NRD-LM-90-10

核四廠數位儀控系統發展作業
復工稽查報告

行政院原子能委員會
核能管制處

中華民國九十年十月

目　　錄

壹、前言 1

貳、稽查項目 2

參、稽查團隊 3

肆、稽查過程 7

伍、結論與建議 19

表一　稽查議程 21

表二　查證項目表 22

表三　奇異公司儀控部門人力異動表 23

圖一　核四廠數位儀控系統發展廠家架構圖 24

圖二　奇異公司龍門計畫組織圖 25

圖三　DFAT 區塊測試示意圖 26

附 件 目 錄

附件一　行文台電公司及核研所

附件二　邀請 NRC 派員參與稽查作業

附件三　奇異公司龍門計畫保密協定草案版

附件四　稽查照片

附件五　反應器保護系統查証紀錄

附件六　預期暫態未急停系統查証紀錄

附件七　新進人員受訓抽查紀錄

附件八　奇異公司保証維護核四整體計畫品質聲明

附件九　奇異公司對 Eaton 公司執行 P&P 紀錄

附件十　奇異公司對 Foxboro 公司執行 P&P 紀錄

附件十一　停工期間工作進度記錄 WPSR 樣本

附件十二　孫博士稽查報告

附件十三　INER 稽查報告

附件十四　NRC 稽查補充資料

附件十五　新開立八件「注意改進事項」

核四廠數位儀控系統發展作業復工稽查報告

壹、前言

核四計畫自今(九十)年二月十四日經行政院宣佈復工續建後，迄今(十月)已近八個月了。對於核四計畫的重新執行，參與計畫的各方都應努力以赴，讓復工的決定證明有利於台灣的永續發展。原能會站在核安管制的立場，更必須使核四計畫能在業主及各承包商的通力合作下，以高品質的施工成果順利完成、安全運轉。因此復工後原能會對台電核四計畫相關部門及國內、外廠家展開一系列的復工視察作業。

鑑於全廠數位儀控系統為核四廠的最大特色之一，其廣泛使用網路多工科技及軟體應用，與傳統核電廠之類比式設計相當不同，是核四計畫成功的關鍵因素之一，爰是將「核四廠數位儀控系統發展作業復工視察」列為整體復工視察工作中重要的一環，乃擬定視察計畫，並組專案小組於本(九十)年十月一日至四日赴美國聖荷西市奇異公司進行復工視察，且以停工期間設計文件與工作成果保護與保存，及復工後人員異動、人力復原及工作接續等相關界面銜接為稽查重點。

貳、稽查項目

核四數位儀控系統發展工作架構圖如圖一所示，主要工作由奇異公司（GENE）負責，奇異公司又將部份系統分包給 Eaton、Foxboro、GEIS（Salem）及 B&V 等公司，惟仍負責主導及整合工作。本次稽查主要目的是對奇異公司核四數位儀控發展作業執行復工品質查證，因此將停工期間奇異公司及其所屬包商（如 Eaton、Foxboro 等）對核四數位儀控系統發展工作相關設計文件與半成品的保存與保護計畫（Preserve and Protection Plan，P&P）落實執行情形，復工後人員歸建及新進人員晉用與訓練情形、新進人員使用各種設計文件的熟稔度，工作接續情形等列為查證重點，以證實復工安全品質連貫性。

另外，除查證去年五、六月間第一次數位儀控發展作業稽查後續追蹤事項執行情形外，並再度將儀控系統安全分析及品保作業績效列為此次稽查項目。

又由於全規模模擬器（Full Scope Simulator）也已由德國 STN 公司送抵奇異公司，該模擬器及工程用模擬器（GE Test System，GETS）對輔助數位儀控系統設計工作及未來運轉員與考官訓練相當重要，故亦列為此次稽查項目。

鑒於廠家接收測試(Factory Acceptance Test，FAT)為系統運抵工地

安裝前，可在廠家執行的最後一項驗證工作，有其特殊的涵意存在。且目前 FAT 相關的研擬工作正展開，原能會對該項目一向甚為重視，冀望能從剛開始的階段便多加關注，期能達到運送工地前整體系統便具有良好的品質，故亦將 FAT 相關規畫列為視察項目。

總計本次稽查項目計有六項，如下所示：

1. 查證去年稽查結果處理情形

2. 數位儀控系統復工安全品質連貫性視察

3. 數位儀控系統品保作業績效查證

4. 數位儀控系統安全分析作業查證

5. 模擬器及人因工程(HFE)執行稽查

6. 數位儀控系統廠家驗收測試(D-FAT)規劃作業查證

參、稽查團隊

此次係原能會第二次赴核四儀控廠家稽查，因此相關作業大體參酌第一次稽查方式辦理，包括行文核研所及台電公司(如附件一)，請其派員會同執行視察作業；根據中美民用核能合作協定「數位儀控系統審照程序」合作案之協議，邀請美國核管會派員擔任觀察員(如附件二)；另外，為求稽查作業更加周延，就近邀請旅美核能專家，同時也是原能會核子設施安全諮詢委員孫國華博士加入團隊，擔任顧問；並於行前邀核研所、台電公司相關人員召開二次稽查準備會議等。

稽查小組領隊由核管處莊技正擔任；核研所派核儀組組長謝得志博士及副研究員易俗博士參與支援，謝博士專精人因工程，易博士專長於軟體品質驗證與確認作業；孫博士也在百忙之中，撥冗參加；美國核管會派資深數位儀控專家 Mr. Matthew Chiramal 擔任觀察員，全程參與稽查作業。

台電公司為配合原能會稽查，派核技處李定遠副處長擔任台電領隊，並率侯明亮副處長、李精一課長、張飛龍股長及林錦銘工程師會同原能會的稽查。另外，台電聘廖本達博士擔任顧問。

台電核四「業主獨立驗證與確認」(Owner Independent Verification & Validation，OIV & V) 專案成員 MPR 公司的 Mr. Robert Fink 與 Mr.

David Herrell 亦全程參與，且負責紀錄。

奇異公司則由負責核四計畫工程經理 Tim O'Neil 及電氣應用部經理 Monty Ross 率發展團隊相關部門主管及簡報負責人共數十人參與。

整個稽查團隊及台電與奇異公司出席人員之名單如下：

原能會：領隊：莊長富技正

團員：核研所謝得志博士、易俗博士

顧問：原能會核子設施安全諮詢委員　孫國華博士

NRC 觀察員：Mr. Matthew Chiramal

台電人員：領隊：李定遠副處長

團員：候明亮副處長、李精一課長、張飛龍股長、

林錦銘工程師

顧問：廖本達博士

MPR 公司：Mr. Robert Fink 與 Mr. David Herrell.

奇異公司：Tim O'Neil (Manager，Project Engineering)、

Monty Ross (Manager，Electrical Applications)、

Brit Grim (Manager，Independent Review Team)、

Steve Stark (Manager，Lungmen Licensing)、

Jim Howard (Manager，Control/Electrical Systems)、

Bishara Kakunda (Manager，NUMAC Applications)、

Kim Yu(Manager，Distributed Control &Information Sys) 、

Peter Holan (Lungmen Project Engineer)、

Rich Wolters (Manager，NPP Quality)、

Dave Chien (Senior Engineer，Lungmen QA)、

Jerry Marks (Principal Engineer，Plant Computer System)、

Steve Baham (Contractor，Independent Review Team)、

Ira Poppel (Principal Engineer，Control Systems Design)、

Steve Sawyer (Principal Engineer，DCIS，Plant Simulator)、

Rich Gutierrez (Principal Engineer，DCIS，HFE)、

Dave Zizzo (Senior Engineer，DCIS，CRDT)、

Rich Oda (Principal Engineer，Lungmen CM)、

Bob Turkowski (Manager，Systems Integration/Plant Performance)

Lisa Moody(Chairperson BRT)、

Carol Buchholz (Leader，Software Safety Analysis) 、

Richard Chiou (Assistant Taiwan Engineering Manager)、

Joe Walker、Bob Morris、Bill Tsai，etc.

肆、稽查過程

第一天早上準備進行稽查時，奇異公司先提出程序問題，其表示稽查簡報內容含有奇異公司商業機密資料(Proprietary information)，在NRC 未與奇異公司針對龍門計畫保密協定簽妥前，希望 Mr. Chiramal 簡報時不要在場，並表示另已備妥辦公室供其使用，經稽查小組表示 Mr. Chiramal 係原能會邀請貴賓，其參與稽查之相關作為由原能會負責，況且核能安全為大家所最關注事項，而在審照過程中有專家參與，其對於最後核照必將有正面積極的意義，且奇異公司係臨時提出簽署保密協定的要求，經審視其協定書又是草案版，如附件三，內容亦非針對此次稽查，故稽查小組認為若需要簽署宜先修改內容並議妥正式文稿後再簽，且從下次稽查時再開始實施，此次宜比照去年五月第一次稽查方式處理。經過一番折衝，奇異公司終於妥協，但表示會後 Mr. Chiramal 不得帶走簡報文件，且會中不許作筆記。稽查小組徵詢 Mr. Chiramal 是否可接受，Mr. Chiramal 輕鬆地表示沒問題，更幽默表示他已達很容易健忘的年紀了，"My age is easy to forget"，使稽查會議未開始便劍拔弩張的氣氛頓時緩和。

稽查活動開始前先舉行開幕式，台電公司及奇異公司先致歡迎辭，隨後各方互相介紹成員，稽查小組感謝台電及奇異公司的配合並表明稽查目的、稽查事項等；隨後進行稽查活動，採簡報、現場視察、

電腦瀏覽、文件抽查等方式交替進行，二天的議程如表一，相當緊湊，延伸觸及之範圍則較原訂六項廣泛。第二天下午則舉行稽查後會議，會中稽查小組提出初步稽查發現；相關稽查作業場景，如附件四照片所示。

簡報

奇異公司針對本次稽查項目，共進行下列十二項簡報，其中第一項至第七項於稽查第一天簡報，其餘於第二天進行。

1. Lungmen PSAR Chapter 7 Update
2. MVD Design Principle to Meet Single Failure Criteria
3. Design Status for Hardwired Backup and Remote Shutdown Panel
4. APR Reliability and Availability

   （註：以上四項係去年五月稽查後之追蹤項目"Previous Audit Follow-Up"）
5. Coherence of Safety Quality in Lungmen Restart
6. Implementation Status for Software Ⅳ&V
7. Simulators and HFE
8. Lungmen Document Control
9. DCIS Software Safety Analysis
10. EQ plan
11. NUMAC Proveness
12. Status of Lungmen DCIS Factory Acceptance Tests

簡報過程中，稽查小組隨時提出問題，未能當場澄清或有需調閱文件進行查證等事項，則登錄下來，在稽查第二天下午進行查證。

現場參觀

第一天參觀龍門儀控系統工程模擬器(GE Test System，GETS)，而德國 STN 公司運抵此間之全規模模擬器（Full Scope Simulator）因尚未開箱，故未安排參觀。GETS 的目的係作為核四控制室發展作業用以檢驗人機介面的工具，以避免控制室發展作業發生缺失，因此具有相當重要之階段性任務，且其發展應走在控制室儀控系統發展之先，雖然展示內容較去年稽查時豐富，但仍進度緩慢，未能適時配置完備功能，影響人因工程驗證與確認之執行，進而影響整體工程品質，殊值得特別關注。

第二天參觀 NUMAC（全名為 NUclear Measurement And Control）系列產品用於核四計畫上之開發情形，及核四反應器保護系統發展情形。與去年相較，已頗有進展。另外，為了裝置這些儀控設備，奇異也作了一個控制室背後盤雛型（Prototype Cabinet）進行耐震與 EQ 測試用，看起來相當堅實(Robustness)。

電腦資料庫瀏覽

核四計畫設計資料檔案的管理、停工期間檔案資料的存放與保

護、復工後新進人員使用設計檔案的熟稔度等議題，是此行稽查的重點項目。為此，奇異公司以電腦瀏覽方式（Navigation）實際展示其用在核四計畫上之電腦資料庫系統，以說明其核四計畫資訊管理系統（Information Management System，IMS）、PSAR 檔案更新等作業。瀏覽過程中稽查小組指定查閱工程設計變更（Engineering Change Notice，ECN）未結案資料及 PSAR 第七章儀控系統修改更新部分，展示人員熟練操作系統，很快將相關資料呼叫出來，充分顯示使用現代化電腦資料庫技術的便捷性。

鑑於汐止遠東科學園區大火，部分廠商電腦遭祝融，因無備份資料致與客戶間之營運產生相當困擾，位於該園區的石威公司，是核四計畫的工程顧問公司，其電腦差一點也遭殃，若發生損毀，對核四計畫的後續工作必定會有相當負面之影響，此可顯示資料備份的重要性。為此特提出詢問資料備份與安全防範的作法？奇異公司表示有備份措施，且送台電的資料雖與奇異公司資料庫之最新資料有一星期之差，亦可視為備份；另外為保護資料之安全性，對人員使用資料庫亦有密碼與等級管理等措施。

整體而言，瀏覽核四計畫相關電腦資料庫後，令稽查小組印象深刻。IMS 資料庫是核四計畫的重要工具，資料庫維護良好意味構型管理良好，是計畫成功的保証，也是未來電廠商轉後維護與運轉不可或

缺的利器，IMS 並將伴電廠一輩子。目前建廠階段由奇異公司負責 IMS 資料輸入與維護工作，電廠商轉後 IMS 將移由台電維護，故核四廠宜有專人參與並熟悉核四計畫 IMS 系統，並強化備份及管制措施。

查証作業

簡報過程中將需進一步作查証之項目，逐一於會議室的白板上登錄下來，最後計有十九項，其與視察計畫六個項目之對應關係如表二所示。在第二天下午進行查證作業時，奇異公司安排相關人員攜帶相關文件供稽查小組逐一查證，茲將重要項次並依視察計畫六個項目分述如下:

1. 查證去年稽查結果處理情形(表二項次 11，16)

◎項次 11 有關 PSAR 第七章部分內容因 ESF 系統改由 Eaton 負責而非原先 NUMAC，致需作更新之追蹤事項，奇異公司表示更新內容預計今年底送石威公司及台電公司，台電表示其將再以一個月時間完成審查後再送原能會。整個 PSAR 的更新及發行工作是石威公司負責的，奇異公司自己可完全掌握的章節是以 PDF 檔送給石威公司(註 PDF 檔不易修改)，其餘則送 WORD 檔給石威公司修改、整合及發行工作。

◎項次 16 有關反應器保護系統（RTIF）與預期暫態未急停系統

（ATWS）的「使用驗証（Proveness）」問題，奇異公司提供該等系統的檔案供查証，稽查小組要求奇異公司提供檔案中數頁作為查証紀錄，如附件五、六。

2. 數位儀控系統復工安全品質連貫性視察(表二項次3，5，12)

◎針對項次 5：新進人員受訓資料，稽查小組表示將索取相關資料影本以作為稽查紀錄用，剛開始時，奇異公司以新進人員受訓資料上有人名，涉及隱私，故拒絕提供，經稽查小組強烈表明原能會執行復工稽查立場，並將於正式稽查報告中附上相關佐證資料後，奇異公司終於讓步，同意將相關資料影本提供稽查小組，但要求准於影本上塗掉新進人員名字，稽查小組同意此項折衷建議。新進人員受訓抽查紀錄如附件七。

基本上，奇異公司龍門計畫的儀控組織人力復原係採調回原班人員與晉用新人並行方式進行，其儀控部門組織如圖二所示。人力異動情形由停工前八十六人降至停工時期的十八人，再回復至現在的六十七人，奇異公司依其公司內部工程相關程序書(Engineering Operation Procedure，EOP)EOP- 75-5.00：品質與技術訓練程序書(Quality and Technical Training)來執行人員訓練，訓練包括自我研讀與課程訓練。訓練結果並由負責部門經理確認後

列入奇異核能部門(GENE)訓練資料，作為人員資格資訊。透過前述程序之執行，使設計人員素質不致因停工而受影響；另外，奇異公司經理Mr. Monty Ross表示雖然停工期間大部分人員離開了計畫，但復工後原班人馬歸建的人力目前已達近60%，再加上新進人員，整個人力恢復情形也達停工前的78%，如表三；同時，不足之人力也陸續晉用新人。其更表明奇異公司不僅重視新進人員能力及與核四計畫相關之受訓紀錄外，更重視整體作業品質，其強調奇異公司保証會維護核四整體計畫品質，同時也保証會以相同標準要求其所屬包商達到品質要求。應稽查小組要求，奇異公司同意將該段口頭保証之聲明寫下來當稽查記錄，如附件八。稽查小組對奇異公司在龍門計畫的儀控組織人力復原的努力情形給予肯定。

◎項次3、12奇異公司對Eaton與Foxboro等公司於停工期間執行保存與保護計畫（P&P Plan）之執行紀錄，稽查小組表示將索取相關資料影本以作為稽查紀錄用，剛開始時，奇異公司以 P&P 計畫執行紀錄有奇異公司商業機密（Proprietary Information）等問題拒絕提供，經稽查小組強烈表明原能會執行復工稽查立場，並將於正式稽查報告中附上相關佐證資料後，奇異公司終於讓步，同意將相關資料影本提供稽查小組，奇異公司對 Eaton 與

Foxboro 公司執行 P&P 紀錄如附件九、十。

停工期間奇異公司以工作進度紀錄(Work Package Status Record，WPSR)之方式進行設計文件保存與保護之工作，工作進度記錄以每一個工作案(Work Package)為單位，每一單元完成後加一摘要，註明設計紀錄檔案(Design Record File，DRF)編號、說明、完成項目、待辦項目、適用系統編號、適用部門、採購編號、廠家名稱、整理者姓名、日期及工作進度紀錄等，WPSR 樣本如附件十一。工作進度紀錄完成後，並以電子檔送出由專人管理，復工後相關文件完整送回給相關工作人員。復工後之工程設計品質可不致因暫停而受到影響，復工後可完整的查閱文件。奇異公司在文件保存與保護方面制度及執行結果可接受。

雖然奇異公司的復工情況堪稱令人滿意，惟其下包之重要儀控廠家 Foxboro 遲至八月上旬才復工，而另一重要下包儀控廠家 Eaton 公司負責 ESF 系統迄今尚未復工，且其間還存有 Eaton 要求於控制室背後盤區增加盤面的設計變更問題存在，奇異公司與 Eaton 公司間為何會有數量頗多之盤面增加的議題，值得深究。奇異公司表示目前正採分開處理之方式進行，先以 Eaton 人員復員為主要目標，至於盤面數目變更等設計問題，則待人員復員後再解決。然此情況對目前復工後，需各廠家都能互相配合、全力

展開設計作業，以進行整體儀控發展作業是一相當不利之因素，亟需儘速改善。

3. 數位儀控系統軟體品保作業績效查證(表二項次 13)

◎核四廠儀控系統採用全數位化設計，而數位化系統運作功能主要係由軟體驅動，因此軟體品質優劣對電廠未來運轉安全影響重大。確保軟體品質安全可靠方法為執行嚴謹之驗證與確認（Verification and Validation）工作，稽查小組將其相關工作之執行情形皆列為查核重點項目。初步查證結論為：維持現行多軌審查作業方式，即 GE 內部 V&V， GE IV&V， CDA 顧問審查，MPR OIV&V， TPC 內部審查，石威公司審查等之作法基本上可接受，惟應將各項審查作業結果予以整合，以決定其最終品質成效；未來更應該加強軟體品質相關文件審查、軟體程式碼審查及軟體功能動態測試等工作。

◎另項次 13 有關 IVVP 版次問題，由於在 PSAR 審照時曾正式要求台電公司在 IVVP 改版時比照 PSAR 內容更新方式需送原能會備查，而目前原能會、台電公司及奇異公司所用版次分別為四、五、六版，台電解釋係因 IVVP 改版時恰逢停工，諸多事情紛至沓來致疏忽了報原能會步驟。惟此案例仍顯示文件版次的管理有加強

空間。

4. 數位儀控系統安全分析作業查證(與表二項次 14，15 相關)

軟體安全分析是數位儀控系統發展作業中居樞紐地位的一項工作，因各發展階段均須將階段成果/成品送交至安全分析工作人員，經由安全分析作業鑑別是否存在潛在的危險因子（Hazards），並分析其效應，同時提出對策建議供原設計部門作修改時參考。該項簡報顯示其已有部份成果及發現，因此稽查小組要求其提出"Critical Findings"資料以供查證(項次 14)，初步檢視發現目前已完成之安全分析階段報告內容並不深入，即所分析內容及結論較偏格式性問題，因此迄今尚無一項發現須要回饋至相關部門以進行修正。

5. 模擬器及人因工程 HFE 稽查(與表二項次 4，6，7，8，9，10，17 相關)

全規模模擬器係依據 1999 年 8 月的設計資料進行發展，目前已由德國 STN 公司運抵奇異公司。此模擬器尚未將核四廠已採用之線上電腦化程序書功能(On-line Procedure System，OLPS)及自動功率調節系統(Automatic Power Regulating System，APR)納入，亦未執行人因工程分析，致產生目前模擬器將與未來實際控制室不盡相同，而需作更新及如何對運轉人員訓練等問題。稽查小組對模擬器與實際控制室間逼真度驗證及模擬器用以訓練成效等二大議題相

當關切，並以運轉員緊急操作程序書(Emergency Operation Procedure，EOP)訓練方式為例，請奇異公司仔細說明，且要求其提供一份 EOP 格式(項次 4，8)。奇異公司回答表示未來訓練運轉人員緊急操作程序書將採用紙本流程圖(Flow Chart)之方式，而不是OLPS，稽查小組質疑此方式之訓練成效及其對電廠運轉安全之影響，並請台電公司說明其立場(項次 9)，台電公司表示此一原能會關切事項亦是其急欲解決之事項，目前其正與奇異公司洽商模擬器更新、人因工程驗證、接收測試、及訓練等相關事宜，在此過程中將把稽查小組關切事項一併納入處理。稽查小組同意並表示此項議題將擇期召開專案會議，屆時將再仔細檢討。

6. 數位儀控系統廠家驗收測試規劃作業查證(與表二項次 18，19 相關)

廠家接收測試(Factory Acceptance Test， FAT)為系統運抵工地安裝前，可在廠家執行的最後一項驗證工作，有其特殊的涵意存在，故原能會對該項目甚為重視。奇異公司簡報目前正進行 FAT 相關工作的研擬規劃，由於整個核四數位儀控是由奇異公司、NUMAC、Eaton、Foxboro 及日本日立等公司共同發展，這些公司分佈美國東、西二岸及日本等地，地緣位置甚遠，且這些系統又有安全系統(1E)與非安全系統(Non 1E)之分，要順利完成整個測試是一項很重要且複雜的工作。奇異公司雖然對整個系統負責主導及整

合工作，然其對 FAT 是採分區塊測試(Segment)方式在各廠家進行，而不是把所有廠家完成的系統與設備集中在一起測試，FAT 區塊測試示意圖如圖三所示，對於不同廠家測試時，不同廠家界面間所需之設備則依需要搬移至相關廠家。

稽查小組對於 FAT 測試程序書由誰撰寫、由誰審核、測試內容與項目、網路負載與資料傳輸品質、測試不順或失敗時之回饋機制、非安全系統信號送至安全系統(註：中子偵測系統 NMS 有此種信號)之測試等事項表示關切(項次 18 與 19)。台電與奇異公司皆表示將把稽查小組這些關切事項納入 FAT 規劃計畫內，台電更表示目前正將 FAT 與工地接收測試(SAT)一起考量，對於 FAT 因受限於區塊測試而有不足之處或有未適當執行之測試，將在 SAT 強化這些項目的測試。稽查小組表示將持續追蹤 FAT 相關工作的進行，並請台電隨時提供 FAT 相關工作進展資料供原能會瞭解。

伍、結論與建議

本次稽查工作經原能會核安諮詢委員孫博士、核研所謝得志博士與易俗博士、及美國核管會 Mr.Chiramal 全力支援，又於執行過程中得到台電、奇異充分配合，因此稽查工作得以順利完成。稽查後孫博士、核研所及 NRC Mr.Chiramal 也都提出報告，分如附件十二、十三、十四，肯定此次稽查對於監督管制龍門儀控系統發展復工作業品質具有一定之成效。

稽查結果顯示奇異公司復工後人力歸建、晉用新人及對新人訓練等方面的復工情況堪稱令人滿意；而在停工期間對核四數位儀控系統發展工作相關設計文件與半成品的保存與保護計畫執行情況亦良好，使復工後可供完整查閱原設計文件，以進行設計工作。惟其下包之重要儀控廠家 Foxboro 遲至八月上旬才復工，而另一負責 ESF 系統之重要下包儀控廠家 Eaton 公司迄今尚未復工，且其間還存有 Eaton 要求於控制室背後盤區增加盤面的設計變更問題存在，此問題無可避免將會產生搶控制室背後盤空間，並迫使其他廠家或系統盤面遷移等連串性問題；奇異公司與 Eaton 公司間為何會有數量頗多之盤面增加的議題，值得深究。此情況對目前復工後，需各廠家都能互相配合、全力展開設計作業，以進行整體儀控發展作業是一相當不利之因素，亟需儘速改善。

至於稽查發現之問題，如 GETS 整體發展作業未能適時配置完備功能，影響人因工程驗證與確認之執行、強化核四計畫 IMS 系統資料備份及管制措施、儘速改善 Eaton 公司未復工及盤面設計變更問題、加強軟體驗證與確認工作、加強儀控發展作業文件版次管理、強化軟體安全分析結果之審查、儘速研擬模擬器與實際控制室間逼真度驗證及模擬器用以訓練成效等相關事宜處理方案、明確表列 FAT 未適當執行之測試並在 SAT 強化這些項目的測試等，則分別開立「注意改進事項」，編號 AN-LM-90-025 至 AN-LM-90-032 共八件，如附件十五，來作進一步處理。

表一　稽查議程

日期	時間	項目	負責人/單位
10月2日	9：00～9：30	Welcome and Opening Remarks	李副處長/Ross/莊技正
	9：30～10：00	Previous Audit Follow-Up *A Changes in the PSAR* *B MVD Design Principle to Meet Single Failure Criteria* *C Status for Hardwired Backup and Remote Shutdown Panel* *D ARP Reliability and Availability*	 Stark Kakunda Howard Howard
	10：00～11：00	Coherence of Safety Quality in Lungmen Restart	Marks
	11：00～11：30	Implementation Status for Software IV&V	Grim
	11：30～12：00	Simulators and HFE	Yu
	12：00～13：00	Lunch	
	13：00～14：00	GETS Tour	Zizzo
	14：00～14：30	Documentation Control Demonstration	Oda
	14：30～17：00	Audits/Discussion	ROCAEC
10月3日	9：00～10：00	Lungmen DCIS Safety Analysis Activities *A DCIS Software Safety Analysis* *B Equipment Qualification Plan* *C Proveness of Safety Related NUMAC*	 Buchholz Kakunda Kakunda
	10：00～10：30	Planning Status of D-FAT	Marquino
	10：30～12：00	NUMAC Tour	Kakunda
	12：00～13：00	Lunch	
	13：00～16：00	Audits/Discussion	ROCAEC
	16：00～16：20	AEC Internal Discussion	ROCAEC
	16：20～17：00	Post-Audit Meeting	ROCAEC

註：實際稽查時之議程因問題討論、文件調閱查證等因素而作動態調整，與表內原排定之議程略有不同。

表二　查證項目表

項　次	查　　證　　內　　容	對應項目
1	Provide any available statistics on customer problems w/MVD system - Kakunda	一
2	Provide a sketch which shows the APR interaction with other systems -Poppel	一
3	Vendor audits for P&P	二
4	EOP Responsibility and Form	五
5	Provide training records of a new hire for review -Marks	二
6	Modify HFE-2 slide to indicate EOPs -Yu	五
7	Provide list of all systems modeled in HFE indicating which are not done yet -Yu	五
8	Provide copy of EOP format	一
9	What is impact of training using paper procedures and not OLPS during operator training on EOPs -Turkowski Morris	五
10	Approximately how many binders do we expect to have for procedures -Walker	五
11	Arrange for demo of PDM process as it relates to PSAR -Oda	一
12	Determine what records can be given ROCAEC to show evidence of the GE P&P audits of Eaton/Foxboro -Ross/Walker	二
13	Provide revision level of IVVP in SJ and in TPC HQ -Baham/Ho	三
14	Show the critical to safety findings from SSA Task 1-Buchholz	四
15	Bring a copy of EOP 42.6 for AEC Inspection - Buchholz	四
16	For RTIF and ATWS ROCAEC would like to see documentation of proveness - Kakunda	一
17	Include EOPs, Human Interaction, Auto-Manual Function in HFE V&V BOX	五
18	Show documentation on process in DFAT implementation plan	六
19	Show throughput on data highway load testing	六

表三　奇異公司儀控部門人力異動表

人力 / 組別 (1)	停工前	停工期間	現　在	備　　註
DCIS	18	6	13	100% former DCIS members, i.e.13
C&ES	27	9	24	67% former C&ES members, i.e.16
NUMAC	38	3	28	68% former NUMAC members, i.e.19
SSA	3-1/2	0	2-1/2	100% former SSA members, i.e.2.5
小計	86.5	18	67.5	50.5

註：(1)名詞

DICS – Distributed Control and Information System

C&ES – Control and Electrical System

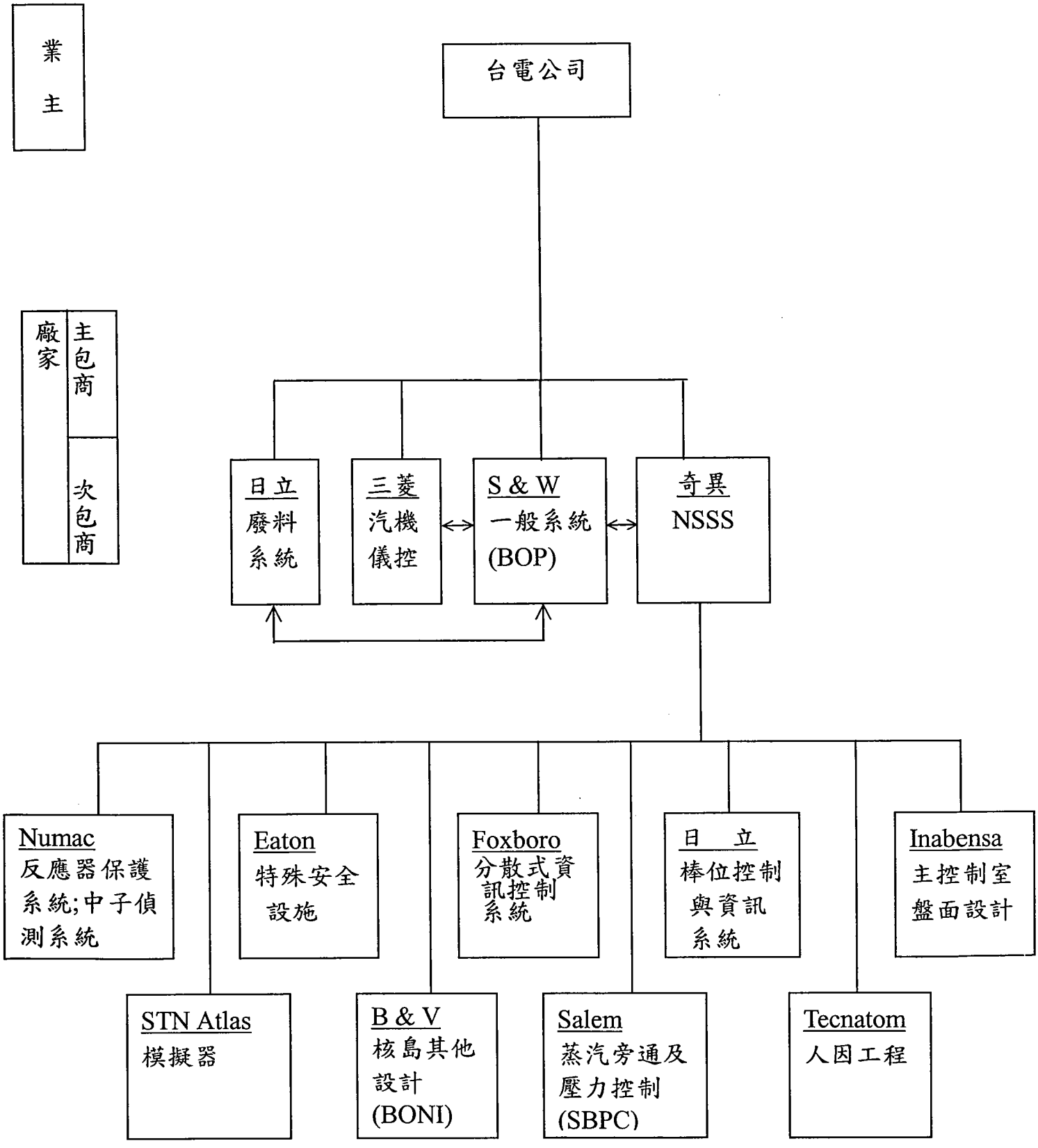
NUMAC – Nuclear Measurement And Control

SSA – Software Safety Analysis

(2)復工後歸建人力百分比：$\frac{13+16+19+2.5}{18+27+38+3.5}$ =60%

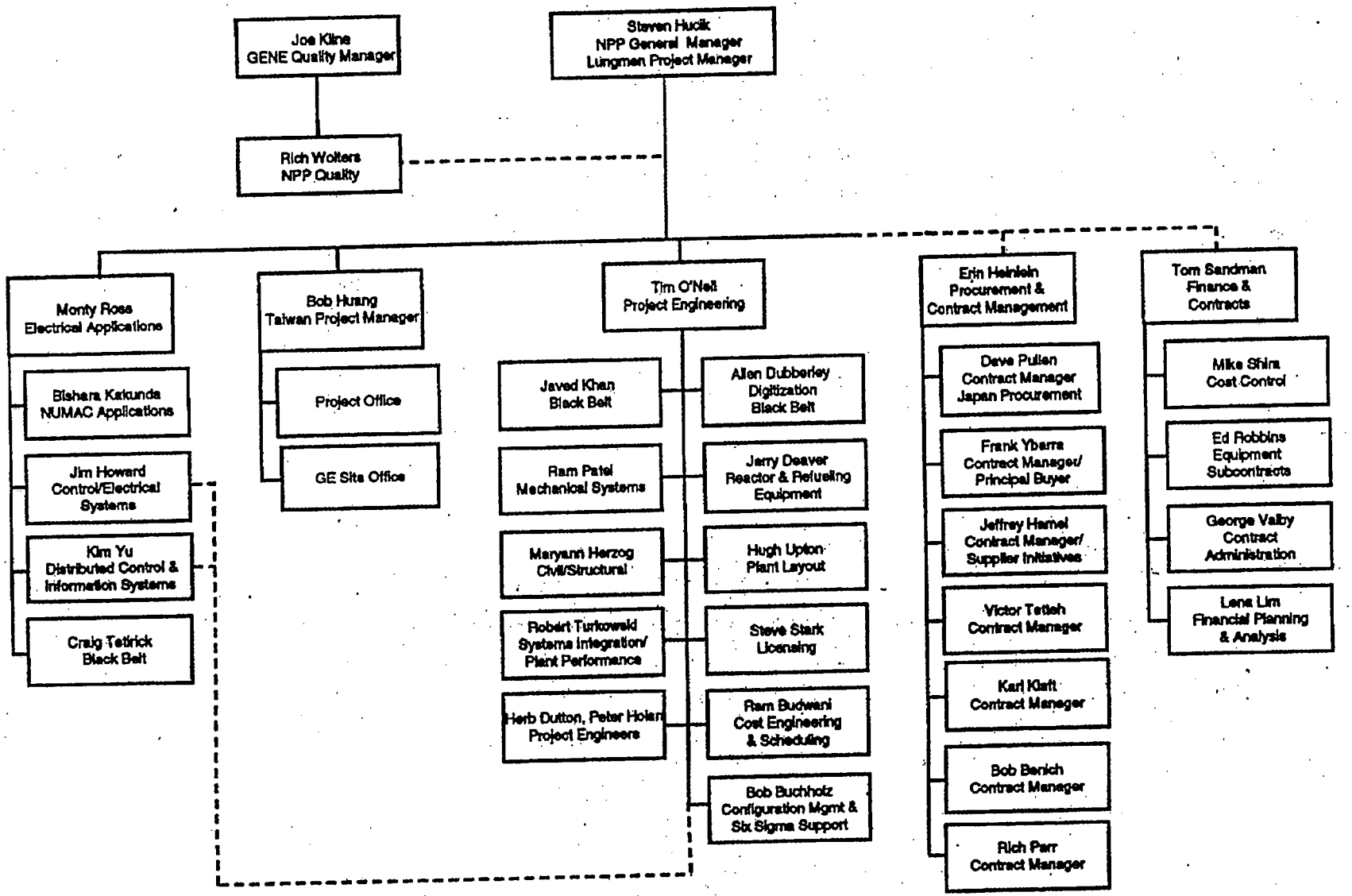
復工後復原人力百分比：$\frac{67.5}{86.5}$ =78%

圖一　核四廠數位儀控系統發展廠家圖

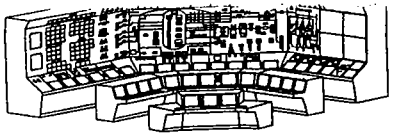


*奇異公司負責數家美、日廠家數位儀控硬、軟體系統整合

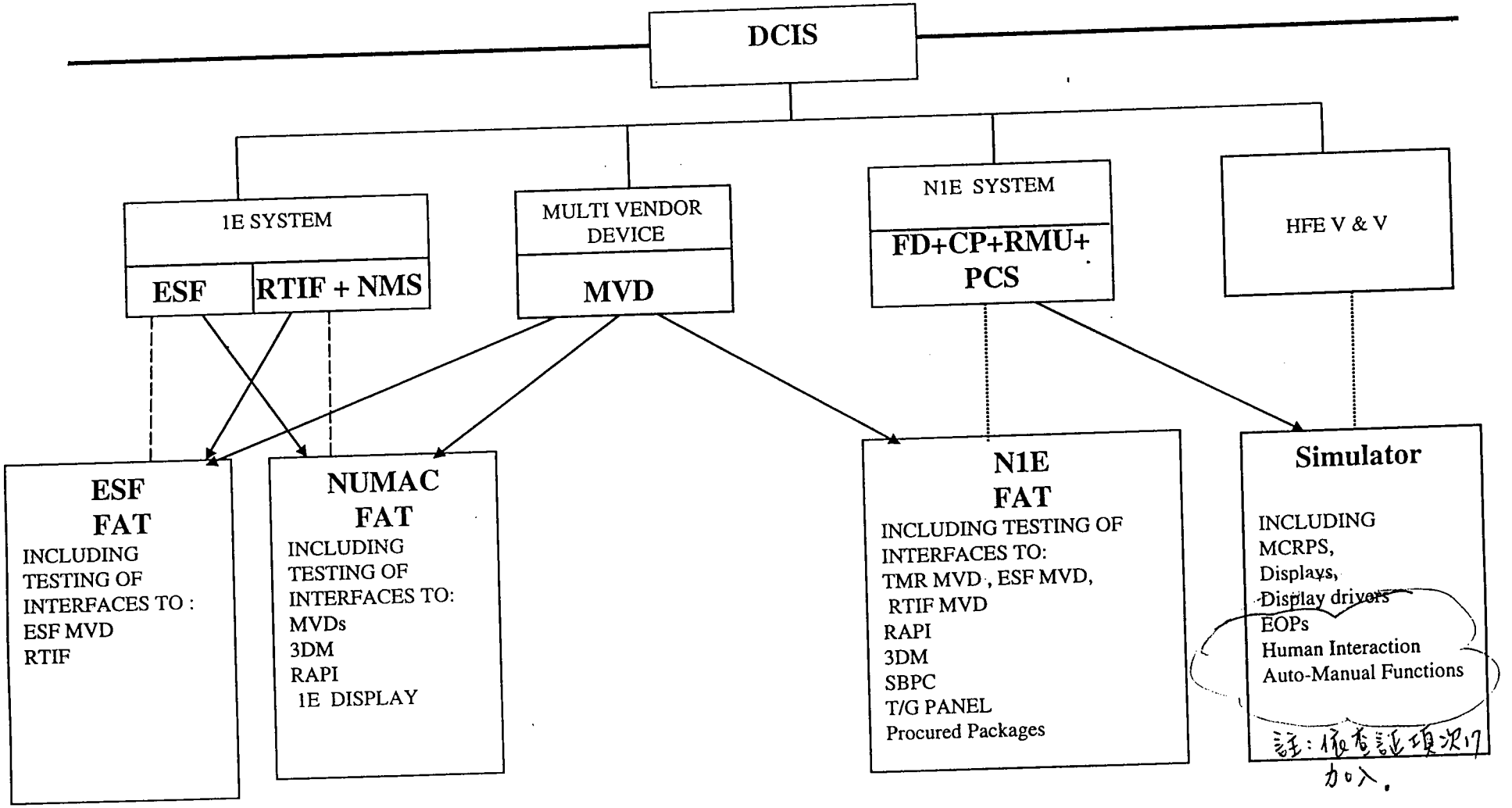
GE Lungmen Project Organization



圖二　奇異公司龍門計畫組織圖



DCIS FAT Segments



Interfaces between NUMAC, Eaton, 1E and Non 1E, are Tested

GE Company Proprietary

圖三　DFAT 區塊測試示意圖

附件一

行文台電公司及核研所

C051 3-2

以稿代簽

行政院原子能委員會　書函（稿）

受文者：如行文單位

檔號：C051
是否續辦：
速別：速件
密等及解密條件：
發文日期：中華民國 90 年 8 月 3 日
發文字號：
附件：核四廠數位儀控系統發展作業復工視察計畫

無法電子交換

主旨：為落實核四計畫復工安全管制，本會將於九十年十月一日至三日執行核四廠數位儀控系統發展作業復工視察，計畫如附，請惠予安排並派員會同執行視察，請　查照。

正本：台灣電力公司、本會核能研究所
副本：

（會戳）

擬奉核可後發

機關地址：台北市基隆路四段一四四巷六十七號
傳真：（〇二）二三六八三五九一

090160D00960

核能管制處處長 沈禮 0826

核能管制處副處長 倪維斌 0824

技正莊長富 0824

核四廠數位儀控系統發展作業復工視察計畫

一、視察時間：

90 年 10 月 1 日至 90 年 10 月 3 日

二、視察地點：

奇異公司(加州聖荷西市)

三、視察項目：

(一)查證去年稽查結果處理情形

(二)數位儀控系統復工安全品質連貫性視察

(三)數位儀控系統品保作業績效查証

(四)數位儀控系統安全分析作業查証

(五)模擬器稽查

(六)數位儀控系統廠家驗收測試規劃作業查證(FAT)

四、注意事項

(一)請核研所、台電公司派員會同執行視察。

(二)請核研所協助就視察項目預先設計問題清單。

(三)本案承辦人：莊長富

電　　話：886-2-23634180 轉 307

傳　　真：886-2-23635377

電子郵件：chuang@aec.gov.tw

附件二

邀請 NRC 派員參與稽查作業

行政院原子能委員會
ATOMIC ENERGY COUNCIL, EXECUTIVE YUAN
67, LANE 144, KEELUNG ROAD, SECTION 4
TAIPEI, TAIWAN 106, REPUBLIC OF CHINA
TEL:886-2-3634180
FAX:886-2-3635377

Dr. Michael C. Cullingford
Special Assistant for Technical
Policy & International Liaison
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington D.C.,20555-0001

Aug. 27,2001

Dear Dr. Cullingford:

As you know that Lungmen Project has gone through a suspension and resumption process. This interruption event poses a challenge to ROCAEC's regulation tasks. Our major concern focuses on how TPC and vendors maintain equivalent quality level before and after project interruption. Since it has been 6 months after the project resumes, we consider it is an appropriate time for conducting a site audit to Lungmen digital I&C development activities. So we are planning to dispatch a task force with three staffs lead by Mr. Chuang to audit GE Nuclear at San Jose ,CA from Oct. 2 to 3,2001.

Based on the AIT-TECRO AE-NR-S24 program and our previous agreements, we cordially invite the NRC staffs to attend this audit plan. Also, we would like to suggest to have a pre-meeting on Oct.1 between ROCAEC and NRC participants to discuss technical issues related to this audit. Due to the limited time available for preparing this audit, your prompt response will be highly appreciated. We do appreciate your continual support in our review activities .

With Best Regards.

Sincerely yours,

L. Shen

Li Shen, Ph. D.
Director
Department of Nuclear Regulation

C.C: Kevin D.Burke
Dr. Thomas T. Tseng

附件三

奇異公司龍門計畫保密協定草案版

Draft, 9/20/01

DRAFT

PROPRIETARY INFORMATION AGREEMENT
PAGE 1/3

General Electric Company
And
Taiwan Power Company
And
Republic of China Atomic Energy Council
And
United States Nuclear Regulatory Commission

THIS AGREEMENT, by and between Taiwan Power Company (hereinafter referred to as "Purchaser"), General Electric Company acting through its GE Nuclear Energy business component (hereinafter referred to as "Seller"), the Republic of China Atomic Energy Council (ROC/AEC) and the United States Nuclear Regulatory Commission (USNRC), (ROC/AEC and USNRC are hereinafter referred to collectively as "Reviewers"), is entered into to provide for the protection of information that Seller considers proprietary, trade secret or confidential (which it is understood may include such information of Seller's suppliers) (hereinafter referred to as "Seller's proprietary information") that will be used in Purchaser's proceedings before the ROC/AEC to obtain an operating license for the Lungmen Nuclear Power Project (NPP) in Taiwan. Seller's proprietary information will be used by Reviewers only in their technical review of the Lungmen NPP design in connection with the Lungmen NPP Operating License proceedings of the ROC/AEC (hereinafter referred to as the "Purpose").

Whereas, Seller's proprietary information has been or will be provided to Purchaser by Seller under Contract No. 8748611M001-1 between Purchaser and Seller for the Lungmen NPP, effective as of October 16, 1996, as amended, (the "TPC/GE Lungmen Contract"), which contains provisions restricting use, publication, and disclosure of Seller's proprietary information provided under such contract; and

Whereas, Purchaser desires to disclose, or have Seller disclose, Seller's proprietary information to Reviewers as necessary for the limited Purpose as described above, and Seller is willing to agree to such disclosure to Reviewers for such Purpose provided that Purchaser and Reviewers agree to be bound by the provisions herein.

1. Purchaser shall clearly identify all of Seller's proprietary information that is furnished or otherwise disclosed to Reviewers. Purchaser shall reproduce all of Seller's proprietary, trade secret and other notices on all documents or copies that are furnished or otherwise disclosed to Reviewers. If ROC/AEC discloses any such information to USNRC directly, ROC/AEC shall be bound by the foregoing provisions in the same manner that Purchaser is bound with respect to any of Seller's proprietary information that ROC/AEC discloses to USNRC. If Seller furnishes or otherwise discloses any of Seller's proprietary

information to ROC/AEC or USNRC, in the course of an audit or otherwise, Seller shall clearly identify such information as Seller's proprietary information.

2. Reviewers shall maintain all of Seller's proprietary information in confidence and not disclose such information or transmit any documents or copies containing such information to any third party, without the prior written consent of Seller. Seller's proprietary information shall be used solely in connection with the Purpose, and shall not be used in any other work without the prior written consent of Seller. In the event Reviewers submit documents to Purchaser that include any of Seller's proprietary information, Reviewers shall specifically identify such proprietary information as Seller's proprietary information.

3. All of Seller's proprietary information furnished by Purchaser to Reviewers remains the property of Seller. Reviewers shall return to Purchaser all of Seller's proprietary information, including all copies thereof and all documents of USNRC that contain any such information, when no longer needed for the Purpose, and in any event upon issuance of the Lungmen NPP Operating License or termination of the Lungmen NPP. Any of Seller's proprietary information included in documents of ROC/AEC that are required to be maintained by ROC/AEC shall continue to be subject to the provisions of this Agreement.

4. Reviewers shall maintain appropriate policies and procedures adequate to protect the confidential nature of Seller's proprietary information to prevent unauthorized disclosure or publication of such information. Access to Seller's proprietary information shall be limited to the employees of Reviewers who need access in connection with performance of their work for Reviewers related to the Purpose.

5. If Seller's proprietary information is required to be disclosed pursuant to lawful subpoena, enforceable law or rule, applicable regulation or judicial or administrative order, the Reviewer that is subject to the requirement shall promptly notify Seller and use its best efforts to limit the disclosure and the information to be disclosed if and as reasonably requested by Seller.

6. The foregoing obligations shall continue in force until the later of December 31, 2020, or fifteen years following termination of the warranty period under the TPC/GE Lungmen Contract.

7. ROC/AEC agrees that no technical data, software, or other information or assistance furnished by Seller, or any product thereof, shall be reexported by ROC/AEC or its authorized transferees, if any, directly or indirectly from the Republic of China, except to the USNRC, unless expressly permitted in writing by Seller in accordance with U.S. export control laws

and regulations. The aforesaid obligation shall survive any satisfaction, expiration, termination or discharge of any other obligation.

8. This Agreement constitutes the entire agreement among the parties with respect to the subject matter hereof and shall supersede any prior discussions, representations and agreements related thereto. It may not be changed in any manner except by a written amendment signed by authorized representatives of the parties.

9. An authorized representative of each party has signed (4) copies of this agreement in the space provided below to indicate acceptance of and agreement with the above provisions, effective as of the last date of signature set forth below.

General Electric Company

Name (typed) Steven A. Hucik
Signature _____
Title: _____
Date _____

Taiwan Power Company

Name (typed)
Signature _____
Title: _____
Date _____

Republic of China Atomic Energy Council

Name (typed)
Signature _____
Title: _____
Date _____

United States Nuclear Regulatory Commission

Name (typed)
Signature _____
Title: _____
Date _____

附件四

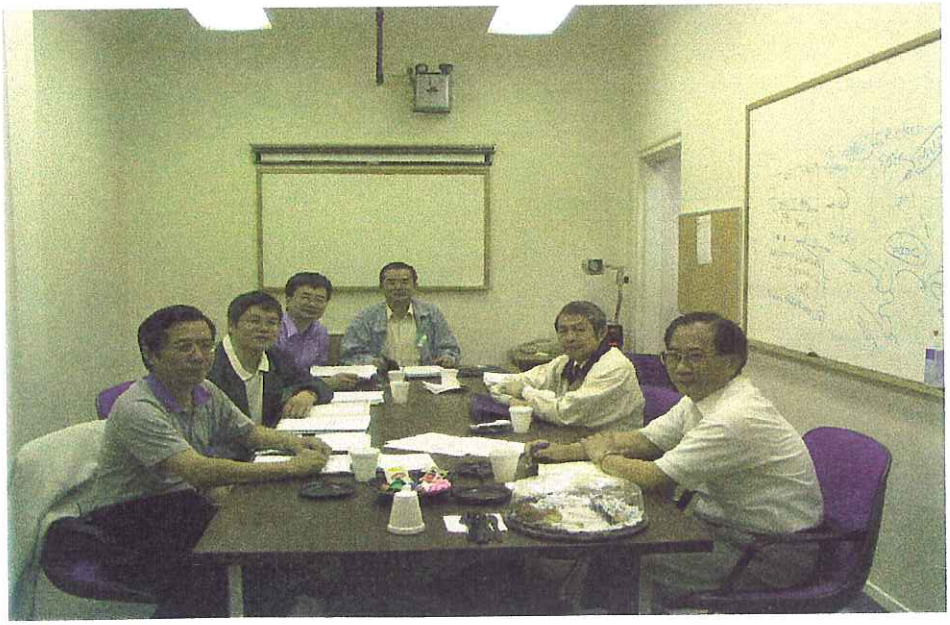
稽查照片

附件四　稽查作業照片

預備會議照片之一

與NRC Mr. Chiramal開預備會議

預備會議照片之二



與台電人員開預備會議

左起：李定遠副處長、莊長富技正、易俗博士、
李精一課長、謝得志博士、侯明亮副處長

稽查照片之一

莊技正稽查前致詞

稽查照片之二

奇異公司簡報復工現況

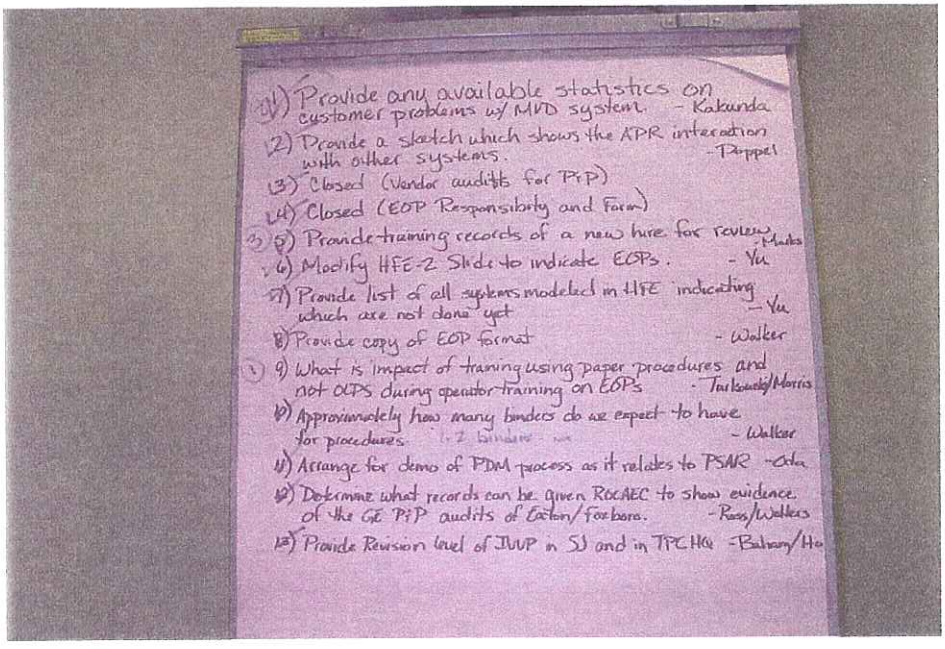
稽查照片之三

視察GETS

稽查照片之四

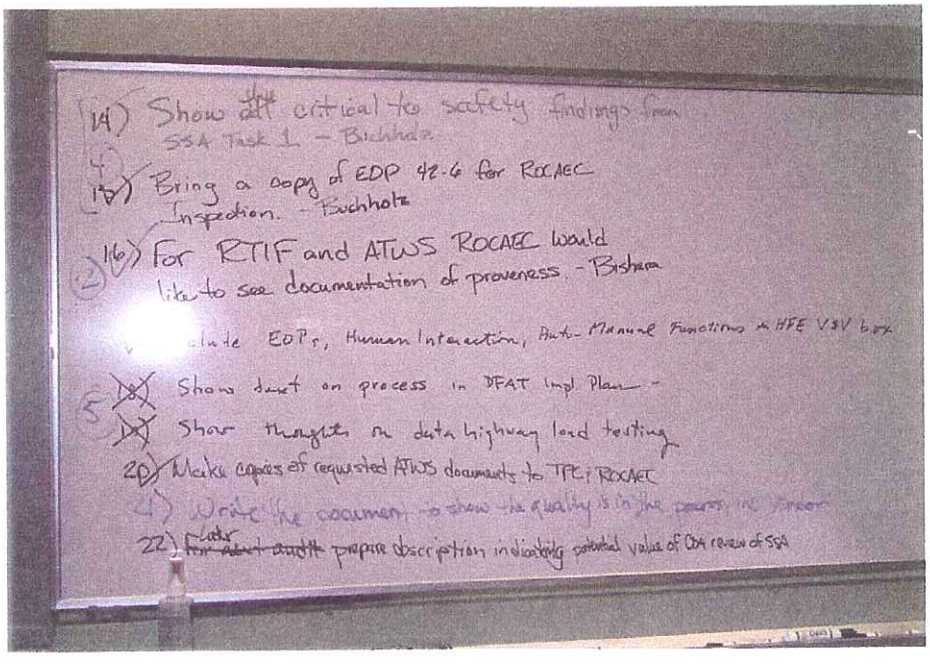
視察奇異公司NUMAC 發展作業

稽查照片之五



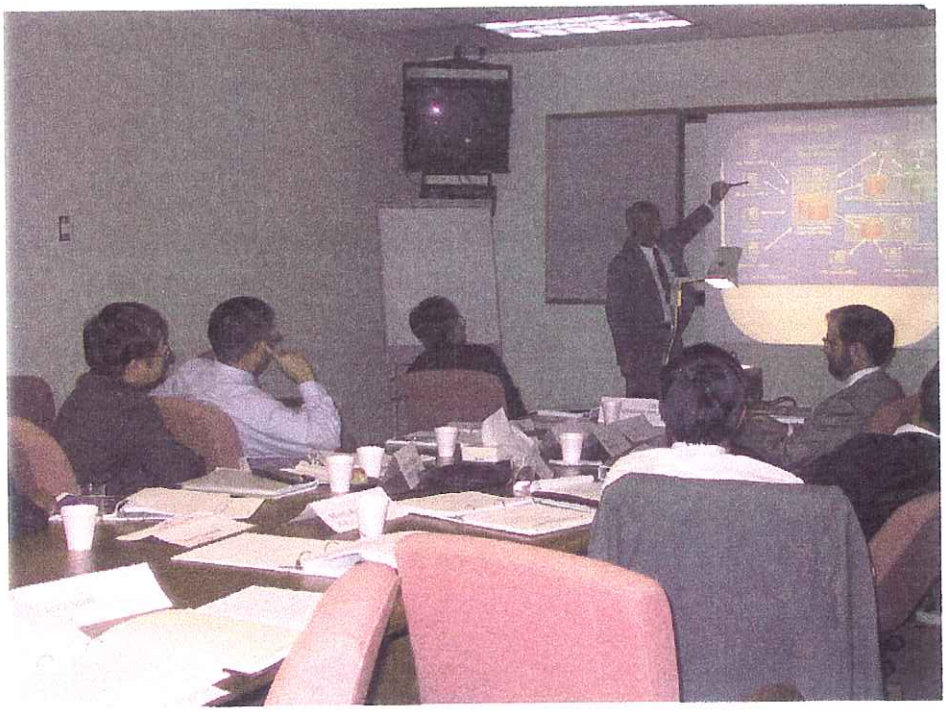
查證項目表之一

稽查照片之六



查證項目表之二

稽查照片之七



奇異公司簡報核四計畫IMS系統

稽查照片之八

進行稽查後會議

附件五

反應器保護系統查証紀錄

（內容涉及廠家 proprietary 資料不予公開）

附件六

預期暫態未急停系統查証紀錄

（內容涉及廠家 proprietary 資料不予公開）

附件七

新進人員受訓抽查紀錄

Training Requirements and Record for: [redacted]

Procedure No.	Title	I have read and understood the procedure.	
		Si	Date
EOP 25-5.00	Work Planning and Scheduling		8/16/01
EOP 25-5.10	Customer Technical Requirements and Design Inputs		8/16/01
EOP 30-3.30	Master Parts List		8/16/01
EOP 30-3.40	Engineering Information System		8/16/01
EOP 40-3.00	Engineering Computer Programs		8/16/01
EOP 40-7.00	Design Reviews		8/16/01
EOP 42-1.00	Design Process		8/16/01
EOP 42-5.00	Engineering Requirements Document Release		8/17/01
EOP 42-6.00	Independent Design Verification		8/17/01
EOP 42-8.00	Document Issue and Application by ERM		8/17/01
EOP 42-10.00	Design Record File		8/17/01
EOP 55-2.00	Engineering Change Control		8/17/01
EOP 55-4.00	Change Control Board		8/17/01
EOP 60-5.00	GE Designated Proprietary and Sensitive Information		8/17/01
EOP 60-5.10	Proprietary and Sensitive Information Received from Companies Outside GE		8/17/01
EOP 65-4.00	Reporting of Defects and Noncompliance Under 10CFR Part 21		8/17/01
EOP 75-3.00	Self-Assessment, Corrective Action and Audits		8/17/01
			8/17/01
GLP 2.2	Quality Classification		8/17/01
GLP 3.1	Engineering Change Control		8/17/01
GLP 3.3	Outside Proprietary Information		8/17/01
GLP 3.4	Resolution of TPC and Team Document Review Comments		8/17/01
GLP 3.6	Design Basis and Document Traceability		8/17/01
GLP 5.2	Use and Control of the Lungmen Codes and Standards Database		8/20/01
GLP 5.3	Issued Document Standards		8/20/01
GLP 5.4	Exporting of Technology and Equipment/Hardware to Taiwan		8/20/01
GLP 5.9	Client Information Request		8/20/01
GLP 5.10	Control of Text-Type Documents (Documentum)		8/20/01
GLP-16.1	Reporting of Defects and Noncompliances (for 10CFR21 and 10CFR50.55(e))		8/20/01
GLP 17.4	Quality Records Classification		8/20/01
			8/20/01
P&P 70-1	GE Nuclear Energy Quality Policy		8/20/01
P&P 70-42	Reporting of Defects and Noncompliance Under 10CFR Part 21		8/20/01

1. EOP = Engineering Operating Procedures for GE Nuclear Energy. These are available on the GE Nuclear Energy Intranet at URL # http://genet.ne.ge.com/procedures/eopindex/eopind.shtml
2. GLP = GE Lungmen Procedures. These are procedures specific to the Lungmen Project and are available in Documentum by performing a Query based on "Object" "begins with" "GLP". Hard copies are also available in the Lungmen Project Quality Manual maintained by Jim Howard in Room J-1382.
3. P&P = Policies and Procedures for GE Nuclear Energy. These are the company policies and are available on the GE Nuclear Energy Intranet at URL # http://genet.ne.ge.com/procedures/genepandp/pandpind.shtml

附件八

奇異公司保證維護核四整體計畫

品質聲明

Summary of the discussion relative to quality

ROCAEC has expressed concern that the quality of the Lungmen design must be continued despite the suspension of the project. Many people were lost to the project due to the suspension, and there may be a potential for a loss of quality as a result of the loss of people.

Monty indicates that it is absolutely true that the people are not immediately replaceable. However, the quality is not in the people themselves, but rather in the process they follow. In order to follow the procedures properly new people will require additional training and guidance. In addition, there may be a need for additional coaching by experienced managers and engineers to ensure that the procedures are being followed properly. Thus, there will be a real effect of the suspension in terms of time and dollars. However, the process mandated by GE procedures will ensure that there will be no loss in the quality of the product.

Similarly, GE has required that its vendors have similar design processes and training to ensure that they will produce a quality product. GE has reviewed these design processes to ensure their adequacy, and will audit the vendors to ensure that the processes are being properly implemented.

附件九

奇異公司對 Eaton 公司執行 P&P 紀錄

（內容涉及廠家 proprietary 資料不予公開）

附件十

奇異公司對 Foxboro 公司執行 P&P 紀錄

（內容涉及廠家 proprietary 資料不予公開）

附件十一

停工期間工作進度記錄 WPSR 樣本

（內容涉及廠家 proprietary 資料不予公開）

附件十二

孫博士稽查報告

Lungmen Plant Safety Audit
Performed by the ROC Atomic Energy Council
General Electric Nuclear Energy, San Jose, California, USA
October 2 and 3, 2001
Reported by Dr. Bill K.H. Sun, October 12, 2001

Dr. Bill Sun served as an advisor in the safety audit. The following are summary remarks and considerations in the general and specific areas of the audit:

1. General Considerations
   - After the order by the Executive Yuan to re-start the Lungmen Project on February 14, 2001, various domestic and international projects have been re-activated. During this audit, it is found that among the major Instrumentation and Control projects, the GENE work has proceeded satisfactorily, the Foxboro project is slowly being re-started, but regrettably the Eaton project which is a subcontract to GENE with major responsibilities on protection and safety systems has not even been given the order by GENE to re-start. The problems associated with the situation, which are not fully disclosed to the auditors, may pose as serious challenges and threats to the final integration and conclusions of acceptance testing of the digital I&C systems.
   - The Preliminary Safety Analysis Report (PSAR) and Final Safety Analysis Report (FSAR) are two important licensing basis documents for the safety and licensing of the Lungmen Plant. GENE and Taipower should review in light of the suspension, preservation, protection, re-start, and re-training activities to determine if changes are necessary, and if so, should submit the revisions timely to ROC Atomic Energy Council for its review and approval.
   - The plan of final integrated verification and validation of the instrumentation and control systems including the control room remains to be an area of great concern. It is not clear and convincible how the integrated systems and components can be well tested to assure its functionality and reliability in the Lungmen plant network of communications under various automated and manual conditions of data uploading and downloading.

2. Specific Considerations
   - In the licensing and regulation of the Lungmen Plant, a crucial licensing deliverable is the full-scope training simulator. The simulator will be used by Taipower and ROCAEC for multiple functions and purposes, including the

following:

- Training of Taipower instructors
- Training of ROCAEC examiners
- Training of Lungmen reactors operators and senior reactor operators for Lungmen operation licenses
- Training of testing, surveillance and maintenance crews
- Testing and verification of operation procedures and emergency operation procedures
- Testing of automation/manual switchover functions
- Final verification and validation of integrated control room human factors engineering, such as alarms, display, operator aid systems, and designed human-machine interactions

During the audit, it is found that significant planning and actual development remain to be worked out to provide assurance that the above activities will be handled satisfactorily.

- It is questionable whether the current planned "baseline simulator" has the simulation capability and fidelity to satisfy all the requirements and expectations for testing, training and licensing of reactor operators.
- In the currently planned deliverable of the Lungmen "baseline simulator", the emergency operation procedure will be delivered in hardcopy binder forms and large size flowcharts, not the designed on-line display version that are well integrated with alarm procedures and piping and instrumentation diagrams. The discrepancy must be addressed in light of human factors engineering for its impact on safety, licensing, and operator's effectiveness in emergency management.
- Two crucial elements that are related to the safety and quality assurance of the software based digital systems for the Lungmen Plant are the independent verification and validation (V&V) and software safety analysis. During the audit, GENE has begun to show encouraging progress, compared to the planning materials that are shown in the previous audit. The work must be produced in good quality to subject to public and licensing scrutiny in the future. In addition, communication with and feedback from the design and review groups are necessary to prove that these activities truly provide assurance of safety.
- The Multi-Vendor Data Acquisition System (MVD) is very important in the functioning of the Lungmen I&C systems as they includes hardware and software products from various vendors, that are designed to communicate, interact, and interface, either directly or through networking. The design

and function of MVD must be fully reviewed and tested to prevent any possible single failures or common cause failures that may disable multiple functions and systems.

- The Lungmen Automated Power Regulator (APR) is an important new feature for the design of full-automated Lungmen Plant. GENE made the point repeatedly that it is just an operator aid system during plant startup and shutdown, and that the operators should be fully capable to start and shutdown the plant manually like the existing Kuosheng Plant. During power startup, the APR is designed to have 35 "stop points" for the operators to verify and activate. However, it should be stressed from safety standpoint that the system must be designed with high reliability and availability, the auto/manual functions must be fully tested to satisfy human factors engineering, and the operators must be well-trained to handle auto/manual switchover interactions.
- In the initial GENE planning of human factors engineering (HFE) testing and V&V, the important elements on procedure, emergency operation procedures, and auto/manual interactions were neglected. GENE staff must pay close attention to the HFE requirements as identified in Chapter 18 of the NRC Standard Review Plan.
- The GE/Taipower Lungmen Information Management System contains data and knowledge from all the vendors about design, construction, licensing etc. The IMS should be continued throughout the whole life cycle of the Lungmen Plant including operations, maintenance, modification, and decommission. It will be the most important source of information and therefore, should be well maintained and well updated according to configuration management guidelines.

附件十三

INER 稽查報告

核四廠數位儀控系統發展作業復工視察

核研所稽查報告

目錄

1. 前言 2

2. 稽查工作規劃 3

3.稽查問題清單設計 4

3.1 設計原則 4
3.2 設計問題關係結構 4
3.3 問題清單 4

4 軟體驗證與確認（V&V）執行績效稽查 10

4.1 稽查目的 10
4.2 稽查方式 10
4.3 稽查過程 11
4.4 稽查發現 11
4.5 後續追蹤管制事項 13

5．軟體安全分析作業概況稽查 14

5.1 稽查目的 14
5.2 稽查方式 14
5.3 稽查過程 15
5.4 稽查發現 15
5.5 後續追蹤管制事項 16

6. 人因工程及模擬器復工稽查 17

6.1 稽查目的 17
6.2 稽查方式 17
6.3 稽查過程 18
6.5 後續追蹤管制事項 20

1. 前言

核四建廠工程因政府於 89 年 10 月 27 日宣佈停工，復於 90 年 2 月 14 日宣佈復工，由於核能電廠對安全品質有極為嚴格之要求，而核四工程規模複雜龐大，在停工、復工間工程單位須面對人員變動、流失，文件保存、移轉等問題，此一斷、續過程及其產生的效應，不可避免會對施工品質造成一定程度影響。施工單位則必須妥善處理此斷、續過程，務必維持停工復工前後工程品質的一貫連續性，以免對日後電廠安全帶來不利影響。原能會因此於復工後隨即執行一系列復工品質視察，對於數位儀控系統工程部份，亦規劃於 10 月 1~3 日赴美國 GE 公司執行儀控系統復工品質視察，以瞭解復工作業實際情況。在視察工作規劃中，核研所支援執行有關軟體 V&V 執行績效、軟體安全分析工作概況及人因工程與模擬器等三項稽查工作。本項復工視察工作已於 90 年 10 月 3 日順利執行，本報告針對核研所負責視察項目，說明視查過程、視察發現及後續追蹤等事項。

2. 稽查工作規劃

本次稽查由原能會規劃及執行，核研所、台電等單位配合執行，稽查小組成員如下：

領　隊：莊長富

核研所：謝得志、易俗

顧　問：孫國華

美國 NRC 觀察員：Mr. Chiramal

核研所參與稽查時程為 10 月 1 日至 10 月 3 日為期三天，第一天（10 月 1 日）為稽查前準備會議，第二、三天為實際執行稽查。

本次稽查項目計下列六項：

1. 查證去年稽查結果處理情形

2. 數位儀控系統復工安全品質連貫性視察

3. 數位儀控系統品保作業績效查證

4. 數位儀控系統安全分析作業查證

5. 模擬器及人因工程 HFE 稽查

6. 數位儀控系統廠家驗收測試規劃作業查證（FAT）

核研所主要負責項目為第 3、4、5 項。

3.稽查問題清單設計

為使本次稽查產生最大效果，核研所支援稽查人員先行針對稽查目的設計相對應之問題清單，並於行前準備會議中提出討論後，交付台電公司預作準備，以增進稽查工作效率。本節對稽查問題設計作一概要介紹。

3.1 設計原則

核安管制係在嚴謹的法規體系下運作，稽查活動亦不例外。因此每一稽查項目皆可追溯其相關法規或標準。以 V&V 為例，稽查問題應依據 V&V 相關法規、審查指引及工業標準，選擇與 V&V 工作績效相關條文規定作為設計本次 V&V 工作績效稽查問題清單的起點。問題清單設計採用反向(Backward)展開原則，即由稽查目的出發，參考相關規定，逐步推演出為達成稽查目的而應查核的事項，據以列出詳細的問題清單。過程如圖 1 所示，

3.2 設計問題關係結構

稽查問題設計完成後可組織成一階層結構，反映稽查目的相關法規標準，與實際問題間之隸屬關係。此一階層關係圖有助於參與稽查各方人員之間的溝通，也有助於提升稽查效率及品質。

圖 2 為針對本次稽查所設計問題關係結構圖。

3.3 問題清單

表一為依據反向展開原則所設計完成之問題清單，經稽查小組討論修正後，擇重點請台電公司轉送 GE 公司先行準備。

A Backward Approach for Audit Questionnaire Design

Step 1: Define Audit purpose
Step 2: Define final **conclusions** to be written in Audit Report
Step3: Define evidence needed that can support reaching the final conclusion
Step 4: Further refine the detail content of evidence
Step 5: Organize the evidence into a hierarchical structure

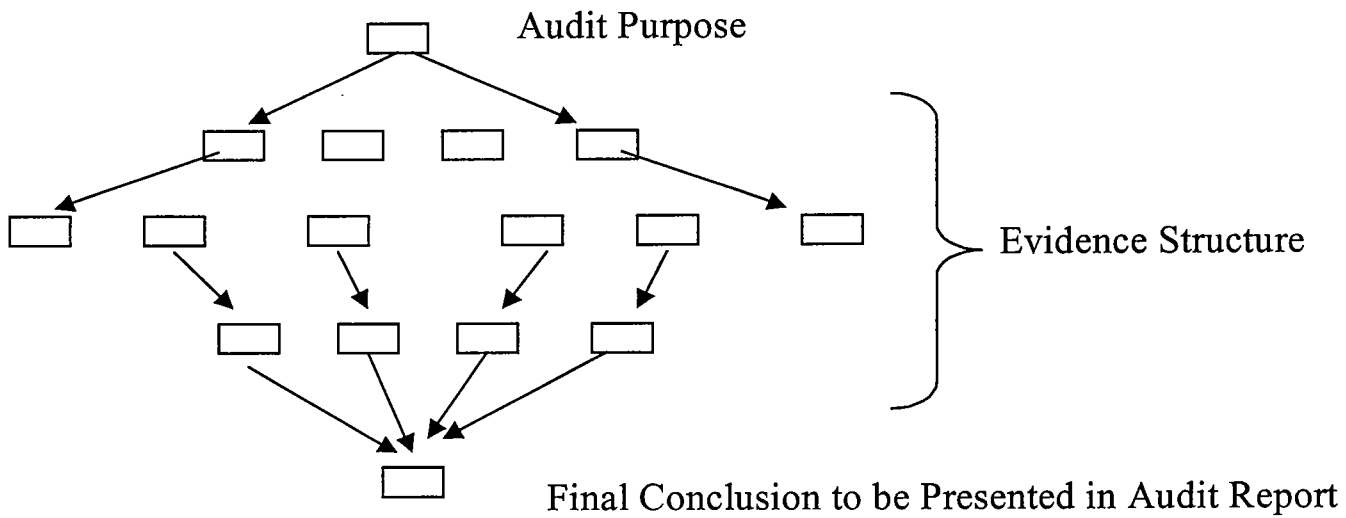


圖 1：稽查問題設計原則

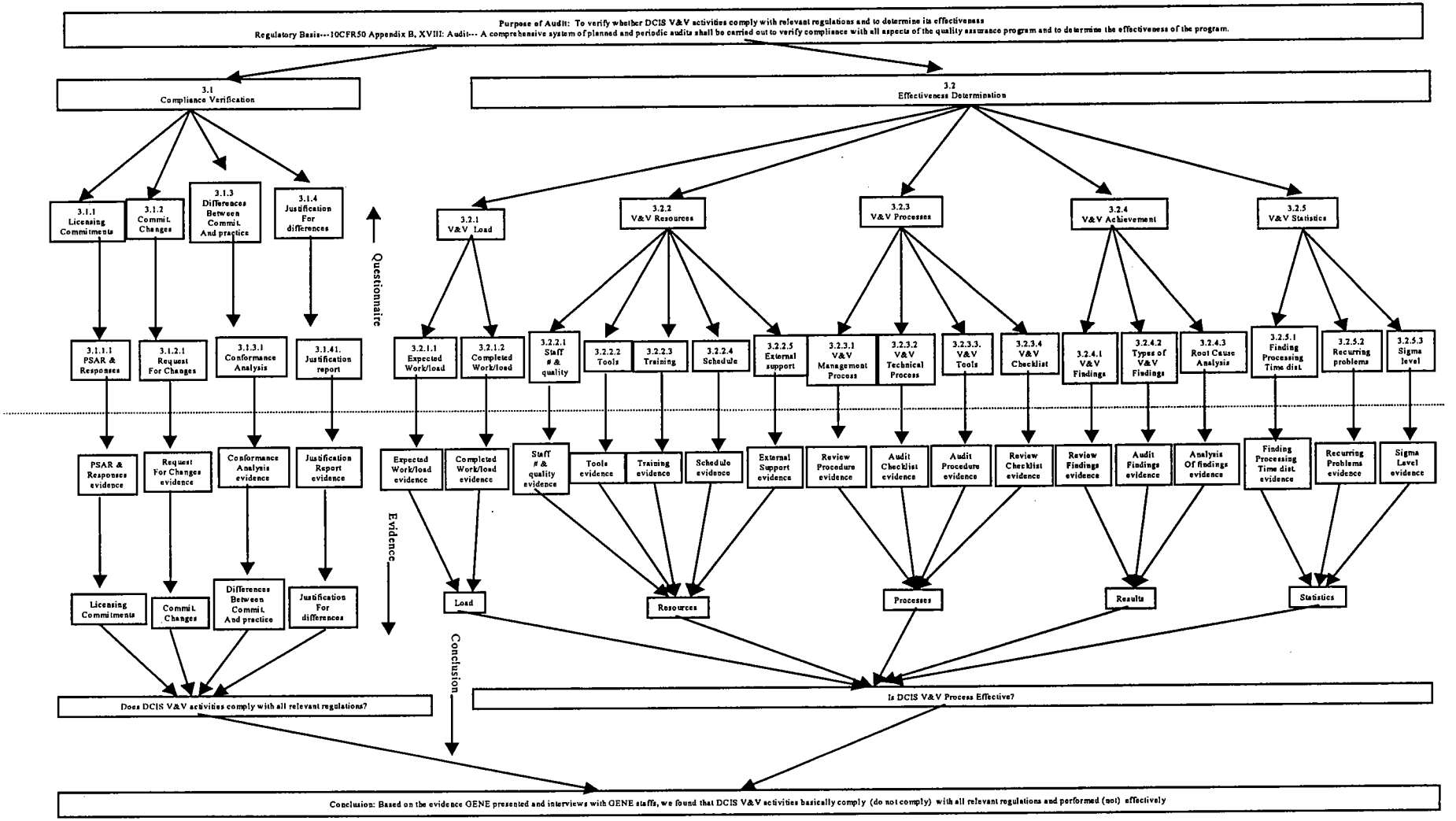


圖 2: 稽查問題問題關係結構

表一：稽查問題清單

No		Evidence.	Evaluation				
			Practice			Product (1~5)	
			Ad hoc	Defined	Quantified	Format	Content
3.1	**Regulation Compliance Verification**						
3.1.1	**Licensing Commitments**						
3.1.1.1	Please briefly describe DCIS V&V related licensing commitments						
3.1.2	**Commitment Changes**						
3.1.2.1	Are there any commitment changes so far?						
3.1.3	**Conformance Analysis**						
3.1.3.1	Please briefly describe how DCIS V&V activities meet licensing commitments						
3.1.4	**Justification**						
3.1.4.1	If there is V&V related licensing commitment change, please provide justification for such change						

表一：稽查問題清單（續）

No		Evidence	Evaluation				
			Practice			Product(1~5)	
			Ad hoc	Defined	Quantified	Format	Content
3.2	**V&V Activities Effectiveness Determination**						
3.2.1	**V&V work scope / Load**						
3.2.1.1	Please describe work have completed by V&V group						
3.2.1.21	Please estimate future load need to be done by V&V group						
3.2.2	**Resources**						
3.2.2.1	Please describe number and qualifications for V&V group staffs						
3.2.2.2	Please describe tools used during conducting V&V activities						
3.2.2.3	Please describe training programs for supporting V&V activities						
3.2.2.4	Please the schedule (past and future) for V&V related activities						
3.2.2.5	Any external support employed for DCIS V&V activities						
3.2.3	V&V Processes						
3.2.3.1	What is DCIS V&V management process?						
3.2.3.2	What is DCIS V&V technical process?						
3.2.3.4	Please demonstrate some sample checklist used for V&V process						
3.2.4	**V&V Achievements**						

3.2.4.1	Please describe major V&V findings						
3.2.4.2	Please describe type of V&V findings						
3.2.4.3	Please discuss the root cause analysis performed for these findings						
3.2.5	**Statistics**						
3.2.5.1	Please show the processing time distribution for findings identified during V&V process						
3.2.5.2	Please describe the ratio of recurring problems						
3.2.5.3	What is the Sigma level achieved based on DCIS V&V performance						
3.2.3.3	What are V&V tools?						

4 軟體驗證與確認（V&V）執行績效稽查

4.1 稽查目的

核四廠儀控系統採用全數位化設計，而數位化系統運作功能則主要係由軟體驅動，因此軟體品質優劣對電廠未來運轉安全影響重大。確保軟體品質安全可靠方法之一即為執行嚴謹之驗證與確認（Verification and Validation）工作。因此在 PSAR 審查階段及歷次國內外稽查，V&V 相關工作執行情形皆為查核重點項目。在核四計畫初期習段，V&V 相關稽查較偏重查核 V&V 工作計畫層面事項，例如組織、人員、時程、V&V 擬採用之方法工具等項目。隨著核四工程逐步展開，V&V 稽查重點亦相對移至技術實質面事項，例如 V&V 審查發現問題統計分類、軟體設計缺失原因分析、問題平均處理時間等與 V&V 工作實質績效相關問題。本次稽查 V&V 主題有二：V&V 作業法規符合性稽查及 V&V 作業績效稽查，而以後者為稽查重點。

4.2 稽查方式

V&V 工作稽查方式包括（一）簡報（二）資料查證

1. 簡報

   由 GE 負責 V&V 工作項目負責人以稽查問題清單內容為重點進行簡報，說明 V&V 工作進行方式及執行績效數據定義與量度結果。

2. 資料查證

   - 針對稽查問題清單涵內容重點準備相關文件供核對
   - 針對簡報過程中所提問題提出相關文件證據

4.3 稽查過程

1. 簡報：十月二日 下午 16：00

由 GE 公司 Independent Review Team 負責人 Mr. Grim 及工作人員簡報，主題為 "Software IV&V"內容包括 GE IV&V, OIVVT 及 IV&V Metrics 三大部份。

2. 資料查證

(1)GE NUMAC 產品 MDV 實際使用過程中遭遇過之故障回報事件統計及處理情形。

(2)GE IV&V 執行審查所採用之查核表。

(3)GE 核四數位儀控發展計畫相關單位之組織架構圖。

(4)Eaton 核四數位儀控發展部門之組織架構圖。

(5)IV&V 審查所發現異常問題清單。

(6)IV&V 工作績效量度指標相關統計數據。

4.4 稽查發現

1. 法規符合性問題

在稽查作業進行過程，我們特別檢視了 GE 內部各項審查編組設置與運作情形，GE 提供了 4 張 GE 內部 V&V 工作組織圖，及一張下包商 Eaton 公司 QA 作業組織圖。在各張組織圖表中可看出執行 V&V 之小組與發展小組間維持明確的指揮、報告及技術上的獨立性，但對於法規上要求的財務獨立性問題，GE 雖宣稱執行 V&V 工作小組財務並非由龍門計畫經費下支付，因此 GE 認為可符合財務獨立的要求，但

稽查人員認為此種作法與一般工業界在執行 IV&V 時工作方式不同，因此 GE 之 V&V 作業是否符合 IV&V 定義仍有疑議。為化解此項疑義，TPC 已另聘請 MPR 公司協助執行 OIV&V 工作，其工作內容與法規認可標準（IEEE 1012）之 IV&V 工作項目仍略有差異。現各方（包括 NRC 專家意見）已初步達成共識，將蒐集龍門計畫中所有參與 V&V 相關工作—例 GE 內部 V&V, GE IV&V, CDA 顧問審查, MPR OIV&V, TPC 內部審查, Stone Webster 審查等，將上述審查工作內容彙整整合後得到的品質效果再與法規所要求的標準比較，作為通過與否的參考。因此本次稽查對 V&V 作業法規符合性的結論為：

- 繼續維持現行多軌審查作業方式
- 應將各項審查作業結果予以整合以研判是否具有 IV&V 的實質效果

2. V&V 績效問題

V&V 績效判定是考量 V&V 工作量、V&V 投入資源及 V&V 所發現問題三者間平衡關係。對於特定之 V&V 工作負荷，如果投入合理之 V&V 資源，亦能有效發掘軟體中之缺失（或是能確定軟體功能之正確性），則為績效良好之 V&V 工作。GE 公司在簡報內容中分別說明執行 V&V 工作時所對應的工作量、投入的資源（包括外界的支援）、採用的工作程序、V&V 工作步驟、V&V 工具、V&V 工作成果、V&V 發現問題分析，及相關的統計數據。由於 GE 宣稱其品保作業採用 6

sigma 制度，因此亦提供 6 sigma 作業相關資料，不過由於軟體之特殊性質，GE 所提供之各種數據無法如同硬體品保數據具相同的預測效力，亦即無法判定軟體 V&V 作業執行的 Sigma level，但如果從相對比較的角度則這些數據仍有參考的價值。亦即以 GE 本次提供的各項數據為參考基準，比較日後 V&V 作業相關數據變化情形，可據以判定 V&V 作業績效變化趨勢，例如可決定 V&V 績效係維持穩定、是進步或是退步。因此將持續追綜比較 GE 軟體 V&V 工作各項績效數據。

4.5 後續追蹤管制事項

法規符合性：

請 TPC／GE 將各項 V&V 相關活動予以整合，釐清各項活動間為互補或重複關係題能達成完整 IV&V 之相同效果。

V&V 執行績效：

請 TPC／GE 列表追蹤比對各項審查作業相關數據，從數據中比較 V&V 作業績效變化趨勢，各項活動間是否具互補效果或只是重覆另一審查活動的工作而未帶來實際品質改進效益，請 TPC／GE 持續提供此類數據以供研判。

5．軟體安全分析作業概況稽查

5.1 稽查目的

軟體安全分析是數位儀控系統發展作業中居樞紐地位的一項工作，因各項發展單元活動均須將其所負責完成工作資訊傳送至安全分析小組，由安全分析小組鑑別是否存在潛在的危險因子（Hazards），分析其效應，並提出對策建議提供原工作單位作修改時參考。因此在安全分析工作未完成前，其餘系統之發展作業不能進入下一階段展開工作。Lungmen 計畫軟體安全分析是核能工業界首次應用，GE 的軟體安全分析技術仍在開發摸索階段，因此安全分析工作進度並未能依預定時程進行，為避免因安全分析工作延後而對 DCIS 其餘系統開發造成影響，GE 擬將軟體安全分析活動與其餘開發活動脫勾，亦即 DCIS 各分系統將依各自計畫執行，待安全分析工作階段完成後再將分析結果回饋至相關系統進行必要修改。本次稽查目的即在瞭解安全分析工作進行現況，並確認安全分析結果能有效的回饋至相關部門進行修正。

5.2 稽查方式

軟體安全分析作業概況 稽查方式包括（一）簡報（二）資料查證兩項活動

1. 簡報

由 GE 負責執行軟體安全分析工作負責人員針對核四數位儀控系統軟體安全分析工作執行狀況，包括軟體安全分析工作規劃、軟體安全分析各分項工作進展情形，及已完成安全分析之結果提出概要說

明。

2. 資料查證

針對 GE 在簡報過程中所作說明，對所提問題所作答覆內容，請 GE 提供對應之文件證據以進行核對。

5.3 稽查過程

1. 簡報：十月三日 下午 16：00

由 GE 公司負責執行軟體安全分析工作人員進行簡報，主題為 "DCIS Software Safety Analysis"，內容包括：軟體安全分析計畫，概念階段軟體安全分析工作概況及完成之分析結果。

2. 資料查證

(1) 已完成軟體安全分析工作項目統計數據。

(2) 安全分析所辨識出與安全功能相關之系統功能、系統介面等資料。

(3) 安全分析方法文件。

(4) 危險因子（Hazard）清單相關資料。

5.4 稽查發現

本次稽查時發現安全分析工作進度仍有落後現像，但 GE 工作人員已承諾將積極增加人手以加快安全分析工作進度。對於目前已完成之安全分析階段報告初步檢視發現內容並不深入，例如所分析內容及結論較偏文件格式性問題，因此分析結果多被列為「不重要」(Non-critical)，迄今尚無一項發現

須要相關部門進行修正。

5.5 後續追蹤管制事項

由於 GE 是首度執行軟體安全分析工作，而核能工業界亦普遍缺乏相關工作經驗。GE 公司目前進行之軟體安全分析作業方式是否有效允當，仍有進一步討論之必要性。在其他領域如航空、太空、軍事等工業界及學術界對軟體安全分析已有多年之經驗，因此建議 GE 公司因將其軟體安全分析作業方式、軟體安全分析工作結果送請相關專家、學者審查，以增進外界對 GE 軟體安全分析工作品質的信心，確保安全分析之工作品質。核研所近年積極投入軟體安全分析相關議題研發工作，因此亦可比照對核四核燃料執行平行安全分析模式，考量執行平行軟體安全分析，藉由交互對照雙方分析結果，應可以更進一步增進各界對軟體安全分析工作品質的信心。

6. 人因工程及模擬器復工稽查

6.1 稽查目的

核四廠採用全數位化儀控系統設計，其人機界面和核一、二、三廠完全不同，因此必須進行人因工程分析，以確保人機界面之妥適性。 模擬器為驗證與確認人機界面妥適性之重要工具。 模擬器包括工程設計用之部份工作模擬器(part task simulator ,GETS) 以及運轉員訓練用之全尺寸模擬器(full scope simulator)，二者都用於驗證與確認人機界面妥適性。 人機界面驗證與確認所發現之缺失(human engineering deficiencies – HEDs)，應該紀錄於人因工程問題追蹤系統(Human Factor Engineering Issue Tracking System , HFEITS)，實施系統化之管理、追蹤與改正。 人因工程問題追蹤系統之確實執行，有助於降低核四廠之停工與復工對人因工程之衝擊。 人因工程缺失資訊管理之重要性在"NUREG-800 APPENDIX II to APPENDIX A of SRP 18.1 MANAGEMENT OF HED INFORMATION"亦特別強調，故列為此次稽查重點之一。

6.2 稽查方式

此次現場稽查分為：(一)簡報與(二)資料查證及訪談兩部份

1. 簡報

請 GE 報告模擬器以及人因工程問題追蹤系統使用現況，說明部份工作模擬器用於人因工程靜態與動態評估之發現及其影響，以及模擬

器未來之開發與使用規劃。

2. 資料查證及訪談

請 GE 準備下列資料

(1) 完整之人因工程缺失(human engineering deficiencies – HEDs)資料。

(2) 此資料應含所發現之問題、對系統設計及安全之影響及改正措失。

(3) 如無需改正，請說明理由。

6.3 稽查過程

1. 簡報: 十月二日

GE 公司 DCIS group leader Kim Yu 簡報 "Simulators and HFE"。

2. 資料查證及訪談: 十月二日

與會人員 : Kim Yu (GE, DCIS group leader),

Jerry Mark (GE, Plant Computer System)

Steve Sawyer (GE, Plant Simulator)

Richard Gutierrez (GE, Human Factors Engineering)

David Zizzo (GE, Control Room Design Team)

Lisa Moody (GE, Chairperson BRT)

李精一課長(台電核技處)

謝得志(原能會核能研究所)

查證資料:

(1) Human Factors Engineering Issue Tracking System (HFEITS) status

(2) Content of HFEITS data base

(3) List of systems which has conducted static verification or dynamic validation

6.4 稽查發現

(1) GE 已依 PSAR 之承諾，完成第零版之"Human Factors Engineering V&V Implementation Plan"。 唯目前之執行方式已與此規劃書不盡相同，奇異公司表示將修改規劃書。 改版時程如下:

Revision 1: 1/2002

Revision 2: 4/2002

Revision 3: 9/2002

(2) 核四廠新採用之自動功率調節系統(Automatic Power Regulating System, APR)之驗證，已規劃於第二階段人因驗證與確認時(Phase 2 HFE V&V)在基準模擬器(baseline

simulator)上實施。

(3) 核四廠將採用之線上電腦化程序書(On-line Procedure System) 不在目前所規劃之人因分析範疇內。

(4) 查證人因工程問題追蹤系統(HFEITS)資料，發現如下：

(a) 2001 年 9 月 7 日和 2000 年 9 月 27 日之 HFEITS 中之問題(issue)數同樣為 39 筆。

(b) 雖然稽查時已有 16 個系統完成靜態驗證(static verification)、5 個系統完成動態確認(dynamic validation)，但是只有 C41 系統之動態確認完成後有問題列入 HFEITS； 其它系統之 V&V 工作完成後均無問題列入 HFEITS。

(c) C41 系統之動態確認於 2000 年 3 月 7-9 日實施，其問題於 8 月 31 日列入 HFEITS。

(d) HFEITS 中有 16 個問題是台電於審查 GE 人因相關文件時，發現問題要求列入。

(e) HFEITS 中沒有問題是由於 GE Baseline Review Team (BRT) 審查後之發現。

6.5 後續追蹤管制事項

1. 由於自動功率調節系統(APR)是核一、二、三廠沒有之系統，其 HFE V&V，台電運轉員務必參加。

2. 線上電腦化程序書(On-line Procedure System) 若要使用，必需有完整的人因分析與驗證，以及模擬器訓練.。

3. "Human Factors Engineering V&V Implementation Plan"改版時，請將軟體安全分析(software safety analysis)發現之重點，加入評估項目中。

4. 請評估 HFEITS 之執行效果

附件十四

NRC 稽查補充資料

Lungmen Project Audit of GENE

October 2 & 3, 2001

Findings and suggestions

The focus of the audit was on preservation and protection of the Lungmen I&C system design during the period the project was in suspension and the re-start of the design. GENE has maintained the project adequately, preserved a core of the staff who worked on the project prior to suspension, and have a good plan for training and integrating new staff for the project. GENE has the overall responsibility for the project, but has other vendors and organizations providing the design and implementation of several I&C systems. The progress of re-start of Foxboro and Eaton are not at the level that GENE maintained. The audit team identified the need for GENE as the prime contractor to accelerate the restart efforts of these vendors.

The audit team re-iterated the concerns regarding the factory acceptance tests of the I&C systems at the various vendors facilities and the integration of these tests between the various vendors. The next major ROC AEC is to focus on the FATs. I would suggest that the AEC request TPC to obtain from GENE the overall I&C system test plans and strategy, including those of Foxboro, Eaton and others, that addresses all the I&C system lifecycle tests such as design tests, integration tests, validation tests, FATs, SATs, and pre-operational, start-up and commissioning tests. An early review of such a test strategy would provide the AEC staff a better understanding of the coverage and overlaps of the various tests and would help in identifying any gaps or deficiencies in the test coverage.

(The findings on the Simulator and operator interface was passed onto Dr. Sun who has included them in his input to the audit report.)

附件十五

新開立八件「注意改進事項」

核能電廠注意改進事項

編號	AN-LM-90-025	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：GETS 整體發展作業未能達到 GETS 的原始使命

注意改進內容：

GETS 的目的係作為核四控制室發展作業用以檢驗人機介面的工具，以避免控制室發展作業發生缺失，因此具有相當重要之階段性任務，且其發展應走在控制室儀控系統發展之先。目前 GETS 整體發展作業未能達到 GETS 的原始使命，此將影響其階段性任務，進而影響整體核四數位儀控工程品質，殊值得特別關注並儘速加以改善。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-026	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：核四計畫資訊管理系統（IMS）備份及管制措施

注意改進內容：

IMS 資料庫是核四計畫的重要工具，資料庫維護良好意味構型管理良好，是計畫成功的保証，也是未來電廠商轉後維護與運轉不可或缺的利器並將伴隨電廠一輩子。目前建廠階段由奇異公司負責 IMS 資料輸入與維護工作,電廠商轉後 IMS 將移由台電維護，故台電核四計畫宜有專人參與並熟悉核四計畫 IMS 系統，並強化備份及管制措施。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-027	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：儘速解決 Eaton 公司未復工及盤面設計變更問題

注意改進內容：

奇異公司的復工情況堪稱令人滿意，惟其下包之重要儀控廠家 Foxboro 遲至八月才復工，而另一負責 ESF 系統之重要下包儀控廠家 Eaton 公司迄今尚未復工，且其間還存有 Eaton 要求於控制室背後盤區增加盤面的設計變更問題存在，此問題將可能產生擠壓控制室背後盤空間並迫使其他廠家或系統盤面遷移等相關性問題；奇異公司與 Eaton 公司間為何會有數量頗多之盤面增加的議題，值得深究。此情況對目前復工後，需各廠家都能互相配合、全力展開設計作業，以進行整體儀控發展作業是一相當不利之因素，亟需儘速改善。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-028	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：加強軟體驗證與確認工作

注意改進內容：

嚴謹執行驗證與確認（Verification and Validation）工作為確保軟體品質安全可靠之方法。維持現行多軌審查作業方式，即 GE 內部 V&V， GE IV&V， CDA 顧問審查， MPR OIV&V， TPC 內部審查，石威公司審查等之作法基本上可接受，惟應將各項審查作業結果予以整合，以決定其最終品質成效；未來更應該加強軟體品質相關文件審查、軟體程式碼審查及軟體功能動態測試等工作。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-029	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：加強儀控軟體發展作業文件版次管理

注意改進內容：

有關 IVVP 版次問題，由於在 PSAR 審照時曾正式要求台電公司在 IVVP 改版時比照 PSAR 內容更新方式需送原能會備查，而目前原能會、台電公司及奇異公司所用版次分別為四、五、六版，此案例顯示文件版次的管理有加強空間。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-30	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：強化軟體安全分析結果之審查

注意改進內容：

軟體安全分析是數位儀控系統發展作業中居樞紐地位的一項工作，因各項發展單元活動均須將所負責資訊傳送至安全分析部門。查證發現目前已完成之安全分析階段報告內容並不深入，即所分析內容及結論較偏格式性問題，因此迄今尚無一項發現須要回饋至相關部門以進行修正。請台電強化軟體安全分析結果之審查。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-31	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：儘速研擬模擬器與實際控制室間逼真度驗證及模擬器用以訓練成效等相關事宜處理方案

注意改進內容：

模擬器尚未將核四廠已採用之線上電腦化程序書功能(On-line Procedure System，OLPS)及新採用之自動功率調節系統(Automatic Power Regulating System，APR)等納入，亦未執行人因工程分析，又目前模擬器將與未來實際控制室不盡相同，而需作更新及如何對運轉人員訓練等問題。台電與奇異公司對模擬器與實際控制室間逼真度驗證及模擬器用以訓練成效等相關事宜，需儘速研擬處理方案。

承辦人：莊長富　　電話：23634180Ext307

核能電廠注意改進事項

編號	AN-LM-90-32	廠別	總公司核技處	日　期	90 年 10 月 25 日

注意改進事項：明確表列 FAT 可能因受限於區塊測試而有不足之處或有未適當執行之測試，並在工地安裝後測試(SAT)強化這些項目的測試。

注意改進內容：

整個核四數位儀控是由奇異公司、NUMAC、Eaton、Foxboro 及日本日立等公司共同發展，這些公司分佈美國東、西二岸及日本等地，地緣位置甚遠，且這些系統又有安全系統(1E)與非安全系統(Non 1E)之分，要順利完成整個測試是一項很重要且複雜的工作。奇異公司雖然對整個系統負責主導及整合工作，然其對 FAT 是採分區塊測試(Segment)方式在各廠家進行，而不是把所有廠家完成的系統與設備集中在一起測試，台電需先對 FAT 可能因受限於區塊測試而有不足之處或未適當執行之測試，明確表列並在工地安裝後測試(SAT)強化這些項目的測試。另外，並請台電提供整個儀控系統各階段完整的測試計畫（包括 design tests, integration tests, validation tests, FATs, SATs, and pre-operational, start-up and commissioning tests 等）與策略說明，並定期提供各階段測試相關工作進展資料供原能會瞭解。

承辦人：莊長富　　電話：23634180Ext307