

出國報告（出國類別：其他）

## 赴美國執行龍門計畫業主獨立驗證及 確認小組技術支援工作

服務機關：核能研究所

姓名職稱：鄭宗杰 副研究員  
楊智偉 副工程師

派赴國家：美國

出國期間：103 年 3 月 22 日~103 年 3 月 31 日

報告日期：103 年 4 月 25 日



## 摘 要

核研所核儀組鄭宗杰與楊智偉於 103 年 03 月 22 日至 103 年 03 月 31 日，配合龍門電廠儀控系統驗證規劃，赴美國奇異公司協力廠家 DRS Consolidated Controls (DRS-CCI) 公司與 Schneider Electric-Invensys 公司參與相關技術會議，執行龍門計畫業主獨立驗證及確認稽查小組 (Owner's Independent Verification and Validation Team, OIVVT) 技術支援工作。本次 OIVVT 主要工作針對 MPR 公司人員在龍門電廠現場評估軟體設計修改後所發現的待結案問題 (Questions)、議題 (Issues) 或關心項目 (Concerns)，品質保證 (Quality Assurance, QA) 作業等有資料不足待澄清的多項議題，赴美國奇異公司協力廠家 DRS-CCI 公司與 Schneider Electric-Invensys 公司進行討論議題澄清與 QA 作業稽查。參與 MPR 人員向 DRS 提出 15 項現場處理指示 (Field Disposition Instruction, FDI) 於龍門現場發現有資料不足待澄清的多項議題，經由 DRS 人員提供相關測試報告內容查核及功能連結圖 (Functional Interconnection Diagram, FID)、影像顯示單元 (Video Display Unit, VDU)、Plus 32 軟硬體設計修改作業流程確認，結果無發現問題或缺失；MPR 人員向 Invensys 提出 12 項 FDI 於龍門現場發現有資料不足待澄清的多項議題，經由 Invensys 人員提供相關差異報告 (Discrepancy Report, DR)、網路壓力測試報告內容查核，及 Invensys 配置控制器 (Integrated Control Configurator, ICC)、客製化警報軟體與系統軟硬體更新設計作業流程確認，結果無發現問題或缺失。

# 目 錄

|              |    |
|--------------|----|
| 摘 要 .....    | i  |
| 一、目的 .....   | 1  |
| 二、過程 .....   | 2  |
| 三、心得 .....   | 10 |
| 四、建議事項 ..... | 12 |

## 一、目的

龍門電廠分散式控制暨資訊系統(Distributed Control and Information System, DCIS)於 97 年開始現場安裝後及試運轉之現場測試工作，期間若發現有需要進行設計修改之問題，均開立現場問題報告(Field Problem Report, FPR)及其他不符合報告單等，依龍門電廠作業程序送設計單位核技處協助處理。DCIS 相關系統設計文件修改由核技處駐工地辦公室(SEO)及奇異公司派駐工地顧問分別發行設計變更通知(Design Change Notice, DCN)或現場偏差處置報告(Field Deviation Disposition Request, FDDR)，據以現場再施工或進行軟體修改。其中涉及安全數位儀控系統的軟體建置變更，均送原設備供應商執行。

美國 MPR 公司接受核技處委託進行龍門電廠 DCIS 獨立驗證及確認，MPR 人員於龍門電廠現場評估，主要針對在現場安裝後及試運轉之現場測試工作軟體設計修改後所發現的待結案問題(Questions)、議題(Issues)或關心項目(Concerns)，品質保證(Quality Assurance, QA)作業等有資料不足待澄清的多項議題，赴美國奇異公司協力廠家 DRS-CCI 公司與 Schneider Electric-Invensys 公司進行議題澄清與 QA 作業稽查。

核研所核儀組鄭宗杰與楊智偉於 103 年 03 月 22 日至 103 年 03 月 31 日，配合龍門電廠儀控系統驗證規劃赴美國 DRS-CCI 公司與 Schneider Electric-Invensys 公司參與相關技術會議，執行龍門計畫業主獨立驗證及確認稽查小組(Owner's Independent Verification and Validation Team, OIVVT)技術支援工作。

## 二、過程

本次出國行程為期 10 天，相關行程及摘要工作項目說明如下：

| 日期                       | 行程                                                             | 摘要                                                                                                                                                                               |
|--------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 103.03.22 至<br>103.03.23 | 由台灣桃園機場經<br>美國紐約機場至美<br>國康乃狄克州                                 | 路程                                                                                                                                                                               |
| 103.03.24 至<br>103.03.25 | 美國康乃狄克州丹<br>伯利市 DRS-CCI<br>公司                                  | 參與 MPR 人員向 DRS 提出於龍門電<br>廠現場評估軟體設計修改後，發現有<br>資料不足待澄清等議題之 15 項 FDI，<br>經由 DRS 人員提供相關測試報告內容<br>查核及 FID、VDU、Plus 32 軟硬體設<br>計修改作業流程確認，結果無發現問<br>題或缺失。                               |
| 103.03.26                | 由美國康乃狄克州<br>至麻薩諸塞州                                             | 路程                                                                                                                                                                               |
| 103.03.27 至<br>103.03.28 | 美國麻薩諸塞州福<br>克斯波羅市<br>Schneider Elec-<br>tric - Invensys 公<br>司 | 參與 MPR 人員向 Invensys 提出於龍門<br>電廠現場評估軟體設計修改後，發現<br>有資料不足待澄清等議題之 12 項<br>FDI，經由 Invensys 人員提供相關差異<br>報告（DR）、網路壓力測試報告內容<br>查核，及應用軟體（ICC）、客製化警<br>報軟體與系統軟硬體更新設計作業流<br>程確認，結果無發現問題或缺失。 |
| 103.03.29 至<br>103.03.31 | 由美國麻薩諸塞州<br>至美國紐約機場返<br>回台灣桃園機場                                | 路程                                                                                                                                                                               |

本次稽查工作主要由台電公司技術顧問美國 MPR 公司人員評估龍門電廠一號機安全與非安全相關分散式控制暨資訊系統測試與現場變更流程，此外，並透過稽查過程中所蒐集之相關資料判斷龍門電廠 DCIS 是否符合相關法規、標準與規範之期望與要求，藉以評估龍門電廠 DCIS 測試適當性並評估選定現場變更之技術完整性。上述過程與結果將作為龍門電廠一號機 DCIS 評估報告資料。

### (一) 於美國康乃狄克州丹伯利市 DRS-CCI 公司之稽查活動

本次稽查與 DRS-CCI 有關之現場處理指示 (Field Disposition Instruction, FDI) 審查項目包括 DRS 網路配置或執行異常的 FDI 案件編號有 LT0-31113-0080, LT1-31113-0197, -0706, -1291 等 4 項、DRS 影像顯示器 (Video Display Unit, VDU) 畫面與警報修改的 FDI 案件編號有 LT0-31113-0203, -0147, LT1-31113-0086, -0125, -0132, -0137, -0681, -0749 等 8 項、流程跳脫邏輯或流量傳送器不穩定更正的 FDI 案件編號有 LT0-31113-0120, LT1-31113-0653 等 2 項、DRS 雙重電力供應失效偵測的 FDI 案件編號有 FDI LT0-31113-0147 等 1 項。參與會議人員如圖一所示，包括 GEH 公司設計部門負責工程師 (Responsible Engineer, RE) Raghu Raghavan 與獨立審查人員 (Independent Review Team, IRT) Larry Chi 等二位、MPR 公司人員 David Herrell 與 Danny Duong 等二位、核研所鄭宗杰與楊智偉等二位、DRS 公司軟體發展部門經理 Kris Kennedy 等四位。



圖一、會議人員合照 (左起 GEH 公司 Larry Chi、DRS 公司 Kris Kennedy、GEH 公司 Raghu Raghavan、MPR 公司 David Herrell、MPR 公司 Danny Duong、核研所鄭宗杰、核研所楊智偉)

會議開始由 MPR 公司人員 David Herrell 自我介紹及說明會議議程，DRS-CCI 負責龍門計畫的經理 Paul M. Stankiewicz 介紹公司組織與相關成員，針對 MPR 公司有疑義的前述 15 項相關問題，由核能品保 (Nuclear Quality Assurance, NQA) 人員 William Kulas 使用其內部專用追蹤系統，

提供相關佐證文件編號資料或由資深軟體發展工程師 Anthony Coppola 等現場人員口頭解釋、或於白板上圖解等方式，提供 MPR 公司人員結案所需資料。David Herrell 針對部分資料表示需要其中幾頁內容參考，計畫經理 Paul M. Stankiewicz 表示只要不是索取整本文件而僅複印幾頁應無問題，但 DRS-CCI 在場的軟體發展部門經理 Krist Kennedy 卻馬上以涉及公司機密（Proprietary）極力反對而作罷，改為現場查閱後退回 DRS-CCI。

DRS 公司回應 R.G. 1.171（1997 年 9 月版）第 2.1 節涵蓋率要求（Coverage of Requirements）與第 2.2 節內部架構涵蓋率（Coverage of Internal Structure）對「Identity」與「Justification」的定義，所謂「Identity」指的是「Qualify」，亦即能夠 100% 符合；在無法滿足 100% 的前提下才會衍伸有關「Sufficiency」的探討，也就是需要「Justification」。DRS 公司對於 FID 的測試採取 100% 的 Functional testing，因此就沒有牽涉到「Justification」。

MPR 依據表二驗證檢核表結果彙整以書面及口頭提出待澄清議題，包括從收到 FDDR 到最後處置的現場修改流程、軟體發展生命週期、模組測試/單元測試方法、VDU 的狀態、程式碼測試涵蓋率評估與量測的測試建立評估等相關議題。經由 DRS 人員提供相關測試報告內容查核及功能連結圖（Functional Interconnection Diagram, FID）、影像顯示單元（Video Display Unit, VDU）、Plus 32 軟硬體設計修改作業流程確認，結果無發現問題或缺失，將彙整各項議題之結果報告於今年 8 月份提供給台電。

表二、MPR 人員驗證檢核表

| No. | Method of Verification                                                                                                                                                               |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Is the FPR a clear, complete, and unambiguous condition report?                                                                                                                      |
| 2   | Is the FDDR sufficient to define which systems are affected, and is a complete list of those systems identified in the FDDR?                                                         |
| 3   | Is the FDDR (for both items identified through an FPR and for items identified by the vendor or other vendor customers) clear, complete, and unambiguous in reporting the condition? |

續表二、MPR 人員驗證檢核表

| No. | Method of Verification                                                                                                                                                                                                                                                                      |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4   | Is the proposed resolution in the FDDR, and the FDI if applicable, clear as to the resolution, complete in terms of defining all of the issues associated with the proposed change, and unambiguous in all details?                                                                         |
| 5   | Have the functional requirements of the change been satisfactorily addressed in the System Functional Requirements Specification(s)?                                                                                                                                                        |
| 6   | Have the functional requirements of the change been satisfactorily addressed in the Software Requirements Specification(s)?                                                                                                                                                                 |
| 7   | Have the functional requirements of the change been satisfactorily addressed in the Hardware Requirements Specification(s)?                                                                                                                                                                 |
| 8   | Has the detailed hardware design been updated appropriately to reflect the new hardware requirements?                                                                                                                                                                                       |
| 9   | Have the functional requirements of the change been satisfactorily addressed in the Software Design Description(s)?                                                                                                                                                                         |
| 10  | Have the changes in the detailed design changed been satisfactorily addressed in the code?                                                                                                                                                                                                  |
| 11  | Have the changes in the Software Requirements Specification(s) been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis and review of the changes against the FDDR and FDI (if applicable)?                                |
| 12  | Have the changes in the Software Design Description(s) been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis and review of the changes against the Software Requirements Specification(s)?                              |
| 13  | Have the changes in the code been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis and review of the changes against the Software Design Description(s)?                                                                |
| 14  | Have the changes in the code been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis, review, and test for the unit/module testing, including regression testing?                                                         |
| 15  | Have the changes in the integrated code been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis, review, and test for the software integration testing, including regression testing?                                     |
| 16  | Have the changes in the integrated code been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis, review, and test for the software and hardware integration testing (i.e., system testing), including regression testing? |

續表二、MPR 人員驗證檢核表

| No. | Method of Verification                                                                                                                                                                                                                                                                                                                                                                      |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17  | Have the changes in the system been satisfactorily addressed, with documented acceptance by the Verification and Validation (V&V) staff through analysis, review, and test by system and M-MIS integration testing, including regression testing?                                                                                                                                           |
| 18  | For changes that have the possibility to affect multiple systems or cross vendor or safety/non-safety boundaries, have the affected systems been determined and testing defined that demonstrates that the change does not have adverse effects on any DCIS system and that the change works correctly on all systems that access the data provided by the changed system?                  |
| 19  | For changes that affect data or status, has sufficient testing been defined to ensure that all users of the data (including but not limited to Multi-Vendor Devices (MVDs), Gateways, value displays, trending displays, computations, data historians, etc.) have been adequately and successfully tested, including maximum and minimum values, values that exceed the range, and status? |
| 20  | For safety system changes, has system/software safety been included and incorporated appropriately?                                                                                                                                                                                                                                                                                         |
| 21  | Have configuration management and change control been included in the change?                                                                                                                                                                                                                                                                                                               |
| 22  | Do software quality assurance records indicate that the change was performed under the approved life cycle process?                                                                                                                                                                                                                                                                         |

## (二) 於美國麻薩諸塞州福克斯波羅市 **Schneider Electric-Invensys** 公司之稽查活動

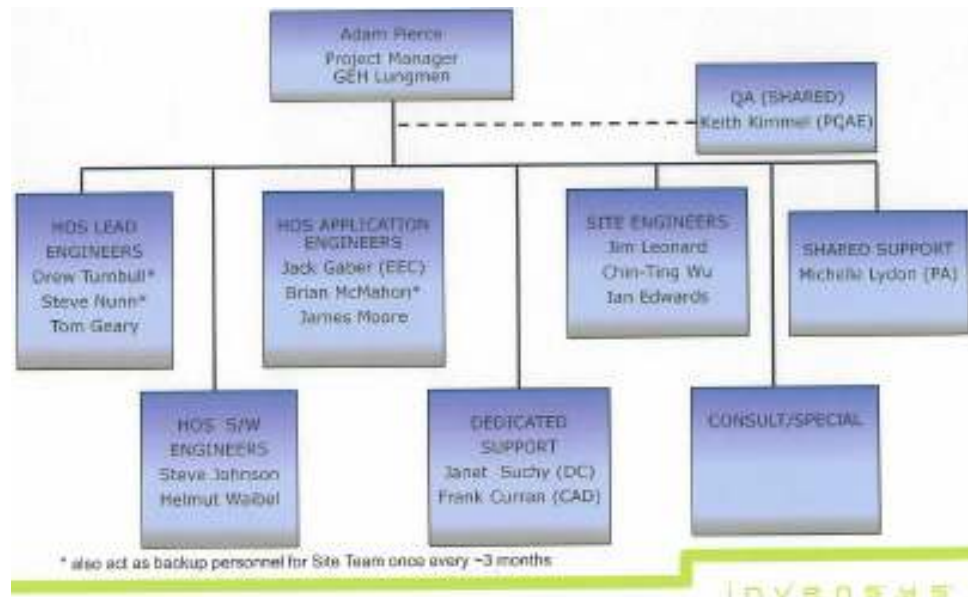
本次稽查與 **Invensys** 有關之現場處理指示 (FDI) 審查項目包括邏輯或設定點修改的 FDI 案件編號有 LT0-31113-0041, -0045, -0050, LT1-31113-0350, -1202 等 5 項、控制處理器雙重電源監視狀態的 FDI 案件編號有 LT0-31113-0025 與 LT1-31113-0173 等 2 項、3D Monicore 運轉顯示或計算相關的 FDI 案件編號有 LT1-31113-0627 與-1196 等 2 項、警報相關的 FDI 案件編號有 LT1-31113-0189 與-1014 等 2 項、功率顯示的 FDI 案件編號有 LT1-31113-1406 等 1 項。參與會議人員如圖二所示，包括 **GEH** 公司設計部門負責工程師 (RE) **Daniel Gould**、**MPR** 公司人員 **David Herrell** 與 **Danny Duong** 等二位、核研所鄭宗杰與楊智偉等二位、**Invensys** 公司計畫經理 **Adams Pierce**、領導工程師 **Drew Turabull**、品保工程師 **Keith Kimmel** 等三位 (如圖三)。

會議開始由 **MPR** 公司人員 **David Herrell** 自我介紹及說明會議議程，計畫經理 **Adams Pierce** 提供龍門計畫之組織架構與人員職稱之簡報資料供與會人員參考 (如圖三)，及說明處置現場修改流程 (如圖四)。

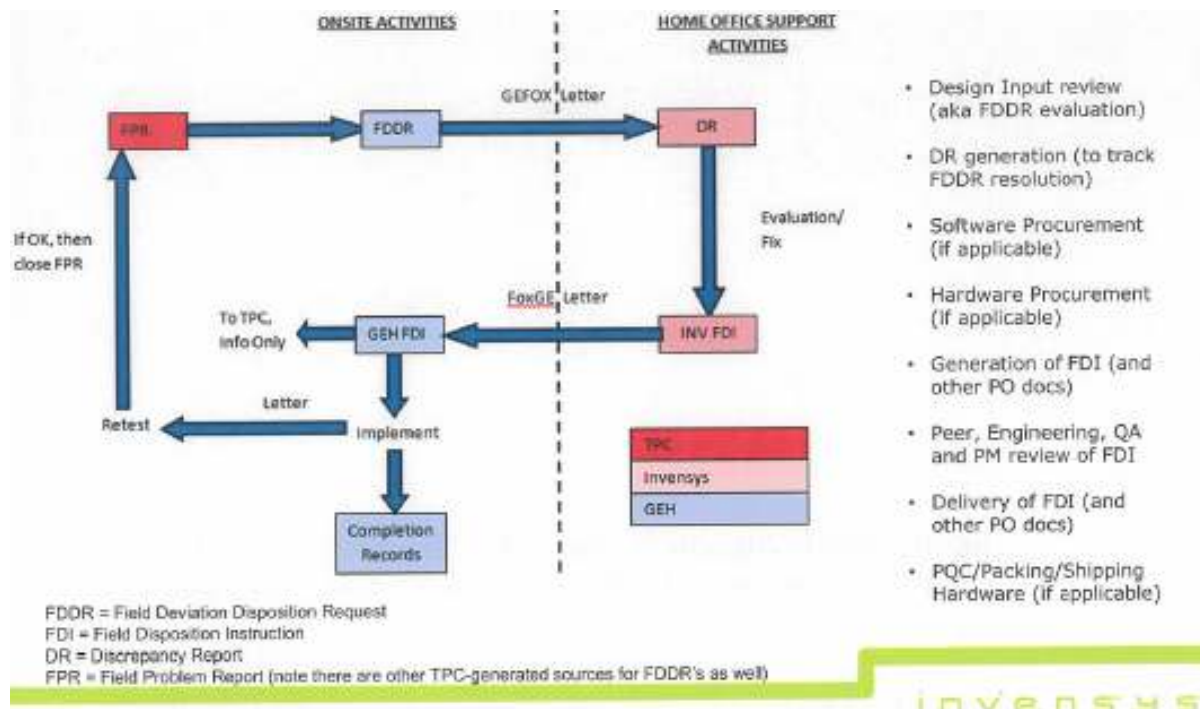


圖二、會議人員合照(左起核研所楊智偉、核研所鄭宗杰、**GEH** 公司 **Daniel Gould**、**MPR** 公司 **Danny Duong**、**MPR** 公司 **David Herrell**)

針對 MPR 公司有疑義的前述 12 項相關問題，MPR 提問這些修改如何在 Invensys 測試，測試的流程與文件的可追溯性說明，若參與會議人員不清楚議題之技術內容時，計畫經理 Adams Pierce 立即電話詢問相關工程師或請工程師直接至會議室進行解釋。



圖三、Invensys 參與龍門計畫人員組織圖



圖四、Invensys 參與龍門計畫執行人員處置現場修改流程圖

當 MPR 人員提出需相關佐證資料時，計畫經理 Adams Pierce 立刻至系統中查詢並列印出相關文件提供 MPR 人員審閱。因此，於 Invensys 的循線稽查與現場變更成套文件審閱工作，大都由 MPR 人員要求 Invensys 提供書面資料，在書面審核後仍然不清楚的部分，再請相關人員輔以口頭解釋或提供更進一步的書面資料。MPR 人員彙集待澄清議題，包括從收到 FDDR 到最後處置的現場修改流程、軟體發展生命週期、模組測試/單元測試方法、評估 Invensys 問題通報/解決與申請軟體錯誤更正流程。經由 Invensys 人員提供相關差異報告（Discrepancy Report, DR）、網路壓力測試報告內容查核，及 Invensys 配置控制器（Integrated Control Configurator, ICC）、客製化警報軟體與系統軟硬體更新設計作業流程確認，結果無發現問題或缺失，將彙整各項議題之結果報告將於今年 8 月份提供。

### 三、心得

本次配合龍門電廠儀控系統驗證規劃，陪同 MPR 公司執行業主獨立驗證及確認稽查小組技術支援工作，參與美國奇異公司（GE）協力廠家 DRS-CCI 公司與 Schneider Electric-Invensys 公司進行設計修改作業流程澄清等相關技術會議，有以下四點心得：

- (一)MPR 公司人員以循線稽查（Tread Audit）方式進行流程與文件的可追溯性（Traceability）確認，在龍門電廠完成現場評估後，認為台電公司目前相關流程與做法已相當完備。在稽查過程中，先確認流程是否正確，在流程中各項經過的活動都應有可見的結果，亦即文件都應該有一個有意義的編號。因此，流程不明確或文件不完整的發現問題（Questions）、有資料不足待澄清的議題（Issues）或關心項目（Concerns）等，經台電與奇異公司現場人員討論後，提出美國奇異公司協力廠家（設備供應商）DRS 與 Invensys 技術會議之議程。
- (二)龍門電廠分散式控制暨資訊系統（DCIS）由奇異公司整合設計，交由 GE 內部的設備供應商 NUMAC、GEIS 與 GNF，及 GE 外部（協力廠家）的設備供應商 DRS 與 Invensys 建置。因此，DCIS 在龍門電廠現場涉及安全數位儀控系統的軟體建置變更，均送原設備供應商（NUMAC 與 DRS）執行。原設備供應商的軟體建置變更有內部作業程序，相關的文件只保留於設備供應商，並不會送交給設備使用者（台電）。所以，MPR 人員在稽查過程中，有些問題要求設備供應商補充相關文件或澄清文件中不足或說明不清的部分，大多能夠在稽核過程中獲得結果；但有些部分的問題與法規或標準有關，無法在一次的稽核活動中獲得令人滿意的結果，則需要有更深入的討論。
- (三)MPR 人員提出 FDI 之重測界限（Retest Boundary）議題，因 GE 與台電公司認知差異，未能明確定義由設備使用者（台電）或由 DCIS 整合設計者（GE）負責，突顯現場系統整合實務上的複雜度。本次稽查過程中，依據 MPR 針對現場修改有關文件表格指出，由於缺乏適當設計細節，故無法確認台電公司如何建立適當的測試邊界與範圍。

實務上台電為設備使用者，僅能以黑箱測試方式，建立適當的測試邊界與範圍；而 GE 為 DCIS 整合設計者，對於內部的設備供應商 NUMAC、GEIS 與 GNF 可以白箱測試方式提出適當的測試細節，但對於協力廠家的設備供應商 DRS 與 Invensys 也僅能以黑箱測試方式，建立適當的測試邊界與範圍。

(四)對於稽查人員活動區域之嚴格管制：DRS-CCI 禁止非美籍人員攜帶任何電子設備，包括電腦、手機、相機、USB 隨身碟等，而美籍人員只能攜帶不具有攝影功能之電腦進入廠區。於 Schneider Electric-Invensys 所進行之稽查氣氛與 DRS-CCI 相當不同，除部分區域(中國核能電廠專區)限制人員進出外，大部分區域之管制就如一般工業廠房一般，較 DRS-CCI 寬鬆，也並未限制攜帶任何電子設備。

## 四、建議事項

本次赴美國奇異公司協力廠家 DRS-CCI 公司與 Schneider Electric-Invensys 公司執行 OIVVT 技術支援工作，協助台電公司了解 MPR 公司現場稽查狀況，並適時協助釐清議題。透過此次參與會議獲得國外廠家寶貴執行經驗，這些經驗與文件（如表二 MPR 針對現場問題報告之驗證查核表與查核項目設計）可做為核研所未來參與電廠數位更新技術支援工作或參與其他產業大型複雜系統建置之參考。