 11 節認證，該技術體現了計算基本故障率所需的數學模型，以協助工程師持續追蹤擴展至故障注入措施(injection measure)的 FuSa 指標與分析。
- ISO 26262 要求啟用可追溯性 (traceability)。新思科技 VC FSM 與 JAMA 等主要需求管理系統 (requirement management systems, RMS) 相互通訊以匯入需求標準，例如：FMEDA 分析中的安全機制定義。
- 現代汽車設計涉及系統的高複雜度，需要能夠高度擴展的 SoC 層級 FMEDA 分析。新思科技 VC FSM 具有高度可擴展性，可因應不斷增加的 SoC設計複雜度。與 FMEDA 分析相關的連設計擷取，於安全分析過程中可產生連續性。該技術中嵌入了設計資料，可以推動故障模式的劃分與連接程序。
- SoC 層級 FMEDA 分析需要高水準的自動化技術。新思科技 VC FSM 使用新思科技驗證與實作技術進行資訊交換，將功能安全生命週期完全自動化。標準故障格式 (Standard Fault File, SFF) 用來與新思科技 VC Z01X 及新思科技 SpyGlass® Fault Analysis 等驗證工具交換故障模式定義和相應的觀察/檢測點。安全規範格式 (Safety Specification Format, SSF) 包含了實施特定安全機制需求 (例如：三重模組冗餘、雙重模組冗餘…)等安全意圖的定義，並與新思科技 Fusion Compiler™ 等實作工具進行通訊，自動化產生安全機制並納入設計中。

因求精簡，後續章節將涵蓋所有功能安全工程師都會面臨的三大關鍵層面，即設計資料擷取、安全機制有效性衡量，以及 SoC 層級的 IP 級別 FMEDA 整合。

設計資料擷取

新思科技 VC FSM 提供結構化、自動化 FMEA/FMEDA 分析的方法，在執行 FMEA/FMEDA 分析期間，透過 GUI 引導功能安全工程師使用預填式功能表與安全資訊，包括但不限於以下列所示：

- 符合 ISO 26262 的故障模式資料庫，可以用於定義故障模式文檔(text)。
- 設計資料瀏覽功能提供可擴展性方法，例如：摺疊階層(collapsing of hierarchies)、追蹤故障模式關聯性等，來處理繁複的設計。

新思科技 VC FSM 流程十分簡單明瞭。該解決方案扮演著驅動其他工具的控制艙(cockpit)，以實際設計資料與晶圓廠資料為依據，運用各種技術提供準確的元件故障指標。

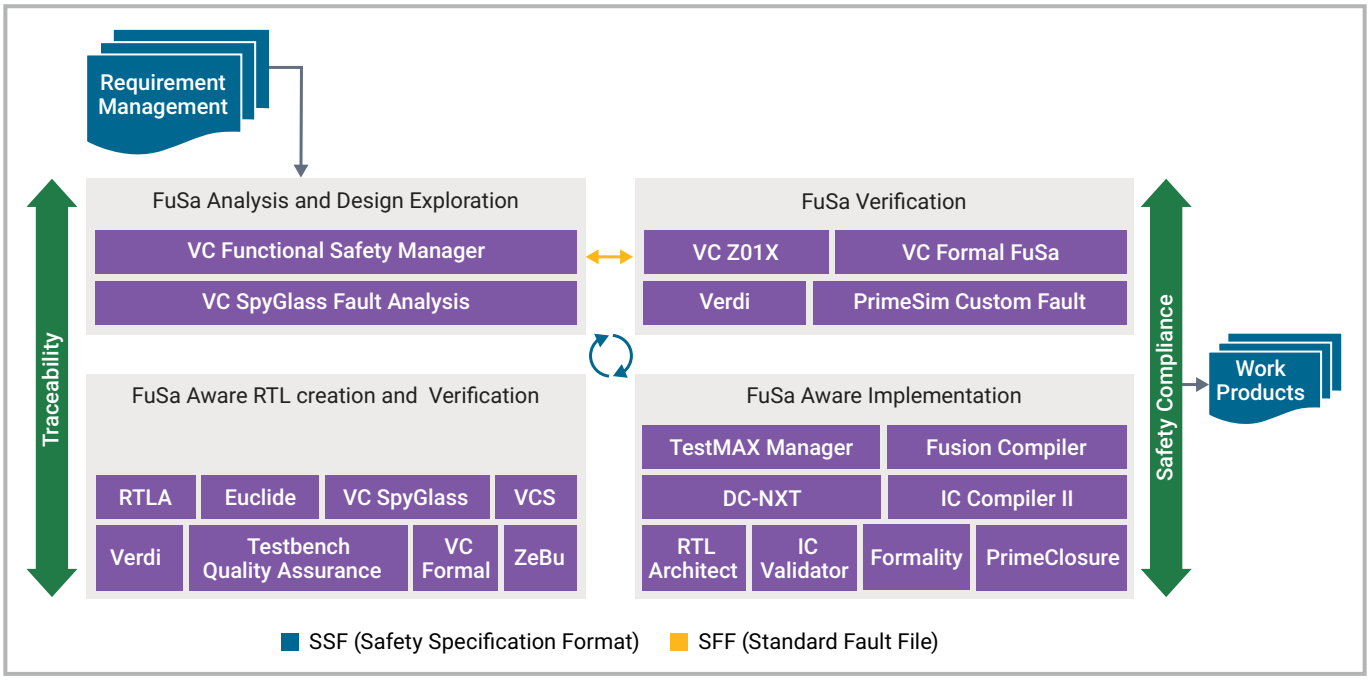


圖4 : 控制艙 (cockpit) 所需的新思科技工具

擷取設計資料可以由新思科技 VC FSM GUI 或 SFF 驅動。而新思科技 Fusion Compiler、SpyGlass 故障分析與 Verdi® 工具能夠根據分析的近似層級，擷取元件總數與面積等設計參數。在設計初期階段，工程師可使用新思科技 SpyGlass 故障分析，利用快速合成取得設計面積與故障模式分佈的初步評估。然後，等網表可以使用時，再運用新思科技 Verdi 取得精準且可設定的設計資料指標。

新思科技 VC FSM 結合永久性故障率和暫時性故障率等從晶圓廠取得的技術資料，或使用工具所整合的 IEC 62380 / SN29500 數學模型，以計算個別設計元件的基本故障率。該工具取得的 FMEA/ FMEDA 結果應直接匯出為一項 ISO 26262 工作成果(Excel 試算表)，且可以自動化地從子元件 FMEA 擷取所需的彙總計算 (aggregated calculation)，並用於建立元件 FMEA。

安全機制的有效性衡量

依據 ISO 26262 第 5 章，必須提供佐證以證明硬體架構設計適合用來偵測與控制安全相關的隨機硬體故障。在設計週期初期，會依據專家判斷以及基於歷史資訊、科學論文等資料歸納的建議實務，執行診斷覆蓋率評估 (FMEDA 估計值)。利用新思科技 SpyGlass 故障分析根據實際設計初步評估診斷覆蓋率，確認與專家判斷的結果之間是否有任何不正常偏差，並執行必要的設計更新。此外，功能安全工程師必須衡量與驗證設計中插入的安全機制有效性，確保設計的容錯能力。而安全機制有效性的量化，則是使用新思科技 Synopsys VC Z01X 故障模擬器的專用故障注入(fault injection)工作來完成的。如圖 4 所示，新思科技 VC FSM 透過 SFF 傳遞資訊，擷取需要驗證的故障模式，以及相應的觀察與檢測點。

針對 SFF 檔案中所指定的每個故障模式，使用新思科技 VC Z01X 執行故障活動和故障注入，以生成所需的測量結果，例如可靠且可以透過安全機制偵測的故障測量結果。故障注入工作結果可以透過新思科技 VC FSM 逆向讀取，來確認必要的「FMEDA 測量值 」。

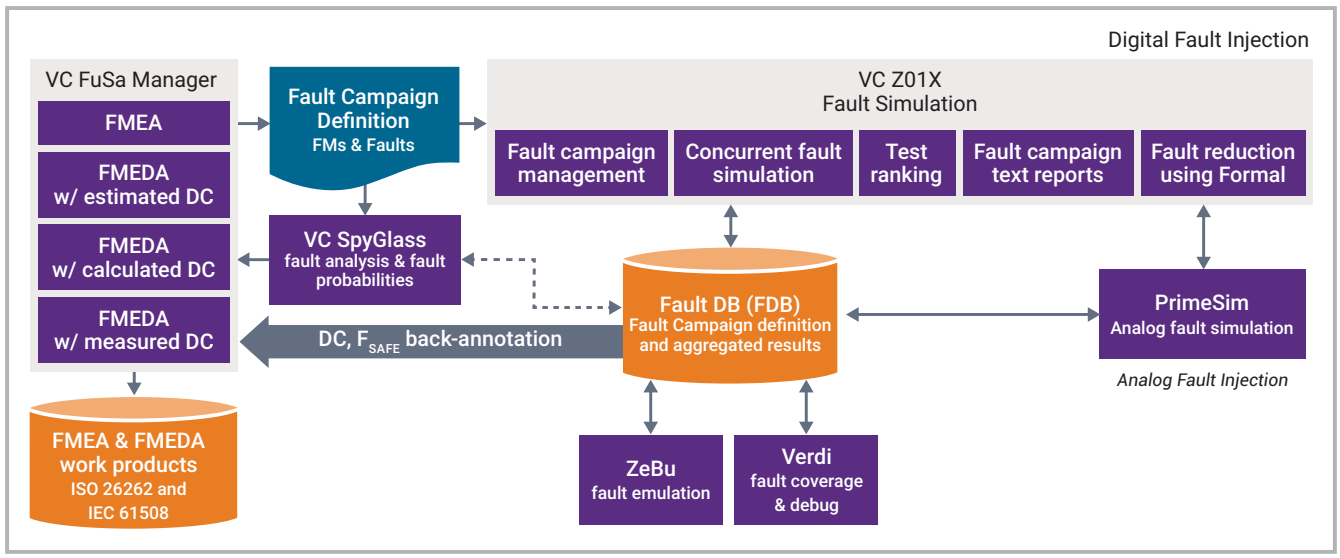


圖5 : 新思科技 VC 功能安全管理器，以及單一整合的 FuSa 驗證流程與新思科技 VC Z01X

圖 5 顯示了新思科技單一整合功能安全 (FuSa) 驗證平台的端到端流程，使用者在該平台描述了 SFF 中的故障活動定義。基本上，SFF 是一個擷取故障活動規範的文字檔案，像是使用者定義故障狀態 (如果有的話)、升級、分組、計算 (覆蓋率) 公式、觀察與檢測點以及故障定義。新思科技 VC Z01X 故障模擬器涵蓋了此種強大的故障活動規範方法。對於單一整合的故障平台而言，SFF 可以選擇性擴展，包含故障模式區塊 (適用於觀察點)與安全機制區塊 (適用於檢測點)。這讓 VC Z01X 故障注入引擎可以在 FuSa 驗證流程中，使用這些設計關鍵位置的單一規範，從而確保故障的統一鑑定條件(uniform qualification)。新思科技 VC Z01X 故障模擬器採用 SFF 中所定義的故障活動定義，並在 FDB 中建立定義的故障活動。此舉展開了所有故障位置，並優化故障活動。之後，如果無法使用新思科技 VC Z01X 進行測試，則會刪除故障，並將產生相同影響的故障合併在一起，進而避免重複 (duplication)。最後，使用新思科技 VC Z01X 執行所有分析和自動化，可以優化故障活動的定義，並產生最佳 (最小) 的故障組合以符合品質條件要求。

不同的故障鑑定引擎，例如用於故障模擬的新思科技 VC Z01X、減少形式故障的新思科技 VC Formal™ FuSa 應用程式以及用於故障硬體仿真 (emulation) 的新思科技 ZeBu® 等，利用故障資料庫 (fault database, FDB) 單一整合的故障活動定義，共同協助縮短整體 FuSa 驗證週期，接著執行後將故障結果回傳(back-annotation)至 FDB。在整個 FuSa 驗證週期中，透過單一流程推理(inference) 故障與故障狀態有助於大幅加速 FMEDA 分析與可追溯性。

在圖 5 擷取的整個 FuSa 驗證週期中，於各種故障條件引擎執行使用者識別故障活動後，取得了 FMEDA 最終測量結果，並將其回傳至新思科技 VC FSM，針對估計的 FMEDA 和測量的 FMEDA 進行比較。

從 IP 到 SoC皆整合 FMEDA

在一般汽車功能安全專案中，選擇適合在安全應用使用的元件和 IP 功能是關鍵步驟，確保安全需求與工作限制符合下列需求，在設計步驟中透過提高 IP 和 SoC FMEDA 自動化程度來改善 FMEDA 產能。

根據以下摘自 ISO 26262-11 的圖文，得出以 IP為基礎的設計及其在 SoC 整合的四大可能方法。

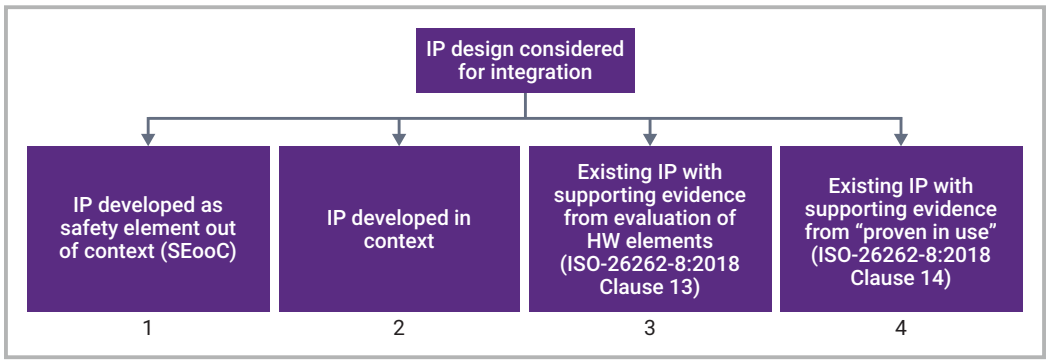
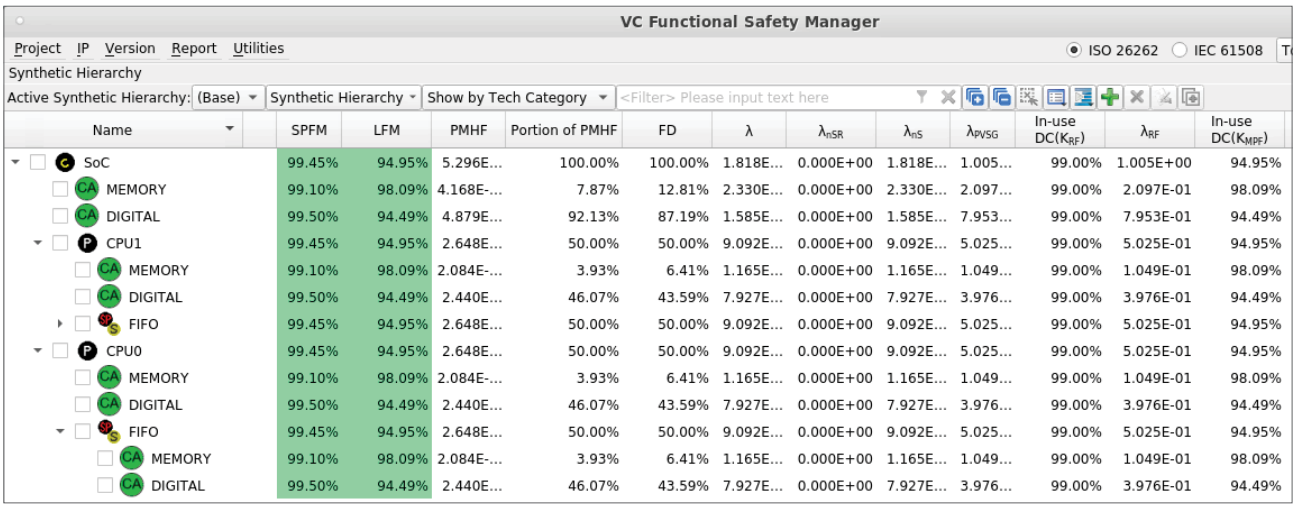


圖6 : 在安全相關設計中使用 IP 的可能方法 [ISO 26262 第 11 章]

若能夠立即存取已符合功能安全資格 (請參見圖 6 的案例 1 和 2) 的半導體資料、IP、開發流程和設計工具，可以顯著地加速整體 FuSa 產品開發流程，並減少對應的工作量。為了支援 FuSa 產品開發工作，新思科技 VC FSM 透過提供不同方法擷取和彙總 IP 層級 FMEDA 格式，支持整合 IP 層級 FMEDA (圖 6 的案例 1 和 2) (*) 作為 SoC 層級安全分析的一部份，包括：

- 以不同格式 (例如：CSV) 將個別 IP 的 FMEDA 自動化匯入新思科技 VC FSM。
- 使用合成層級 (參見圖 7) 整合 IP 的 FMEDA 與對應的安全指標計算。

*圖 6 的案例 3 和 4 是不符合 ISO 26262 的 IP，其中 FMEDA 無法使用，且應透過安全管理器採取額外措施。



Name	SPFM	LFM	PMHF	Portion of PMHF	FD	λ	λ_{nSR}	λ_{nS}	λ_{PVSG}	In-use DC(K_{RF})	λ_{RF}	In-use DC(K_{MPF})
SoC	99.45%	94.95%	5.296E...	100.00%	100.00%	1.818E...	0.000E+00	1.818E...	1.005...	99.00%	1.005E+00	94.95%
MEMORY	99.10%	98.09%	4.168E-...	7.87%	12.81%	2.330E...	0.000E+00	2.330E...	2.097...	99.00%	2.097E-01	98.09%
DIGITAL	99.50%	94.49%	4.879E...	92.13%	87.19%	1.585E...	0.000E+00	1.585E...	7.953...	99.00%	7.953E-01	94.49%
CPU1	99.45%	94.95%	2.648E...	50.00%	50.00%	9.092E...	0.000E+00	9.092E...	5.025...	99.00%	5.025E-01	94.95%
MEMORY	99.10%	98.09%	2.084E-...	3.93%	6.41%	1.165E...	0.000E+00	1.165E...	1.049...	99.00%	1.049E-01	98.09%
DIGITAL	99.50%	94.49%	2.440E...	46.07%	43.59%	7.927E...	0.000E+00	7.927E...	3.976...	99.00%	3.976E-01	94.49%
FIFO	99.45%	94.95%	2.648E...	50.00%	50.00%	9.092E...	0.000E+00	9.092E...	5.025...	99.00%	5.025E-01	94.95%
CPU0	99.45%	94.95%	2.648E...	50.00%	50.00%	9.092E...	0.000E+00	9.092E...	5.025...	99.00%	5.025E-01	94.95%
MEMORY	99.10%	98.09%	2.084E-...	3.93%	6.41%	1.165E...	0.000E+00	1.165E...	1.049...	99.00%	1.049E-01	98.09%
DIGITAL	99.50%	94.49%	2.440E...	46.07%	43.59%	7.927E...	0.000E+00	7.927E...	3.976...	99.00%	3.976E-01	94.49%
FIFO	99.45%	94.95%	2.648E...	50.00%	50.00%	9.092E...	0.000E+00	9.092E...	5.025...	99.00%	5.025E-01	94.95%
MEMORY	99.10%	98.09%	2.084E-...	3.93%	6.41%	1.165E...	0.000E+00	1.165E...	1.049...	99.00%	1.049E-01	98.09%
DIGITAL	99.50%	94.49%	2.440E...	46.07%	43.59%	7.927E...	0.000E+00	7.927E...	3.976...	99.00%	3.976E-01	94.49%

圖7 : 新思科技 VC 功能安全管理器合成層級檢視

如圖 7 所示，合成層級樹狀結構顯示了累積的 IP 設計指標與生成的 SoC 層級 SPFM 和 LFM 指標。此可操作檢視讓使用者得以處理合成檢視中的多個 IP 層級 FMEDA，不僅簡化了計算整體安全指標，甚至在涉及諸多設定版本的 SoC 情況下，也能夠簡化相同 IP 的多個執行個體 (instance) 或相同 IP 不同 FMEDA 設定的管理。

總結

因應減少碳排放並降低事故風險，提升汽車電氣化程度以及改善自動駕駛功能，汽車設計的複雜度也隨之提高。這促成了 FuSa 驗證技術與方法論的革新，進而加速安全關鍵 (safety-critical) 設計的開發與驗證速度。

傳統安全分析方法以 Excel 試算表為基礎，無法擴展以處理現代 SoC 的複雜度，包括數以千計的故障模式。於FMEDA 分析與探索期間，使用新思科技 VC 功能安全管理器無縫接軌地推動設計開發，接著採用橫跨整個功能安全生命週期的驗證與實作技術，將有助於簡化實現 ISO 26262 認證資格的過程，同時也不會對測試周轉時間產生任何重大壓力。將故障模式分佈等繁複工作流程自動化，可以減少出錯，並滿足功能安全專家的三大需求，即自動擷取資料設計、衡量安全機制有效性，以及無縫接軌整合可設定 IP 層級 FMEDA，以取得最終 FMEDA。此文章概述之 FuSa 方法與流程完全符合 ISO 26262，從而使終端用戶能夠藉由遍及 IP 與 SoC 功能安全生命週期的安全分析可追溯性，高效率地取得 ISO 26262 認證。