使用先進故障模擬技術，確保功能性安全

作者

Rimpy Chugh
資深產品行銷經理

Kirankumar Karanam
主任應用工程師

簡介

在現代生活中，有許多晶片設計應用於攸關安全的領域，而這些領域是絕對不容許在現場操作中發生有害安全的情況。該類應用程式必須在功能上是符合安全的，以便能偵測到故障並採取更正措施。ISO 26262 等功能性安全標準需要設計團隊評估實地應用時出現故障的影響，並確保該設計能做出適當的回應。採用故障模擬(fault simulation)技術是最有效率並可在設計最初階段進行評估的方式，但傳統方法和工具無法有效擴展以滿足這些標準的要求。本白皮書將揭示一個功能更強大、更全方位的解決方案，可將功能驗證(functional verification)和故障模擬整合至單一流程中，即使是針對最大型的系統單晶片(SoC)設計，也能滿足其功能性安全需求。

背景

攸關安全的應用必須確保在實地應用時發生的故障不會導致系統等級的錯誤，或發生嚴重後果的不安全行為。發生故障的心律調節器可能會造成患者死亡；核電廠安全系統錯誤更會導致數百萬人死傷。圖 1 顯示包括汽車等數個關乎安全應用的範例。先進駕駛輔助系統(ADAS)技術和自動駕駛等電子產品的重要性日益增加，伴隨而來的是安全性挑戰。設計團隊必須運用適當的功能安全設計來避免任何 SoC 故障，排除任何導致汽車偏離駕駛軌道的可能性。若因為半導體老化(aging)效應或 α粒子(alpha particle)撞擊造成汽車晶片故障，系統必須能夠偵測故障並採取適當更正措施。這可能會需要透過系統重設進行故障修復、使用修正錯誤的方法來抵銷故障或讓車輛能安全的停止下來。

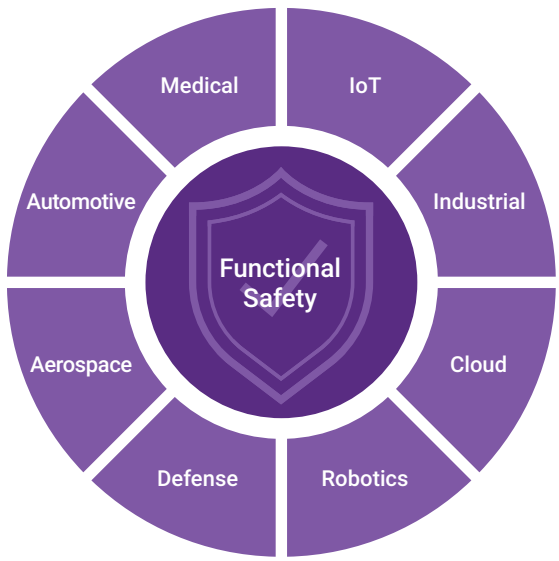

圖1 : 攸關安全的應用範例

大部分攸關安全的應用都需要遵循功能安全標準嚴格且強制的要求，例如降低硬體故障可能性、在故障發生時偵測到故障、修正錯誤或讓系統進入安全狀態等。這些標準包括用於道路交通工具(包括汽車)的 ISO 26262 和用於一般工業安全的 IEC 61508。「安全機制」一詞意指增加可用於偵測和回應故障的硬體或軟體。為符合功能安全標準，也要求對安全機制作業情況進行量化評估。事實證明，傳統上用於衡量晶片製造測試效率的故障模擬，也是一種用於評估和確保功能安全的自動化、且功能強大的方法。

故障模擬可用來模擬實地故障(field failure)和製造瑕疵，並檢查在發生危險故障情況時是否能採取正確的措施。然而，還有一些傳統故障模擬器無法滿足功能安全需求的原因。在故障模擬時注入(inject)的故障可能不同於用來對製造進行測試的故障，但使用者不希望手動指定這些故障。他們也不想要對結果進行說明，或依據這些結果手動計算功能安全標準所要求的故障模式與影響分析(FMEA)以及故障模式、影響和診斷分析(FMEDA)。

此外，傳統故障模擬器的功能遠不如用於功能驗證的模擬器，因為它們只執行硬體設計，沒有測試工作台(testbench)的概念。故障模擬測試必須從功能驗證流程中費力擷取，且通常需要人工手動操作。從龐大的迴歸(regression)套件中選擇正確的測試非常困難，而且可能需要大量反覆試驗，嘗試錯誤。由於故障模擬和功能驗證測試流程兩者是分開的，當故障模擬找到一些未被偵測到的故障時，要透過加入更多功能驗證測試來強化覆蓋率就變得具有挑戰性。因此，不僅故障覆蓋率收斂(coverage closure)難以實現，也難以達到功能安全標準的要求。再者，傳統故障模擬器也沒有軟體概念，而對於SoC而言，可能的故障情況和採行的修正措施通常同時涉及硬體和軟體。顯而易見地，故障模擬需要更好的解決方案。

集結功能驗證和故障模擬的整合流程

解決前一章節所提出的問題和挑戰的最佳方式是將功能驗證和故障模擬整合到單一流程中。有鑑於使用單點工具是不可能達成設計目標，因此解決方案必須從一開始就使用通用的模擬平台進行設計。此舉帶來許多優勢。故障模擬可以使用從功能模擬中，透過波形檔案擷取的測試來執行，或使用與功能模擬相同的反應測試工作台來進行模擬。這代表故障模擬器必須支援 SystemVerilog 驗證結構、通用驗證方法(Universal Verification Methodology，UVM)，以及PLI 和 C/C++ 等程式語言介面。

功能模擬和故障模擬可使用相同設定，以減少從一個模擬器轉換到另一個模擬器所需的工作和耗費的時間。由於對輸入語言的不同解釋、競態條件(race condition)以及模擬代碼中評估的順序不一致，切換模擬器一般也意味著將造成發散(錯誤配置)的結果。然而，單一的整合流程可以消弭前述所有問題，讓功能驗證順利轉移至故障模擬。整合平台也能確保設計和驗證 IP (Verification IP, VIP)、檔案格式、除錯(debug)以及模擬器周邊工具生態系統的共通性。

為了在晶片開發專案早期階段獲得故障覆蓋率的參考指標(indication)，並解決那些使覆蓋率收斂變得困難的問題，必須能夠在暫存器傳輸邏輯(RTL)執行故障模擬。簽核故障覆蓋通常使用設計的閘級網表(gate-level netlist)執行，其中用於該設計的故障模型和故障指標比用於 RTL 的更精確。統一的流程還能讓這些轉換更容易，因為從 RTL 移到閘級模擬(gate-level simulation, GLS)傳統上會導致錯誤匹配(mismatch)結果。對於在通用的平台上執行的相同測試而言，出現的任何訊號競爭或其他問題都是必須要解決的設計問題，而非肇因於使用不同模擬器所產生的假像(artifacts)。相同的偵錯工具可用於RTL模擬和GLS模擬，無論兩者的結果是從功能模擬或故障模擬產出的。

現代高效的故障模擬解決方案也需提供適合先進開發流程的高水準支援。該解決方案必須能夠管理在ISO 26262 等標準中明確規範的故障項目(fault campaign)，包括將故障注入至模擬中。還必須能夠在運算伺服器叢集(compute grid)或雲端同步執行故障模擬，藉由靈活和動態的作業排程，在給定的可用運算資源下盡快完成整套模擬作業。最後，故障模擬流程必須連接至整個功能安全基礎架構。並依據 ISO 26262的要求，將故障指標標註到 FMEDA 中，以符合汽車安全完整性等級(ASIL)分類。此外，需求規畫和系統管理工具也需要連結至該架構。

新思科技故障模擬解決方案

領先業界的新思科技 VC Z01X 新一代故障模擬器可以滿足上一章節中列出的所有需求。VC Z01X提供數位故障注入(digital fault injection)，並利用新思科技 VCS 模擬引擎(用於 RTL 和 GLS 功能模擬的黃金標準)，實現同步故障模擬演算法。這個共用模擬平台確保使用者得以在最低限度變更設定、設計或測試工作台代碼或偵錯方法的情況下，從功能模擬轉移至故障模擬。如圖 2 所示，新思科技 VC Z01X 是新思科技統整為一的功能安全(FuSa)驗證平台關鍵元素之一。該平台讓涉及功能安全的新思科技產品能夠在中央故障資料庫(fault database，FDB)進行溝通。

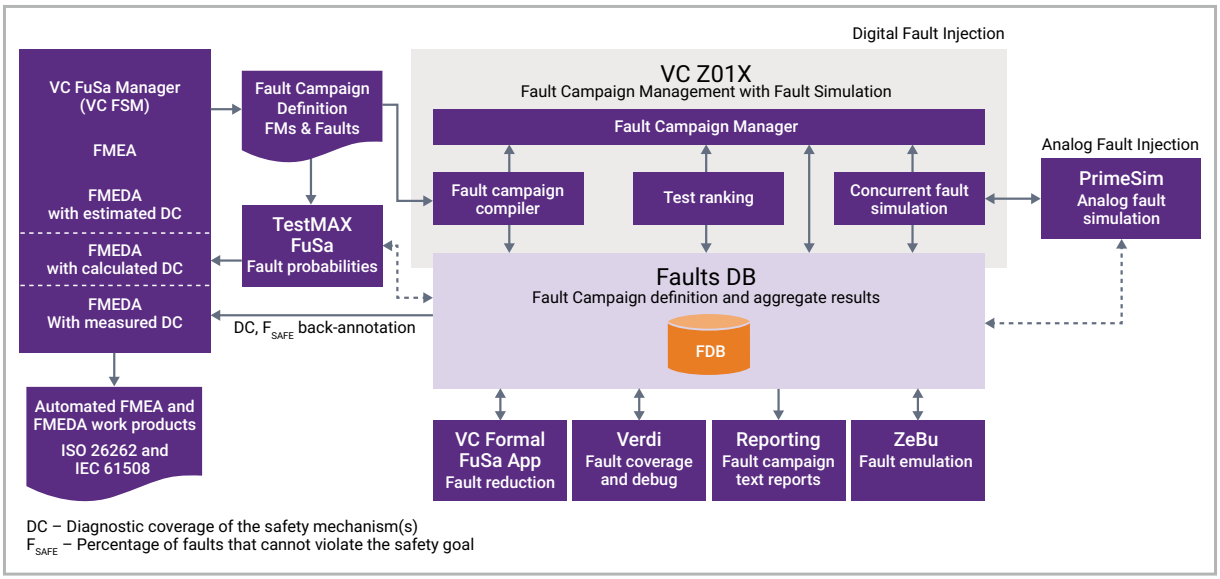

圖2 : 新思科技統整為一的功能性安全(FuSa)驗證平台

FDB 在資料庫中定義故障位置、類型和狀態，所有工具都可以完全掌握這些內容並獨立作業，同時加以利用其他已完成個別故障分析的結果。每個工具都為最終的 FMEDA 提供測量診斷覆蓋率，並且可以視需要插入(plug into)流程，以解決功能性安全驗證各方面需求。

除了新思科技 VC Z01X，這些工具還包括：

- 新思科技VC功能安全管理器(FSM)，用以建立、管理和回報FMEA 和 FMEDA 指標
- 新思科技TestMAX FuSa，用於計算 ISO 26262 硬體隨機故障指標(PMHF)，進行故障機率靜態分析
- 新思科技PrimeSim CustomFault，用於類比(analog)故障模擬
- 新思科技VC Formal功能安全應用程式，用於減少故障和識別安全無害的故障
- 新思科技 ZeBu模擬系統，用於模擬長時間執行測試和大型SoC設計仿真(emulation)
- 新思科技 Verdi 故障分析，可加速故障覆蓋收斂(coverage closure)

圖 3 顯示從 VCS 為主的功能驗證環境轉換為故障模擬所需的步驟。新思科技 VC Z01X 及其故障項目管理(FCM)協調整個支援流程，可生成故障、執行動態可測試性分析、執行故障模擬和建立報告。標示為綠色的步驟可以透過手動建立檔案，或使用 VC Functional Safety Manager解決方案來自動建立標準故障格式(SFF)的故障項目定義檔案和為FMEDA結果進行註解與說明。

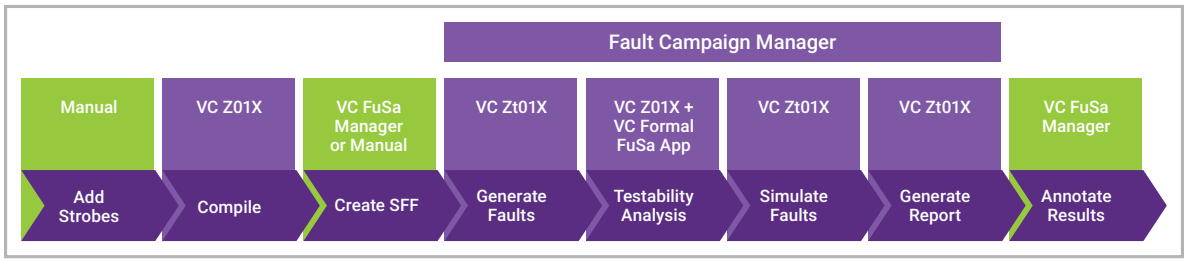

圖3 : 從功能驗證順利轉換至故障模擬

首先是定義三件事：新思科技 VC Z01X 應在每次模擬中注入故障的時間，以及何時、何地針對注入故障的故障機器(faulty machine, FM)模擬與良好機器(good machine)參考(無故障)模擬進行比較。在功能安全模擬中，strobing通常分為兩部分，一部分用於標記已觀察到的故障，另一部分用於標記被安全機制檢測到的故障。故障注入通常發生在Time 0，但使用者可以依需求在strobe文件檔中指定延遲。觀察點和偵測點可以在strobe檔中完成靜態定義或由 SFF 檔案讀取。一旦strobe定義完成，新思科技 VC Z01X 就可以編譯設計。設定程序和 VCS 的設定相同，只是新增strobe檔和一些參數(argument)。將 SFF 檔案用於動態定義的觀察點和檢測點，可以在不需要重新編譯的情況下，執行具有不同比較位置的多個故障模擬。

定義strobe points並編譯設計後，使用者使用 SFF 定義「故障範圍(fault universe)」，以指定模擬期間要注入故障的位置和標記。SFF 檔案可以由 FSM 自動產生，或手動建立文字檔。此外，SFF 檔案也定義了要注入的故障類型，並允許排除特定的設計區塊。由於這些故障不會影響設計執行，VC Formal FuSa 應用程式將結構化、可控制性和可檢視性分析應用於故障清單，減少等效故障(equivalent faults)並消除原本就有的安全故障。此舉不僅減少了故障數量，也讓故障模擬更加有效率。

在此階段，使用者在 FCM控制台中可以配置並執行新思科技 VC Z01X來進行故障模擬，包括作業啟動和網格/雲端互動等。FCM可支援同步故障模擬，讓多個注入故障在單一作業中一起執行；這個功能是讓新思科技 VC Z01X 具有無與倫比性能的關鍵。FCM 也支援序列故障(serial fault)模擬，讓個別FM在注入單一故障的模擬作業中獨立運作，並涵蓋不適合採用同步故障模擬的結構來增加覆蓋範圍。

一旦完成故障模擬並取得覆蓋率結果，必須將資料記錄下來以用於 FMEDA 計算。儘管可以手動完成記錄，但手動轉譯結果耗時費力，同時可能會產生人為錯誤的可能性。如圖 4 所示，可以使用FSM 自動化執行資料記錄的步驟，不但能自動匯入結果也能自動更新各項 FMEDA 指標。這些結果可用於計算該裝置的整體故障率，以符合 ISO 26262 的 ASIL 分級。

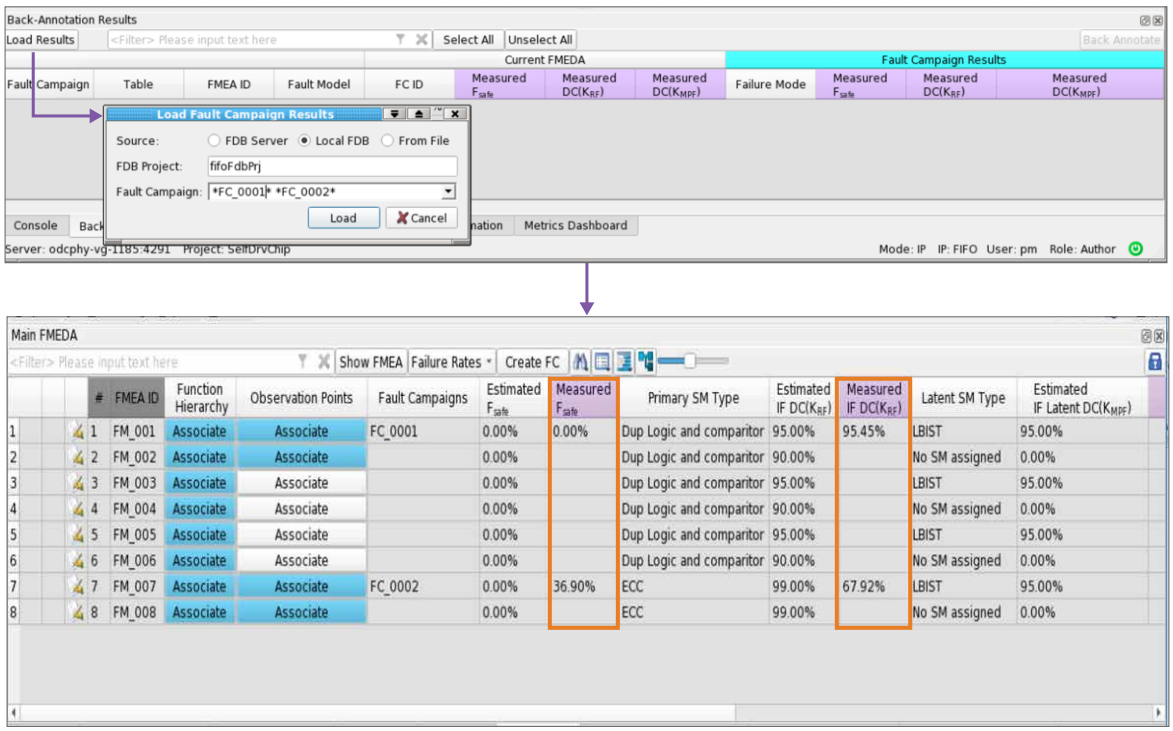

圖4：使用「新思科技 VC 功能安全管理」計算 FMEDA

實現故障覆蓋率收斂

故障覆蓋率與其他覆蓋指標一樣，不會在模擬結束時立即產生，而是需要結合手動和自動分析來識別遺漏的覆蓋範圍，並判定如何彌補這些差距。如圖 5 所示，新思科技 FuSa 平台中的 Verdi 故障分析系統可以簡化此流程。Verdi 故障分析使用與其餘流程相同的 FDB，因此與故障模擬的結果直接相關。可協助使用者視覺化故障覆蓋率，並包含整合式偵錯工具以識別設計中可以作為改進目標的低覆蓋率位置。Verdi 故障分析可以：

- 逐塊(block-by-block) 交互顯示故障覆蓋率
- 自動轉儲(dump)和檢閱具有已標註故障狀態之個別故障波形、原始程式碼和原理圖(schematics)
- GM和FM結果之間波形不匹配(mismatch)說明及偵錯
- 為錯誤配置波形提供追蹤功能

Verdi 故障分析建置於業界領先的Verdi模擬偵錯平台，因此也得以利用Verdi偵錯系統具有的所有強大功能。

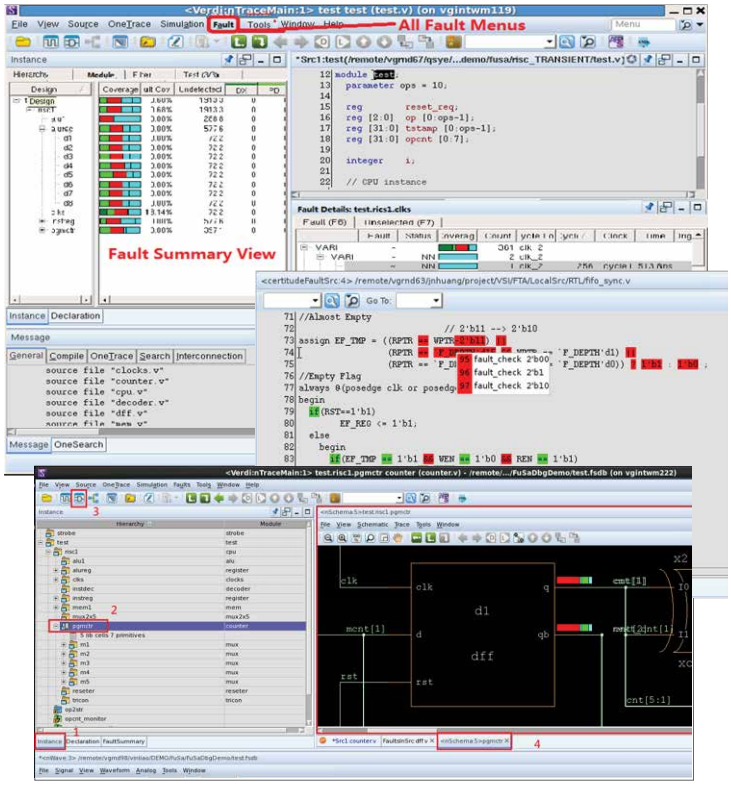

圖5 : 使用「新思科技 Verdi 故障分析」進行故障覆蓋率收斂

故障覆蓋率收斂需要識別在故障模擬中執行的其他測試。在選擇用於故障模擬的測試時，最好選擇能有效提高整體設計故障覆蓋率的測試目標。一種方法是在模擬時，選擇更活躍的測試和測試工作台。在減少動態故障期間進行分析測試時，判定故障可控制性和可檢視性的關鍵指標之一是故障和選通位置之間發生的活動。過往經驗顯示，透過更高的切換計數(toggle count)來衡量，具有高活性的測試工作台會更活躍，有助於更輕易地讓故障播及到可以偵測到它們的位置。高切換覆蓋率不能保證產生高故障覆蓋率，但它是一個實用的指南，有助於選擇要考慮進行故障模擬的功能測試。圖 6 顯示前述功能使用Verdi 故障分析運作的方式。

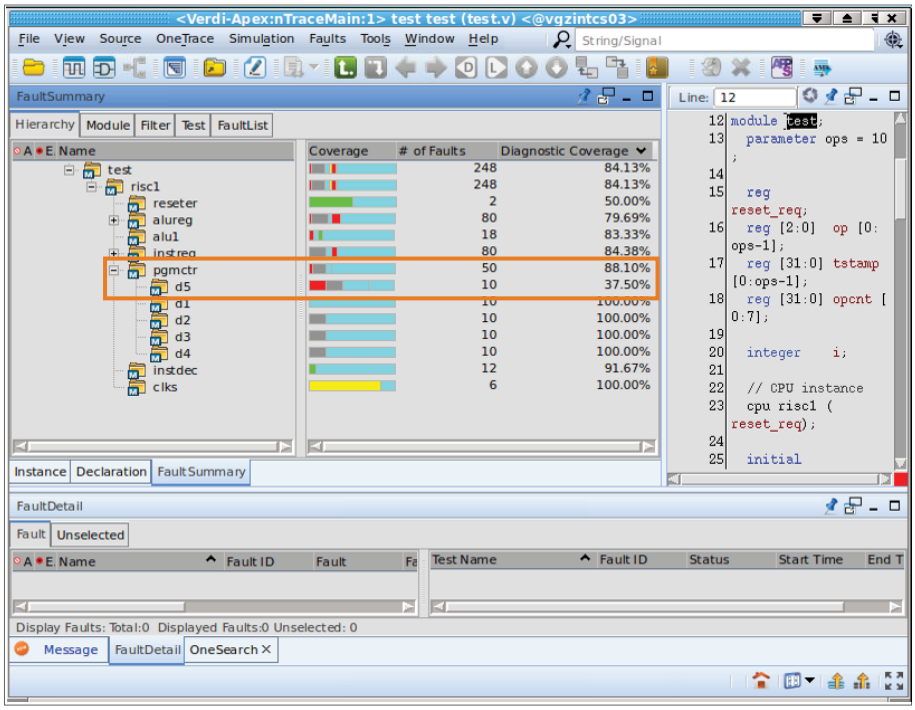

圖6 : 運用新思科技 Verdi 故障分析檢查故障覆蓋率

另一種加快故障覆蓋率收斂的方式是專注於識別「高數值」故障。如圖 7 所示，可依據可檢視性或可控制性對未涵蓋的故障進行排序。這讓使用者得以識別阻礙故障可能被偵測到的位置，並專注在那些於疏通情況下有助於故障覆蓋率的功能區域。使用 Verdi 結合活動測量、故障分類排序、可視化以及故障覆蓋率和行為的交互式檢閱等技術，可增加自動化程度，並大幅改善透過繁瑣手動分析仍未能發現的故障，以提高覆蓋率。

```
FaultList
{
    ### Location: test.risc1.instreg.d2.q_
    ## Number of Prime Faults: 100
    ## Number of Total Faults: 100
    NC 0 {VARI "test.risc1.alu1.alu_out[7]"}
    . . .
    # Test: 1, 2
    ### Location: test.risc1.alureg.d8.q_
    ## Number of Prime Faults: 78
    ## Number of Total Faults: 86
    NC 0 {PORT "test.risc1.alureg.d8.d"}
    . . .
    # Test: 1, 2
    ### Location: test.risc1.accum[7]
    ## Number of Prime Faults: 10
    ## Number of Total Faults: 10
    NC 0 {PORT "test.risc1.alureg.d8.q"}
    . . .
    # Test: 1, 2
```

圖7 : 依據可控制性排序未涵蓋的故障

總結

故障模擬於開發晶片製造測試中的傳統作用已經擴展到其他同樣關鍵的領域。它在晶片開發過程中有助於確保驗證方法足夠強大，以擷取所有設計錯誤。ISO 26262 等功能安全標準的嚴格要求，需要故障模擬來證明安全機制可以在實地應用時偵測到故障，以便採取修正措施。然而，傳統故障模擬工具已經無法滿足現今龐大 SoC 設計的要求。

新思科技 VC Z01X 提供集結功能驗證和故障模擬的單一流程解決方案。將故障模擬功能延伸至 VCS，僅需要對驗證設定和指令碼進行最低限度的變更，並重複使用現有的測試工作台；為負責功能安全的專業人士提供一項高效的故障模擬解決方案。新思科技 VC Z01X 的同步(concurrent)模擬功能搭配新思科技 Verdi 故障分析的視覺化效果和偵錯功能，將加速實現覆蓋率收斂。而切換覆蓋、功能覆蓋定位和尋找高價值故障等技術，可進一步幫助快速收斂覆蓋率差距；有助於縮短上市時程、執行高效製造測試，造就最適合攸關安全應用的晶片。