出國報告（出國類別：開會）

參加 NPIC & HMIT 2006 研討會

服務機關：台灣電力公司

姓名職稱：李家光 儀控課長

派赴國家：美國

出國期間：95.11.11~95.11.18

報告日期：96.1.12

行政院及所屬各機關出國報告提要

出國報告名稱：
參加 NPIC & HMIT 2006 研討會

頁數 37 含附件：■是□否

出國計畫主辦機關/聯絡人/電話
台灣電力公司（313310000K）/陳德隆/ (02)2366-7685

出國人員姓名/服務機關/單位/職稱/電話
李家光/台灣電力公司/第四核能發電廠/儀控課長/02-24902401-2940

出國類別：□1 考察□2 進修□3 研究□4 實習■5 其他 開會

出國期間：95.11.11- 95.11.18　　出國地區：美國

報告日期：96.1.12

分類號/目

關鍵詞：ANS、DCIS、核四廠、核能儀控

內容摘要：（二百至三百字）

美國核能學會主辦的核電廠儀控系統與人機介面技術（簡稱 NPIC/HMIT）爲核能儀控系統界最重要之學術研討會，本屆 NPIC/HMIT 2006 於 95 年 11 月 12 至 95 年 11 月 16 日於美國新墨西哥州 Albuquerque 舉行，研討主題包括「核電廠現代化經驗」、「軟體品質保證」、「安全關鍵軟體發展與檢證」、「核電廠內無線通訊技術之應用」、「人機界面發展技術」等五十多項。研討內容包括核能儀控系統之最新發展趨勢及管制單位對核能儀控之管制重點等，另本次會議核四廠在大會發表一篇論文「核四廠儀控網路架構與現場測試，The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station」，藉由參加本次會議吸取新知與國外專家的經驗，將有助於核四廠的設計、安裝、測試及維護等工作。

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

目　錄

壹、國外公務與過程

一、出國任務緣起

美國核能學會(ANS)主辦的核電廠儀控系統與人機介面技術（簡稱 NPIC & HMIT）為核能儀控系統界最重要之學術研討會，本屆 NPIC/HMIT 2006 於本年 11 月 12~16 日於美國新墨西哥州 Albuquerque 舉行，研討主題包括「核電廠現代化經驗」、「軟體品質保證」、「安全關鍵軟體發展與檢證」、「核電廠內無線通訊技術之應用」、「人機界面發展技術」等五十多項。本次會議職核四廠李家光投稿論文一篇「核四廠儀控網路架構與現場測試，The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station」，並獲大會同意發表論文。因此參加 NPIC&HMIT 2006 學術研討會並發表學術論文，同時了解核能儀控界的設計、維護、管理的趨勢，以利將來應用在核四廠的儀控維護上。

二、國外公務之行程

奉派至美國新墨西哥州 Albuquerque 參加美國核能協會主辦之 NPIC & HMIT 2006 研討會，為期 8 天，詳細行程及工作項目如下表：

起始日	迄止日	地點	工作內容
11/11	11/12	往程	台北-洛杉磯- 新墨西哥州 Albuquerque
11/13	11/16	美國新墨西哥州 Albuquerque	參加 NPIC & HMIT 2006 研討會、核四廠儀控網路架構與現場測試於 11/15 2:00 PM~2:30 PM 報告
11/17	11/18	返程	新墨西哥州 Albuquerque－洛杉磯--台北

三、NPIC & HMIT 2006 研討會內容

本次研討會由美國核能協會主辦，協辦單位有 NRC、IAEA、KNS、EPRI、CAES、SNM、和 CNS。會議為期四天，在新墨西哥州 Albuquerque 的會議中心的 8 個會議室舉行，第一天為由美國核管會的 Commissioner Peter B. Lyons 主講，主題為”Achieving Improved Nuclear Plant Safety Through Digital Technologies The Regulator’s Perspective”為本次研討會的重點，第二至第四天為各技術分組專題研討，共計有 38 個分組專題，同一時段分別有六至八個分組專題同時進行，內容甚為豐富，

參加者視需要參加有興趣的研討分組，研討會之時程與內容摘要如下表：

時程	內容(上午 8:00~12:00)	內容(下午 1:00~5:30)
11/13	開幕典禮	
11/14	分組專題研討： 1. Advances in Control Room Design, Modernization, and Maintenance 2. Regulatory Challenges and Approaches to Advanced Systems－Panel 3. Digital System Reliability—I 4. Advanced Sensors and Measurement Techniques—I 5. Reactor Noise Analysis 6. Education of NPP I&C Professionals 7. Safety Critical Software System Development and Qualification 8. Innovative Approaches to Training and Training Technologies	分組專題研討： 1. User Interaction with Automation 2. Regulatory Oversight and Involvement in Safety Culture－ Panel 3. Digital System Reliability—II 4. Advanced Sensors and Measurement Techniques—II 5. Advanced Signal Processing Methods for Reactor Monitoring 6. Gen IV and Research Reactor I&C 7. Digital Upgrade and Qualification Issues in an Evolving Regulatory Environment 8. Knowledge Capture and Engineering
11/15	分組專題研討： 1. Visualization Technology to Support Decision-Making and Other Activities 2. Visualization Technology to Support Decision-Making and Other Activities	分組專題研討： 1. Designing Better Alarm Systems 2. GNEP: I&C Issues－ Paper/ Panel 3. Designing Better Alarm Systems 4. GNEP: I&C Issues－ Paper/ Panel

11/15 (續)	分組專題研討： 3. Computerized Procedure Systems 4. Controls Systems 5. Cyber-Security and Wireless Applications—I 6. Diagnostics and Predictive Maintenance－I 7. Applications of Next Generation I&C Systems 8. Licensing Issues for Advanced I&C Technologies 9. Function-Based Approaches to Control Room Design	分組專題研討： 5. HFE Design and Analysis Tools－I 6. I&C Architectural Approaches 7. Cyber-Security and Wireless Applications—II 8. Diagnostics and Predictive Maintenance－II 9. Current Regulatory Challenges for I&C 10. Lessons Learned in Digital Upgrades 11. Virtual Reality: Applications and Issues
11/16	分組專題研討： 1. Computerized Operator Decision and Support Systems 2. HFE Design and Analysis Tools－II 3. Digital I&C Technology 4. Aging and Environmental Compatibility 5. Diagnostics and Prognostics 6. Setpoints 7. Digital I&C Design, Development and Assessment 8. Advances and Challenges in HRA	分組專題研討： 1. Wireless Communications Technology 2. Digital Platforms and Tools 3. Software Quality Assurance 4. ICHMI Startup Experience at New Facilities－Panel 5. New HMI Technology 6. Approaches to HFE Verification and Validation

貳、研討內容與心得

一、專題演講

專題演講由美國核管會的 Commissioner Peter B. Lyons 主講，主題為”美國核管會對「以數位科技來增進核電廠安全」之展望”，Achieving Improved Nuclear Plant Safety Through Digital Technologies The Regulator’s Perspective”。由此專題演講可推測美國核能管制單位對核能儀控關心的重點，其演講內容如下：

1、核能儀控界的設計趨勢

老舊的核電廠使用過時的類比式儀控系統，由於經濟的利益趨使工業界繼續發展數位儀控產品來更新這些過時的產品，並研發製造具有全電腦化控制室的核電廠/設施，使用數位科技的核電廠/設施/研究機構如下：

(1)日本 Kashiwazaki Kariwa 核電廠六號機及七號機：全電腦化的控制室。

(2)瑞典 Oskarshamn 核電廠：一號機控制室更新。

(3)法國 Civeaux N4 reactor：全電腦化的控制室及功能非常強的人機界面設備。

(4)澳洲研究中的 OPAL 設施和中國的清華大學：開始進行現代化數位儀控系統的研究。

(5)挪威 Halden 設施：開始研究數位儀控系統與人機界面。

(6)美國海軍核能推進力研究計畫(Nuclear propulsion program)之新反應爐：使用新的數位科技。

(7)龍門計劃的全電腦化控制室、先進的警報系統與電廠全自動化系統。

2、數位科技的應用：

可應用於電腦化的控制室和人機界面等二方面，亦可提供精進核電廠安全的機會。

3、數位儀控之優點及潛在問題：

數位儀控具有許多優點，但仍有安全方面的問題，如安全軟體的共模故障、資通安全，但這些問題在業界和政府管制單位的努力下應可克

服，使得數位儀控的優點能應用在核電廠上。

4、經驗回饋

由於美國核管會預期將有許多新核電廠的申請，國際上新建核能電廠的經驗亦可提供給美國新建核電廠的經驗。

5、資通安全議題(Cyber-Security Issues)

資通安全是數位系統必須考慮的重要議題。在緊急計劃演練或實際事故時，數位系統可提供大量的電廠參數和狀態至核管會的事故應變中心。同時數位系統之設計必須確保其可防止外界入侵者侵入網路及電腦系統和數位系統不能干擾廠內系統的運作。除此之外，數位系統必須經由多項的策略(例如有效構型管理和登入管制)，以避免病毒、木馬程式和其他惡意程式破壞數位系統的運作。美國核管會積極的參與此議題，2005 年已更新法規指引，已審查工業界的資通安全指引並提出新的資通安全需求(10CFR73.55)。經由上述的努力我相信核管會將能滿足資通安全演進所帶來的挑戰。

6、近期核電廠儀控改善和新建核電廠的執照申請所帶來的挑戰

急迫性的管制相關相關議題如下：

- 對安全與非安全控道間的通訊(如單向/雙向通訊)、安全系統之內部通信等，其可接受的獨立性爲何?
- 可接受的多樣性與深度防防禦爲何?
- 可接受的數位儀控可靠性爲何?能否以信心度來預測儀控系統的可靠度?
- 數位儀控產生的新失效模式爲何?這些失效模式是否會影響安全系統的可靠性與維護性?
- 如何合理地確保緊急應變設備、電廠保安系統和電廠安全不受資通安全的威脅?
- 依美聯邦法規 10CFR Part 52 核發的 ABWR、CE System 80+、AP600 和 1000 之設計憑證，儀控系統與控制室之高階架構之細部設計審查深度爲何?此部分仍需工業界與核管會間之密集對話以解決雙方的歧見，目前審查中的 ESBWR 核電廠，亦需相同模式的對話。

- 為了儀控更新改善和新建電廠執照申請，核管會正在準備數位儀控為基礎的安全系統法規標準和可接受的準則以更新法規指引和標準審查計劃。
- 工業界與核管會之對話應在法規需求方面(例如:數位系統失效模式之分類、如何減緩數位系統失效對電廠的衝擊、對特定電廠當一個數位系統失效時整個電廠的安全如何能維持等議題)。
- 核管會的法規指引數應跟上數位科技發展的腳步。

7、進步型的控制室設計(Advanced Control Room Designs)

由於數位科技的進步，核能電廠資訊與控制系統可收集大量的資訊供運轉及維護人員使用。挪威建置的 Halden 實驗室，該實驗室的模擬器可規畫為 PWR 或 BWR 模擬器，且具有整合的偵測、控制系統和資料收集設施。在 Halden 實驗室執行人員疏失、人員效能、團隊作業和電腦驅動界面對人員效能影響等之相關研究。核管會將使用 Halden 實驗室的人因研究成果作為法規指引(例如警報系統、控制室設計、螢幕切換和人員效能量測)之技術基礎，上述成果可作為標準審查計畫之基礎，同時這些指引亦可作為現有反應爐檢查之基礎、新的反應爐執照申請審查的基礎。

8、人力資源與技術專家

核能界由於長期未蓋新電廠，因此核能優秀人員漸漸老化並退出核能界。適逢核能復甦，核能界需要吸引更多的優秀人才參與，但最要的挑戰之一為核能界須與其他工業界在人力市場上競爭以吸引優秀的數位技術專家參與新建核能電廠計畫。從美國核管會的立場，他認為建立國家實驗室與美國核管會緊密的結合，利用國家實驗室的設備及人員可協助管制單位執行重要議題之研究，例如安全軟體研究。

核能界的另一個展望為核能電廠進步型數位系統和人機界面以替代過時的儀控產品，這趨勢將可吸引學生加入核能工業。但當我訪問美國的研究型反應爐時，其儀控系統尚未更新為數位儀控系統，這對吸引優秀的學生投入核能界將有負面的影響。

最後美國核管會需要持續的對其官員加以訓練，尤其在數位儀控技

術及數位儀控管制要求方面之訓練，我們已在可程式控制器訓練方面實施自我學習課程，2007 年將對檢查官及其他官員實施數位儀控設計、執照申請、運轉等基本課程訓練

9、美國核管會參與的國際研究活動

(1)MDEP 計劃：

美國核管會與九個國家參與 MDEP 計劃(Multi-National Design Evaluation Program)，該計劃的第一階段為美國核管會與芬蘭、法國核能管制單位共同審查 AREVA 公司的 EPR 核電廠設計，同時美國核管會與芬蘭核能管制單位共同審查/討論 Olkiluoto 三號機的數位儀控設計。雖然目前 MDEP 計劃參與者為各國的核能管制者，未來將建立與工業界互動的機制。

(2)數位儀控和人機界面研究：

美國核管會經由參與 Halden 反應爐計劃以了解數位儀控和人機界面之軟硬體相關的技術基礎(包含線上偵測技術、診斷技術、監測技術、偵測技術及先進的決策法則)。

(3)COMPSIS 計畫

Halden 與 NEA 共同主持的計劃，其目的收集數位儀控系統失效之資料，經由此系統我們可了解數位儀控系統的失效模式和頻度，並加以改進數位儀控系統。

(4)數位系統研究計劃

此為美國核能管制單位需求的研究計劃，其研究範圍包含數位系統特性、軟體品質保證、風險評估、資通安全、緊急應變的新技術和先進的反應爐儀控系統和控制室設計。經由此計劃，我們對數位儀控的安全功能將有較深入的了解，以便我們能了解數位控制所衍生的風險。

二、核四儀控網路架構與現場測試

此部分為在 ANS 會議發表的文章(詳附件)，特別中譯如附下

1、核四廠儀控系統簡介

核四廠有二部機組，每部機組產生 135 萬千瓦，台電為業主，核四

廠 DCIS 儀控系統由下表之七個重要廠家依最新的電腦與網路技術整合而成。

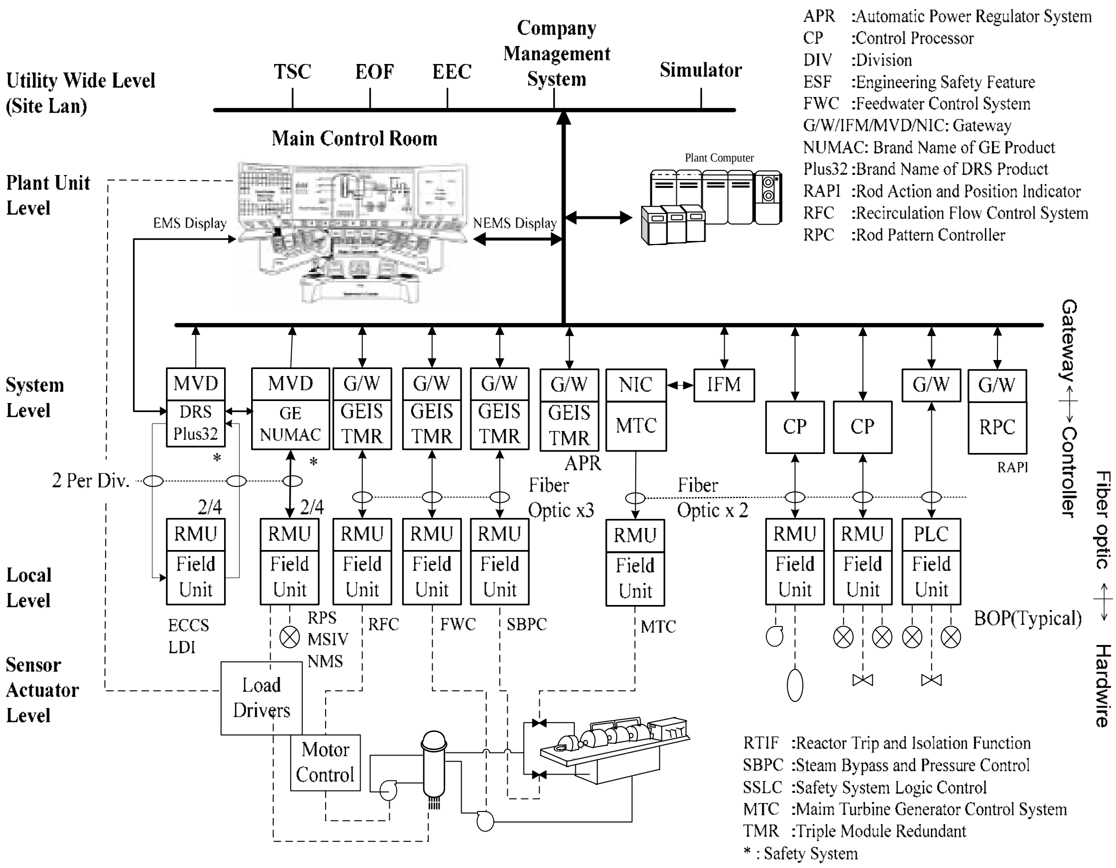
	Major Systems	Logic Designer	H/W Supplier
1	NMS,RPS	GENE	GE NUMAC
2	MMI(1E)、ECCS	GENE	DRS
3	MMI(N1E)、Alarm、PGCS	GENE	Invensys
4	RFC、FWC、SBPC、APR	GENE	GEIS(GCS)
5	RCIS	GENE	Hitachi
6	DEH	MHI	MHI
7	BOP Control System	Stone and Webster	Invensys

核四廠儀控系統(圖 1)由安全儀控系統與非安全儀控系統所組成,安全儀控系統包含 DRS 產品及 GE NUMAC 產品。DRS 公司提供緊急爐心冷卻系統(ECCS)和洩漏偵測與隔離系統(LDI);中子偵測系統(NMS)與反應爐保護系統(RPS)和主蒸汽隔離系統的產品是 GE NUMAC 之產品。

非安全有關儀控系統包含 GEIS、MHI 和 Invensys 的產品。GE Industry System (GEIS)提供三重容錯儀控系統(TMR),包含再循環量控制系統(RFC)、反應爐飼水控制系統(FWC)、蒸汽旁通和壓力控制系統(SBPC)和自動功率調整系統(APR)。三菱重工(MHI)提供汽機控制系統(DEH)和和其輔助系統。Invensys 公司提供廠用電腦系統(PCS)和大部分平衡控制系統(BOP)和緊急應變中心的設備(包含 TSC、EOF、EEC)。

所有非安全有關的人機介面(MMI)置於 Invensys 的平面顯示盤(Flat Display)、凝態顯示盤(Mimic)和警報系統(AAS),安全有關的人機介面(MMI)置於 DRS 的平面顯示盤(Flat Display)。由於安全考量,安全有關的設備不能在非安全有關的人機介面上操作,只能在安全有關的人機介面上操作,同時安全有關的資訊單向傳至 Invensys 的平面顯示盤、凝態顯示盤和警報系統。

圖 1:核四廠儀控系統功能圖



2、主控制室佈置

核四廠控制室(圖 2)的人機界面與傳統核電廠的人機界面極大的差異,傳統的人機界面以類比式開關、類比式儀表和小型凝態顯示板為主。

核四廠控制室人機界面由寬螢幕顯示盤(WDP)、主控制台(MCC)和值主任操作台(SSC)等三部份所組成，WDP 提供(1)運轉員監視全廠的能力(2)假設事故時之監測和控制盤面(3)作為定期偵測試驗的盤面。電廠在正常運轉時，二位運轉員在 MCC 盤面監視和控制電廠設備。SSC 提供值班主任監視電廠狀態。WDP 盤有平面顯示盤、廠級警報、系統級警報、凝態顯示盤、硬接開關和大型顯示盤(LVD);MCC 盤有平面顯示盤和硬接開關。平面顯示盤為觸控螢幕，並讀取設備運轉狀態(例如泵的運轉/停止、閥的開/關)。因乙太網路的對等特性(PEER-TO-PEER)，運轉員能在 Invensys 任何一台平面顯示盤上操作同一設備。由於硬接線路及開關具有反應較快的特性，除了提供重要設備在緊急時之控制(例如緊急柴油機的手動啓動、反應器的急停)外，並作為觸控開關之多樣性設計。

警報系統分為廠級警報(Plant Level Alarm)、系統層級警報(System

Level Alarm)和元件級警報(Component Level Alarm)。廠級警報位於WDP盤的左側、系統層級的警報位於凝態顯示板(Mimic)上方，元件層級的警報位於非安全有關的平面顯示盤上。廠級警報其警報窗文字、顏色、聲響屬性依電廠運轉狀況/事件條件而改變，系統層級警報其警報窗顏色、聲響屬性依警報的優先等級而改變，每個警報之優先等級依運轉狀況/事件條件而訂定，電廠的警報其優先等級分為P1、P2、P3、P4等4個等級，只有優先等級為P1及P2的警報會送至系統層級的警報窗。

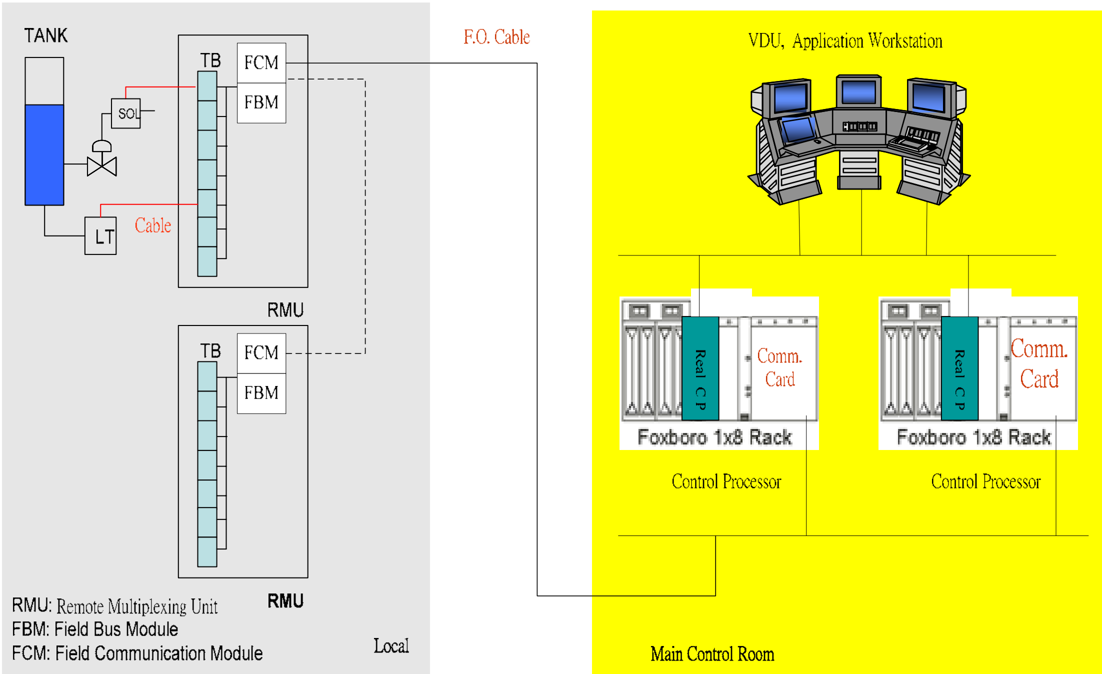
圖 2:核四廠主控制室

3、核四廠儀控網路架構(The Network Architectures of DCIS in LMNPS)

典型的DCS系統功能圖如圖3所示，現場感測器所送出的電氣訊號(例如水位傳送器之4~20 ma)送至鄰近的多工處理單元盤(RMU)並在RMU盤之現場模組卡片(FBM)執行數位/類比轉換，轉換後的數位訊號經由通訊模組卡片(FCM)處理後以網路封包方式送至位於控制室的控制處理器(Control Processor)執行PID控制、計算和邏輯處理。控制處理器發出命令要求終端元件動作(如閥的打開)時，則控制處理器的命令要求以封包方式傳送至位於現場RMU盤的通訊模組卡片(FCM)來解封包，再傳至現場模組卡片(FBM)以電氣的訊號要求閥執行打開的動作。此外，DCS

的人機界面除了傳統的硬接開關/儀器表頭外，亦可為觸摸式的螢幕供設定點之調整、設備狀態及流程參數的讀取及執行手動命令。

圖 3：典型的 DCS 功能方塊圖



核四廠每一個儀控廠家的架構以邏輯的觀點來說，其功能架構與上述類似。但實際的架構可分為環狀網路與排式架構，然後每一家的儀控網路經由閘道器連結形成一個大型的核四儀控系統。

核四儀控網路系統由 21 個儀控廠家(表一)之系統整合而成，部分廠家僅提供小規模的儀控系統(例如 PLC)，部分廠家(例如 Invensys、DRS、GE)提供大型的儀控系統。

表 1：核四廠儀控系統製造商及其提供之儀控盤數量

項次	製造商	控制盤數量
1	Invensys	165
2	Hitachi	67
3	DRS	65
4	MHI	39
5	GE-NUMAC	29
6	Harding /Smith	27
7	Toshiba	16
8	Inabensa	14

9	GE Industry System	8
10	Pall Filters	6
11	Siemens	6
12	York	5
13	Tough	4
14	Aptec-NRC	2
15	Preferred MT	2
16	Weir Pumps Ltd.	2
17	Chung-Hsin	1
18	Kinemetrics	1
19	PAR System	1
20	PHYS Acoustics	1
21	SACO	1

核四廠重要的儀控系統由 GE NUMAC、DRS、Hitachi、MHI、GEIS, Invensys 和 SACO 等廠家所提供。表二爲這些廠家所使用的儀控架構及其通協定。本論文僅敘述三種網路架構分別爲 Invensys HPS 系統、DRS PERFORMNET 網路和 GE NUMAC 平台。此外，連接各家網路之資料鏈亦會在論文中討論。

表 2：核四廠儀控系統使用的網路架構和通訊協定

系統	製造廠家	網路架構	通訊協定
Major BOP Control system	Invensys	網狀網路/乙太網路	TCP/IP
Non-1E MMI	Invensys	網狀網路/乙太網路	TCP/IP
ECCS/LDI 系統	DRS	環狀網路	Perform Net
Class 1E MMI	DRS	環狀網路	Perform Net
RPS/MSIV 隔離系統	GE NUMAC	點對點	RS485
NMS 系統	GE NUMAC	點對點	RS485
SBPC System	GE Mark VI/VIe	乙太網路	TCP/IP
FWC 控制系統	GE Mark VI/VIe	乙太網路	TCP/IP
RFC 控制系統	GE Mark VI/VIe	乙太網路	TCP/IP
APR 系統	GE Mark VI/VIe	乙太網路	TCP/IP
RCIS 系統	日立	環狀網路	Proprietary
汽機控制系統	MHI	乙太網路	UDP/IP

4、Invensys 儀控網路架構

Invensys 儀控網路共分三種網路，分別爲 Invensys 控制網路，Enterprise 網路及 Time Strobe 網路，首先我們討論 Invensys 控制網路，由於該網路的輸入及輸出點數量高達 6 萬點(表三)及其對反應時間的要求，Invensys 控制網路採用最新的 Invensys HPS 系統,HPS 系統包含數個網路交換器(Network Switch)並以網狀方式連結，其所採用通訊協定爲 RSTP 而非傳統的 Foxboro I/A 系統所使用的 Nodebus/Fieldbus 架構。

表 3：核四廠 Invensys HPS 系統的規模

名稱	數量
Hard I/O Point	17,000
Gateway I/O Point	40,000
Cabinet	165
Fault- Tolerant Control Processor	98
Single Control Processor	18
Application Processor	35
Workstation Processor	43

A、核四廠 Invensys 控制網路

Invensys HPS 系統(圖 4)以光纖 1Gbps Switch 架構爲主，該光纖網路爲一 1Gbps 雙重主幹的光纖網狀網路(A 和 B 網路)，每一個網狀網路由 6 個 Entersys Matrix E7 Switch(一號機 5 個、共用機組 1 個)經由 Switch Uplink 互連所組成。A 網路與 B 網路共有 4 個互連通道，二個節點有雙重通道，一個通道爲正常的通道，當正常的通道不通時另一個通道提供備用的通道，但乙太網路只能有一個通道，雙重通道將會形成一個迴路並產生“data storm”，因此利用 RSTP 通訊協定來阻斷(Block)其中一條通道。

核四廠應用 RSTP 協定後，Switch 部分 Port 爲“active”，部分 PORT 爲“block”(表 4)，整個網狀架構以邏輯觀點來看變爲樹狀架構(圖 5)。

圖 4：網狀網路的實體架構

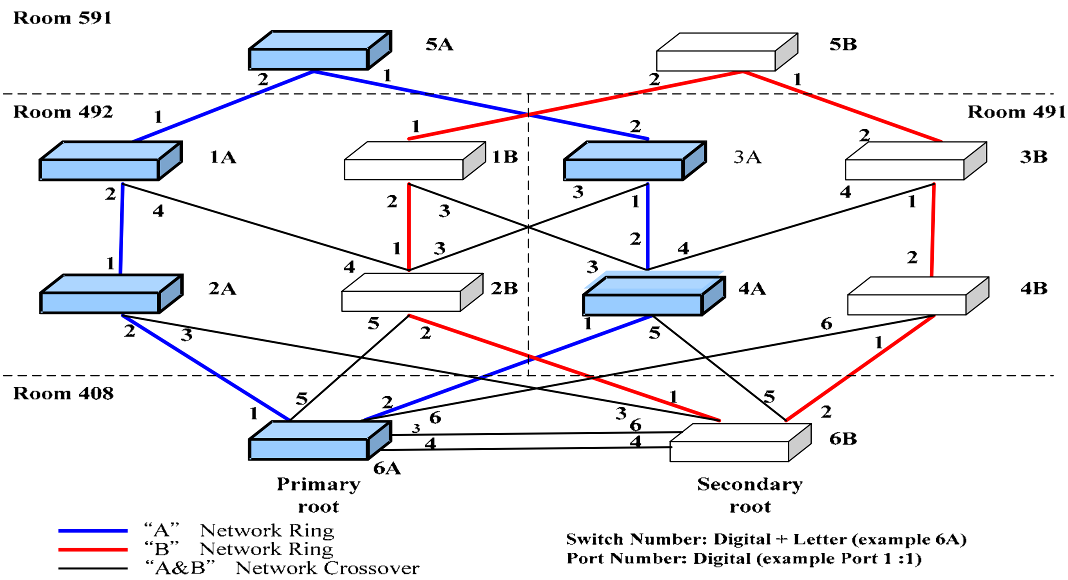
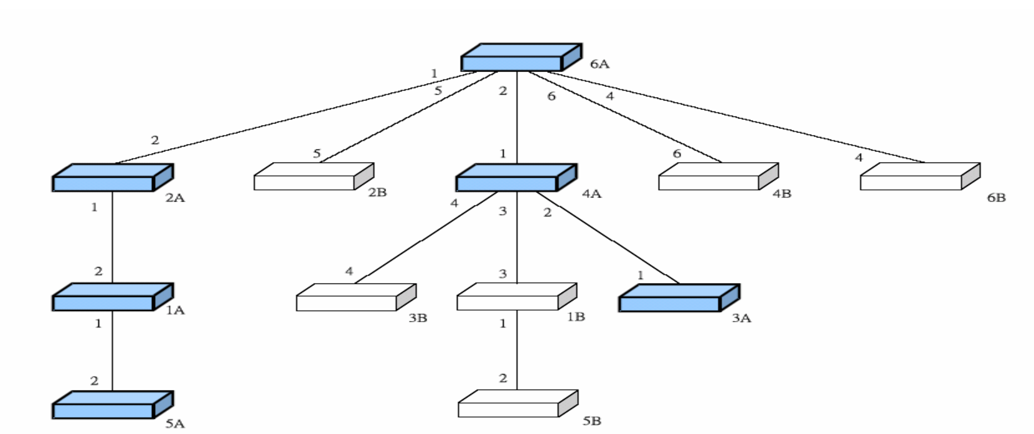


表 4：Network Switch 各 Port 之狀態表(A:Active,B:Block)

Switch # / PORT#	1A	1B	2A	2B	3A	3B	4A	4B	5A	5B	6A	6B
PORT 01	A	A	A	B	A	B	A	B	B	B	A	B
PORT 02	A	B	A	B	B	B	A	B	A	A	A	B
PORT 03	NA	A	B	B	B	NA	A	NA	NA	NA	A	A
PORT 04	B	NA	NA	B	NA	A	A	NA	NA	NA	A	A
PORT 05	NA	NA	NA	A	NA	NA	B	NA	NA	NA	A	B
PORT 06	NA	NA	NA	NA	NA	NA	NA	A	NA	NA	A	B

圖 5: Network Switch 之實際通路圖

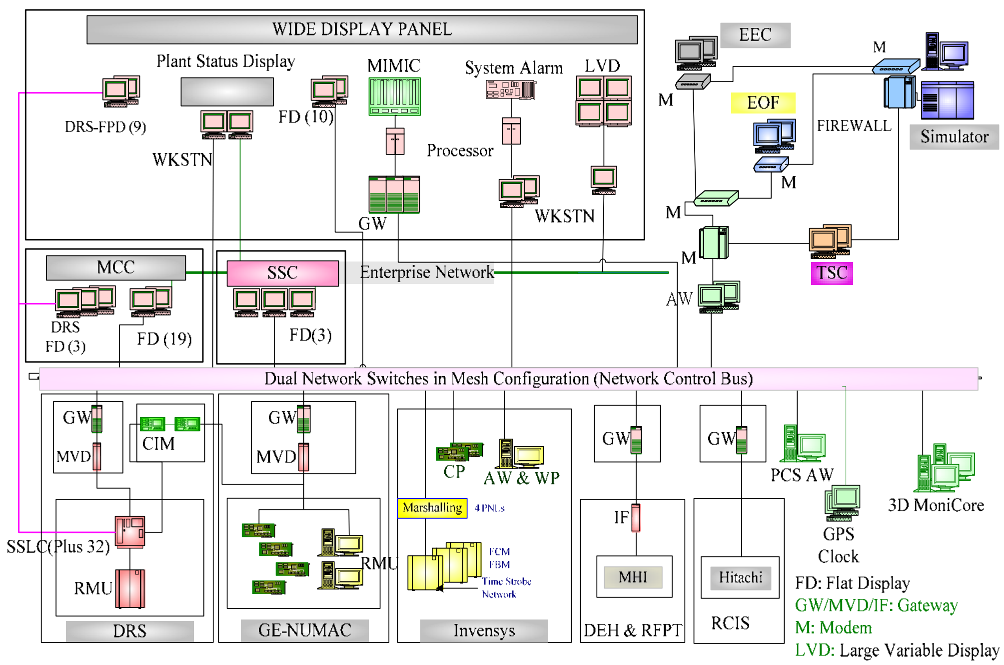


核四廠 Invensys HPS 系統如圖六所示，網狀網路包含六個雙重

Network Switch，每一個 Network Switch 有 7 個 Blade，每個 Blade 有 48 個 100Mbps Port 及 2 個 1Gbps 之 Uplink Port，Uplink Port 為網狀網路互連之用，Invensys 處理器模組(如 AP、WP、AW、CP)及通訊模組(FCM、Gateway)接至 Switch 之 100Mbps Port，現場的設備經由 FBM/FCM 接至 Switch 100Mbps Port。

FBM/FCM 等工作原理已於前敘述，另閘道器為一個二個廠家間通訊協定轉換之設備，以作為 Invensys 系統與其他非 Invensys 設備，例如 DRS equipment, GE NUMAC equipment, PLC, GEIS equipment, WDP, and Multi-Vendor Device (MVD)之界面。

圖 6：核四廠 Invensys HPS 系統



安全性、可靠性、與效能為控制網路的三個特性，為了確保 Invensys 控制網路在電廠暫態期間之可靠性(即網路不會崩潰)，除了執行 DCIS 資料流量反應時間、資料鏈總量和網路負荷分析外，另執行實體的 Invensys 網路應力測試(Network Stress Test)，結果均能符合設計要求。

因為 Invensys HPS 系統為雙重網路的設計且二個網路間亦有互連

網路，單一的網路或網路交換器故障不會影響控制系統之功能。不同組的二個網路交換器同時故障時，會依 RSTP 通訊協定重組網路架構，二個節點間之資料傳輸時間會增長，但仍能符合設計要求。

B、LVD 企業網路

該網路由運轉員之操作處理器(WP)、應用處理器(AW)、網路交換器(Switch)與 LVD 所組成。操作處理器(WP)、應用處理器(AW，包含 PGCS、和 3D Monicore)連接至網路交換器的一般 port，網路交換器的 uplink port 連接至 LVD。因此，運轉人員除了可將系統操作之 WP 畫面透過企業網路送至位於寬螢幕顯示盤上的 70 吋大型可變螢幕(LVD)外，另可將一些 AW 螢幕畫面送至 LVD 以提供資訊給其他運轉人員用。企業網路作為控制網路與 LVD、PGCS、和 3D Monicore 間的隔離器，任何連接至企業網路的設備故障時，不會影響控制網路的運作。

C、時間戳網路

時間戳訊號係由全球衛星定位系統之時間信號所產生，經由 Time Strobe Converter 送至 FCM/FBM、控制處理器模組與、閘道器之 TOD 端做為其時鐘訊號，同步全廠控制處理器、FBM 模組與閘道器之時間標識 (時間差在 0.5 毫秒內)，以確保 SOE 系統之時間準確性。

安全有關儀控系統主要由二個廠家所供應，一為 GE 廠家之 GE NUMAC 產品，另一為 DRS 廠家。

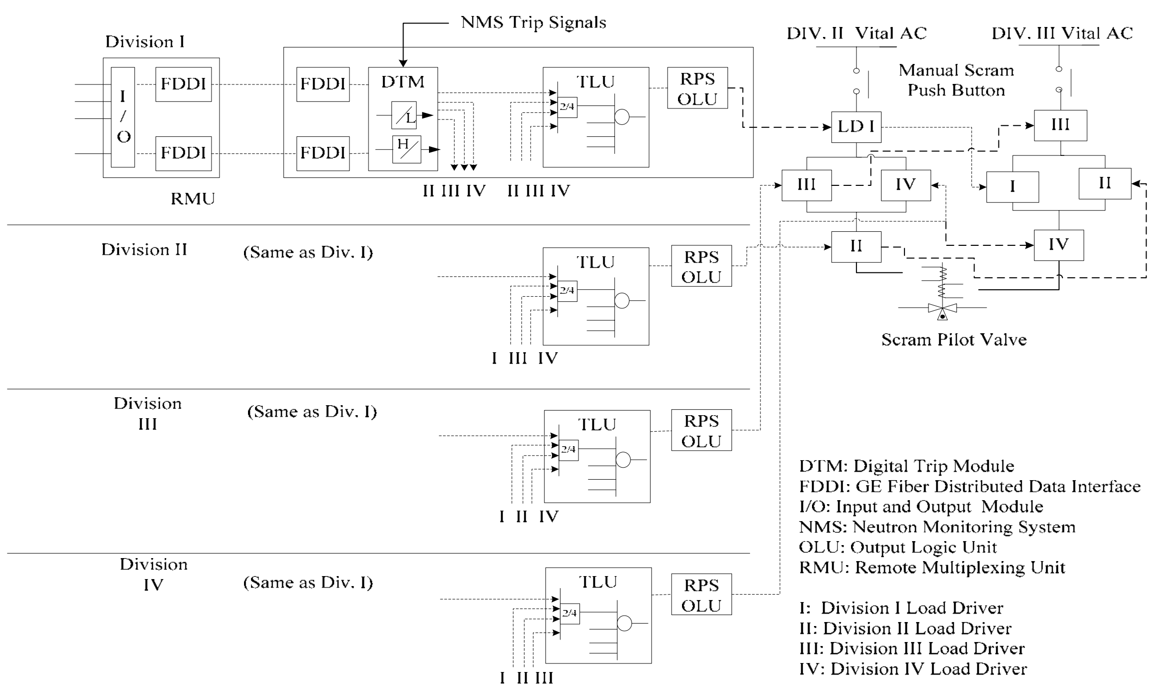
5、RPS 系統之 NUMAC 架構

GE NUMAC 產品為點對點架構，此論文僅敘述 GE NUMAC 之反應器保護系統之架構，核四廠 RPS 跳脫邏輯為四選二邏輯而非傳統 BWR 電廠之重複二選一邏輯，參考圖七 RPS 系統有相同的四個控道，控道間為實體隔離，控道間以光纜相連以滿足電氣隔離。大部分的感測器(例如反應器水位傳送器)直接連至 RMU 的輸出入模組(IO Module)，然後 RMU 之輸出入模組經由光纜送至位於控制廠房之 DTM 模組(Digital Trip Module)，一些訊號(例如中子偵測跳脫訊號)因需較快的反應而直接送至 DTM 模組而非送至輸出入模組(IO Module)。每個控道之 DTM 模組執行設定點比較和送出”跳脫”訊號，DTM 之”跳脫”訊號經由光纜送至

四個控道之 TLU 模組。每個控道之 TLU 接收到該控道與其他三個控道 DTM 之”跳脫”訊號，執行四選二邏輯，若其中二個控道以上之 DTM 模組輸出訊號爲”跳脫”時，則 TLU 之輸出訊號爲”跳脫”，TLU 送出訊號給同一控道之 OLU 模組 Output Logic Unit。OLU 模組執行該控道之”跳脫”、”跳脫自保”與復歸等功能。OLU 跳脫訊號再送至 Load Driver (LD) ，LD 是一個電流中斷設備 ，當 OLU 輸出訊號爲”跳脫”時，則無電流流過 LD，四個 LD 再形成一個四選二邏輯。

任何二個 OLU 在跳脫狀態，則二串的 LD 會中斷電流流經急停響導電磁閥(Scram Pilot Valve Solenoid)，最後反應爐急停。任何一個元件故障或失效(例如感測器 DTM、TLU、OLU、電源、LD、急停響導電磁閥和連接線、光纜)都不會中斷急停的動作或造成系統的誤動作。RPS 系統有感測器旁通和控道旁通設計，當感測器 A 被運轉員手動旁通時，TLU 之感測器跳脫邏輯從四選二邏輯變成三選二邏輯。當一個控道被運轉員手動旁通時，則系統跳脫邏輯從四選二邏輯變成三選二邏輯。RPS 系統間的模組通訊採用 RS485 的點對點通訊。

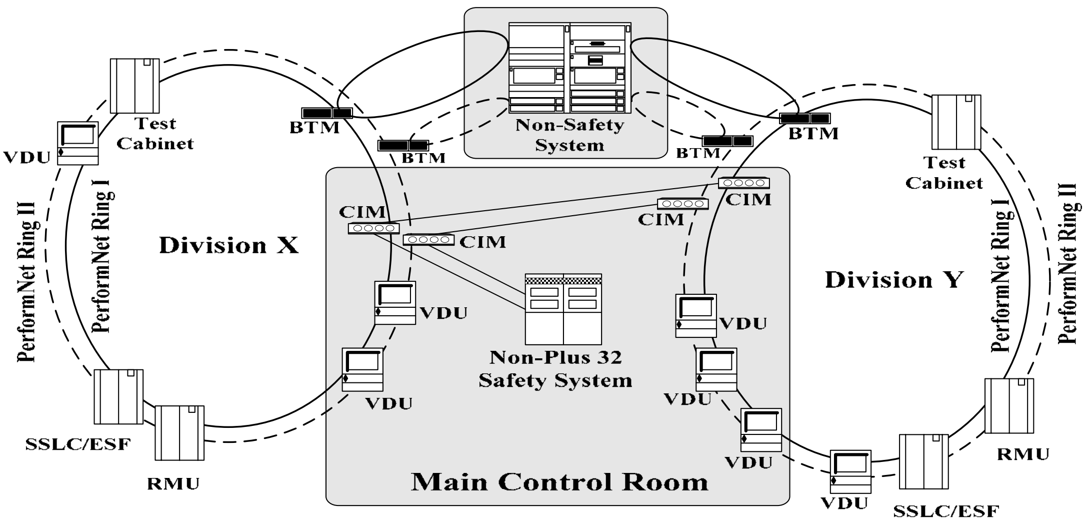
圖 7:核四廠反應器保護系統架構圖(RPS System Configuration in LMNPS)



6、DRS PERFORMNet 的網路架構

SSLC/ESF 系統採用 DRS PLμS 32 系統(Programmable Logic Microprocessor System: 32 bit)，DRS PLμS 32 系統採用 PERFORM Net (Performance Enhanced Redundant Fiber Optic Replicated Memory Network)。核四廠之 SSLC/ESF 系統共有 5 個獨立的環狀網路，分別用於控道 0、控道 I、控道 II、控道 III 和控道 IV(圖 8)。電廠正常運轉時，SSLC/ESF 系統使用控道 I 至控道 IV 來控制 ESF 設備，控道 0 用於 Swing 柴油發電機的控制。Swing 柴油發電機可以替代入一號機或二號機的任何一台緊急柴油發電機。每個控道包含 RMU、SSLC/ESF 盤、VDU、測試盤(Test Cabinet)和閘道器盤。

圖 8：DRS PERFORMNet 架構圖



DRS PERFORMNet 共有三種通訊介面分別爲

A、CIM(Communication Interface Module)模組：提供低頻寬之資料傳輸，如各 ESF 區域間(Division I, II, III, IV)之相互通訊和 ESF 區域與 RPS/RTIF 之通訊(雙向)。

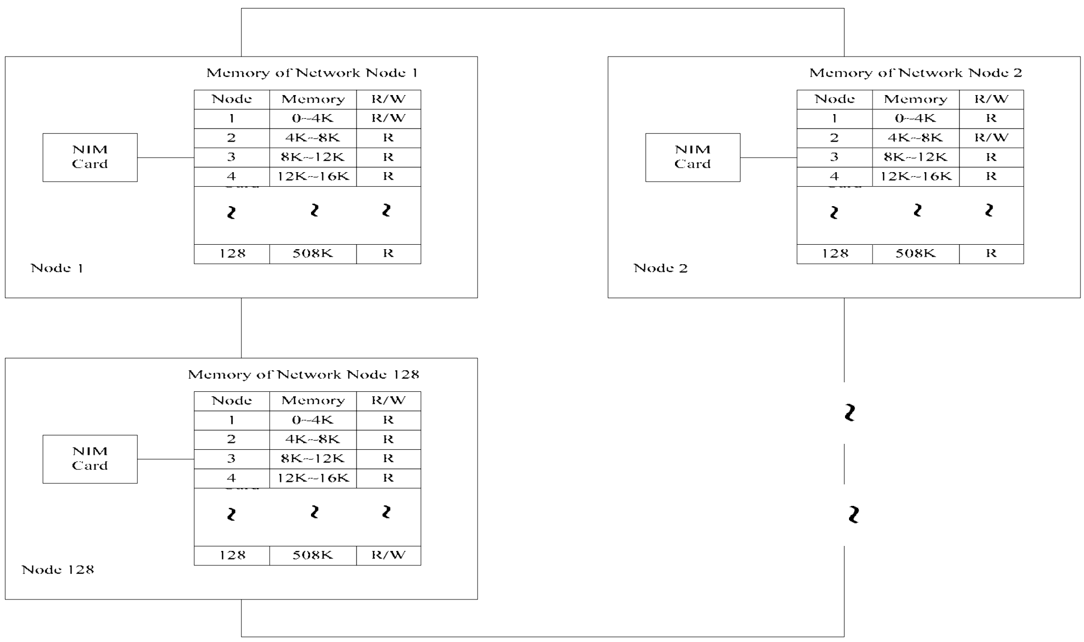
B、BTM(Bridge Transfer Module) 模組：安全有關系統(SSLC/ESF、SSLC/RTIF)與非安全有關系統 Foxboro 間之通訊，此通訊爲單向的通訊。

C、NIM(Network Interface Module) 模組:同區域間之 PLμS32 設

備(如 RMU 、SSLC/ESF 機櫃、VDU、CIM、BTM)之通訊則以 NIM 做資料傳輸，例 RMU 從現場收集資料後，經其 NIM 卡片將資料傳遞至 PERFOMNet，SSLC/ESF 機櫃透過其 NIM 卡片讀取 PERFOMNet 上的資料。

PERFORMNet 使用複製記憶體(Replicated memory,圖 9)之概念,核四廠每一個控道複製記憶體的大小爲 512K 位元，每一個節點都有一個相同大小的複製記憶體，核四共有 128 節點，因此每一個節點的複製記憶體的大小爲 4K 位元。每一個節點只能將資料寫入其複製記憶體之指訂位置，然後該資料被自動的複製至下個節點相同位置的記憶體，依序複製直至所有的節點相同位置的記憶體都被複製。但任一節點可讀取節點所有複製的記憶體資料，因此複製記憶體爲節點間交換資料的地方。二個節點以光纜連接，光纜提供二個節點的電氣隔離。PERFORMNet 爲雙重的架構，每一個節點有二個 NIM 卡片(NIM-A、NIM-B)，所有節點的 NIM-A 卡片以環狀方式相連在一起形成 A 網路;所有節點的 NIM-B 卡片以環狀方式相連在一起形成 B 網路，因此任一 NIM 卡片或光纜的故障，系統仍能正常的工作。

圖 9：複製記憶體的概念圖



7、資料鏈(DATALINK)

二個不同網路平台間的通訊以資料鏈爲之，核四廠超過 100 條的資料鏈(圖 10)，GE 爲核四廠各個儀控廠家整合設計之主導者。核四廠原則上使用開放式的通訊界面(即 OPC 和 Modbus)，但因開放式的通訊協定不符核四廠之要求，因此有二個特殊通訊界面，一爲 MHI 與 Invensys 的通訊界面，另一爲安全有關系統與非安全有關的通訊界面(MVD)，表 5 爲核四廠使用的通訊協定。

圖 10：核四廠 DCIS 界面圖

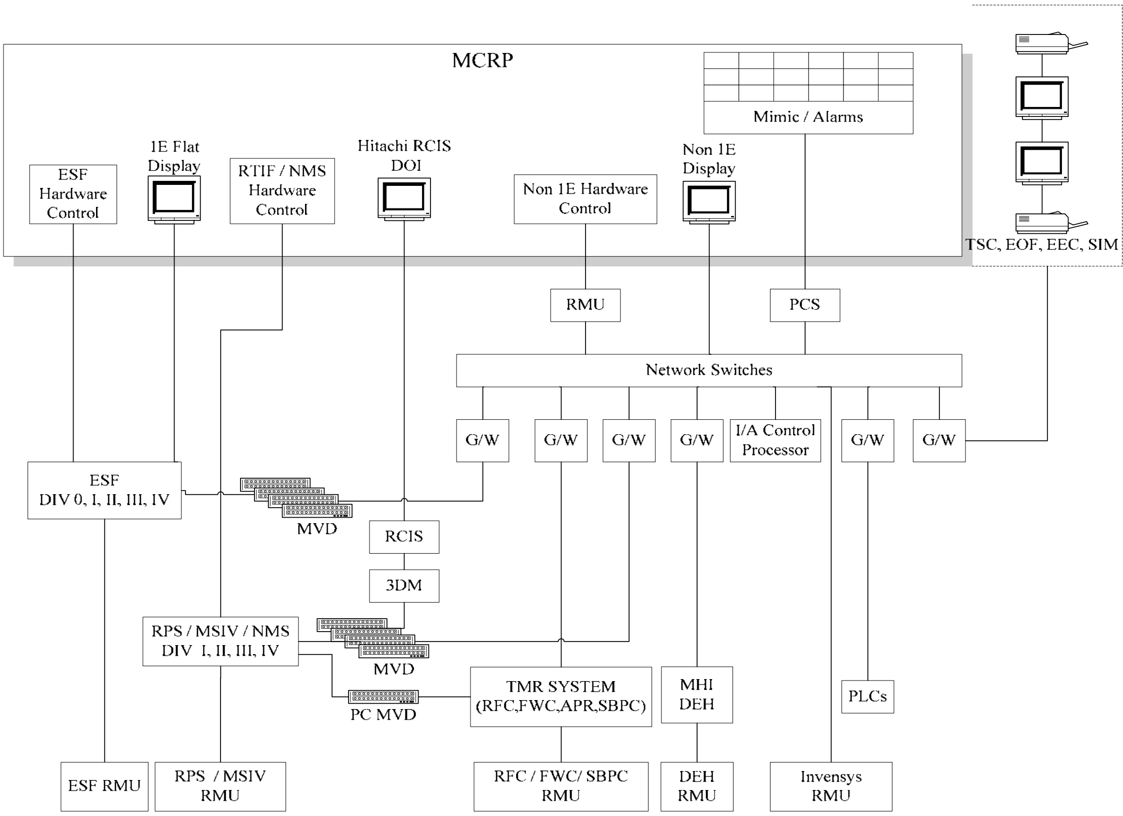


表 5：核四廠重要的通訊協定(Major protocols used in LMNPS)

	FROM /TO	PROTOCOL
1	GE NUMAC (RPS/NMS) → DRS (ESF)	RS-485 / PERFORM NET
2	GE NUMAC (RPS/NMS) → MVD→ INVENSYS	RS-485 / TCP-IP
3	DRS (ESF)→ MVD → INVENSYS	PERFORM NET / TCP-IP
4	GE NUMAC (RPS/NMS)→ MVD → TMR (RFC/APR)	RS-485 / TCP-IP (EGD)
5	TMR← → INVENSYS	MODBUS OVER TCP/IP

6	MHI (EHC) ← → INVENSYS	MODBUS OVER TCP/IP
7	PLC	MODBUS OVER TCP-IP OR OPC

爲了確保資料從一個廠家傳遞至另一個廠家，二個廠家的界面設計者要溝通並建立一個二者都可接受的通訊界面需求(包含實體層及網路層)。表 6 爲補水系統與 Invensys HPS 系統之界面需求表。

表 6：Invensys HPS 系統與補水系統可程式控制器的界面需求表

	INTERFACE REQUIREMENT
1	IDENTIFICATION: MAKEUP WATER SYSTEM
2	FUNCTION: TO TRANSMIT MW STATUS INFORMATION TO THE DCIS FOR INDICATION AND ALARM
3	DATA THROUGHPUT REQUIRED: 49KBIT PER SECOND
4	REDUNDANCY REQUIREMENTS: YES
5	ASSOCIATED DATA LINKS: NONE
6	DATA LINK RESTRICTIONS: N/A(DEDICATED, ONE TO ONE)
7	DATA LATENCY: 100 MILLISECOND
8	CLOSED LOOP CONTROL: NONE
9	PHYSICAL MEDIUM: FIBER OPTIC
10	STANDARD APPLICATIONS: GRAPHIC & DISPLAY
11	RELATIONSHIP: PLC: SLAVE, DCIS: MASTER
12	PROTOCOL DIAGRAM: OPEN MODBUS/TCP
13	TIMEOUT VALUES WHERE APPLICABLE IN THE PROTOCOL DIAGRAM: REFER TO OPEN MODBUS / TCP/IP SPECIFICATION
14	APPLICATION CONNECTION IDENTIFICATION SUCH AS PORT NUMBER OR SERVICE NAME: DITTO
15	HOW FUNCTIONS ARE DIFFERENTIATED, BY DIFFERENT END POINTS OR BY MESSAGE CONTENT: DITTO
16	DETAIL PACKET FORMAT SPECIFICATION FOR ALL TRAFFIC ON THIS DATALINK: DITTO

8、電廠自動化(Plant Automation)

電廠自動化(Plant Automation)爲 ABWR 電廠新增的的一個特性，以

往 BWR 電廠若要增加功率，運轉員必須手動抽棒或增加再循環流量，但在 ABWR 電廠有一個系統稱爲電廠自動化系統”PGCS”，運轉員可在”PGCS”系統執行指定的步驟以提升功率，之後 PGCS 會自動送出”抽棒訊號”給 RCIS 系統或”增加流量”訊號給”再循環流量系統”以提升反應器功率。

PGCS 系統共有三個階段分別爲電廠正常啓動(Normal Plant Startup)、功率運轉(Power Range Operation)和電廠停機(Plant Shutdown)，PGCS 系統對此三階段事先訂有設備啓動的順序，因些 PGCS 如同一個順序器。PGCS 送出一個命令訊號給系統層級的的控制器執行一個特定的工作，例如汽機控制系統之控制閥打開，當特定工作完成後，系統層級的控制器發出完成訊號給 PGCS 系統，然後 PGCS 系統再出下一個命令訊號。

爲了完成儀控系統的自動化，所有廠家的儀控系統經閘道器交換的資訊或命令需求訊號必須正確，且各個廠家的儀控系統必須能正常的工作，因此資料鏈的現場測試與系統之試運轉測試對電廠自動化的功能息息相關。

9、161KV 加壓與 DCIS 現場測試

在 DCIS 設備運至電廠前，所有的儀控設備在廠家執行深入的廠家測試，廠家測試包含模組測試(Module Test)、整合測試(Integration Test)和確認測試(Validation Test)和 DCIS 廠家測試(FAT)，然後 DCIS 已運至/將運至台灣執行安裝工作及執行現場測試。台電將負責未來的安裝工作及現場測試工作，因 DCIS 之複雜性，台電已建立現場測試計劃書，計劃書爲二部分，一爲 DCIS 初始架構的建立，另一爲 DCIS 現場測試計劃。測試計劃書依美國核能法規指引 Reg. Guide 1.68、美國電子電機協會文件 (IEEE 7-4.3.2)、廠家建議及以往儀控更新的經驗所書寫。

A、DCIS 初始架構建立

Invensys HPS 系統爲乙太網路，網路層必須先建立，網路層包含所有網路交換器、至少二個運轉員操作站(MMI)。然後 161KV 加壓相關的 RMU 盤、控制處理器及其應用處理器必須安裝。之後現場設備及

其至 RMU 盤之電纜須安裝，最後依現場測試計劃書/程序書執行測試。

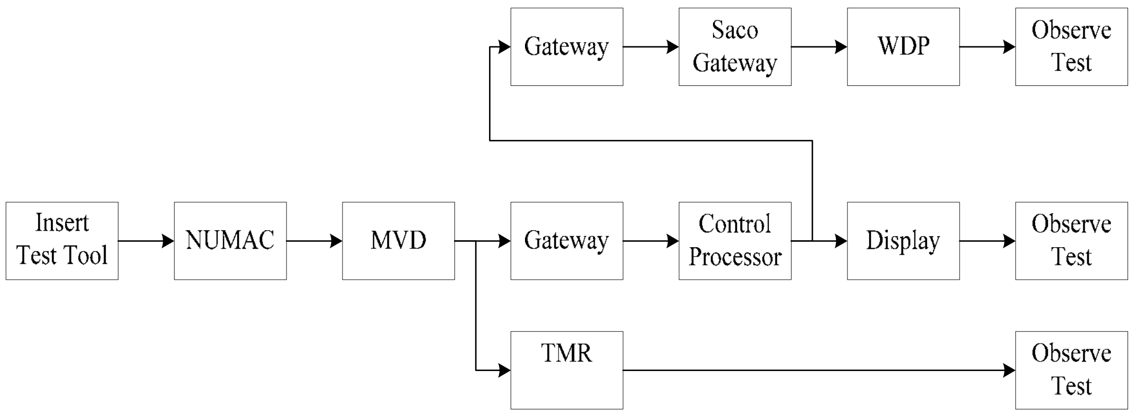
B、DCIS 現場測試計劃(DCIS Site Test Program)

在儀控盤面送電前，盤面送電端點的絕緣測試須執行，之後外接電源的電壓及頻率須調整。爲了避免不正確的電源燒毀電子卡片，電子卡片在送電前可先移除，送電後電壓及頻率量測正確後再插回卡片。之後,視需要安裝軟體,執行自我檢測以查證 DCIS 的設備功能正常(含連接光纜、終端接頭、DCIS 設備..等)。

在 RMU 盤之端點改變電氣數值(4~20ma)或在感測器端改變流程值並檢查 VDU 之工程值以執行輸入訊號迴路檢查;而輸出迴路檢查爲輸入迴路檢查反向查驗，在 VDU 上輸入一個工程值，然後在 RMU 盤之端點查看在電氣訊號或在終端元件上查看其動作情形。另一測試爲雙重測試(包含雙重電源單一故障測試、雙重網路之單一網路故障測試、雙重控制處理器之單一故障測試)，這類之測試可將系統置於閉迴路環境，再執行單一故障之模擬，再查看 VDU 上的流程參數應不變。

當 DCIS 界面盤建置完成，資料鏈必須開始確認，有些訊號送至多處(例如中子偵測系統之訊號經由 MVD 送至 WDP、VDU、TMR 等系統，圖 11)，在測試前這些訊號的傳遞路徑要加以了解並建表。測試方法爲在 NUMAC 的輸入端送一個已知的模擬訊號，然後在 WDP、VDU、TMR 等設備端查驗證其讀數是否正確。

圖 11：GE NUMAC 系統至 WDP、TMR 系統與 Invensys MMI 之路徑圖



10、改善現場測試時程之測試工具

FSIM 測試設備是 Invensys 產品,台電已購買該產品用於核四廠邏輯修改後驗證工作以縮短現場測試時程。假如在試運轉期間，系統的邏輯測試結果為不正常，邏輯必須修改/建置在 Invensys 設備上，並執行修改後的邏輯測試，修改後的邏輯測試可在實體執行或在 FSIM 測試設備執行。

核四廠選擇在 FSIM 測試設備上執行離線測試，測試完成後再將控制資料庫上載至實體設備之後，再執行試運轉測試。使用 FSIM 測試設備之優點為(1)容易建立測試環境(2)容易模擬輸入訊號(3)在驗證期間不會造成設備的損壞。除此之外，光纜時域反射儀(OTDR)、光纜測試儀、網路測試儀器、封包分析儀等都是量測光纜/網路重要特性或解決問題的工具。

11、結語

核四廠儀控系統(DCIS)規模巨大且為第一次整合多廠家之儀控設備用於 ABWR 電廠,因此核四儀控系統之現場測試只能參考日本核電廠 DCS 系統、廠家測試及儀控更新的經驗。

儀控系統之成敗首在各廠家儀控系統之整合，由於 DCIS FAT 採用分區塊(Invensys、GE 和 DRS)的方法來執行測試，區塊的互相連接的資料鏈以 Overlap 方法來測試，部分的資料鏈採取實體測試，部分的資料鏈採取模擬測試，又部分測試採取樣測試的方法。為了確保資料鏈所傳遞的訊號為正確的，理論上執行全部的輸出/輸入測試可確保資料傳遞百分百的正確，但核四廠資料鏈輸入/輸出點約有四萬點，要執行端點對端點之測試需要非常多的人力與物力，為了在期限內完成資料鏈的測試，核四廠採取的策略為，有些資料鏈需採最取樣測試，有些則執行全部輸入/輸出點之測試。

在試運轉期間，由於管路內沒有蒸汽及水，飼水控制系統、再循環量控制系統、汽機控制系統等無法執行閉迴路控制測試，上述系統的閉迴路測試將在機組啓動後執行，為了啓動時之順利，部分的邏輯及設定需要以人工查驗

。最後一項爲電廠自動化測試，此測試亦需在機組啓動時執行，其順利與否與 DCIS 資料鏈測試息息相關。

核四廠儀控系統爲複雜的、大規模的和整合的系統，對台電、各儀控廠家、設計者、安裝包商都是一大挑戰。爲了在 DCIS 現場測試期間，順利的整合各廠家的儀控系統，台電需要各單位的協助以完成此一任務。

參、國外公務之心得與感想

美國核能學會主辦之核電廠儀控系統(NPIC)與人機介面技術(HMIT)會議爲核能儀控界的最重要的研討會之一，今年在美國新墨西哥州 Albuquerque 舉辦。本屆會議規模相當龐大，與會國家計十七個，共發表論文 200 餘篇，研討主題包括「核電廠現代化經驗」、「軟體品質保證」、「安全關鍵軟體發展與檢證」、「核電廠內無線通訊技術之應用」、「人機界面發展技術」等五十多項。核四廠儀控設計廠家 GE 及製造廠家 Invensys 代表亦參與並發表相關論文，藉由與會發表論文 ┌核四廠儀控網路架構與現場測試┘ 之機會，與製造廠家之研發人員及其他與會代表就核四儀控相關議題討論並交換意見，獲得許多實務經經驗。

美國南方德州電廠(STP)新建核電廠計畫，由奇異公司提供相關的儀控設備並設計，主要參考電廠爲核四廠，會後美國南方德州電廠儀控顧問公司(Hurst 公司)負責人在會後與與職討論相當多的核四儀控議題(包含 DRS 儀控平台、NUMAC 儀控平台、Invensys 網路架構等、人因部分等)以作爲該公司對美國南方德州電廠採用儀控設備之建議。在會談中，儘可能讓 Hurst 公司了解核四儀控的優點，若美國南方德州電廠(STP)新建核電廠計畫採用本廠相同的儀控設備時，對核四儀控備品取得及維護將有極大的助益。

此次參與國際性會議，由會中研討的主題及各國管制單位發展的論文議題可推測核能儀控界，管制單位關心的重點爲網路安全(Cyber Security)、軟體共模故障、深度防禦與多樣性(簡稱 3D)、人因工程、軟體可靠性等。因此數位儀控的設計發展過程/安裝過程之驗證、構型管理、軟體安全分析非常重要。雖然核四廠採用的儀控法規符合上述的

要求，重要幹部亦有相當的了解，此方面的議題在電廠建廠告一段落後應再深入的了解。

肆、對公司之具體建議

核能儀控與人機介面技術國際研討會產官學界均會派員參加，藉由參與此會議的機會可知核能儀控界管制單位關心的重點，並與參加人員面的面的溝通，可得到核能界人員寶貴經驗，經驗與新知對將來的維護有助益，因此建議電廠人員多參與此類的會議。

由於核四廠儀控系統由多廠家的儀控網路整合而成，且各廠家的通訊協定亦不同，此次藉由發表「核四廠儀控網路架構與現場測試」的機會與儀控網路專家深入探討儀控網路，獲得許多的原本不知道的知識，這些知識對將來的核四控制網路維護極有助益。建議電廠人員參與較深入的網路課程訓練。

附件、核四廠網路架構與現場測試

The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station

Chia-Kuang Lee

Section Chief of Instrument and Control Section,
Lungmen Nuclear Power Station, Taiwan Power Company, Taipei County, Taiwan, ROC
Tel: 886-2-29402401 Ext. 2940, e-mail: u826154@taipower.com.tw

Abstract –*The Lungmen Nuclear Power Station (LMNPS) is located in North-Eastern Seashore of Taiwan. LMNPP has two units. Each unit generates 1350 Megawatts. It is the first ABWR Plant in Taiwan and is under-construction now. Due to contractual arrangement, there are seven large I&C suppliers/designers, which are GE NUMAC, DRS, Invensys, GEIS, Hitachi, MHI, and Stone and Webster company. The Distributed Control and Information System (DCIS) in Lungmen are fully integrated with the state-of-the-art computer and network technology. General Electric is the leading designer for integration of DCIS. This paper presents Network Architecture and the Site Test of DCIS. The network architectures are follows. GE NUMAC System adopts the point to point architecture, DRS System adopts Ring type architecture with SCRAMNET protocol, Inevnsys system adopts 1Giga Byte Backbone mesh network with Rapid Spanning Tree Protocol, GEIS adopts Ethernet network with EGD protocol, Hitachi adopts ring type network with proprietary protocol. MHI adopt Ethernet network with UDP. The datalinks are used for connection between different suppliers. The DCIS architecture supports the plant automation, the alarm prioritization and alarm suppression, and uniform MMI screen for entire plant. The Test Program regarding the integration of different network architectures and Initial DCIS architecture Setup for 161KV Energization will be discussed. Test tool for improving site test schedule, and lessons learned from FAT will be discussed too. And conclusions are at the end of this paper.*

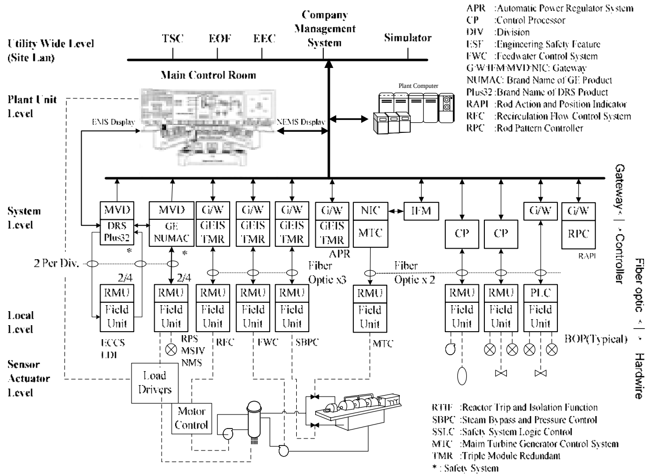
I. Introduction of DCIS in LMNPP

The Lungmen Nuclear Power Station (LMNPS) has two units. Each unit generates 1350 Megawatts. Taiwan Power Company (Taipower) is the Owner of the LMNPS. The Distributed Control and Information System (DCIS) in LMNPS is fully integration of seven large I&C suppliers / designers by using the state-of-the-art computer and network technology. The following is the description of the DCIS system in LMNPS.

Refer to functional Diagram of Lungmen DCIS system (Figure 1), Lung men DCIS I&C systems consist of safety and non-safety I&C systems. Safety I&C systems contain DRS products and GE NUMAC. DRS Company provides I&C system for Emergency Core Cooling System (ECCS) and Leak Detection and Isolation Systems (LDI). Neutron Monitoring System (NMS) and Reactor Protection System (RPS) and MSIV Isolation System are GE NUMAC products. Non-safety I&C systems contain GEIS, MHI, and Invensys products. GE Industry System (GEIS) provides the triple module redundant systems which include Recirculation Flow Control System (RFC), Reactor Feedwater Control System (FWC), Steam Bypass and Pressure Control System (SBPC) and Automatic Power Generation Control System (APR). MHI Company provides the Turbine and Generator Control System and its auxiliary system. Invensys Company provides Plant Computer System (PCS), most of Balance of Plant (BOP) Control Systems, and I&C equipment of remote facilities, including Technical Support Center (TSC), Emergence Offsite Facility (EOF), and Emergence Executive Center (EEC), and Simulator, via firewall wall.

All non-safety Man-Machine Interfaces (MMIs) is located in the Invensys Flat-Displays, Mimic and Alarm. Due to safety concern, non safety-related equipment can not control the safety-related equipment. The safety MMIs are located in the DRS Flat-Displays. However, the safety-related information is also to Invensys Flat-Displays, Mimic and Alarm in one way.

Figure 1: Function Diagram of the Lungmen DCIS system



II. MAIN CONTROL ROOM ARRANGEMENT

The MMIs in LMNPS Main Control Room (figure 2) are tremendous different from MMIs of traditional control room which has analog meters, hard switches, and small mimics. The MMIs of Main Control Room in LMNPS are allocated in Wide Display Panel (WDP), Main Control

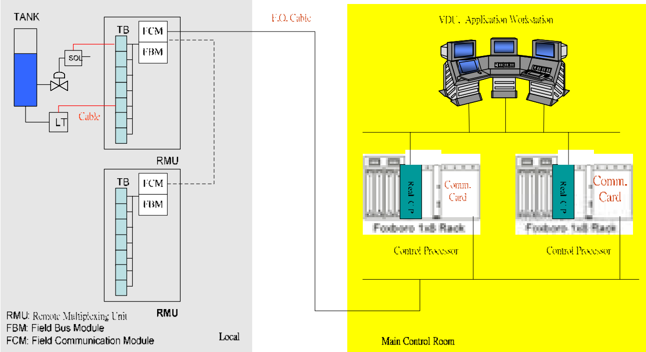
Console (MCC), and Shift Supervisor Console (SSC). The WDP, the highest panels, provides operators with an overview of the plant level parameters and their status and to perform the surveillance, and to monitor and control the plant during any postulated events. The MCC, directly in front of WDP, provides two operators to monitor and control the plant during the normal operation. The SSC, directly in front of MCC, provides Shift Engineer to monitor the plant status. Flat Displays, Plant Level Alarm, System Level Alarm, Mimic, hard switches, and Large Variable Display are allocated in WDP. Flat Displays and Hard Switches are allocated in Main Control Console (MCC). The Flat Displays are the MMI for operator to manipulate the equipment by touch screen and get the equipment status such as valve opening, component level alarm message. Operator can manipulate the same equipment at any Flat Display through network technology due to peer-to-peer characteristic of Ethernet network. The hard switches, on the WDP, for emergency control are provided for faster response or diversity control. The Annunciator and Alarm System consist of Plant Level Alarm, System Level Alarm and Component Level Alarm. Plant Level Alarms are on the left of WDP; System Level Alarms above the fixed mimic display on center of the WDP; Component Alarm available on the non-Class 1E Flat Display in the MCC. The windows of Plant Level Alarm will change text, audio alerting tones and voice commands depending on plant operation condition and alarm status. The System Level Alarms are also located on Wide Display Panel, and it has the priority and suppression schemes. The priority and suppression variable will be vary depend on plant operation condition. Component Level Alarms only show off on the Flat Display. In addition, Flat Display provides Touch Screen capability for operator to manipulate the equipment.

Figure 2: LMNPS main control room

III. The Network Architectures of DCIS in LMNPS

The typical DCS Functional Block Diagram is shown in the figure 3. The field sensors, such as level transmitter, are sent to nearby Remote Multiplexer Unit (RMU) at field. The analog input is delivered to analog input modules for signal conditioning and Analog-to-Digital (A/D) conversion in the RMU, the discrete data are delivered to the digital input modules in the RMU. Then, the field RMUs format and transmit input signals in network packet to the Control Processor in the Main Control Room for PID control, calculation and logic manipulation. The field RMUs de-multiplex the network packet received from Control Processor to analog or digital command signal to final element by traditional cable. In addition, the major MMIs used by the operator in Control Room are Visual Display Units (VDUs) rather than the “hard-switches” and “lamp-type indicator.

Figure 3: Typical DCS Functional Block Diagram



The DCS functional block diagram for each manufacture is very similar in the logical view. The physical architectures of the DCS networks used in LMNPS are ring type network and bus type network. Then, the networks of all I&C systems are integrated through gateway to form the large scale Lungmen DCIS system.

There are twenty one (21) manufactures to supply I&C system to LMNPS. Some manufacture provide small scale I&C systems, such as Programming Logic (PLC). Some provide large scale I&C systems. Table 1 shows the manufactures and their cabinet quantity used in LMNPS.

Table 1: I&C manufacture and cabinet quantity in LMNPS

Item	Manufacture	cabinet quantity
1	Invensys	165
2	Hitachi	67
3	DRS	65
4	MHI	39
5	GE-NUMAC	29
6	Harding /Smith	27
7	Toshiba	16
8	Inabensa	14
9	GE Industry System	8
10	Pall Filters	6
11	Siemens	6
12	York	5
13	Tough	4
14	Aptec-NRC	2
15	Preferred MT	2
16	Weir Pumps Ltd.	2

17	Chung-Hsin	1
18	Kinemetrics	1
19	PAR System	1
20	PHYS Acoustics	1
21	SACO	1

The important I&C systems in LMNPS are provided by GE NUMAC, DRS, Hitachi, MHI, GEIS, Invensys, and SACO Company. Table 2 is the summary table of I&C Manufactures, the system they provided, the protocol and network architecture they used. This paper only presents three network architectures, Invensys HPS system, DRS PERFORM NET, and GE NUMAC platform used by RPS System. The first system is called the NEM system, non-safety related multiplex system in LMNPS, and other two are called EMS system, Essential MUX System. The datalinks for integrating all I&C manufactures will be discussed too.

Table 2: Network Architecture and Protocol used in LMNPS

System	Equipment Manufacture / Product	Network Architecture	Protocol
Major BOP Control system	Invensys	Mesh / Ethernet	TCP/IP
Non-1E MMI	Invensys	Mesh / Ethernet	TCP/IP
ECCS/LDI	DRS	Ring Type	Perform Net
Class 1E MMI	DRS	Ring Type	Perform Net
RPS/MSIV Isolation	GE NUMAC	Point to Point	RS485
NMS	GE NUMAC	Point to Point	RS485
SBPC System	GE Mark VI/VIe	Ethernet	TCP/IP
FWC Control System	GE Mark VI/VIe	Ethernet	TCP/IP
RFC system	GE Mark VI/VIe	Ethernet	TCP/IP
APR System	GE Mark VI/VIe	Ethernet	TCP/IP
RCIS	Hitachi	Ring Type	Proprietary
Turbine Control System	MHI	Ethernet	UDP/IP

III.1: Invensys HPS system

Invensys HPS network consists of control network, enterprise network, and the time strobe network. At first, we will discuss the control network. Base on the scale of Invensys HPS system, see table 3, and time response requirement, the Invensys Control Network adopts latest Invensys HPS system, which consists of a number of network switches in the mesh configuration with Rapid Spanning Tree Protocol (RSTP) rather than nodebus / fieldbus configuration in traditional Foxboro I/A system.

Table3: Scale of Invensys HPS System in LMNPS

Description	Quantity
Hard I/O Point	17,000
Gateway I/O Point	40,000
Cabinet	165
Fault- Tolerant Control Processor	98
Single Control Processor	18
Application Processor	35
Workstation Processor	43

Invensys Control Network in LMNPS is a dual mesh network based on 100Mbps switched Ethernet with a 1-gigabit per second backbone. [1] The mesh networks contain six redundant switches per unit (one for common equipment, five for unit one). Figure 4 show the physical configuration of the mesh network. The uplink ports of switches are interconnected in the mesh configuration to form network A and network B. There are four data path between network A and network B. The redundant data path is to provide another reroute between two nodes, when the normal path failed. However, the redundant data path will form the loop, and the “data storm” will happen.

The main purpose of mesh network with the Rapid Spanning Tree Protocol is to block data path, only one data path is left between two nodes. After Rapid Spanning Tree Protocol applied to mesh architecture, some ports are acted as “block”; some are “active” as shown in Table 4 (Switch Uplink Port Assignments and Normal Status Table). Finally, the actual communication paths are the tree structure, as illustrated in figure 5.

Figure 4: Physical configuration of the mesh network

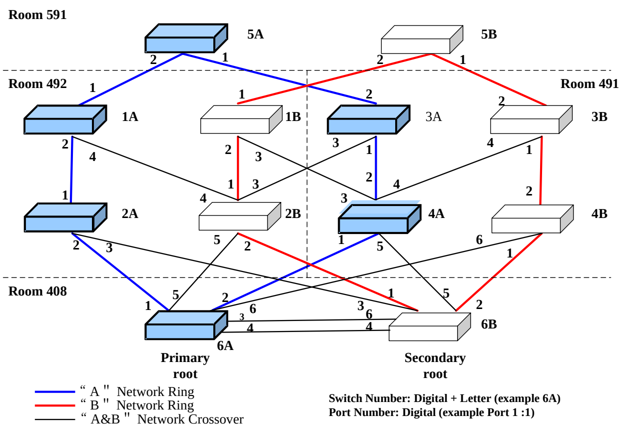
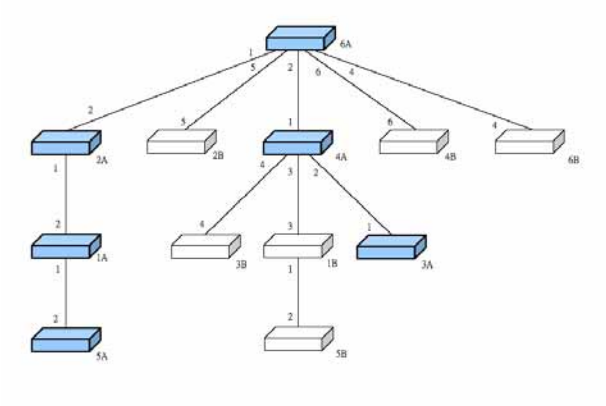


Table 4: Switch Uplink Port Assignments and Normal Status Table

Switch # / PORT#	1A	1B	2A	2B	3A	3B	4A	4B	5A	5B	6A	6B
PORT 01	A	A	A	B	A	B	A	B	B	B	A	B
PORT 02	A	B	A	B	B	B	A	B	A	A	A	B
PORT 03	NA	A	B	B	B	NA	A	NA	NA	NA	A	A
PORT 04	B	NA	NA	B	NA	A	A	NA	NA	NA	A	A
PORT 05	NA	NA	NA	A	NA	NA	B	NA	NA	NA	A	B
PORT 06	NA	NA	NA	NA	NA	NA	NA	A	NA	NA	A	B

Figure 5: Actual communication paths of the control network switches



The Invensys HPS System in LMNPS is illustrated in figure 6. The mesh control networks contain six redundant switches per unit. Each switch has forty-eight 100Mbps ports and two uplink 1Gbps ports. The Control Processor, Workstation Processor, Application Processor, Gateway Processor, and Field Communication Module (FCM) which located in the RMU are connected to the 100Mbps ports of network switches via marshalling cabinet by Fiber-Optic Cable. The Fieldbus Module (FBM) collects the local sensor data and sends control demand to final element such as valve, and breaker. FBM in the RMU are connected to FCM to digitize the local sensor signal to Control Processor for providing the monitoring and control function for operator. In addition, FBM receives the control demand from Control Processor to actuate the final element. The function of marshalling cabinet is nothing but interconnection jumper cabinet for Fiber-Optical Cable to easy F.O cabinet installation. The Gateway (GW) Processor is the protocol transfer mechanism between Invensys System and the products of other I&C manufactures such as DRS equipment, GE NUMAC equipment, PLC, GEIS equipment, WDP, and Multi-Vendor Device (MVD).

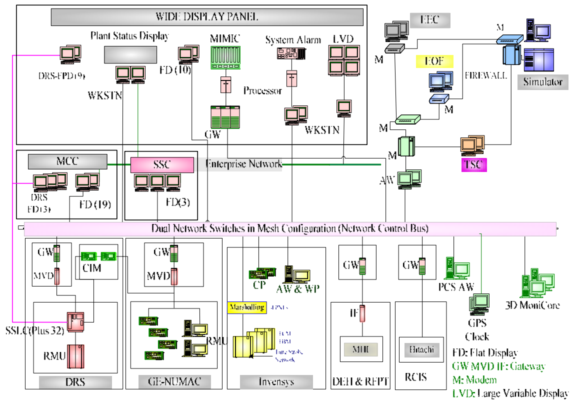


Figure 6: Invensys HPS System in LMNPS

Safety, Reliability, Performance are three important attributes [2]. To ensure Invensys Control Network reliability, that is no corruption, during plant transient period, GE performs the “DCIS Data Flow Response Time, Data Link Volume and Network Loading Analysis”. In addition, Invensys performs the network stress test. To ensure Control Network performance, the longest data path between any two nodes is four switches. That means a maximum latency of 100 microseconds round trip between any two nodes. Due to redundant configuration and interconnections between network A and B, single switch/network failure will not effect on the plant operation. Multiple switch failures will cause the reconfiguration of the tree structure per RSTP, and the data transmission time between two nodes still meets the requirement.

The second network is Enterprise Network, independent of the Invensys Control Network, which supports the Large Variable Display, Plant Generation and Control System (PGCS), and 3D MONICORE by using network switch. All Flat-Displays of Invensys, PGCS Server, and 3D MONICORE are connected to the switch port, the uplink port of switch connect to Large Variable Display. Therefore, Large Variable Display can show the identical image of any display from Flat-Displays, PGCS System, and 3D MONICORE for more operators to watch the plant operation. The Enterprise Network acts as the isolator for the control network. Any failure of the equipment which connected to the Enterprise Network will not impact the control network operation.

The last network is time strobe network, which synchronizes the clocks in the Control Processor and Fieldbus Module as well as the gateways. All signals are time-stamped in the front end of Invensys HPS system. Therefore, it ensures the accuracy of timing sequence in the Sequence of Event (SOE) Software. The Global Positioning Satellite (GPS) system provides the Time Strobe Signal to this network.

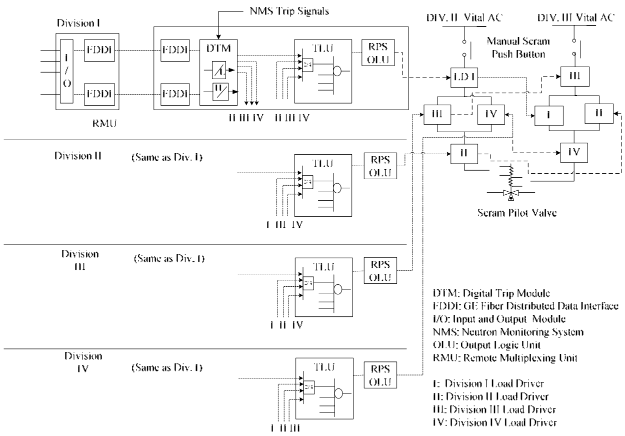
The safety I&C system has two major manufactures. One is GE NUMAC, the other is DRS. GE NUMAC is point to point architecture, in which only RPS architecture will present.

III.2B: NUMAC architecture for RPS System

The RPS trip logic is “two of four” logic rather than “one of two twice” logic in traditional BWR plants. In LNMPP, RPS system, as illustrated in Figure 7, has four redundant, physically separate, and electrically independent instrument channels. Most of the sensors, such as narrow range water level, are connected to I/O module in RMU, then transmission these signals to Digital Trip Module (DTM) via fiber optic cables. Some signals, such as NMS trip signals, are directly send to DTM, due to response time consideration. DTM of each instrument channel performs setpoint comparison and trip determination for each sensor. A “Trip” or “No-trip” is generated by the DTM and transmitted to all four RPS Trip Logic Unit (TLU) channels over fiber optic data links. The TLU of each division receive DTM “Trip” or “No-trip” of four divisions, and performs two-out-of-four voting.

Based on voting in TLU, the TLU provides trip signals to the Output Logic Unit (OLU) of the same logic division. The OLU of each trip logic division performs divisional trip and trip seal-in, reset, and trip test functions, then OLU trip output signal send to Load Driver (LD) which is “current-interrupting devices” controlled by the output signal of the OLU. If the OLU sends trip signal to the LD, then no current flows through LD. The four LDs form the other “two out of four” logic”. Two solenoids are installed on the scram pilot valve. Both solenoids on the scram pilot valve de-energization will cause reactor scram. Any two OLU in trip conditions, then both trains of LDs will interrupt the current flow from Power Source to the scram pilot valve solenoids. Finally, the reactor scram happens. Any one component failure or malfunction, such as sensor, DTM, TLU, OLU, power source, LD, Scram Pilot Valve Solenoid, and interconnection cable and fiber optical cable will not impact reactor scram action. The RPS system has sensor bypass and division bypass capability. When sensor “A” is bypassed by operator, the TLU voting logic will change from “two-out-of-four” logic to “two-out-of-three” logic. When one division is bypassed by operator, then the system trip logic will change from “two-out-of-four” logic to “two-out-of-three”. The communication between two modules in RPS is “RS-485” which is point-to-point type communication.

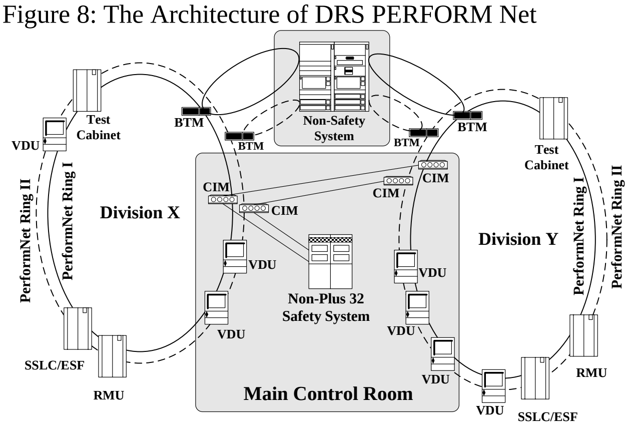
Figure 7: RPS System Configuration in LMNPS



III.3: The Architecture of DRS PERFORM Net

The SSLC/ESF system adopts DRS PLµS 32 system. PLuS 32 stands for Programmable Logic Microprocessor System: 32 bit. The network used in DRS PLµS 32 system is called PERFORM Net. PERFORM Net stands for Performance Enhanced redundant Fiber Optic Replicated Memory Network. There are 5 independent serial-ring networks, which serve for SSLC/ESF Division 0, I, II, III, IV, as illustrated in Figure 8. Division 1 to 4 will be used for normal operation of the plant. The fifth Division has been developed to support for swing Emergency Diesel Generator Control. This Division allows the Emergency Diesel Generator to replace either Unit 1 or Unit 2 Diesel Generator. Each division consists of RMU, SSLC/ESF logic, VDU, Test Cabinet, and gateway nodes. The RMUs are located in each of the equipment rooms in the Reactor Building (RB), Control Building (CB), Auxiliary Fuel Building (AFB) and safety-related pumphouse.

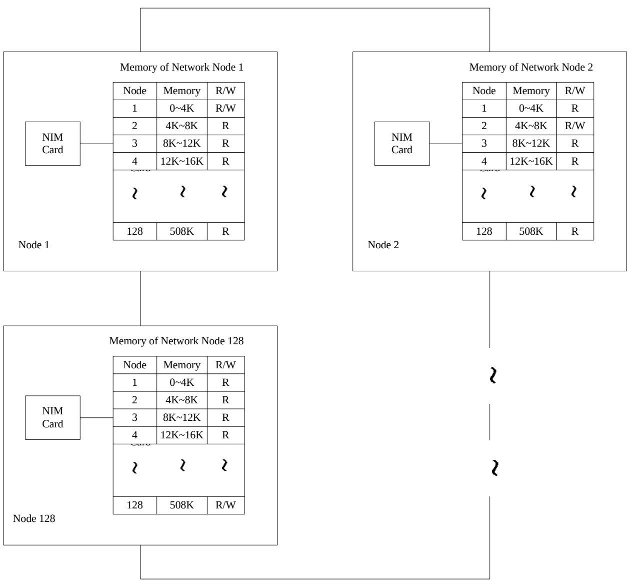
Figure 8: The Architecture of DRS PERFORM Net



A communication link is between the four Divisions, NMS, RPS, Division 0, and the non-safety related Gateway. All other data inputs / command output” will be through “hard-wiring” I/O at a RMU. MMI will be through touch screens or hard switches. The RPS System will share the VDU as its operator interface. The data from the RPS, NMS will be transmitted to same division’s DRS PERFORM Net via CIM card. Any data located on any Division's DRS PERFORM Net can exchange data from other Division's DRS PERFORM Net via CIM card. The BTM card is to transmit the data in the DRS PERFORM Net to Invensys HPS System via MVD device.

To understand the PERFORM Net, the concept of the replicated memory, as illustrated in Figure 9, will be present first.[3] Each node within the division has same size replicated memory, which is 512K bytes for LMNPS. The memory is segmented into 4K bytes blocks (per node), and the maximum number of nodes in LMNPS is 128. However, data can only be written to its own memory address, which is 4K bytes, for each node. The data written into its own memory address are automatically sent to same memory location in the next node. Finally, data are replicated to the same memory location for all nodes. Secondly, the interconnection between nodes is fiber optic cable, which provides for electrical isolation of nodes and equipment. Thirdly, the PERFORM Net is redundant to ensure ESF/SSLC system availability. Each node has two Network Interface Modules (NIMs), said NIM-A card and NIM-B card. All the NIM-A card of all nodes form the network A, and all the NIM-B card of all nodes form the network B. The function of the NIM card is to place the data into replicated memory for transmission the data over PERFORM Net to other nodes. Therefore, single failure of NIM cards or single fiber optical cable broken will not impact the control function of the ESF/SSLC system. Fourthly, the PERFORM Net provides several enhancement features, such as fault detection, recovery and stability, to standard replicated memory network to increase reliability.

Figure 9: The concept of the replicated memory



IV: DATALINKS

The datalink is used for data transfer between two different network platforms. More than 100 datalinks, as illustrated in Figure 10, are used for connection between different suppliers. GE is the leading designer for integration of DCIS in LMNPS. The basic design philosophy of the DCIS system in LMNPS is to adopt the open platform structure as much as possible, especial for non high-speed datalinks. The interface protocols of the datalinks are limit to "OPC" and "modbus" for non high-speed interface between PLC and Invensys. In addition, two types of special interfaces are designed for used in the LMNPS. One is interface between MHI Main Turbine Control/ Feedwater Turbine Control System and Invensys HPS system, the other is MVD which is interface between class-1E system to non- class 1E system. Table 5 is the major protocols used in LMNPS

Figure 10: Interface Block Diagram of DCIS in LMNPS

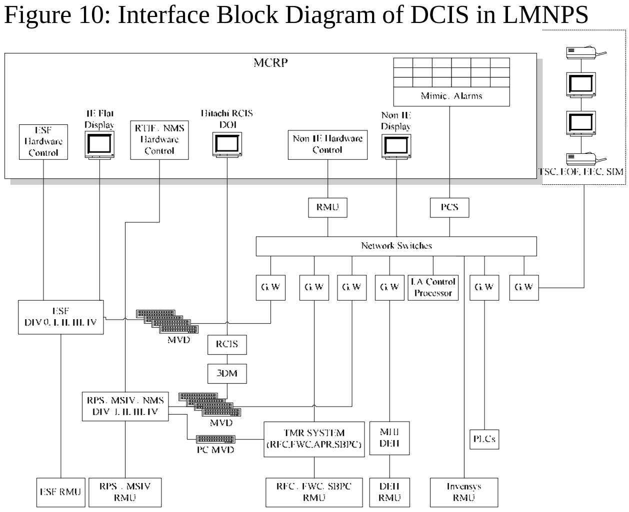


Table 5: Major protocols used in LMNPS

Item	From /To	Protocol
1	GE NUMAC (RPS/NMS) → DRS (ESF)	RS-485 / PERFORM Net
2	GE NUMAC (RPS/NMS) → MVD→ Invensys	RS-485 / TCP-IP
3	DRS (ESF)→ MVD → Invensys	PERFORM Net / TCP-IP
4	GE NUMAC (RPS/NMS)→ MVD → TMR (RPS/NMS) (RFC/APR)	RS-485 / TCP-IP (EGD)
5	TMR← → Invensys	Modbus over TCP/IP
6	MHI (EHC) ← → Invensys	Modbus over TCP/IP
7	PLC	Modbus over TCP-IP or OPC

The datalink is to exchange the data between two manufactures. To ensure the data correct propagation from one node to the other node, the design engineers of two manufactures should communicate well and establish the interface requirement, on physical layer as well as protocol. Table 6 shows the example of interface requirement between Makeup Water PLC and Invensys HPS system

Table 6: Interface requirement between Makeup Water PLC and Invensys HPS system

Item	Interface Requirement
1	Identification: Makeup Water System
2	Function: To transmit MW status information to the DCIS for indication and alarm
3	Data Throughput Required: 49Kbit per second
4	Redundancy Requirements: Yes
5	Associated Data Links: None
6	Data Link Restrictions: N/A(Dedicated, one to one)
7	Data Latency: 100 millisecond
8	Closed Loop Control: None
9	Physical Medium: Fiber Optic
10	Standard applications: Graphic & Display
11	Relationship: PLC: slave, DCIS: Master
12	Protocol Diagram: Open Modbus/TCP
13	Timeout Values where applicable in the protocol diagram: Refer to Open Modbus / TCP/IP Specification
14	Application connection identification such as port number or service name: Ditto
15	How functions are differentiated, by different end points or by message content: Ditto
16	Detail packet format specification for all traffic on this datalink: ditto

IV: Plant Automation

The improvement in the plant operation from BWR to ABWR is that "Plant Automation". In BWR plant, if the plant wants to increase power, the control rod is manually withdraw by the operator to place "Control Rod Movement Switch" in "withdraw" position or manually increase the core flow. However, the "power increase" can be achieved by sending the "withdraw" demand signal to Rod Control and Information System or by sending the "increase flow" demand signal to Reactor Flow Control System from Plant Generation and Control System" (PGCS) in ABWR plant.

Three phases of PGCS system are normal plant startup, power range operation, and plant shutdown. The PGCS has the pre-defined sequences for three phases. To achieve the plant automation, PGCS look like the sequence controller. That is, PGCS will send the control demand to the system level controller to perform the specific task, such as Turbine Controller to open the control valves, after the sequence is completed, then PGCS send another command to perform the another task.

In order to support the plant automation, all I&C systems should exchange the data through gateway correctly and should work proper function. Therefore, the post-construction test of datalink is very important.

V: 161KV energization and Site test of DCIS

Before the DCIS Equipment shipped to site, the equipment has performed extensive testing in the factory. (1) Module Test. (2) Integration Test (3) Validation Test (4) DCIS Factory Acceptance Test (FAT). Then, DCIS equipment was/is shipped to Taiwan for installation and perform site test. Taipower is response for installation and site test. Due to complexity of the DCIS system, Taipower has setup the site test plan. [4] There are two parts in the site plan, one is initial DCIS architecture setup and the other part is site test program. The test program is written according to Reg. Guide 1.68, IEEE 7-4.3.2, recommendation by manufactures and the experience learned from previous I&C upgrade projects.

V.1: Initial DCIS Architecture Setup

Basically, the backbone of Invensys HPS system is Ethernet type network. Some stations can be connected to the backbone later. Firstly, network switches and at least two Visual Display Units for MMI should be installed. RMU Cabinets, Control Processor Cabinets which related to the 161KV Energization should be installed and the Application Workstations which host the Control Processor should be installed. After the equipment installed, the interconnection cables and field cables, which connected from switchgear to RMU cabinets, can be installed, tested and terminated.

V.2: Site Test Program.

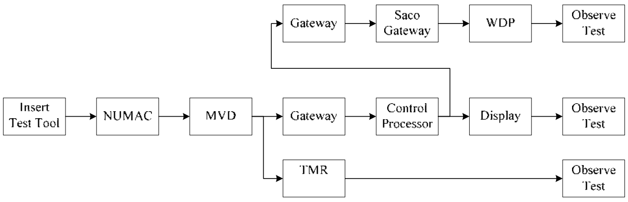
Before the cabinets energized, the insulation test of incoming power terminal should be perform and voltage and frequency of each cabinet power feed should be verified within specification. To prevent the inappropriate power to damage the electronic cards in the cabinet, the cards may be removed. Then, energize cabinets and insert the card modules. After power on, each station loads software, if need, and perform self diagnostic to check the cable and all the equipment of DCIS function properly.

Perform the input signal path check (I/O check) by changing the value at the sensor side or at RMU terminal and verify the proper response, i.e. status, engineer value, at any VDU. The output path check is to key in the value in the VDU and verify the proper response on the terminal or on the final element.

The other test is related to the redundant tests, which include the dual power supply check, dual network check, dual control processor check. The method of these types test is to setup the close control loop environment, and disable one component and to verify the process parameter in the VDUs does not change.

Once the various DCIS interface cabinets are set up, the data links must be verified. Some times, the signal will be delivered to many devices. For example, figure 11 show the data path from GE NUMAC system to the WDP, TMR system and Invensys MMI display. Before testing, the data propagation path between among manufactures should be understood, and make the data path checkpoint table to record the data. The test method is to simulate the "Known Test Input" from the input of the NUMAC chassis, then verify the test output signal at the WDP, at any one Flat Display on MCC, and at the TMR panel.

Figure 11: The data path from GE NUMAC system to the WDP, TMR systems and Invensys MMI display



VI: Test tool for improving site test schedule

The FSIM Test Bed (FSIM) is the product of Invensys Company, and is purchased by Taipower to perform the after-modification logic test for improving the site test schedule. If the system is not function properly in logic during the pre-operation test, the software-related logic must be check, modified and after-modification retest. It can be done in the Invensys HPS System or in the offline FSIM. Taipower choose the FSIM to perform the offline test. Then, after the logic is confirmed in FSIM, the control database re-import to the Invensys HPS System to perform the pre-operation test. The benefits we gain by using FSIM to test the logic are (1) Easier to setup the Test Environment, (2) Easier to setup the test input (3) No plant equipment damaged during the confirmation test. In addition, the fiber optical cable tester, network diagnostic tool and Fiber Optical Time Domain Reflectometer (OTDR), are the important instruments to solve problem and measure the characteristics of the fiber optical cable and network.

VII: Lessons learned from FAT and Conclusions.

It is the first large scale of DCIS system implemented in ABWR plant. There is no similar experience for us to learn or follow, especial in the DCIS Site Test. However, some lessons can be learned based on DCIS Factory Acceptance Test. Datalink Test will be discussed first. A segmented DCIS Factory Acceptance Test is performed at the Invensys, GE, and DRS Company. The datalinks between two platforms are tested by overlap method, or by interface-software simulator. However, the actual data propagation path is much complex than the test environment. The number of datalink I/O is around 40,000 point. To perform end-to-end test of datalink I/O, which discussed in section IV, will need a lot of man-power and time consuming. In order to complete the site test in time, datalink I/O test strategy, which including sample check criteria setup, or seeking the semi-auto datalink test tool is undergoing. Secondly, during the system pre-operation test, most of important control system, such as Feedwater Control system, Reactor Flow Control System, can not perform the close loop test due to no steam in the reactor. The test equipment with plant model may be setup, and hook to the control system to performed close loop test. The plant automation system need all datalink work properly as well as all I&C system work properly too.

The DCIS in LMNPS is complex, large scale, and full integrated system. It is a big challenge for all parties, which include I&C designer, manufacture, install-contractor, Regulatory Authority, and Taipower, to successful integrate multi-vender's device together and function properly during installation, site-test, system pre-operation, and plant startup phase. Now, the test method for "Data Propagation Test" and "Plant Automation Test " need tune to short the site test schedule. Taipower still need all DCIS participators work together to discuss the test tool, test method which will help the schedule improvement, and to solve the deviations from design specification during install and test phase.

ACKNOWLEDGMENTS

Thanks for all the DCIS participators, including GE, Invensys, and DRS to provide the valuable documentations to Taipower for performing installation, site test and future maintenance. Above documentations is the major guidance to write this paper. It is also grateful for the comments and suggestions from Hwai-Chiung Hsu of Superintendent of Lungmen Nuclear Power Plant.

REFERENCES

[1] "Lungmen DCIS Data Flow Response Time, Network Data Link Volume and Loading Analysis", General Electric Nuclear Energy, 2003

[2] C. F. Chuang and H. P. Chou, "Potential Issues on Data Communication Systems in Lungmen Nuclear Power Project", Nuclear regulation Division, Atomic Energy Council, Taiwan, ROC, 2005.

[3] "PERFORM Net DESCRIPTION FOR PLuS 32 PLANT CONTROL SYSTEM", EATON CORPORATION, 2001

[4] "DCIS Site Test Plant for Lungmen Nuclear Power Plant", Lungmen Nuclear Power Plant, 2003

[5] "DCIS Architecture and Network of LMNPS Advance Boiling Water Reactor Technology" Lungmen Nuclear Power Plant, 2005