出國報告（出國類別：其他）

赴大陸上海參加第二屆德國萊茵 TUV 集團功能安全中國峰會，及順道參訪核能相關單位等。

服務機關：核能研究所
姓名職稱：徐獻星　研究員
派赴國家：大陸
出國期間：104 年 10 月 18 日~104 年 10 月 24 日
報告日期：104 年 12 月 2 日

摘 要

核研所徐獻星研究員此行赴大陸上海參加第二屆功能安全-核能及工業峰會，並順道參訪德國萊因 TÜV 集團大中華地區總部、台塑寧波石化廠、以及大亞灣核電廠，進行技術交流，並討論合作機會。

參加第二屆功能安全-核能及工業峰會，除參與技術研討會，瞭解功能安全最新的法規要求及技術發展外，徐員主要著重於國際間最新之功能安全平台與核研所開發之 SCS-2000 功能安全平台性能比較，並透過此機會，檢視核研所現有軟體驗證與確認(Software Verification and Validation, SV&V)發展工具及方法，與國際間功能安全技術廠家所使用工具及方法之優缺點比較。

參訪台塑寧波石化廠之行，最主要目的為瞭解核研所與台塑公司合作開發之整合性控制與安全系統監控介面應用經驗，以及後續因應大陸新制定之加強化工安全的趨勢，討論降低 SCS-2000 安全系統的製造成本，以增加競爭力。

訪問大亞灣核電廠，係回應該廠之邀請，交流核電廠老化管理相關工作經驗，此行可瞭解大陸之核電廠老化管理技術才在萌芽階段，而我們已累積長足之經驗，可考慮於大陸有此技術需求時，循兩岸技術交流相關規定，規劃有益雙方之工作交流項目。

目　錄

一、目的

此行核研所徐獻星研究員赴大陸上海參加第二屆功能安全-核能及工業峰會，瞭解中國大陸功能安全發展現狀與展望、軟體驗證與確認(Software Verification and Validation, SV&V)在功能安全的應用、以及功能安全在核能工業的應用，掌握最新技術及研發方向，可對國內日後的功能安全及核能技術研發策略進行規劃。此行並順道參訪德國萊因 TÜV 集團大中華地區總部、台灣塑膠公司寧波石化廠之電子專案組、以及大亞灣核電廠，進行技術交流與討論合作機會。此出國報告分段敘述上述行程之討論過程，以及心得與建議。

二、過程

(一) 104/10/18

徐獻星搭機由台北前往大陸上海。

(二) 104/10/19~104/10/20

徐員參加第二屆功能安全-核能及工業峰會，並參訪德國萊因 TÜV 集團大中華地區總部。

(三) 104/10/21

徐員搭動車由上海轉往寧波。

(四) 104/10/22

徐員參訪台塑寧波石化廠，搭機由寧波轉往深圳。

(五) 104/10/23

徐員參訪大亞灣核電廠。

(六) 104/10/24

徐員回程，返回台北。

三、心得

(一) 參加第二屆功能安全-核能及工業峰會

徐員此行參加德國萊因 TÜV 集團舉辦之第二屆功能安全-核能及工業峰會，瞭解中國大陸功能安全發展現狀與展望、軟體驗證與確認在功能安全領域的應用、以及功能安全在核能工業的應用。為期 2 天的會議議程如下：所有研討會論文皆以電子檔方式上傳於雲端，由與會人士自行下載，網址為：http://www.tuvasi.com/de/component/content/article/214

10 月 19 日(Day1)

1. 開幕
2. 中國核電發展現狀與展望
3. 功能安全和軟體驗證與確認在核電中的應用
4. 功能安全－在核工業中的應用
5. 修訂後的中國國標 GB/T21109 內的技術要求
6. IEC 61511 標準新的變化
7. 功能安全管理
8. 功能安全和資訊安全之間的關係
9. 工業控制系統中功能安全和資訊安全的結合
10. 網路安全分析中之 I&C (Instrumentation and Control)建模
11. 在風險管理之後的安全儀表功能設計
12. 更為嚴格的方法－LOPA (Layer of Protection Analysis)

10 月 20 日(Day2)

1. 驅動系統、閥門、和鐳射系統的功能安全
2. 功能安全和資訊安全認證流程
3. 工業製程中 SIL3 (Safety Integrity Level, SIL)的安全控制系統的開發－總結和經驗
4. 功能安全管理－對客戶和公司的好處
5. 功能安全－在過程工業中的應用

6. 滿足功能安全要求的應用工程
7. 基於 SIS (Safety Instrument System)安全生命週期的完整性管理
8. 為核電廠正常運行和安全儀表系統建造的保護系統設備
9. 對核電廠儀控系統危害分析要求的比較
10. 基於現場可編程邏輯閘陣列(FPGA)之安全設計

功能安全和資訊已經成為工業自動化中重要的發展項目之一。德國萊因 TÜV 集團之功能安全專家團隊於大陸上海舉辦第二屆功能安全-核能及工業峰會，主要目的是促進功能安全之相關計畫、生產、運轉、測試、及評估等領域人員之經驗和知識交流。

峰會同時展覽最新功能安全平台與系統之動態和發展趨勢，與核研所先前發展經驗及未來研發方向有關之項目，摘要如下：

1. NASPIC 之功能安全平台

中國核動力研究設計院(以下簡稱核動力院)隸屬於中國核工業集團公司，自 1965 年以來，是中國唯一具備核反應爐工程研究、設計、試驗、和運行的大型綜合性研究單位。

NASPIC (Nuclear Advanced Safety Platform of I&C)是由核動力院自主開發的核電安全級 DCS (Distributed Control System)平台，主要包括：現場控制站、安全顯示站、網路閘道、工程師站等，提供完整的核電廠安全級 DCS 系統設備整合解決方案。

NASPIC 平台採用 ARM (Advanced RISC Machine)系列微處理器、及高速串列匯流排等數位技術，可以依據用戶對系統整體可靠性的要求進行彈性地配置,包括單控制器模式、主從控制器模式、及 1oo2D (One out of two, Dual)模式等，如圖 1 所示。

NASPIC 平台於 2015 年初，以大陸華龍一號核電廠反應爐保護系統 2oo4 (Two out of Four)應用為基礎，透過 TÜV SÜD 依據 IEC 61508 等相關功能安全的要求，進行認證，通過一系列嚴格的認證標準審查，並取得 IEC 61508 SIL3 等級認證證書。

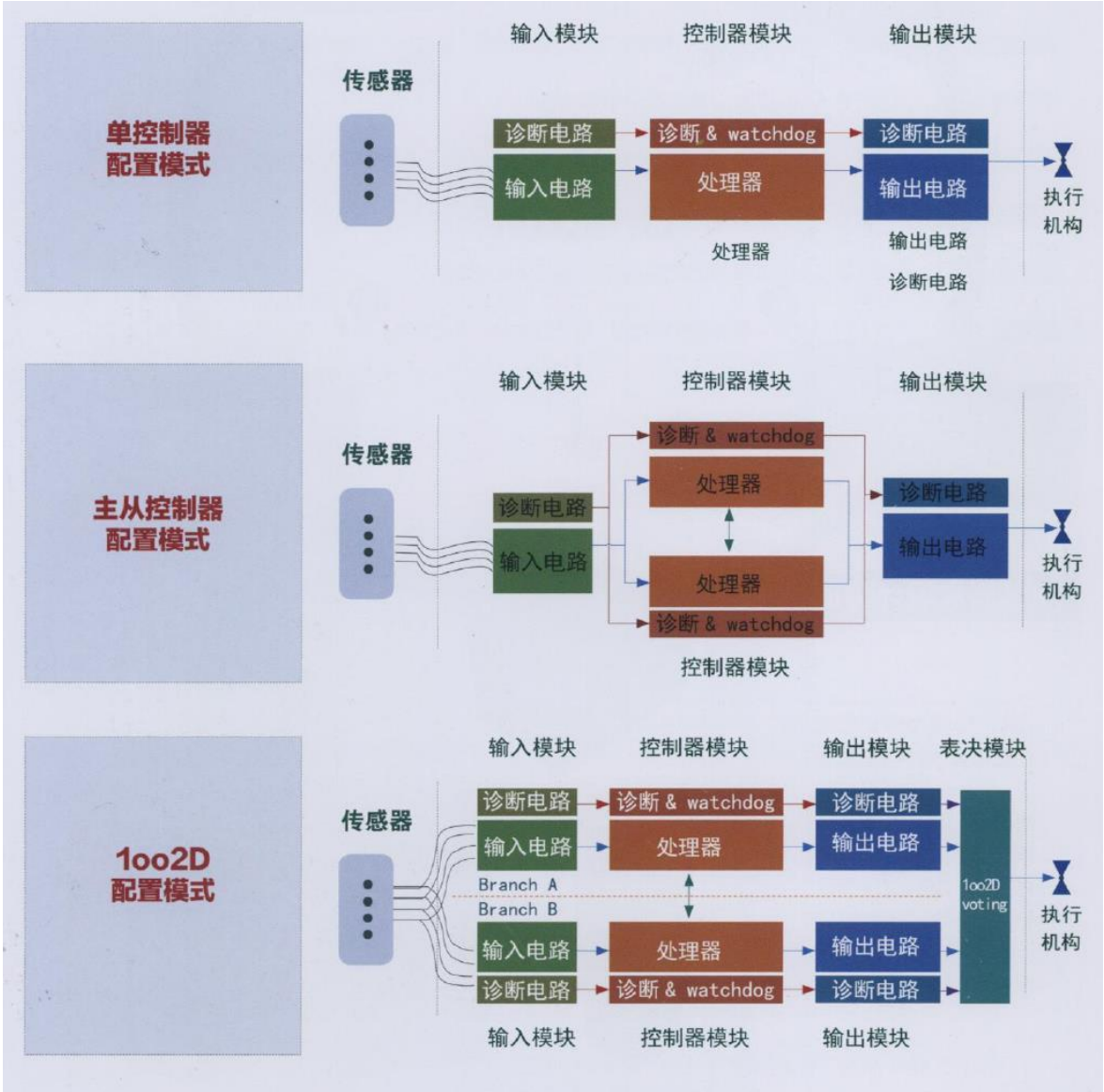

圖 1. NASPIC 平台可配置模式

2. ProSafe-RS 之功能安全平台

橫河電機(YOKOGAWA)在日本已有近百年的悠久歷史，為全球工業自動化產業的主要供應商及技術先驅之一，在全球 32 個國家設有近 90 個服務據點，提供客戶多元化產品及服務。

ProSafe-RS 是橫河電機的 SIL3 安全控制器，採用獨特的泛用模組備援(Versatile Modular Redundant, VMR)結構，除了每個模組內採用備援結構外(即符合 SIL3 之 1oo2D 架構)，這些模組本身也支援備援組態。這種結構可同時具備最大的安全性和可用性，且相對獨立，互不影響。這種彈性的系統組態可以以模組為基礎進行配置，實現每個系

統部件的高可用性，實現更高強健性(Robustness)，即使在輸入故障、CPU 故障、輸出故障等情況下仍可保持 SIL3 的安全等級。與完全依賴備援來實現安全性和可用性的系統不同，VMR 既沒有降級模式，也沒有該模式下的時間限制，如圖 2 所示。

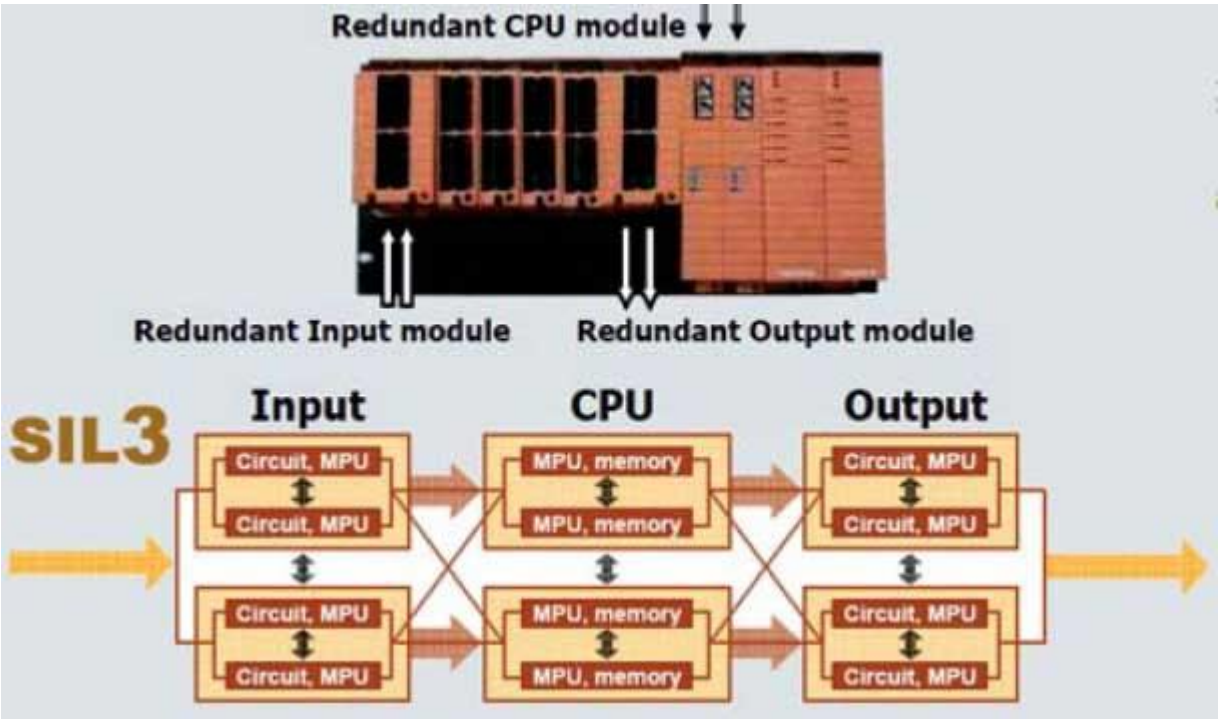

圖 2. 泛用模組備援(Versatile Modular Redundancy, VMR)結構

由於橫河電機在工業自動化領域的長期經驗，考慮所有安全回路都需要快速反應，故 ProSafe-RS 具備 50ms 快速執行安全邏輯的能力。(目前文獻蒐尋結果，以全球而言，美國 RTP 公司的 RTP3000 安全控制平台之反應時間最快，約 12-16ms)

另外，ProSafe-RS 採用鏈型或星型拓撲的 I/O 模組的連接組態，最遠控制器與遠端 I/O 模組可相距 50km，有效地降低系統硬體成本和維護成本，透過專用 Vnet/IP 通訊協定，可與橫河電機的 DCS (CENTUM)、SCADA 系統(FAST/TOOLS)、和資產管理系統(PRM)無縫整合，實現更有彈性的系統組態，如圖 3 所示。

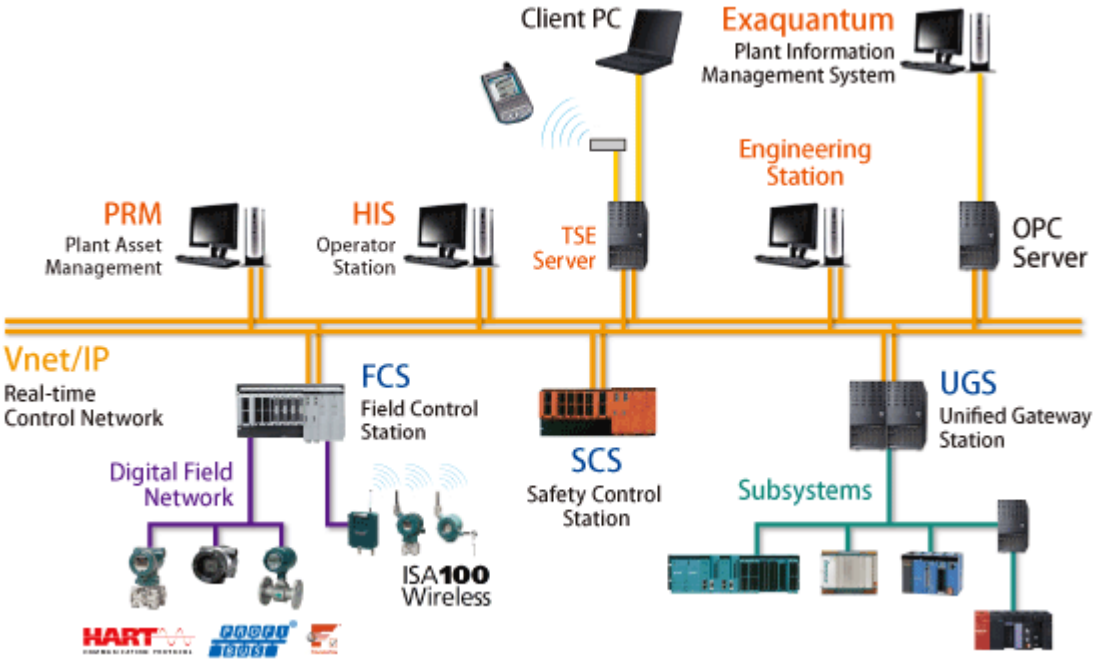

圖 3. ProSafe-RS 系統組態與配置

3. HIMax 之功能安全平台

德國 HIMIA 公司創建於 1908 年，是全世界著名的安全控制系統專業製造商。HIMA 公司生產的安全控制系統已有 30,000 多套投入全球應用，廣泛分佈於世界各地的石化、電力、機械製造、交通運輸、及大型公共建設等領域。

HIMax 是 HIMA 新一代的安全控制器，所有軟硬體均通過 TÜV 的 SIL3 認證。在系統架構上，HIMax 內的每個模組均為 SIL3 等級之 1oo2D 架構，且整體採用了革命性的 XMR (X Modular Redundant)架構，具有完美的可用性。當 XMR 中的 X 為數字 1-2-3-4 時，HIMax 提供單重化、2 重化、3 重化、及 4 重化的系統結構，如圖 4 與圖 5 所示。這種架構使得 HIMax 可以避免任何單點故障，甚至多重的故障也不會引發機組停車。任何軟硬體的擴充或維護均無需中斷 HIMax 系統運行。

此外，HIMax 系統支持所有國際通用的標準協定，如 Modbus、Profibus、OPC 等，可完成和所有國內外主流 DCS 控制系統及其他自動化系統的無縫整合。

圖 4. HIMax 之 XMR 架構

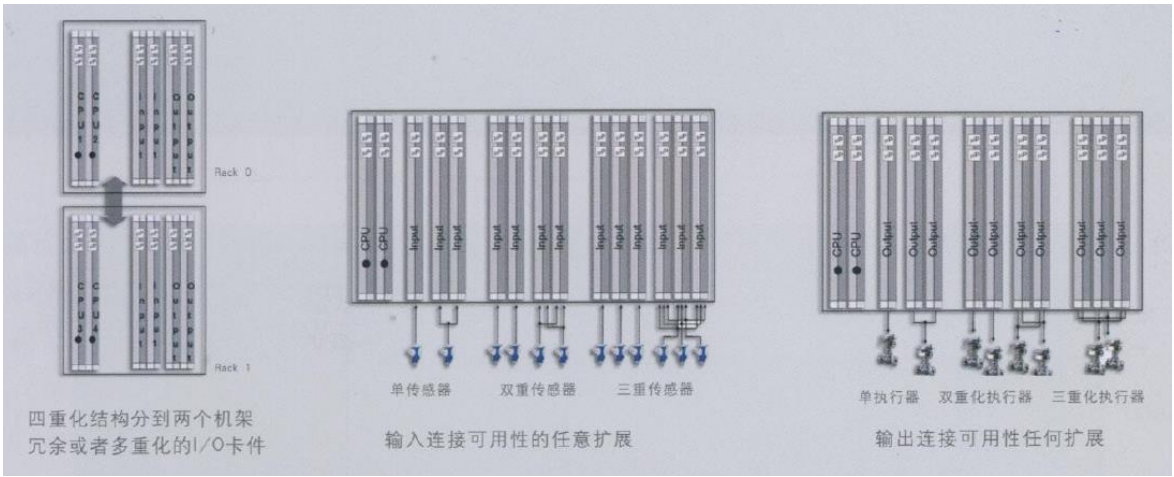

圖 5. HIMax 之 XMR 架構範例

4. PSR-TRISAFE 之功能安全平台

Phoenix Contact 是世界電氣工程、電子工程、及工業自動化的領導企業，成立於 1923 年，總部位於德國，擁有 14,000 多名員工，在海外

超過 50 個國家設有子公司。

PSR-TRISAFE 是 Phoenix Contact 的可編程安全模組，如圖 6 所示，該模組具有 20 個安全輸入信號，4 個安全輸出信號，時間功能、報警功能、及接地開關輸出，增加了監視回路的安全功能。透過 SAFECONF 組態軟體設定，PSR-TRISAFE 可以組態成符合 SIL3 等級的安全系統，如圖 7 所示。

PSR-TRISAFE 安全模組兼顧功能性與使用彈性，透過單一裝置，即可監控應用程式中的各項安全功能。且模組可自由設定和擴充，或是依個別機器或系統的安全需求，進行調整。

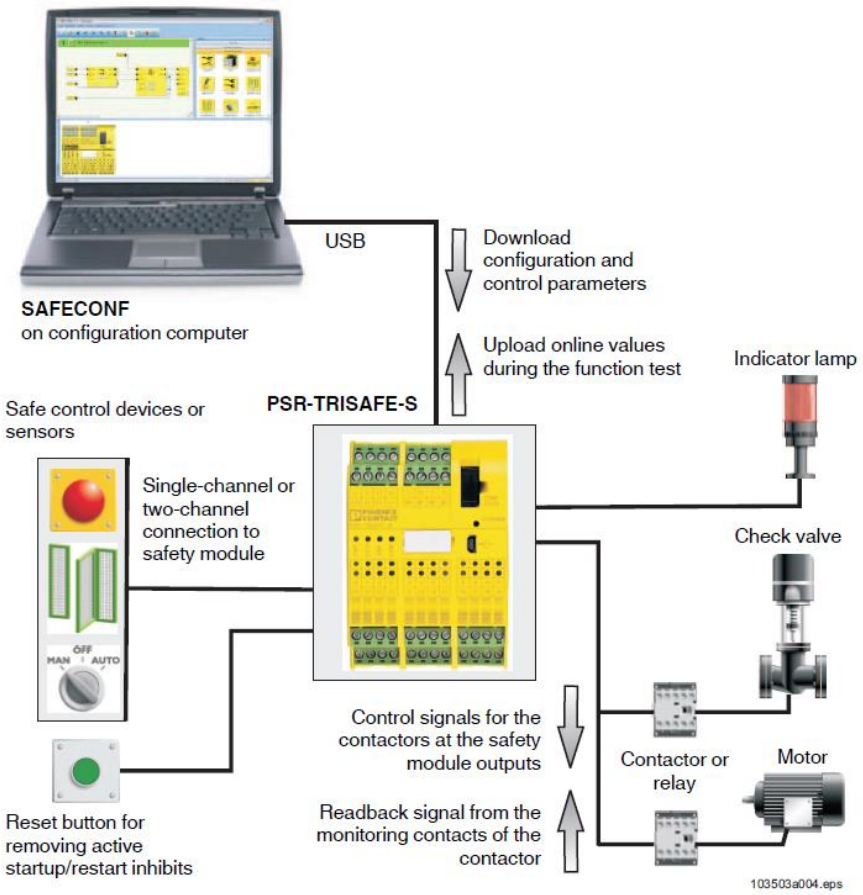

圖 6. PSR-TRISAFE 系統組態

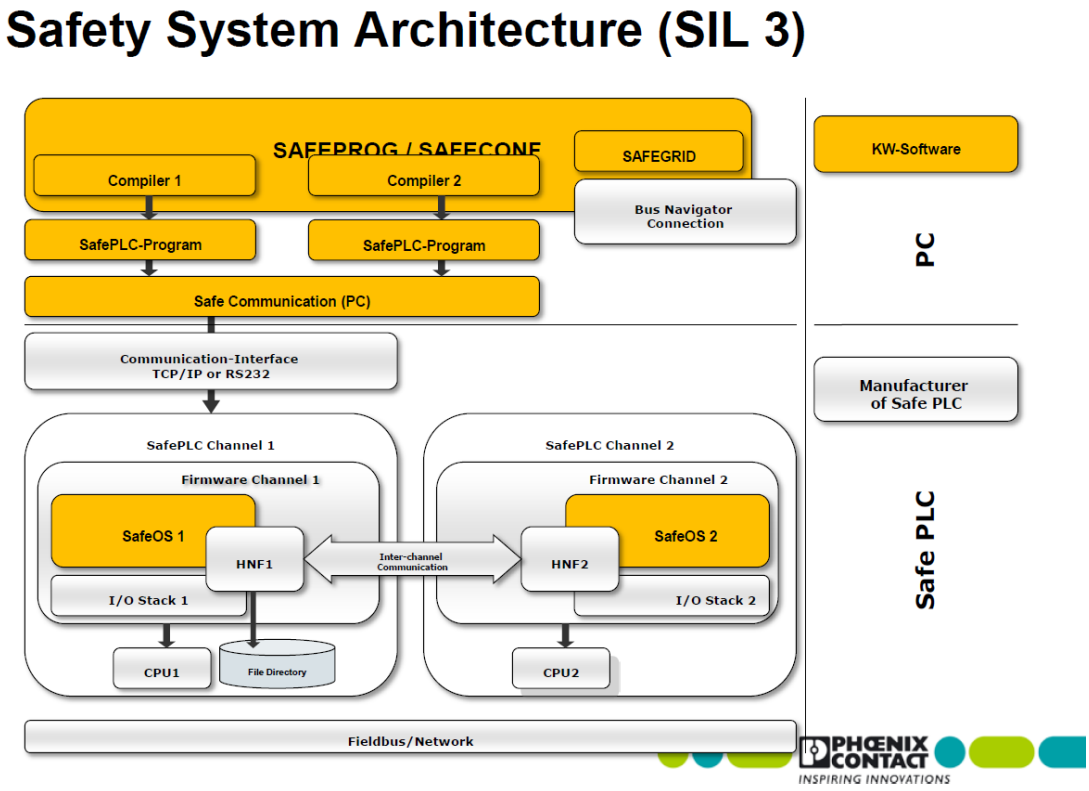

圖 7. SIL3 等級之 PSR-TRISAFE 系統組態

5. Trinity 之軟體測試工具

Trinity Technologies 總部位於美國加州，在北美和亞太設有分支機構和研發團隊，目前中國總部位於上海，在中國設有上海和成都兩個辦公室，而台灣也設有分公司。公司專注於嵌入式系統之軟體研發品質和自動化測試的方案和諮詢服務。主要針對嵌入式系統開發客戶，包含：航空電子設備、汽車工業、及半導體等。主要產品包括：

- VectorCAST：軟體程式碼(C/C++)測試工具。測試工具通過 TÜV SÜD IEC61508-3 及 ISO 26262-8 認證。在發展系統欲取得 IEC 61508 及 ISO 26262 時，使用此工具可支援相關軟體發展的測試工作，並減少重複的品質驗證工作。
- PRQA：軟體程式碼(C/C++)靜態分析工具。可作為程式碼編碼導則(例如：MISRA)之符合度分析。
- DT10：可針對嵌入式系統之軟體進行模擬測試，在軟體安裝至作業系統與硬體前，進行動態模擬測試。

- Squore：軟體程式碼與測試之管理工具。

其中 VectorCAST 與 PRQA 屬於軟體程式碼靜態分析及動態測試的驗證方法。DT10 為嵌入式系統之軟體模擬測試，當安全設備採用嵌入式作業系統時，可作為良好的參考。

Trinity 產品應用產業主要針對嵌入式系統開發客戶，包含：航空電子設備、汽車工業、及半導體等。核研所在軟體驗證與確認(Software Verification and Validation, SV&V)工作上，也應用很多類似工具，針對核研所已採用之 SV&V 工具，與該公司產品比較，重點如下：

- 目前核研所使用於軟體程式碼的驗證方法包括靜態分析及動態測試兩種。靜態分析使用 MathWorks 公司的產品 Polyspace；而動態測試則使用 Reactive System 公司的產品 Reactis for C。Polyspace 產品通過 TÜV SÜD IEC61508-3、EN 50128、及 ISO26262-8 認證，而 Reactis for C 則符合 ISO 26262 的使用導則。此兩項產品功能與 Trinity Technologies 公司的項次 1 (VectorCAST)及項次 2 (PRQA)類似，具有程式碼靜態分析功能，並提供動態測試與測試涵蓋率的度量。
- 現階段工業界所驗證的安全系統，為確保其可測性與降低系統的複雜度，因此要求安全系統盡量避免使用軟體作業系統，減少其複雜行為帶來不可預期的影響，因此，核研所軟體驗證計畫大都針對非具有作業系統的安全設備執行軟體驗證，Trinity Technologies 公司項次 3 (DT10)的產品係針對嵌入式系統之軟體進行模擬測試，核研所目前並無此應用需求，不過未來如果安全設備使用嵌入式作業系統的話，仍可提供良好的參考。Trinity Technologies 公司的項次 4 (Squore)產品為管理工具。

(二) 參訪德國萊因 TÜV 集團大中華地區總部

德國萊因 TÜV 集團是一全球領先的技術服務供應商。自 1872 年成立以來，該集團已從一家地區性檢測機構發展成為全球領先的技術服務商。徐員此次參訪由工業服務事業群－工廠完整性管理服務處暨工業檢驗處之高鴻鈞總經理接待。

徐員此行與高鴻鈞總經理及該公司其他成員討論中國大陸核電發展現狀與展望，以及功能安全和軟體驗證與確認在核電廠的應用，並就功能安全在核能工業的應用議題，進行意見交換。

(三) 台塑寧波石化廠參訪心得

徐員此行赴位於寧波的台灣塑膠電子專案組參訪。由電子專案組謝錫福協理接待。

首先參觀台塑電子專案組在工廠內組裝之整合性控制與安全系統展示平台，如圖 8 所示，在左手邊為核研所開發認證之 SCS-2000 安全系統，右手邊為台塑之 FCS-2000 控制系統，中間為整合性監控平台介面。核電安全要求在系統參數超出可控制範圍時，安全系統要動作，跳脫反應器，使核電廠安全停機，所以控制系統與安全系統必須完全獨立。基本上，核電廠跳機後無損於反應器，如果能找到失控肇因，機組可以很快再度啟動。

不同於核電安全要求之嚴格分界，石化廠在跳機後，一些原物料在管路內凝結或轉態，後續之清理及重新啟爐相當麻煩。台塑電子專案組因此思考，將控制與安全系統整合於一監控平台內，透過數據引擎技術，在控制系統內複製安全系統之動作邏輯，在安全系統監控參數達到跳脫設定點之前，預警並連動控制系統，設法使安全參數回到正常值，避免跳機。當然如果控制系統無法挽回安全參數，安全系統一樣會執行跳機動作。此整合性平台已由台塑電子專案組在不同場合介紹推廣，並將基於台塑「機爐電一體」之目標，規劃應用於汽機、鍋爐、及發電機監控平台內。

圖 8. 整合性控制與安全系統展示平台

另外，由於大陸近來工安事件頻傳，尤其是今年天津大爆炸之後，大陸已由安全監督總管單位下達《關於加強化工安全儀表系統管理的指導意見》，要求工業製程需設計符合國際要求的安全儀表系統(亦即功能安全儀表系統)，訂定 2016、2018、及 2020 年三期目標，時程要求相當急迫。核研所之 SCS-2000 安全系統，先前已經德國萊因 TÜV 集團認證為符合 IEC 61508 SIL-3 安全等級之控制器。對應上述大陸將對功能安全儀表系統加強要求情況下，我們也想進軍大陸功能安全市場，擴展成果應用。但大陸市場剛開始，都是以價格決定採用之系統。因此，此行雙方也針對降低 SCS-2000 安全系統製造成本上，進行討論。可行的方案包括將一些周邊組件，譬如電纜、連結器等，改用台灣生產較低成本之零件。另一方案為應用現場可編輯閘道陣列(Field Programmable Phase Array, FPGA)取代中央處理器(CPU)，以降低成本。此兩方案將持續討論，以達到降低成本之目標。

最後，此行也檢討一些 SCS-2000 安全系統可改進加強之部分，包括：

- 加裝 SCS-2000 安全系統 RACK 底板的保護。
- 直接將終端電阻置於 RACK 背板上。
- 將電源模組加以保護，並改善接線柱設計。

徐員於參訪返國後，也請相關同仁，進行相關之改善規劃。

(四) 大亞灣核電廠參訪心得

徐員此行應邀，赴中廣核集團轄下大亞灣核電廠參訪。由方思豪副廠長及技術部王春暉科長等接待。大亞灣核電廠係大陸早期興建之大型核能機組，自商轉以來，已運行 20 多年，圖 9 為該電廠外觀。

圖 9. 徐員於大亞灣核電廠外留影

大亞灣核電廠運維單位，現也擬依照國際標準與作法，對該電廠進行老化管理，並將原有之 40 年運轉執照，向大陸監管單位申請更新為 60 年運轉執照。核研所在台灣已對台電運轉中之核電廠進行老化管理評估，以及不易更換組件之壽命評估工作，累積長久之經驗，因此回應該廠方思豪副廠長之邀請，交流核電廠老化管理相關工作經驗，並討論可能之合作機會。

經徐員介紹核研所在台灣已執行之工作經驗，並回答大亞灣現有老化管理工作所遭遇問題之可能解決途徑後，方副廠長及其他中廣核集團技術同仁皆認同我們的能力與經驗，可作為大亞灣後續執行老化管理工作之參考。未來針對此議題之再交流或相關合作規劃，將待大亞灣方面正式提出後，我們再循兩岸技術交流相關規定辦理，雙方合照如圖 10 所示。

圖 10. 徐員與大亞灣核電廠員工合影

四、建議事項

(一) 現在國際間對工業製程需設置安全儀表系統(亦即功能安全儀表系統)之要求漸增，核研所先前在核能安全之經驗，可轉移至此需求上。建議應多增加功能安全儀表之投資及工作參與。

(二) 核研所發展核電廠安全儀控系統多年，具相當之專業與經驗。非核領域之火力電廠及石化廠，現也正在加強其安全設計及標準要求，核研所可憑此專經，協助非核領域之安全管理，達到較嚴謹之設計標準及執行程序，加強國內火力電廠及石化廠之安全運轉。

(三) 國內執行核電廠老化管理工作已有多年，累積長足之經驗，建議在大陸有此需求時，可循兩岸技術交流相關規定，規劃有益雙方之工作交流。