出國報告（出國類別：考察）

核能電廠儀電設備老化更新實務經驗

服務機關：台灣電力公司核能發電處

姓名職稱：楊文龍　儀電組長

派赴國家：德國

出國期間：98.10.22～98.10.31

報告日期：98.12.23

行政院及所屬各機關出國報告提要

出國報告名稱：核能電廠儀電設備老化更新實務經驗

頁數 33 含附件：□是■否

出國計畫主辦機關/聯絡人/電話

台灣電力公司/陳德隆/(02) 2366-7685

出國人員姓名/服務機關/單位/職稱/電話:

楊文龍/台灣電力公司/核能發電處/儀電組長/(02) 2366-7061

出國類別：■1 考察□2 進修□3 研究□4 實習 5□其他(洽公)

出國期間：98.10.22～98.10.31　　出國地區：德國 法蘭克福

報告日期：98.12.23

分類號/目

關鍵詞：AREVA NP　SWV&V　TELEPERM　儀電老化更新

內容摘要：(二百至三百字)

一、AREVA NP 公司概況

AREVA 企業集團在法國核能工業的發展過程中居於領導的重要地位，基於全球化發展的策略，其旗下組織依業務範圍涵蓋能源燃料、建造、發電、維護等以至輸配電系統的綜合國際能源企業。

二、TELEPERM 儀控系統介紹

可分為安全系統(Safety)、安全相關系統(Safety Related)及非安全相關系統(Non-safety)，使當安全控制系統失效時，亦可透過安全相關系統來啟動安全相關設備，使核電廠的安全功能防禦度仍然有效維持。

三、考察 AREVA 公司儀電系統組件老化管理機制

選定相關組件/結構、系統，分析其失效狀況以及對安全可用性的影響，由運轉的行為、偵測，以判定老化狀況。

四、Oconee 核電廠 RPS 數位化更新計畫

AREVA 規範 Oconee 核電廠軟體 V&V 方案(ONS SVVP)。包括：審查、驗證軟體之需求追蹤與分析，以提供系統與軟體的需求之正確、精準可追溯性以及可測試的保證。並建制安全有關軟體確認與驗證(V&V)的準則。

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

目　　次

頁次

壹、出國目的 4

一、緣由 4

二、計畫目標 5

貳、公務的過程與內容 6

一、出國過程 6

二、公務內容 7

(一) AREVA NP 公司概況 7

(二) TELEPERM 儀控系統 10

(三) AREVA 公司儀電系統老化管理機制 17

(四)安全有關軟體確認與驗證(V&V) 23

(五) Oconee 核電廠 RPS 數位化更新計畫 26

參、出國期間所遭遇之困難與特殊事項 29

肆、國外公務之心得與感想 30

伍、對本公司之建議事項 32

壹、出國目的

一、緣由

台電公司三個核能電廠已運轉近 30 年，儀電設備都逐漸出現老化的現象，而且公司又積極推動延役與提升功率的策略，在諸多因素的考量之下，儀電設備的老化防制及更新計畫已是刻不容緩，但其規劃與系統整合的經驗依然不足。如關鍵儀控系統數位化、重要電氣設備(如發電機、大型變壓器等)的更新、各種先進線上偵測系統的應用、重要維護技術的開發等，皆是整個設備更新與可靠性提升方案的關鍵項目。主管處須主動赴歐美日等先進國家瞭解其核電廠現代化的策略與經驗，進而回饋給各核電廠，以精進營運業務，才可落實對核電廠監督與協助的責任。

西歐國家的工業技術精緻而多樣化，其研發能力與創意之豐富一向視爲業界的楷模，而德國的科技又爲其中的翹楚，德國工業產品的品質與性能之優舉世聞名，尤其尖端科技甚多值得我國學習之處。

AREVA 公司爲國際知名的核能電業集團，其多角化企業營運項目，涵蓋核燃料供應、設計、製造、維護、運轉、改善 等領域。而其中儀電系統則源自德國西門子電器公司，西門子公司的儀電產品品質與技術爲世所推崇。考察 AREVA NP 公司相關核能發電設備的維護、運轉的制度與策略，必能有助於我方的營運參考。

二、計畫目標

核電廠儀電設施的現代化於歐美先進國家已有相當經驗，設備更新策略如關鍵儀控系統數位化、重要電氣設備(如發電機、大型變壓器等)的更新、各種先進線上偵測系統的應用等，皆是機組現代化方案的關鍵項目。而 AREVA/西門子公司已累積豐富的儀電實務經驗，考察其儀電系統設計與更新機制，以資借鏡，期以提昇核電廠營運績效。

而本出國計畫的目的，即赴德國 AREVA NP 公司考察德國儀電設備老化更新的經驗以及核能電廠儀控數位化的方案與實務經驗，尤其儀控設備數位化爲目前各核能電廠配合延役所必須推動的策略，其相關法規的引用、軟體驗證與確認(V & V)程序等必須參考國外先進廠家的技術與經驗；尤其美國 Oconee 核電廠擬採用 AREVA TELEPERM XS 數位控制平台，其與 NRC 對此數位平台的討論議題更是值得我們深入去瞭解，以爲國內安全數位儀控更新的參考。

貳、公務的過程與內容

一、出國過程

(一)98 年 10 月 22 日～98 年 10 月 23 日

往程　(台北 → 德國 法蘭克福)

(二)98 年 10 月 24 日～98 年 10 月 29 日

法蘭克福　AREVA NP GmbH

參訪 Erlangen AREVA I&C Test Bay

(三) 98 年 10 月 30 日～98 年 10 月 31 日

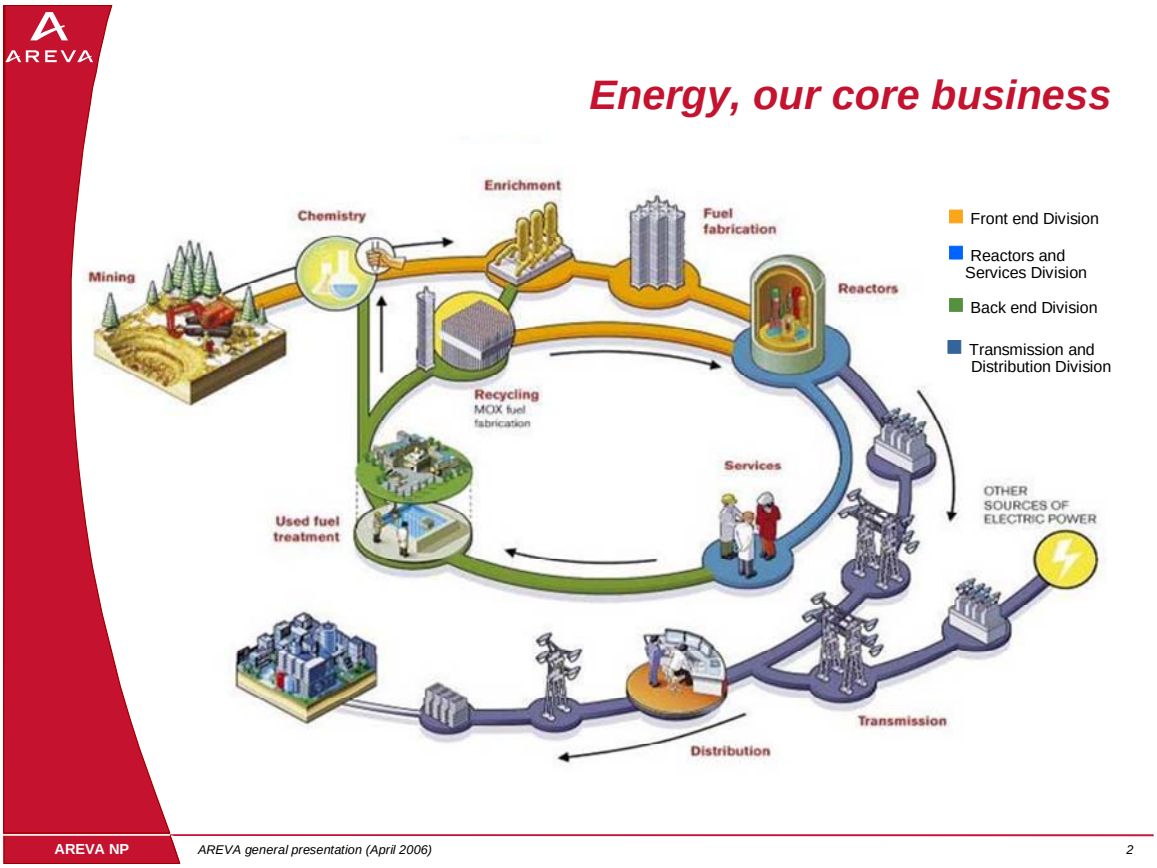
返程　(德國 法蘭克福→台北)

二、公務內容

本次出國的主要公務內容是考察德國 AREVA NP 公司核能電廠儀電設備老化更新以及儀控系統數位化的相關改善經驗，並瞭解美國 Oconee 核電廠對數位儀控軟體 V&V 所建制的審查體系。AREVA 公司一向重視台電人員的參訪，本人與多位 AREVA NP 公司儀電部門的主管進行考察主題的深入討論，洽談內容如下：AREVA 人員先行詳細介紹其公司的營業體系，以加深訪客對該公司的認識，期強化對 AREVA 系統的信賴度。

(一) AREVA NP 公司概況

AREVA 企業集團在法國核能工業的發展過程中居於領導的重要地位，基於全球化發展的策略，AREVA 集團與歐美相關同業進行策略聯盟的合併後，其總部設於法國巴黎，其旗下組織依業務範圍分爲 AREVA NC、AREVA NP、AREVA TA 及 AREVA T&D 等部門，涵蓋能源與輸配電系統的相關業務，如下圖所示：



1.核能發電前端(Front end division)部份：

①鈾礦開採　AREVA NC

②鈾原料化學提煉 AREVA NC

③鈾濃縮處理 AREVA NC

④鈾燃料製造 AREVA NP

2.核子反應器製造與技術服務(Reactors & Services division)

①核能電廠設計、建造、起動、運轉、設備改善　AREVA NP

②核能電廠關鍵設備製造　AREVA NP

③核能設施維修與改善　AREVA NP

④核能量測　AREVA NC

⑤資訊管理與服務　AREVA NC

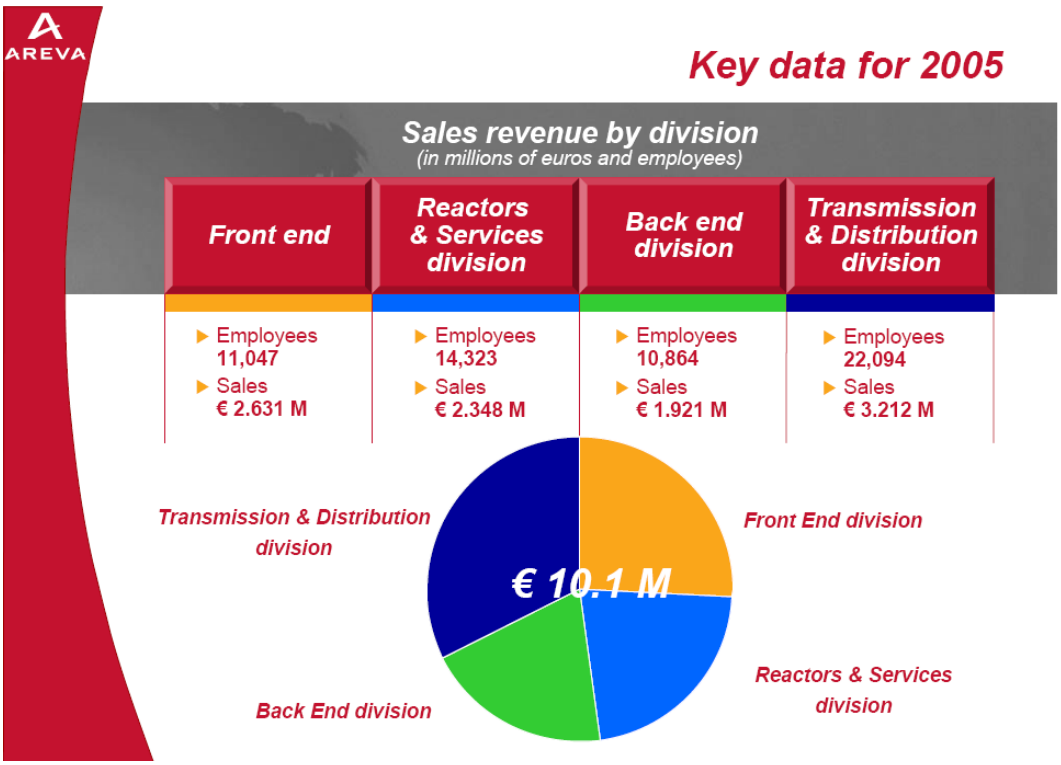
⑥核子潛艇與航空母艦反應器設計與生產、維護　AREVA TA

3.核能發電後端營運 (Back end division)　AREVA NC

4.輸配電業務(Transmission & Distribution division)

AREVA T&D

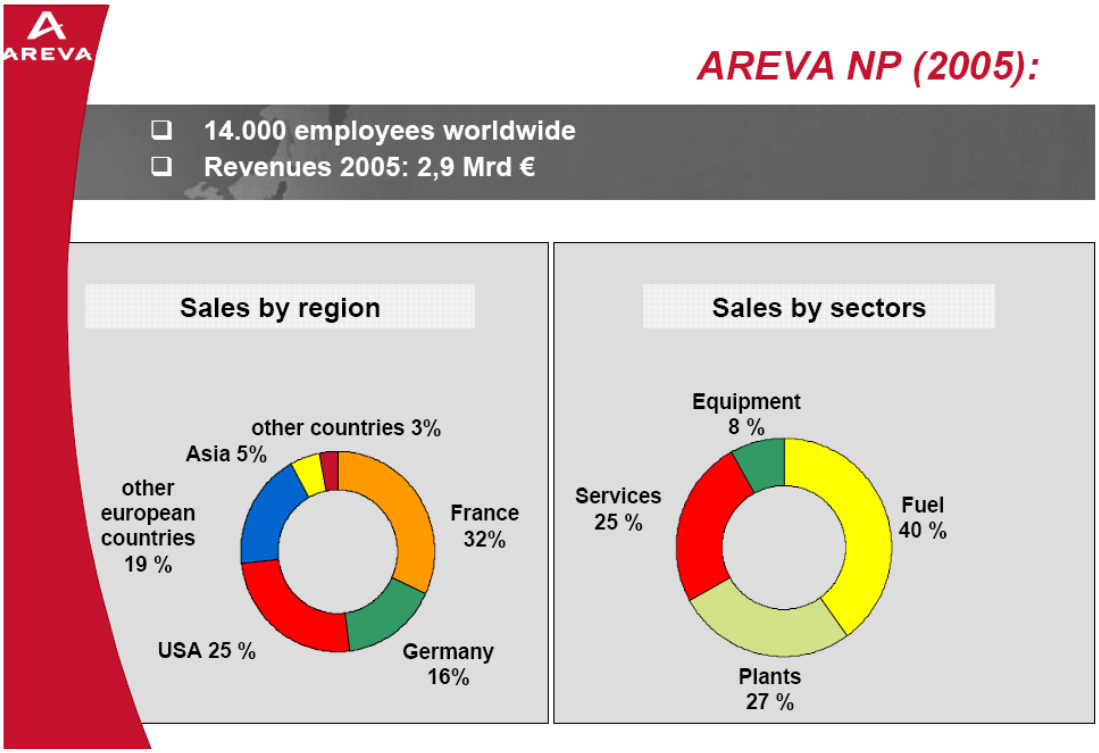
而各部門的年營業額比例，參考如下圖所示：



由上述 AREVA 公司的組織與業務分工，可瞭解 AREVA NP 主要業務在於核能電廠反應器的設計與製造、技術服務、核能儀控系統製造、現代化的維修服務及燃料元件的製造、改善電廠發電績效與核電廠現代化等尖端科技的提供與服務，其業務與本公司目前核能電廠的營運改善實有相當的關連性。

AREVA NP 由 AREVA 和 SIEMENS 合組的公司，爲 AREVA 旗下的一家以核能設計、服務爲主的公司，其前身爲 FRAMATOME ANP；FRAMATOME 負責核島部份，SIEMENS 則負責儀控部份。AREVA NP 的核能企業網遍佈全球，在世界各地的工程、製造、維修服務及分公司，是一個跨國的核能工業集團。而其在德國境內的重要部門據點及員工人數如下：

AREVA NP 的經營地區別及營業項目的比例，如下圖所示，地區性仍以歐美爲主，但近年來中國大陸則是其相當重視的新興市場。而營業項目以核能燃料生產與供應爲最大比例約 40%，核能電廠的工程建造及維修均約佔 1/4。



原來 AREVA NP 公司的經營策略是以對歐洲核能電廠提供營運、改善、規劃爲主，但近十年來由於核能工業的不景氣，才轉而向亞洲其他地區開展市場的開發。兩年來，世界核能發電業有明顯“復興”的跡象，乃更積極將其觸角伸向世界各地，尤其亞洲地區。

(二)TELEPERM 儀控系統

1. AREVA NP 公司數位儀控系統源自 SIEMENS POWER GENERATION 之 SPPA-T2000(即 TELEPERM XP)，再經 AREVA NP Erlangen Office 研發部門之 Test Bay 測試驗證，而提昇爲 TELEPERM XS：

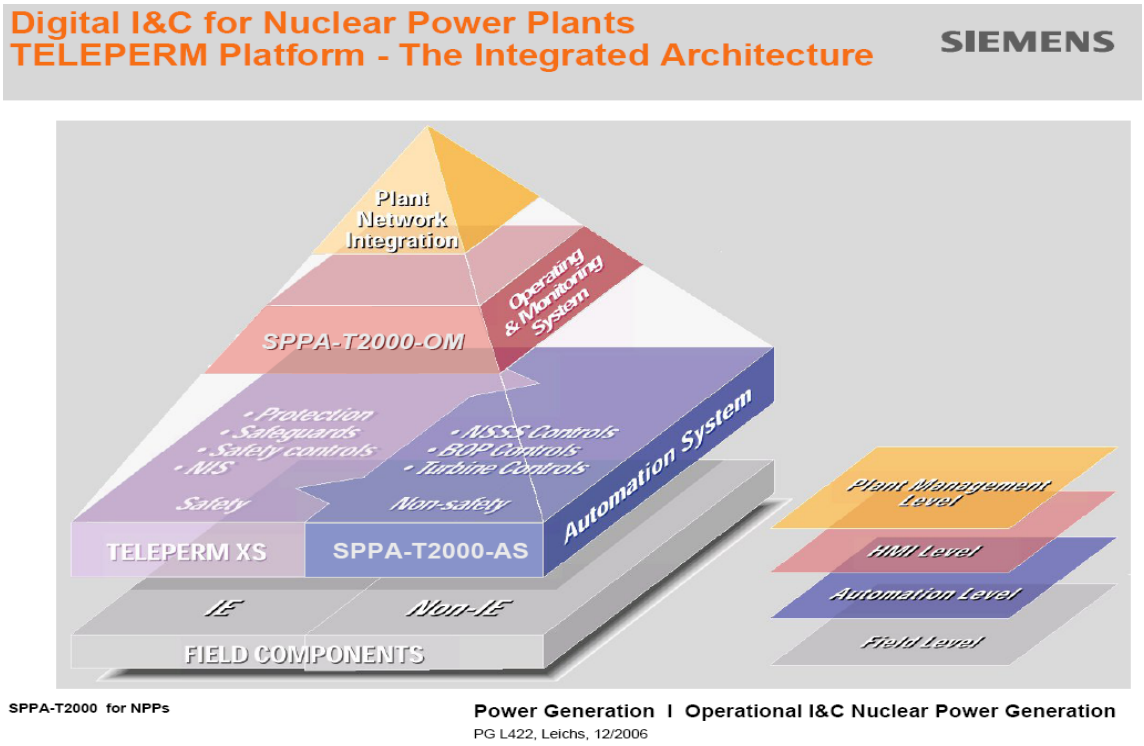
①TELEPERM XS 用於安全相關儀控系統

②TELEPERM XP 用於一般非安全之儀控系統

以上兩者以 Gateway 隔離而合併應用於核能電廠，可降低維修人力、操作便利，可用性高，而使電廠的控制功能更爲靈活，提昇運轉的可靠度。除大量採用於新建核能電廠中，對現有類比儀控系統的數位化更新有相當高的相容性。

2. TELEPERM (XP/XS)系統的整合平台機制，TELEPERM XS 用於較

高階的安全儀控系統，而在系統現代化(Modernization)的計畫中，與其他較低階安全或非安全相關系統之間，可以 TELEPERM XS 建立界面將其整合， 如下示意圖 ：



註：SPPA-T2000 即 TELEPERM XP 之新型號

TELEPERM XP 系統主要設計應用於不需核能認證的核能電廠非安全相關儀控系統，主要包括下列子系統：

① ES 680 工程設計系統

② OM 690 程序控制及監測系統

③ DS 670 自動診斷系統

④ AS 620 自動化系統

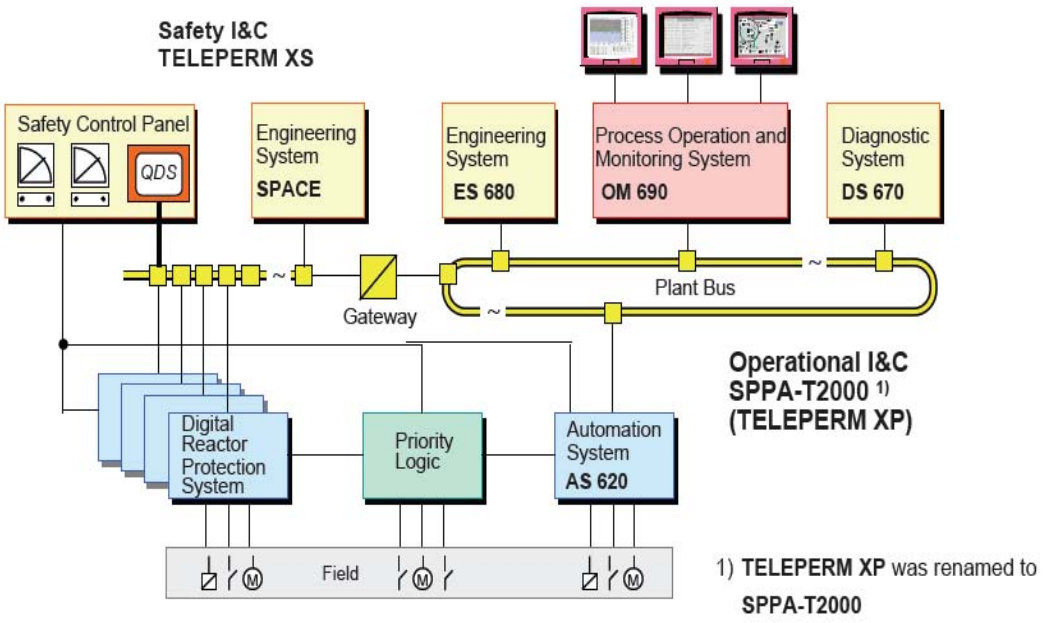
⑤ 廠內網路匯流排(Plant Bus)

TELEPERM XS 系統主要設計應用於多重性、多樣性且需核能認證的核能電廠安全相關儀控系統，對事故後圍阻體完整性及放射性物質外洩至週遭環境的防範功能的絕對可靠性要求極高；其採完全分散式控制，在任何層次皆有多重數位控制系統。

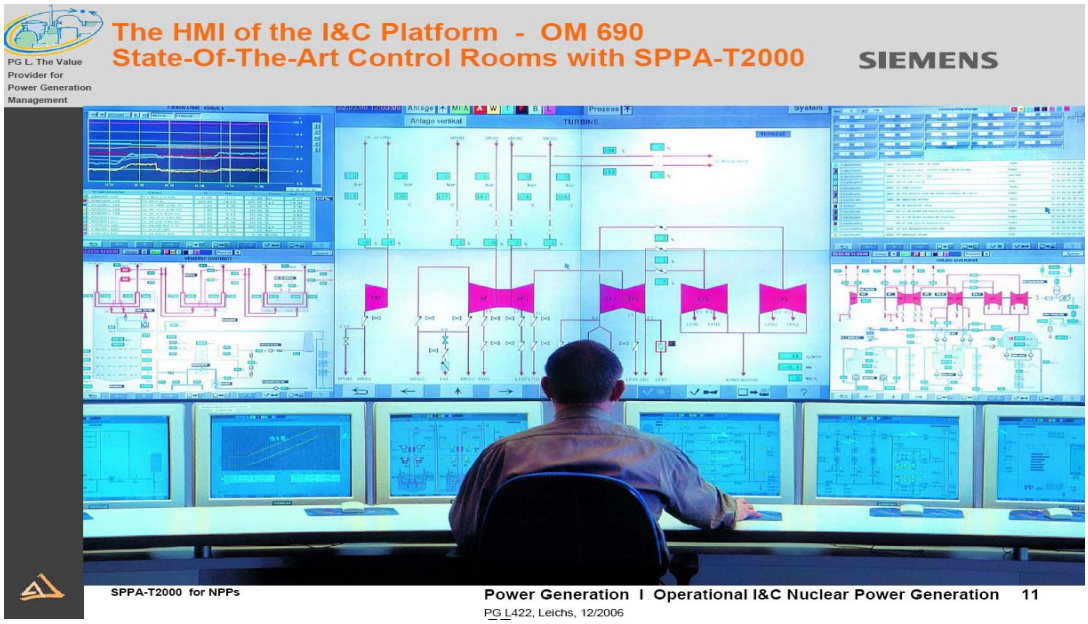
AREVA TELEPERM 控制系統應用於核能電廠儀控系統，可

分爲安全系統(Safety)、安全相關系統(Safety Related)及非安全相關系統(Non-safety)，以引用 Priority Logic 的觀念，使當安全控制系統失效時，亦可透過安全相關系統來啓動安全相關設備，使核電廠的安全功能防禦度仍然有效維持。

以上所述 TELEPERM XP/XS 儀控系統示意圖如下：



採用 SPPA-T2000 (即 TELEPERM XP)系統之新型控制室如下圖：



3.TELEPERM XS 數位儀控系統的特色

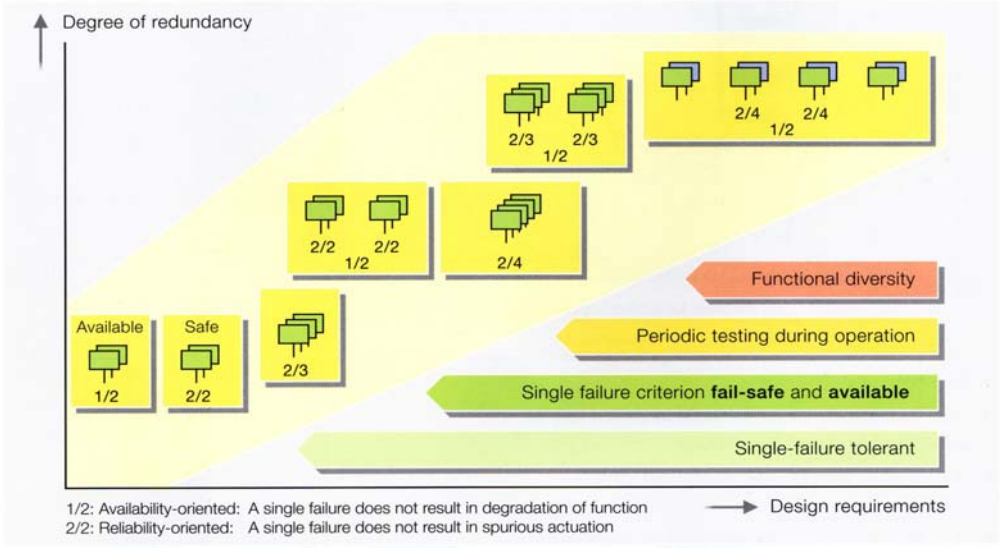
TELEPERM XS 系統的設計特點與應用是考察的主題，其引用的法規能否應用於台電核能電廠，與國際 IEC 及美國 NRC 準則是否相容，能否獲得原能會的認可，也是討論的重點

TELEPERM XS 數位儀控系統具有以下的特色：

①每一個處理器的應用軟體都有固定順序，且週期性地執行工作。

②TELEPERM XS 系統架構完全採用雙重(Redundant)設計，皆符合 IEC 61226、IEC 61513 及 IEC 60987 的標準，容許單一故障。反應器保護系統(RPS)具有最大的安全性需求，對於故障(Fault)與失效(Failure)組合的異常狀況，必須有最合理及符合電廠安全考量的判定準則，以確保電廠最高的運轉效益，在安全與可靠之間取得最佳的平衡點。如包括單一故障及維護、單一故障與火災、外在事故(如飛機撞擊、地震)。以上考量導致須有實質隔離、電氣隔離、獨立子系統設計的雙重(Redundant)系統。

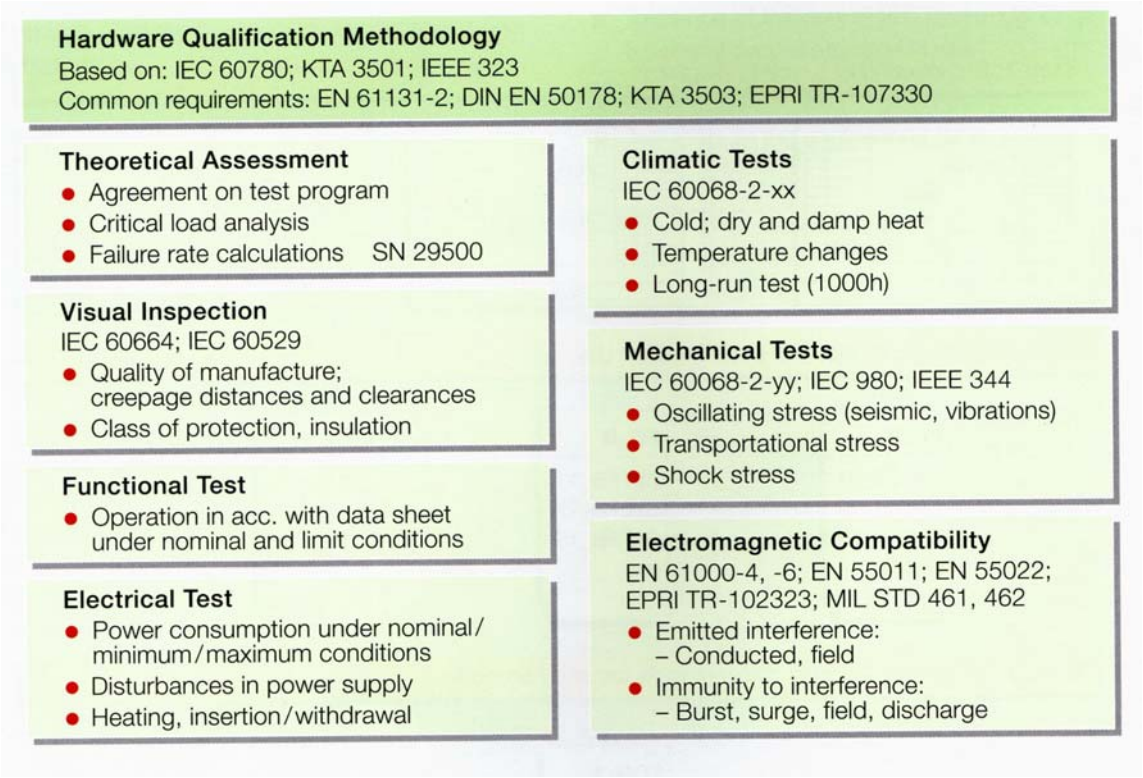
而 TELEPERM XS 系統利用電腦擷取各項系統數位信號，建立符合需求的邏輯串，以防範單一或更多感測器(Sensor)失效導致誤跳脫。可根據設計的需求，而建立下圖的多重保護邏輯。



Design requirements and associated architectures.

③TELEPERM XS 系統以 IEC 60780、IEEE 323 以及 KTA 3503 作爲

硬體驗證的標準。如下表所示：



④TELEPERM XS 系統應用軟體的發展都經過嚴謹的 V & V 程序，符合 IEC 60880 標準的要求。

⑤TELEPERM XS 系統設計具有未來擴充能力。

⑥TELEPERM XS 系統的硬體設計可耐強震及抗電磁輻射的功能。

⑦TELEPERM XS 系統爲第一套經美國 NRC 以新法規 NUREG-0800 認證爲適用於核能電廠安全數位儀控的系統。

⑧TELEPERM XS 系統具有早期偵錯、失效隔離、防範事故擴大及不同安全系統鑑別優先處理順序的功能。

⑨TELEPERM XS 系統應用於核能電廠的安全相關系統，如反應爐控制系統、反應爐保護系統(RPS)、控制棒位偵測系統、核能安全設施引動系統(ESFAS)、中子偵測系統、輻射偵測系統、緊急柴油發電機系統等。

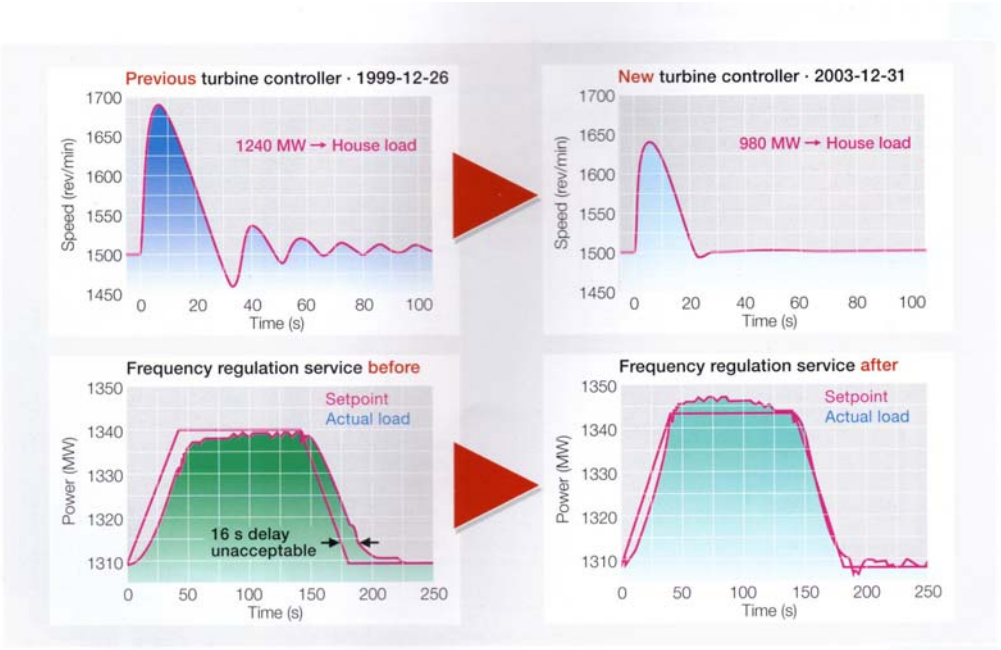
■TELEPERM XS 系統相關品質認證標準：

①供應商資格安全有關品管評估，依據 KTA 1401、IAEA 50-C/SG-Q、ANSI/ASMW NQA-1 。

②安全有關技術評估由供應商之 FANP 技術單位執行評估認可。

③品管系統符合國際性法規與標準，如 ISO 9001(2000)、IAEA 50-C/SG-Q (1996)、ISO 14001 (2004)等；另符合各國家核能法規與標準，如 10 CFR 50 App.B/NQA1 (1983)美國、KTA 1401(1996) 德國、Arrete Qualite(1984)法國。

■TELEPERM XS 系統係適用於大範圍的系統架構，以及因應強力電腦功能和通訊元件需求而開發設計的系統。但其運用於非安全有關系統，亦能提供高層次的可靠度和績效，尤其重要的是縮短暫態反應時間。如下汽機功率輸出與頻率(轉速)於修改前後的比較圖。



Increase in control quality thanks to new TELEPERM XS turbine controller:
Load rejection to house load and frequency regulation service before and after.

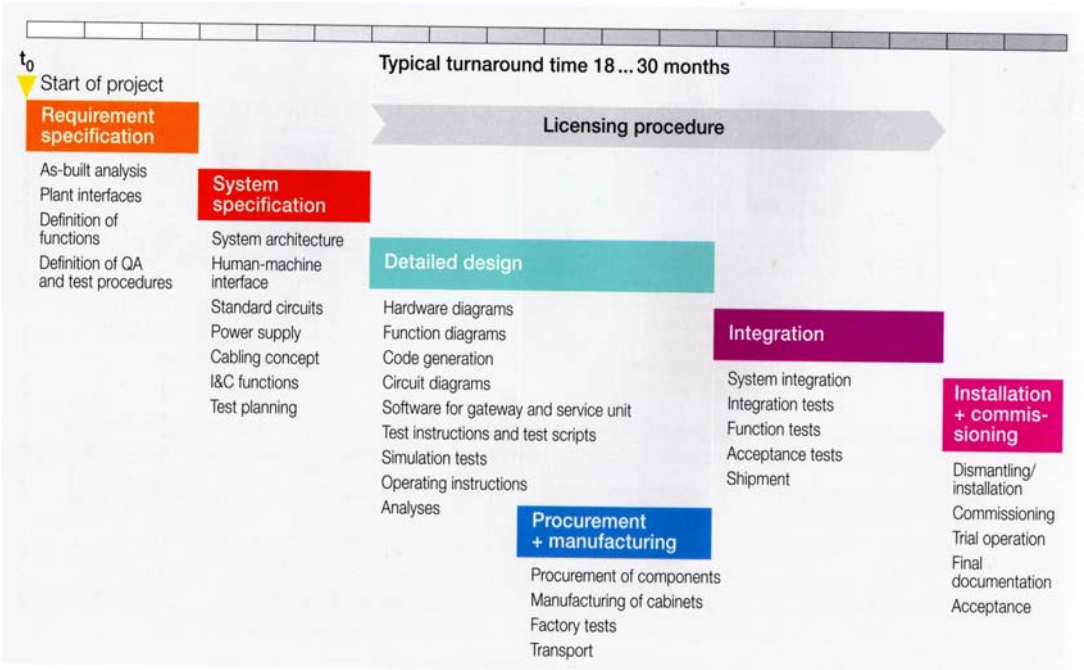
4. TELEPERM XS 數位儀控系統的計畫執行時程與重點

數位安全儀控計畫的策略是以執行時間交錯(Time-staggered Phases)的階段方式推動，各階段期間的執行重點如下圖所示，

其中計畫之始，需求規範(Requirement Specification)與系統規範(System Specification)須儘早確定，而據以建立高品質的系統程序書與基本資料庫。在詳細設計(Detailed Design)階段確定硬體的詳細規範並開始採購作業;同時相關的軟體在稍早階段已以模擬器測試過。而詳細的執照審核程序開始準備，嚴格的構型管理(Configuration Management)與程序書變更在本階段後期才開始進行。硬體與軟體的整合(Integration)在 AREVA Test Bay 驗證完成後才運出設備。程序書必須符合相關安全儀控技術標準，並構成整個計畫的主要成份與基礎。執照程序書在每一狀況，都須編寫成符合國家與顧客的需求。

依照以上各階段的執行模式以確保失誤及改正均已及早確認並避免造成系統潛在的陷阱，以保證此數位安全系統運轉上的高品質。

根據廠家經驗，整個計畫從開始規畫到安裝及相關文件允收完成，約需 18---30 個月；從得標後開始 Basic Design Phase 至 FAT 完成，約需 20 個月。對電廠即將進行的安全數位改善計畫，此推動的時程，必須詳加注意。



5.安全相關電氣設備之改善案討論

相關品保及安全評估制度

①品管制度

◆通過 NUPIC 成員的稽查---由 Duke Energy 電廠率領 NUPIC 小組在 2004 年四月稽查過。

◆符合 10 CFR 50 Appendix B 要求。

◆符合 10 CFR Part 21 要求。

②工程設計方案

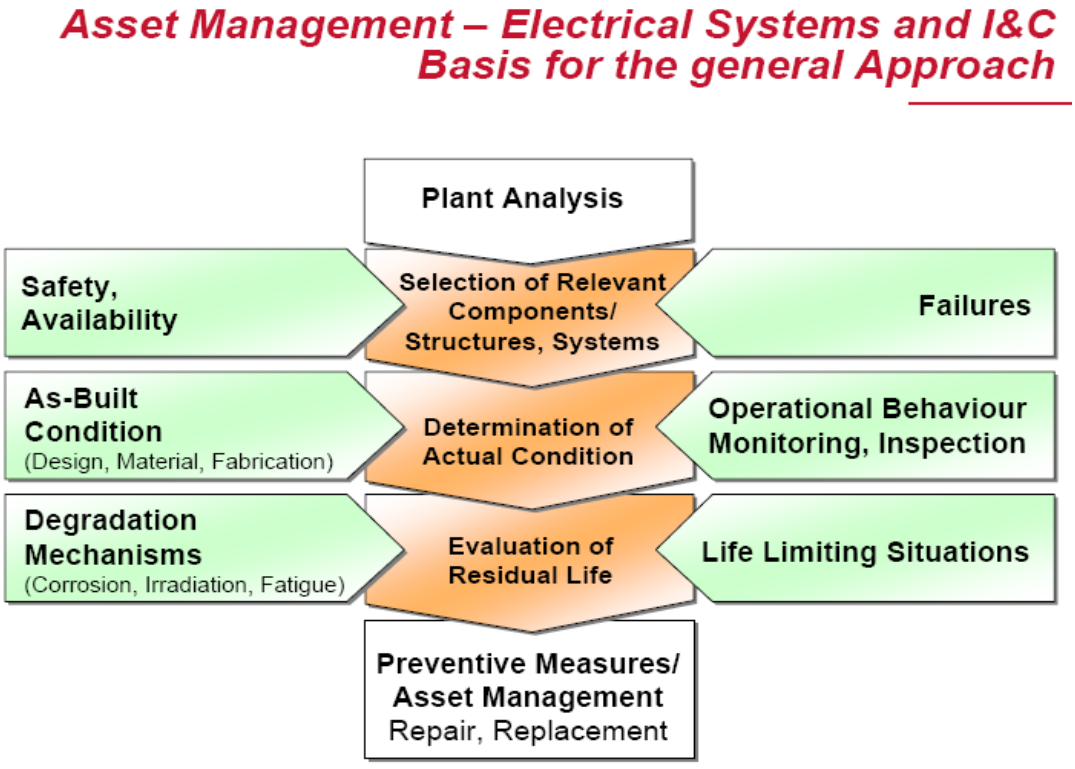
◆具有安全相關設備組件製造的品保計畫。

◆具有安全相關設備組件核能檢證品的檢證能力。

◆支援 50.59 的安全評估。

(三) AREVA 公司儀電系統老化管理機制

1. 老化管理依據的一般基本原則



①. 選定相關組件/結構，系統，分析其失效狀況以及對安全可用性的影響。

②. 由運轉的行爲、偵測與檢查觀察其改善前狀況，以判定其實際現況。

③. 應用壽命極限的情況瞭解其其劣化的機制，而評估其殘餘壽命。

④. 訂定預防維護/老化管理方案，採取修理或更換策略。

一般老化管理的方案，重點在於:

◆判定環境條件以爲建立老化管理的方案的基礎。

◆應用自動殘餘壽命評估資料庫(AUREST-Database)持續評鑑嚴酷環境的老化管理方案。

2. 系統、組件的一般分類

①. Cat. 1, Replacement judged to be necessary(要更換)
(預估殘存壽命近於零)

②. Cat. 2, Decision (replacement or not) requires additional analyses (參考廠家意見，需要另外分析)

③. Cat. 3, Components / systems judged to be able to operate during the extended operation time(可延續運轉一段時間)

④. Cat. 4 replacement (s) or repair(s) necessary, but for normal maintenance. (適用正常維護，需要更新或修理)

3. 就 Cat. 2 必須考慮的重要因素(適用於主動裝置與被動裝置)

①. 分析、考慮成本效益比

②. 更換的順序與時機考慮已計畫的大修時程或其他時間。

③. 硬體成本與人員規畫及執行更換的成本

④. 可能延長大修造成額外經濟的損失

4. 可能須更新的系統與組件

①. Transformers

②. Switchgears

③. Protective Relays

④. Battery Chargers

⑤. Batteries

⑥. Inverters

⑦. EDG & Controls

⑧. Cabling(Harsh、Mild)

⑨. Drives (Pumps、Fans、Valves)

⑩. Control Room

⑪. Operational I&C (Signal Processing、Automation、Drive Control)

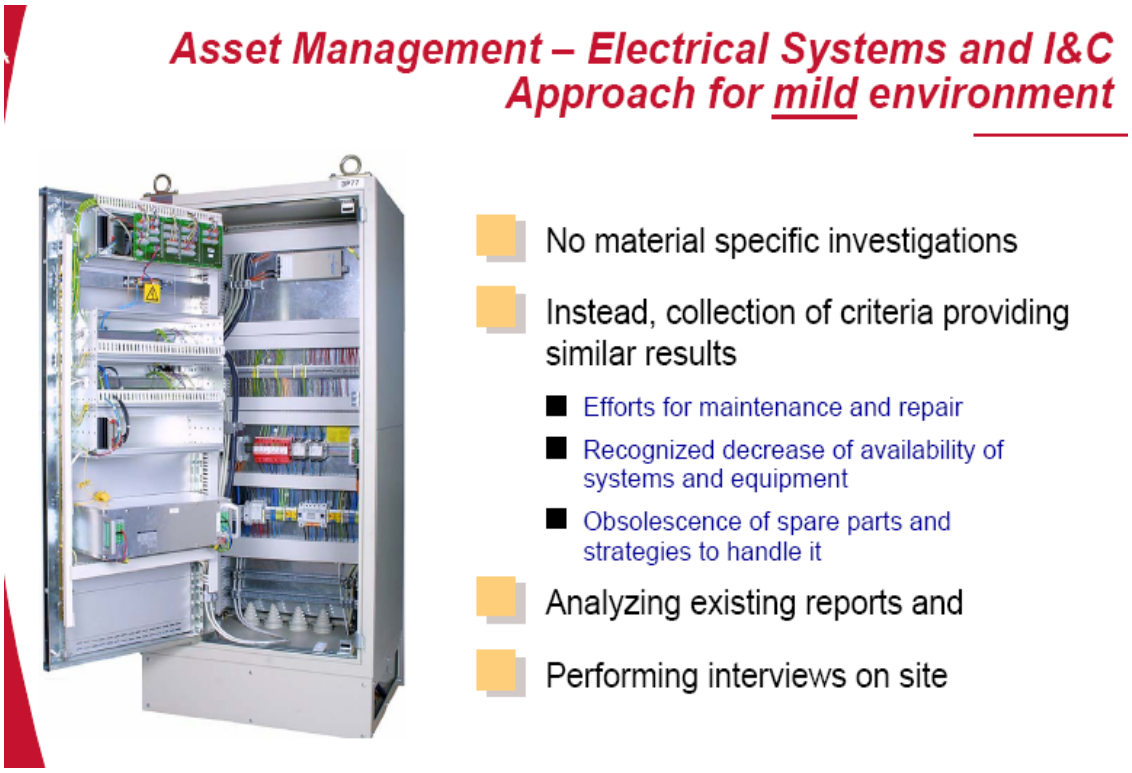
⑫. Safety I&C (RPS、ESFAS、Limitations、Priority Control

⑬. Control Valve Drives

⑭. Sensors

⑮. Transducers

5. 溫和環境(Mild Environment)評估管理



◆ 重點在不需特定的材料研究。

◆ 蒐集現行的維護準則及分析現有的報告。

6.嚴酷環境(Harsh Environment)評估管理

Asset Management – Electrical Systems and I&C Approach for harsh environment, Other Equipment

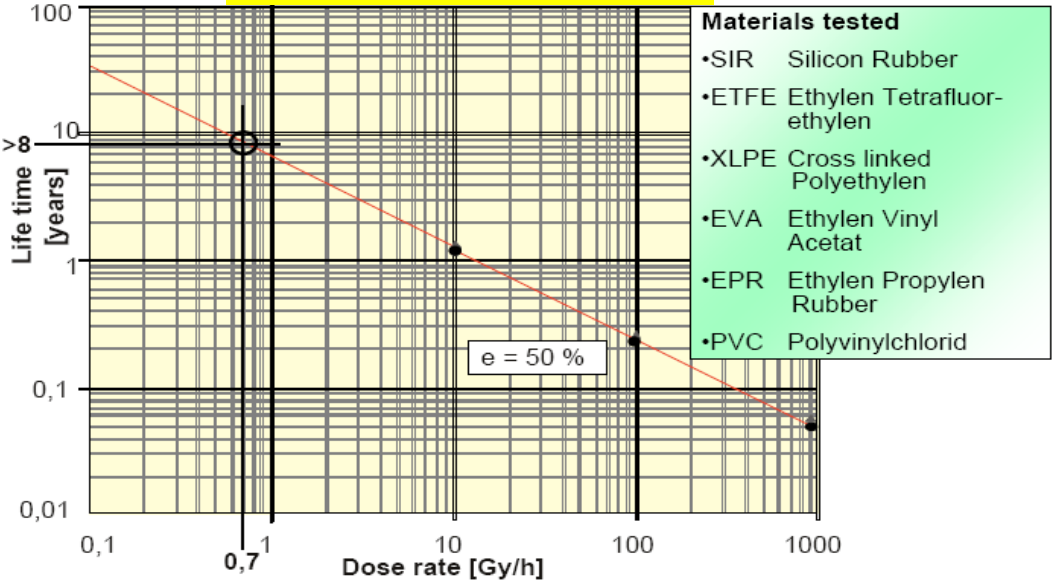
- Analyzing the qualification documents (if there are any), looking for "qualified life time" values (temperature and radiation) and
  - Activation energies (according to Arrhenius Law)
  - Dose rate effects
- Measurement of operational thermal and radiation loads for relevant locations (in parallel to cables)
- Deriving remaining qualified life time corresponding to the local operating condition

重點在於：

- ◆ 分析品質文件以確定設計壽命值。
- ◆ 於相關位置量測熱與輻射量。
- ◆ 對應於現場環境導出殘餘壽命值。

Asset Management – Electrical Systems and I&C Life Time Prediction based on Dose Rate effect

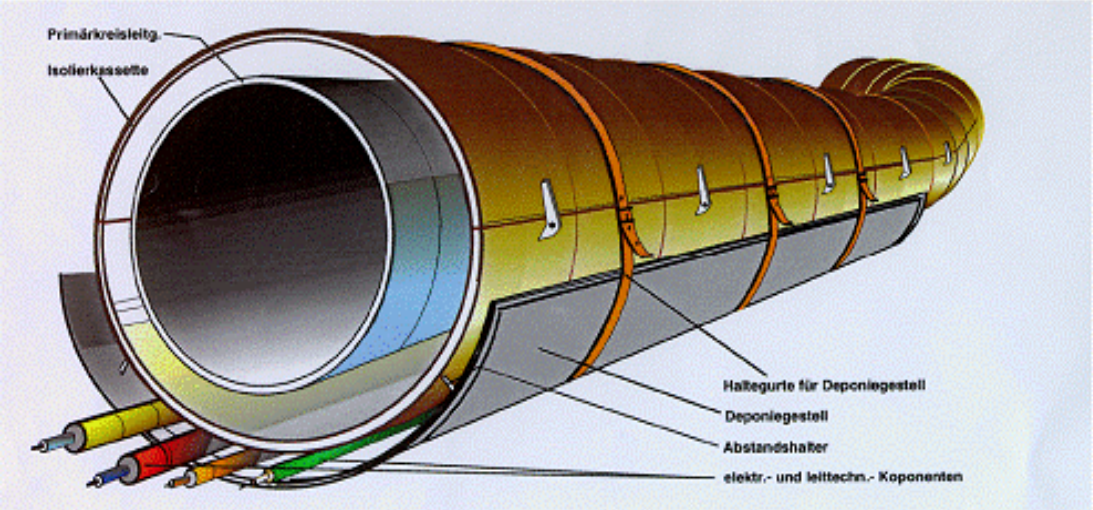
輻射劑量對電纜壽命的關係



7.試樣電纜預先建置

參考下圖的評估機制範例，如圖所示，將樣本電纜預先放置於高輻射管路旁，量取、建立劣化的變化趨勢、紀錄。藉以研判各式材料的老化期間，各項特性參數的變化趨勢，而爲新建電廠或現運轉中電廠延壽計畫評估的重要參考資料。

Cable Deposit at Primary Cooling Circuit Pipe
Principle Diagram



8.儀電設備老化評估

①設備老化評估與自動殘餘壽命計算

(Automatic Residual Time of Life Calculation，AUREST)

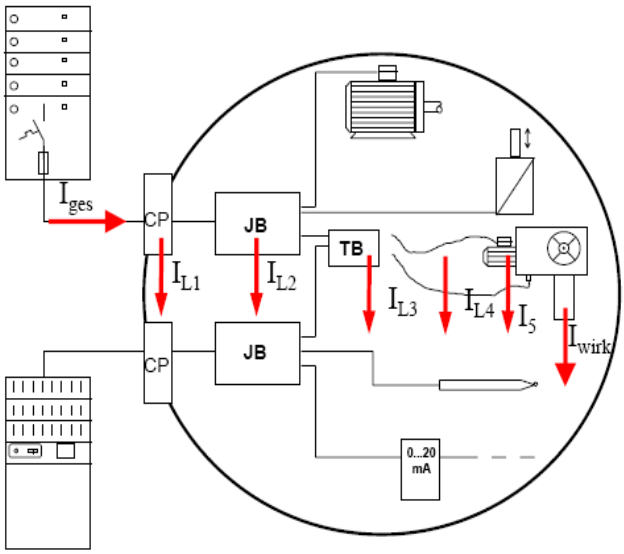
於電廠運轉開始即將相同規格電纜樣本置於同一高輻、高溫度、高振動等惡劣環境中，研判其承受溫度與輻射劑量的程度，將實驗所得數據、紀錄，以觀察實物的劣化狀況，建立自動電腦計算分析系統。以最少的人力、物力做最適的判斷，AREVA 已累積約 20 年的實驗數據與評估經驗。

②對輻射劑量效應的評估不需要過渡保守。

③訂定設備組件的的 Critical Function 及 Function Chain

界定組件受環境影響劣化的機制，建立邏輯判定的軟體系統，僅要一個電腦按鍵動作，即可以“極少量”數據的蒐集，而完成老化評估的工作。如下圖，依據 Function Chains 的觀念，依據環境惡劣程度而執行緊要功能(Critical Function)的評估，可據評估的弱點，而採取改善對策。

LOCA-Resistance of Qualified El. & I&C-Components: Typical Function Chains within Reactor Containment

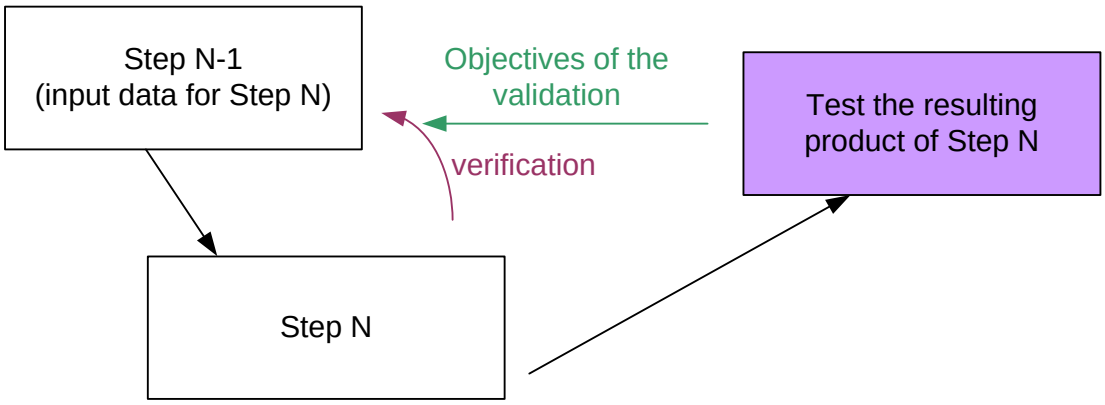


④迅速、可靠的評估特點

在歐洲與德國已有多年使用的實績，參考上圖的評估機制範例，如圖所示，將樣本電纜預先放置於高輻射管路旁，量取、建立劣化的變化趨勢、紀錄。藉以研判各式材料的老化期間，各項特性參數的變化趨勢，而爲新建電廠或現運轉中電廠延壽計畫評估的重要參考資料。

(四) 安全有關軟體確認與驗證(V&V)

1.基本 V&V 工程原理



① 任一活動(Step N)的執行係依據從前一活動(Step N-1)來的輸入信號。

② 驗證(verification)旨在確保工程的方法被正確的執行(品質建置在設計中)。

③ 驗證(verification)旨在確保工程的產品適合於預期的用途。此通常透過測試(testing)而完成。

④ 確認(validation)計畫也必須在活動執行之前予以分析與驗證。

2. Verification(驗證) and Validation(確認)

- Validation:

① “Are we building the right system?”
(我們是否建置對的系統？ “結果”考量)

②我們對問題的陳述是否精確地點到真正的問題？

③我們是否考慮到所有“賭金保管者”(stakeholders)的需要？

- Verification:

① “Are we building the system right?”

(我們是否將系統建置對？ “過程”考量)

② 我們的設計是否符合規範要求？

③ 我們的執行是否符合規範要求？

④ 此遵循的系統是否依我們的指示執行？

⑤ 我們的需求模式是否互相之間保持一致性。

3.確認與驗證(V&V)的目標

- 軟體 V&V 係決定是否符合下列要求的一種程序(IEEE 1012-1998):

①對一系統或組件完整性與正確性的需求。

②每一階段發展出的產品必須符合前一段的需求或條件。

③最終的系統或組件必須符合原設計特定的需求。

- IEEE 1012-1998 所述

①軟體 V&V 是一種系統工程的技術性紀律。

②軟體 V&V 的目的是要幫助發展組織在軟體發展的生命週期間，將品質建置在軟體內。

③V&V 程序透過軟體的生命週期提供一種軟體產品的目標評估(objective assessment)以及程序。

④此評估可驗證軟體需求是否符合正確性、完整性、準確性、一致性與可測試性。

4.軟體 V&V 的計畫與執行

爲確保將品質建置在設計之中：

①產生軟體 V&V 計畫。

②在軟體生命週期過程中，均遵循(執行)軟體 V&V 計畫。

③此程序產生結果(包括 V&V 彙整報告及終結報告)。

5.V&V 準則文件(from a top level hierarchical order)

①10 CFR 50 Appendix B

②NUREG-0800, BTP 7.14

③RG 1.168

④IEEE-1012 Standards

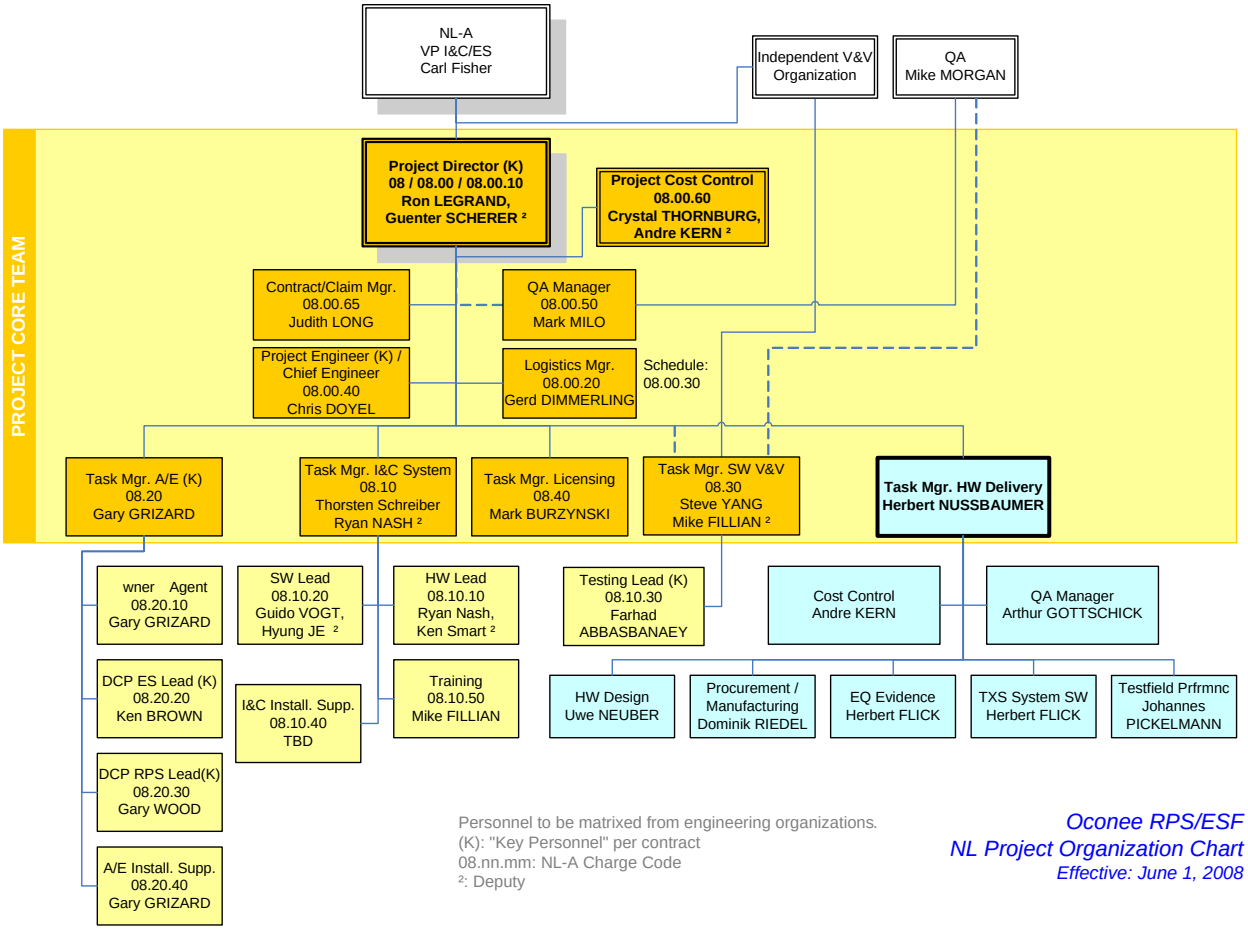
⑤Software Verification and Validation Plan

⑥Specific Procedures or Instructions

6. Regulatory Guide 1.168 and IEEE Std 1012-1998 Guidance on V&V Independence

爲在安全有關軟體及系統中獲得高信心與可靠度，V&V 團隊必須在技術上、經濟上、管理上獨立於發展組織。

(五) Oconee 核電廠 RPS 數位化更新計畫



由以上的數位化更新計畫的組織架構圖可以看出 V&V 工作小組並不隸屬於品保(QA)小組，且位階高於品保小組；其獨立於計畫核心團隊之外，且直接向計畫核心團隊的主管副總負責。而品保小組僅向團隊內的品保經理負責即可。

因此，獨立的 V&V 小組的超然地位相當重要，其獨立於一般電廠的行政體系，不受一般行政體系的拘束，才能發揮確實的查證效果。

1. V&V 程序(Processes) & 活動(Activities)

◆ (管理)Management

Activity: Management of V&V

◆ (發展)Development

① Activity: Concept Phase V&V

② Activity: Requirements Phase V&V

③ Activity: Design Phase V&V

④ Activity: Implementation Phase V&V

⑤ Activity: Test Phase V&V

⑥ Activity: Installation Phase and Checkout V&V

◆ (程序)Process: Operation and Maintenance V&V

2. V&V 工作範圍(Tasks)

① 軟體設計審查與驗證。

② 軟體的追蹤性分析。

③ 軟體評估

④ 軟體界面分析

⑤ 軟體危急度分析

⑥ 軟體確認測試

⑦ 允收試驗

⑧ 風險度分析

⑨ 安全度分析(資通安全)

⑩ V&V 報告

3. V&V 最終報告(Final Report)

V&V 最終報告提供有關在V&V成果的結論中軟體V&V計畫執行狀況的彙整， 包括如下項目：

①所有 V&V 文件的確認。

②所有生命週期 V&V 活動的彙整。

③所有 V&V 工作成果的彙整。

④所有 V&V 活動未決議題與其解決辦法的彙整。

⑤藉著 V&V 活動的審查，執行全面軟體品質的評估。

⑥有關全面發展的程序對未來核能安全有關應用軟體的計畫，從本 V&V 計畫執行中所學到的經驗/程序改善與建議。

4. AREVA NP 在 Oconee Nuclear Station (ONS) Project 的經驗

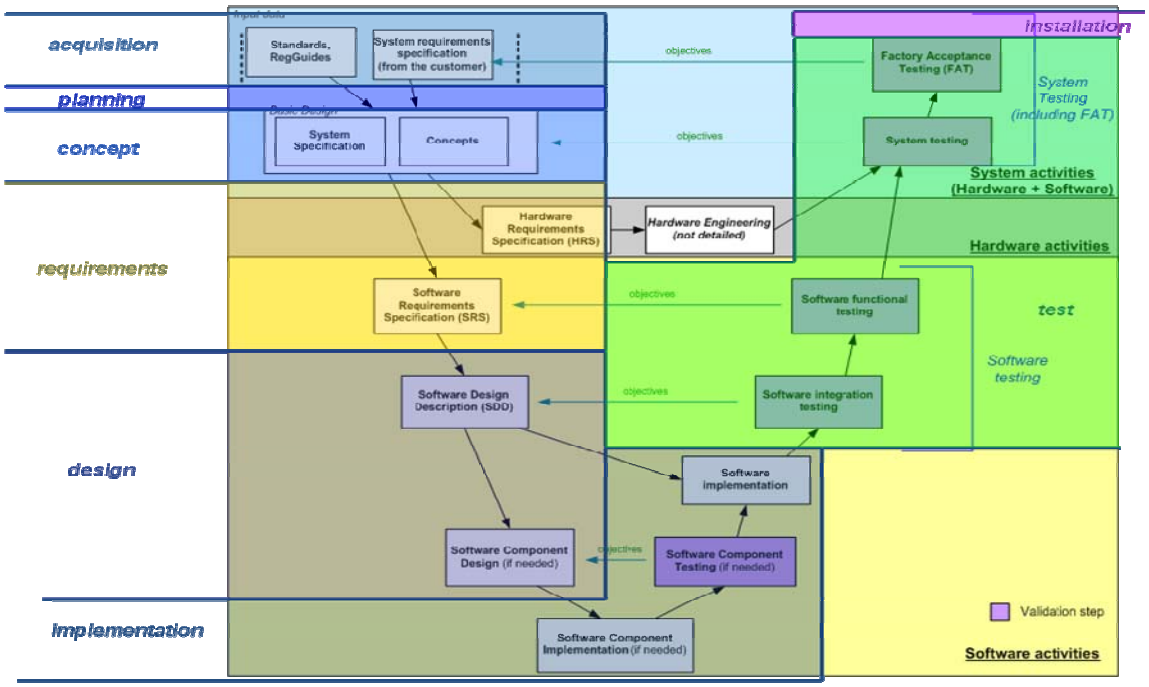
①AREVA 依 IEEE Std 1012-1998 規定，爲軟體與系統制訂了 V&V 方案。其軟體生命週期方法論的範圍、程序以及活動皆規範在 Oconee 核電廠軟體 V&V 方案(ONS SVVP)中。

② 軟體 V&V 計畫已被有效地執行.

③ 審查、驗證、法規檢視、軟體危急性分析、軟體需求追蹤與分析等提供系統與軟體的需求爲正確、精準、完整、一致性、可追溯性簽以及可測試的保證。

④ 在 Oconee 核電廠一號機 RPS/ESFAS 控制系統數位化更新計畫的成果已建立了確實保證 RPS/ESFAS 系統建置符合規範要求而且遵循 Oconee 核電廠軟體 V&V 計畫的方案落實執行。

5. The V-model – Overview of the V&V Process



由上圖示出 V&V 處理程序的概觀，可瞭解在確認(Validation)過程，可從 N-1 的項目定出步驟 N 的可追蹤性(Traceability). 一個互補性的有效範圖分析是必須的。以確保所有的初始需求在最終的產品中完全滿足。宜制定一種追蹤的模式(Model)，建制需求的追蹤性矩陣(如上圖之 V-model)，以執行需求性的追蹤。

參、出國期間所遭遇之困難與特殊事項

一、本次赴德國考察儀電設備更新技術、經驗，由於三年前來洽公過，此次已是第二次赴德國出任務。自以爲“已有經驗”，且由於不想麻煩德國朋友接送，決定自行搭乘大眾交通工具到目的地，之前雖聽朋友談過自動購票機的操作要領，但不同的交通工具有不同的購票機，且無詳細的圖文說明(英文)，除了法蘭克福週遭的捷運外，其餘車種試了半天，依然毫無頭緒，只得放棄。德國境內的交通網相當完備，各種交通工具四通八達，只要瞭解其操作規則，可花最少的車資而完成所需的旅程。

二、德國的高速公路“無速限”的傳聞，令人嚮往，而德國汽車大都性能優良，一踩油門車子往前衝，皆可迅速到 200 km/hr 速度，但每部汽車都似乎同樣高速行駛，並無預期的“快感”。事實上，德國高速公路並非皆無速限，一些路段視路況而有速限，且一旦狀況排除，該路段的電動路標即顯示“速限解除”，又可恢復高速行駛，一般而言，皆在 120 km/h 以上。

三、本次出國期間爲 10/22～10/31，在西歐已進入深秋，在四季分明的德國，到處可見楓紅落葉，在公園、路邊、市中心、鄉間，處處可見各種鮮艷的紅、黃落葉，應不是所有變色樹種全都是楓葉，對來自亞熱帶的我們而言，這景色真是令人感到驚艷。

肆、國外公務之心得與感想

一、此次出國考察擬討論的議題，已事先送給 AREVA NP 公司參考，讓其預先規畫訪談人員及討論主題；其中議題除了計畫內的儀電設備老化更新與儀控系統數位化更新的實務經驗外，尚包括目前各國內各核能電廠的發電機更新、大型電力變壓器的線上偵測技術、部份放電技術應用於變壓器的經驗、電力電纜劣化偵測參數的研判準則等。

可能由於訪談的時間不夠充裕，除了主題的儀電設備老化更新與儀控系統數位化更新實務皆約花了一天的時間詳談外，其餘皆僅能重點式的交換經驗，未能深入詳談，或答應日後提供補充資料。

此次考察原訂唔談項目或許太多，以致無法完全談論到，訪談議題數量應與時間相配合，下次宜注意之。

二、AREVA 公司相當重視本公司核電廠儀電系統數位化更新計畫，在訪談的過程中，多次詢及本公司對儀控數位化的策略，似在瞭解其對此數位化計畫過程中所扮演的角色，其多次強調在此儀控系統現代化的策略，充份顯示其強烈的企圖心。近年來，對台電/核研所的參訪人員主動安排核能電廠及儀器工廠的參訪，其目的在於加深我們對 AREVA“TELEPERM”儀控系統的瞭解，以提高我們對該系統的信心，期待該系統能進入台電核能電廠安全系統。

在本次考察行程，AREVA 公司特別安排參觀其要交給美國 Oconne 核能電廠的 TELEPERM XS 系統的測試情況，並請測試負責人詳細說明測試的程序、系統特色，安裝經驗以及未來美國 Oconne 核電廠的更新時程，並強烈說明美國管制單位 NRC 相當關切此第一次美國核電廠安全儀控系統由類比更新爲數位系統的過程而派員現場查證，美國 NRC 的態度可爲我國 AEC 的參考。

三、最近幾年來，德國核電國外市場的競爭相當激烈，各跨國大企業的合併也常耳聞；AREVA NP 爲經濟效益，爲德法合作公司，發展標準型的“歐洲型壓水式反應爐”(EPR)積極爭取海外核能市場，建立各立足據點。除了要配合美國系統的核電廠的運轉規範與 NRC 的規定，在美國設立分公司，其產品“自然符合”美國法規，可減低對引用(歐洲)法規的差異性，而促使其系統易於銷售美系國家。另外中國則是一個相當重視的新核能市場，如秦山(Qinshan)、田灣(Tianwan)核電廠的儀控系統更新或新廠，都引用 TELETERM XP/XS 數位儀控系統，此成功的經驗成爲 AREVA 強力推銷的範例，而考慮未來中國核能電廠的急速成長，亦將在中國成立亞洲的分公司，配合中國市場龐大的發展潛力。

AREVA 推展世界核能版圖的強烈企圖心從以上其發展的藍圖可以觀其一斑。

因此，對 AREVA TELEPERM XS 系統的特性及美國 NRC 態度的重點，確應予以關注。

四、TELEPERM XS 系統爲高品質核能級產品

(一) TELEPERM XS 數位儀控系統是專爲安全系統設計的產品，其各項特性都較 TELEPERM XP(使用於非安全有關系統)爲優，可靠度都較 TELEPERM XP 爲高，符合各種法規對安全系統的規範，其爲真正核能級產品，並非商業級產品經檢證後的核能同級品。

(二) TELEPERM XS 數位儀控系統亦可應用於非安全有關系統，可提昇可靠度與暫態反應能力。

(三) 可以“模組式”的更新取代舊有類比組件，不須整個組件連控制盤一併更換。

(四) 要更新爲 TELEPERM XS 系統計畫，最好連 Cabinet 一併更新，且要考慮一部機須 18 個 Cabinets 的空間。

伍、對本公司之建議事項

一、考察安全數位儀控改善的實務經驗爲此次出國的主題，安全有關儀控系統的數位化爲本公司目前的重要策略，經考察 AREVA 公司的作法後，有以下幾點建議：

(一) 安全有關數位儀控系統應使用真正“核能級”產品，不宜使用“核能檢證品”，才可確保高階的可靠度。

(二) 國內各核電廠安全有關儀控系統數位化的改善案必須經過主管單位原能會的審查核准，才得以正式推動，因此，原能會的態度攸關此改善案能否順利進行。目前，在總處有許多儀控數位化相關的研發案正進行著，每一階段皆有期中工作報告會，皆會檢討未來儀控數位化的原則與方向，尤其核研所的相關研發報告更具有相當的代表性，於適當時機可邀請原能會參加，初步溝通兩方的看法，有助於減少未來改善案審查的岐見。

(三) 原能會審查的重點必然參考美國 NRC 的經驗，因此，Oconne 核電廠爲美國第一個安全有關儀控系統的數位化的改善案例，由 AREVA 承標此更新案，因此，AREVA 對本案處理的方式與 NRC 審查的回應必須多加關注，以爲公司擬提改善建議書的參考。

(四) AREVA 公司在其 Test Bay 測試將提交 Oconne 核電廠的 TELEPERM XS 系統，皆有美國 NRC 人員在場作重點的 Audit，顯示 NRC 對本案的重視。日後，本公司進行類似的改善案，亦可邀請原能會參加工廠的 Audit，可提昇原能會對此系統的信賴度，降低 V&V 的疑慮。

二、在考察安全有關儀控系統的數位化的實務經驗時，AREVA 說明 Oconne 核電廠有關數位軟體的 V&V 的作

法，包括人員建制、目標、組織、工作範圍等，相當具體，目前，該廠的安全儀控數位化方案已獲 NRC 核准通過，若未來國內各核電廠進行此改善案時，可考慮至該廠觀摩，吸收其經驗以爲我方的參考。

三、核電廠儀控數位化的 V&V 計畫，並非所有步驟皆須執行 V&V，可視其必要性決定參與的程度。

四、輻射劑量對電纜老化效應的評估不需要過渡保守，宜透過合理的分析與計算以判定其殘留壽命。