行政院及所屬各機關出國報告提要

出國報告名稱：執行龍門計畫分散式控制暨資訊系統整體功能驗證工作評估

頁數 9 含附件：□是■否

出國計畫主辦機關/聯絡人/電話

台灣電力公司/陳德隆/23667685

出國人員姓名/服務機關/單位/職稱/電話

廖學志/台灣電力公司/龍門電廠/電腦工程監/24903550 分機 3930

出國類別：□1 考察□2 進修□3 研究□4 實習■5 其他 洽公

出國期間：102.12.10~102.12.19　　出國地區：美國

報告日期：103.02.08

分類號/目：控制

關鍵詞：分散式控制

內容摘要：(二百至三百字)

查證顧問公司對DCIS廠家(DRS, Invensys)要求之相關資訊及有關DCIS設備運抵龍門工地安裝後在廠家執行現場處理指示(Field disposition instruction, FDI)之修改、建置及測試等程序及品保等相關作業，以確保符合法規及規範之要求。例如：查核DRS網路相關軟體修改之建置及測試程序:功能驗證控制器STC(Surveillance Test Controller)軟硬體建置及修改測試程序:以及Invensys廠用電腦系統軟體修改及構型管理之管制流程。

本文電子檔已傳至出國報告資訊網（http：//Report.nat.gov.tw/reportwork）

出國報告（出國類別：洽公）

執行龍門計畫分散式控制暨資訊系統整體功能驗證工作評估

服務機關：台灣電力公司

姓名職稱：廖學志/電腦工程監

派赴國家：美國

出國期間：102.12.10 到 102.12.19

報告日期：103.02.08

目　錄

壹、出國內容概述

一、目的

赴美查核龍門電廠數位儀控與資訊系統建置廠家(DRS 公司及 Invensys 公司)之軟體修改、建置及測試等程序及品保等相關作業，以確保符合法規及規範之要求。出國期間自中華民國 102 年 12 月 10 日至 102 年 12 月 19 日止，共計 10 天。

二、緣起及目標

1.龍門計畫分散式控制暨資訊系統(DCIS)係由奇異公司(GEH)因專業分工及採購考量分包給 3 家專業公司(NUMAC, DRS 及 Invensys)。由於廠家間之界面眾多，技術整合較為複雜；同時，DCIS 在廠家之出廠驗收測試(FAT)採區段加界面重疊測試方式執行。雖此做法符合法規之要求及業界之慣例，但未能將三個廠家整合在一起執行整體測試，亦深受外界及管制單位質疑。故，台電聘請具有核電廠數位儀控專業經驗之顧問公司(MPR 公司)獨立評估，透過顧問公司之獨立作業，從 DCIS 之規範、設計、建置、出廠驗收測試到工地測試等各階段之工作內容及成果執行評估，進而可加強對龍門 DCIS 之信心及確保龍門電廠運轉安全。

2.查證顧問公司對 DCIS 廠家(DRS, Invensys)要求之相關之修改、建置及測試等程序及品保等相關作業，以確保符合法規及規範之要求。例如：查核安全系統邏輯控制建置廠家 DRS 公司，有關網路相關軟體修改之建置及測試程序以及功能驗證控制器 STC(Surveillance Test Controller)軟硬體建置及修改測試程序；以及查核廠用電腦系統建置廠家 Invensys 公司，關於軟體修改及構型管理之管制流程。

貳、行程

本次任務出國期間自中華民國 102 年 12 月 10 日至 102 年 12 月 19 日止，共計 10 天，行程內容如下：

起迄日期	停留機構	所在地點	工作內容
102.12.10-102.12.11		台北→美國紐約	往程
102.12.12-102.12.13	DRS 公司	Danbury, CT	查核 DRS 公司軟硬體建置及測試程序
102.12.14-102.12.16	Invensys 公司 (英維斯公司)	Foxboro, MA	查核英維斯公司軟硬體建置及測試程序
102.12.17-102.12.19		美國紐約→台北	返程

參、執行過程與內容

核能電廠的儀控設計朝數位化設計演變，龍門核能電廠的數位儀控與資訊系統(DCIS)為全數位化設計。在數位儀控技術逐漸取代原先類比儀控技術的同時，工業界也發現了一些與安全和運轉績效相關的議題亟待解決。有鑑於此，美國核管會(NRC)成立了數位儀控指導委員會(Digital I&C Steering Committee)，主要目的除了與工業界聯繫以了解其關注的關鍵數位儀控議題外，並提出暫行管制人員指引(ISG，Interim Staff Guidance)以指導及監督其相關技術議題的解決。為回應工業界對數位儀控審照與相關準則的疑慮，數位儀控工作小組(Digital I&C Task Working Groups, TWG)共發行六件數位儀控相關的 ISG，包括：

(1).ISG-01 數位儀控電腦系統資安(Cyber Security Associate With Digital Instrumentation and Control)
(2).ISG-02 多樣化與深度防禦(D3，Diversity and Defense-in-Depth)
(3).ISG-03 風險告知數位儀控審查(Risk-Informed Digital I&C Reviews)
(4).ISG-04 高整合控制室-數位通訊系統(HICR-C，Highly Integrated Control Rooms - Digital Communication Systems)

(5).ISG-05 高整合控制室-人因(HICR-HF，Highly Integrated Control Rooms - Human Factors)

(6).ISG-06 數位儀控許可程序(Digital I&C Licensing Process)

本次公差係查核龍門電廠安全系統邏輯控制建置廠家DRS公司以及查核廠用電腦系統建置廠家 Invensys 公司，GEH 均派員與會。查證其數位儀控軟體修改程序等，以確保符合龍門計畫規範及相關法規與 ISG 標準之要求，查核內容及結果如以下之說明：

(一) 赴 DRS 公司之查核：

DRS 查核內容主要為安全系統網路相關軟體修改之建置、測試程序以及維護功能驗證控制器 STC(Surveillance Test Controller)軟硬體建置及其修改測試程序。擬就查核內容整理如下：

1. 會議參與人員：

   GEH：McCowen, Mark、Mohsen, Nik-Ahd、Meek Lee

   DRS：Kennedy, Kris、Coppola, Anthony、Stankiewicz, Paul、Kirk, Peter

2. 美國核能電廠安全軟體發展驗證作業與構型管理程序要符合工業標準與NRC認可的做法，並符合MUREG 0800 BTP 7-14 (儀控系統數位電腦軟體審查指引)。龍門電廠安全軟體修改與建置需依其修改後之設計，評估是否會增加風險因子(Hazards)，依原軟體發展程序，其軟體之設計修改必須經過所要求之軟體安全分析(SSA，Safety Software Analysis) 、獨立驗証與確認(IV&V，Independent Verification And Validation)及GEH 品保作業(QA)，整個修改的程序才算完成，我們稱之為(Final conditional release)。DRS安全系統網路相關軟體修改系在GEH的品保程序下完成，由DRS執行程式碼修改、驗証與確認(V&V)及相關測試，GEH執行構型管理程序(CM，Configuration Management)及軟體安全分析(Software Safety Analysis)。

3. DRS安全系統網路相關軟體修改之建置與測試：

   A. DRS安全系統網路由兩個重複(Redundant)環狀光纖網路組成，稱之為PERFORMNet(Performance Enhanced Redundant Fiber Optical

Replicated Memory Network）。資料傳輸由環狀網路節點(Node)上的NIM網卡(Network Interface Module)送到每個輸出/入控制模組(Control Input/Output Module)。原先輸出/入控制模組接收兩個網卡(NIM 1及NIM 2)資料後，先使用NIM 1資料，若NIM 1資料失效則取用NIM 2資料。現在將修改為NIM 1與NIM 2的數位訊號(Digital Signal)先比對一致性，若連續5次不一致，則採用較安全的預先設定值。

B. 整個網路相關軟體修改之建置與測試，包括：程式檢查、比對、除錯，功能測試、韌體建置(EPROM燒錄)及相關報告，預計於103年2月19日完成。

4. DRS維護功能驗證控制器STC(Surveillance Test Controller)軟硬體建置及其修改測試：

A. STC設計目的在於滿足運轉規範內屬於DRS範疇的SR 3.3.1.1.5及3.3.1.4.3 Divisional Functional Test，目前有以下問題：

i. STC建置有遺漏(新增SR)。

ii. STC建置不完整。

B. 前述問題，經龍門電廠開立現場問題報告FPR-12-0474、FPR-13-0035及FPR-13-0045後，GEH頒行現場差異處置需求FDDR LT1-10349及FDDR-12086（STC改善專案)執行設計變更。預計影響約500張FID(Functional Interconnect Diagram)。

C. 為了確保STC軟硬體修改能滿足運轉規範要求，GEH/DRS同意先提供每個SR(Surveillance Requirement)相關的警報與顯示供台電審查。

D. 交運時程以103年4月底為目標，細部的時程規劃DEH將另送台電審查。

E. STC軟硬體修改的測試報告必須依照品保程序及作業標準，提供驗証與確認(Validation And Verification)，構型管理程序(CM)及軟體安全分析(Software Safety Analysis)。

F. GEH/DRS對安全軟體的修改符合BTP 7-14 "Guidance on Software

Reviews for Digital Computer-Based Instrumentation and Control Systems" 安全系統軟體變更各階段的要求；執行軟體驗證與確認、軟體安全分析與軟體構型管理等三項活動。執行軟體驗證與確認活動及軟體構型管理活動可提高軟體品質，降低軟體缺失；執行軟體安全分析活動可確認發生軟體失效時，數位儀控系統具有減緩失效之防禦機制。

G. DRS數位儀控系統Plus 32控制器之認證，因係美國國內的認證資格，美國核能管制會(NRC)將待美國核能電廠安裝使用Plus 32控制器時，才會審查相關的報告。

H. 運轉維護手冊(Operation and Maintenance Manual)缺少VDU診斷警報的部分，GEH/DRS同意提供。

I. 本公司委託MPR公司執行業者獨立驗證與確認工作(Owner Independent V&V)，將於2014年三月赴DRS稽核，GEH/DRS應準備各類品保相關文件供MPR審查。

J. 相關會議記錄如附件一。

(二) 赴英維斯公司(Invensys)之查核：

Invensys 公司系龍門電廠非安全數位儀控系統 DCIS 的主要供應廠商，包括一百多個非安全系統的控制、主控制室的顯示與操作及廠用電腦系統。本次查核內容主要是廠用電腦系統，內容整理如下：

1. 會議參與人員：

GEH：Gould, Dan

Invensys：Turnbull Drew

2. 龍門電廠廠用電腦系統為控制網路上層之各項應用，包括資料的顯示、擷取、計算與貯存，為進步型反應器(ABWR)的特色。共有 14 個次系統，分別為：

A. 控制室顯示系統(Control Room Display System)

B. 安全參數顯示系統（SPDS，Safety Parameter And Display System）

C. 爐心監測（3D MONICORE）

D. 警報/警示系統(AAS，Alarms And Annunciators System)

E. 功率產生控制系統（PGCS，Power Generation Control System）

F. 線上程序書（OLPS，On-line Procedure）

G. 運轉規範遵行監測器（TSM，Technical Specification Monitor ）

H. 設備績效監測（TPMD，Thermal Performance Monitor& Diagnostic）

I. 爐心熱功率(CTP，Core Thermal Power)

J. 歷史資料庫（Historian）

K. 暫態紀錄分析事件序列(TRA/SOE，Transient Recoding Analysis And Sequence Of Event)

L. 報告編寫（Report Generator）

M. 電廠配置資料庫系統（Plant Configuration Database System）

N. 權限(Permission)

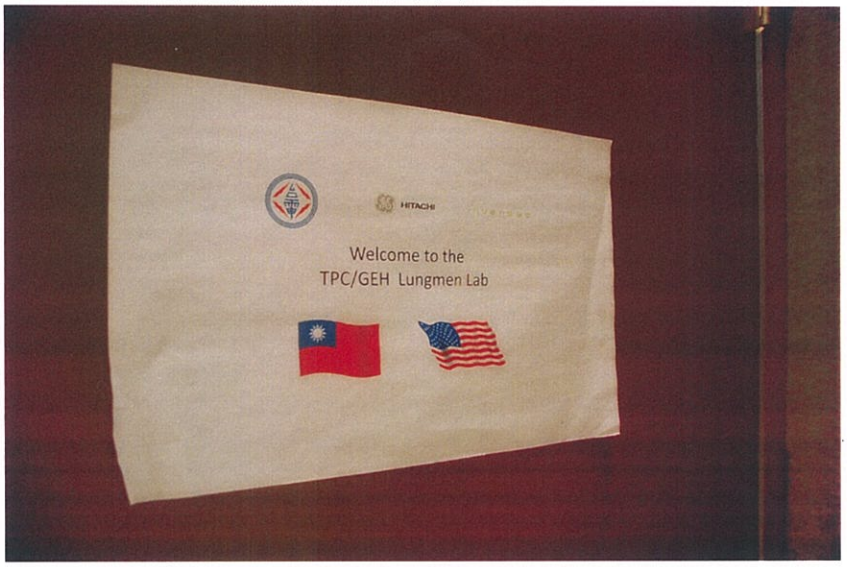
3. GEH/Invensys 為測試龍門電廠龐大而複雜的廠用電腦系統(Plant Computer System)，設立了龍門專案實驗室(如圖一)，實驗室中建置了 15 台 FSIM (Foxboro Simulator)模擬器，12 個 ZCP270(Z-Module Control Processor)控制處理器及 8 個 FCP270(Field Control Processor)控制處理器，每一台 FSIM 模擬器對應有 5-8 個 ZCP270 控制資料庫，FSIM 與控制處理器和 FBM(Field Bus Module)之間透過光纖網路傳輸資料，以模擬龍門電廠運轉狀態。龍門電廠現場測試時發現的 Invensys 有關的現場問題報告(Field Problem Report)或不符差異(Non-Conformance Disposition)，都會在此實驗室中重新檢視與驗證。

圖一、Invensys 龍門專案實驗室

4. 廠用電腦系統為 DCIS 控制序列的後端，應隨著前端各系統修改而變動，故其構型管理益顯重要，目前針對台電所提之現場問題報告(FPR，Field Problem Report)、不符合偏差(NCD，Non-Conformance Deviation)及客戶資訊需求(CIR，Client Information Request)等問題，GEH/Invensys 將其解決方式詳列於現場差異處置需求(FDDR，Field Deviation Disposition Request)，確認所影響廠用電腦系統之次系統，並於發行之現場處置指示(FDI，Field Disposition Instruction)執行程序書中詳列廠用電腦系統更改之資料庫，以確保變動的一致性。
5. Invensys 為處理台電及 GEH 所提的各項 DCIS 的設計問題，將其所發行的 FDI (Field Deviation Instruction)依問題的難易度分門別類成“U1 Easy”，“U1 Hard”，“GE Questions/Issues”，縮短處理問題時間，以迅速回應客戶。
6. 相關會議記錄如附件二。

肆、心得與建議

一、 Invensys 公司的專案實驗室設立門禁管制，非專案人員的權限不得進入。並於實驗室門口貼上台電與 GEH 的標誌、中華民國與美國國旗，令人備感窩心(如圖二)。其實驗室的規模足以測試與驗證廠用電腦系統等大型系統，並可用於新設備的相容測試。目前龍門工地的 FSIM 測試平台分屬龍門電廠與核能技術處，規模較小，無法驗證機組自動化 PGCS 之測試，應及早規畫整併工地的測試實驗室，建立設備維護及未來設備更新的測試平台。



圖二、Invensys 龍門專案實驗室門口的國旗

二、 此次訪問 Invensys 公司巧遇龍門計畫的前技術經理 Len Meter 先生，Len Meter 先生離開龍門計畫後，高昇至 Invensys 負責核能系統的主管，並曾負責中國大陸的核能電廠數位儀控系統(DCS)與模擬器業務。今年一月初大陸的福清電廠請世界核能協會(WANO，World Association of Nuclear Operators)執行啟動測試前同業評估(PSUR，Pre-Start Up Review)，其數位儀控系統與模擬器都是採用 Invensys 公司的產品。龍門電廠的數位儀控系統扮演著試運轉測試及啟動測試的重要關鍵，爾後應增加兩岸核能技術交流，汲取運轉維護的經驗。