出國報告（出國類別：洽公）

美國 Oconee 核能電廠
安全儀控系統數位化更新經驗

服務機關：台灣電力公司核發處

姓名職稱：李明宗主管核工儀控

派赴國家：美國

出國期間：99.06.19~99.06.27

報告日期：99.08.09

行政院及所屬各機關出國報告提要

出國報告名稱：美國 Oconee 核能電廠安全儀控系統數位化更新經驗

頁數 45 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

李明宗/台灣電力公司/核能發電處/主管核工儀控/(02) 2366-7062

出國類別：□1 考察□2 進修□3 研究□4 實習■5 其他

出國期間：99/06/19~99/06/27　　出國地區：美國

報告日期：99/08/09

分類號/目

關鍵詞：Cyber Secuity、D3、ESPS、ISG、Oconee、RPS、SER、SIVAT、TELEPERM TXS、V&V

內容摘要：（二百至三百字）

美國 Oconee 電廠反應器保護系統與特殊安全設施保護系統儀控設備數位化更新，是 1993 年美國核管會提出“數位系統軟體共因模式失效”議題 (SECY 93-087) 後，美國第一個反應器保護系統儀控設備更新案，已於 2010 年元月經美國核管會核准，申照過程歷經五年以上。

本公司核三廠 7300 電子卡片 、SSPS、ESF、SSILS 等安全儀控系統未來預計更新為數位化系統，由於原能會依循美國核管會法規，基於 Oconee 電廠申照過程冗長，本公司應及早因應，以利未來更新案之規劃。本次出國任務之目的為赴美國洽商 AREVA TELEPERM TXS 儀控平台技術與 Oconee 電廠 TXS 變更申請案，了解美國電廠安全儀控數位化之過程與經驗，擬以 Oconee 電廠之申照經驗 (例如送交文件)，規劃本公司核三廠安全儀控系統數位化之更新策略，協助核三廠未來執行安全儀控系統數位化更新。

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

目　　錄

壹、出國目的

本公司核一、二、三廠自商轉至今已運轉多年，儀控系統均面臨設備組件老化、備品取得困難等問題，數位化更新乃是必經之路，未來幾年將汰舊換新以數位化系統來替換現有的類比儀控系統，提昇機組運轉之可靠度；而安全儀控系統之更新須先經原能會核准，申照過程中，需審慎的評估及考量例如數位化系統之網路資通安全等諸多問題。

美國 Oconee 電廠反應爐保護系統與特殊安全保護系統 RPS/ESPS (Reactor Protection / Engineered Safeguard Protection system) 安全儀控系統數位化更新，是 1993 年美國核管會提出 SECY 93-087“數位系統共通模式失效 (Common Mode Failure)”之議題後，美國第一個反應爐保護系統儀控設備更新案，已於 2010 年元月經美國核管會核准，申照過程歷經五年以上。

本公司核三廠 7300 電子卡片、SSPS、ESF、SSILS 等安全儀控系統未來預計更新爲數位化系統，由於原能會依循美國核管會法規，基於 Oconee 電廠申照過程冗長，本公司應及早因應，以利未來更新案之規劃。本次出國任務之目的爲赴美國洽商 AREVA TELEPERM TXS 儀控平台技術與 Oconee 電廠 TXS 計畫，了解美國核電廠安全儀控數位化之過程與經驗，擬以 Oconee 電廠之申照經驗規劃本公司核三廠安全儀控系統數位化之更新策略，協助核三廠未來執行安全儀控系統數位化更新。

貳、任務過程與內容

本次出國任務之行程爲前往美國洽談核能電廠安全儀控系統數位化更新業務，出國行程及工作項目詳如下表：

起迄日期	前往/停留城市	工作項目
99.06.19~ 99.06.20	台北－洛杉磯 (留宿) －亞特蘭大	往程
99.06.21~ 99.06.22	亞特蘭大	奧科尼 (Oconee) 核電廠安全評估報告 (SER)
99.06.23	奧科尼	參訪奧科尼核電廠 TELEPERM TXS 數位平台維護測試機構
99.06.24	夏洛特市	TELEPERM TXS 數位儀控技術之應用
99.06.25	亞特蘭大	奧科尼核電廠申照經驗與美國核管會關切之議題
99.06.26~ 99.06.27	亞特蘭大－ 洛杉磯－台北	返程

本次出國任務爲參訪 AREVA 美國分公司，前後行程共五天，第一、二天停留在亞特蘭大區 AREVA 辦公室，第三天驅車前往 Oconee 核電廠，第四天前往 AREVA Charlotte 辦公室，第五天折返亞特蘭大，五天行程中主要的工作項目與討論議題如下：

- 美國 Oconee 電廠反應爐保護系統與特殊安全保護系統數位化更新經驗；
- AREVA 公司其他數位更新計畫；
- Oconee 電廠申照經驗，美國核管會核准過程與關切議題；
- 參訪 AREVA 公司在 Oconee 電廠之 TELEPERM TXS 儀控平台，並與 Oconee 電廠人員洽談反應爐保護系統與特殊安全保護系統數位化更新經驗；
- 參訪西門子 T3000 數位儀控平台組裝測試工廠。

叁、心得與感想

一、 美國核電廠安全儀控系統數位化更新經驗

1. Oconee 變更案簡介：

Duke Energy 公司旗下的 Oconee 核電廠共有三部 B&W PWR 機組，裝置容量各爲 846MW，商轉日期分別爲 1973 年 7 月 15 日、1974 年 9 月 9 日及 1974 年 12 月 16 日。Oconee 核電廠計畫更新原有之反應爐保護系統與特殊安全保護系統 (RPS/ESPS)，每部機組更新 18 個儀器盤面，包括十個跳脫訊號與四個事故減緩訊號。新的反應爐保護系統由四個控道組成，採用四選二邏輯，電驛輸出訊號選取邏輯採用第二大值或第二小值 (2^{nd} Min / 2^{nd} Max)；新的特殊安全保護系統則由三個控道組成，採用三選二邏輯，訊號選取邏輯同樣採用第二大值或第二小值。

在原有的設計上增加 ESPS 系統的多重性與訊號驗證邏輯，增加額外的類比高壓與低壓反應爐注水系統作爲多樣性注水系統 (Diverse High Pressure and Low Pressure Injection Actuation Systems DHPIAS / DLPIAS)，以改善系統之可靠度與可用性。

Duke 公司於 2008.01.31 提交執照變更要求申請(LAR)，欲修改運轉技術規範及最終安全分析報告(FSAR)，美國核管會審查期間共提出兩輪 128 個問題，其中 35 個問題與網路資通安全有關；爲了 Oconee 變更案，美國核管會執行五次稽查作業，Duke 總共交付給美國核管會 158 份，共 29,695 頁文件，NRC 稽查結果僅發現文件問題，沒有技術問題：

(1) 2008 年五月在 Oconee 核電廠審查 Duke 公司之相關開發文件。
(2) 2008 年九月在 AREVA 辦公室審查 AREVA NP 公司之相關開發文件。
(3) 2008 年 11~12 月間在德國埃朗根 (Erlangen) 測試場，觀察測試情形與審查測試結果文件。
(4) 2009 年四月：測試階段追蹤。
(5) 2009 年七月：維護作業管控。

2009 年 10 月 23 日，NRC 依據 10 CFR 2.390 章節核准變更，寄出安全評估報告(SER)草案，並要求 Duke 公司提供澄清說明，2009 年 11~12 月 Duke 公司提交澄清說明及解決方案給 NRC，NRC 於 2010 年元月 28 日寄出核准之安全評估報告(SER)，安全評估報告中之發現事項如下：

- 符合 1954 年修訂之原子能法標準與需求以及委員會 10 CFR 第 I 章之規範。
- 確保不會危及大眾的健康及安全。
- 此變更案的發行不會損害通用之防禦及安全性。
- 符合委員會 10 CFR Part 51 之法規要求。
- 運轉技術規範修改部份須於執照變更附件中載明，並且依照修訂過的運轉技術規範運轉。
- 執行設備變更前需完成所有維護與運轉程序書的修改、完成必要的訓練、並修改最終安全分析報告。
- 反應爐熱功率不得超過 2568MW。

Oconee 反應爐保護系統與特殊安全保護系統儀控設備更新計畫是第一個美國核管會審查通過的大型變更案，美國核管會於 2000 年五月核准 TELEPERM XS (以下簡稱 TXS) 爲安全系統數位儀控平台，但經過十年後才核准 Oconee 變更案，#1 號機預計 2011 年、#3 號機 2012 年、#2 號機 2013 年安裝。

NRC 關切的是使用於電廠的 TXS 平台做了什麼改變及如何改變，任何改變皆需要管控。Oconee 變更案專用的軟體開發程序與 TXS 軟體計畫專題報告 (Topical report) 無法及時被核准，原因是 NRC 缺乏大量需求文件之審查經驗，主要的挑戰還包括 TXS 數位平台的一般設計與驗證程序，和應用於核電廠更新案中專有的特殊設計與驗證必須區隔。

工廠允收測試 (FAT) 共歷時七週，測試項目包括軟硬體體與系統測試，亦包括平台驗證的網路資通安全測試；軟體測試包括 RPS、ESPS、GSM (Graphical Service Monitor) 圖控監測、網路閘道與網路資通安全；硬體測試包括 RPS 反應時間、ESPS 反應時間、硬體失效、DHPIAS 高壓注水系統、DLPIAS 低壓注水系統；系統測試包括一個泵浦降速運轉、小破口爐水喪失事件 SBLOCA (Small Break Loss of Coolant Accident)、啓動/停機、反應爐冷卻水泵功率偵測 RCPPM (Reactor Coolant Pump Power Monitor)、核能儀器功能等，測試結果之缺失報告共 56 件，其中包括三件軟體錯誤。

審查期間，Duke 公司人員與美國核管會顧問多次開會談論反應器安全系統的議題，每週利用電話快速回應 NRC 之問題，同時 NRC 透過有效的稽查去瞭解系統的細部設計，最後於 2009 年九月完成技術審查，並於 2010 年元月 28 日發行 SER 安全評估報告。

Oconee LAR 是美國核管會在現行法規標準下審查的第一件大型變更申請案，TXS 平台透過驗證測試使用 SIVAT (Simulation Validation Test Tool) 模擬驗證測試工具，偵測應用軟體的錯誤，提早在開發階段發現錯誤降低計畫風險。法規審查的部份有幾項獨一無二的經驗：例如大型數位儀控改善計畫軟體生命週期審查、軟體生命週期文件需求、及針對網路資通安全與全面性的通訊獨立提出新導則。

2. 業界的發展

早期美國核管會管制的依據缺乏了解安全數位儀控系統的設計，九〇年代美國數位儀控的發展歷史如下：

1990 – 第一個美國核能電廠 (Sequoyah) 安裝數位安全保護系統。

1993 – 第二個美國核能電廠 (Diablo Canyon) 安裝數位安全保護系統。

1993 – 美國核管會提出數位系統共因模式失效 (Common Mode Failure) 之議題 (NRC 委員文件 SECY 93-087)。

1997 – 美國核管會發佈第一份數位儀控導則文件，重點集中在程序的需求。

AREVA TXS 儀控平台在美國的發展歷史如下：

2000 – 美國核管會發行 TXS 平台之安全評估報告(SER)。

2005 – Oconee 核電廠向 NRC 提出申請，使用 TXS 數位儀控平台更新安全保護系統，此為美國第三個核能電廠安全保護系統之更新案。

2006 – 由於美國核管會缺乏審查經驗，管制立場不確定，加上下列議題不夠明確，Oconee 核電廠因此抽回申請案：

- 不同控道訊號間、與安全系統到非安全系統之溝通，通訊獨立性的要求標準；
- 多樣性引動機制 (手動) 的設計需求；
- 對於應用軟體開發的程序缺乏共識；
- 對於系統平台應用 (包括概念層次與完整設計) 的各個階段缺乏共識。

業界經由 Oconee 變更案的經驗，學習到應以積極的參與來支持新的數位儀控更新申請案；2006 年 11 月業界與美國核管會開會討論，條列四個焦點領域的立即措施：

(1) 通訊 (不同控道訊號間、與安全系統到非安全系統) 獨立性的要求標準；

(2) 網路資通安全需求的平衡點；

(3) 解決支援應用的需求層面；

(4) 改善 D3 多樣性與深度防禦 (Diversity and Defense-in-Depth) 分析方法與接受標準。

美國核管會對於數位儀控議題之作法，首先由 NRC 高階經理人員參與數位儀控的指導委員會，並組成六個優先議題之工作團隊；指導委員會主要的責任為：

- 與電力公司代表溝通數位儀控議題之解決辦法；
- 監控管理與協助數位儀控開發技術與法規等相關議題；
- 針對數位儀控議題，確保 NRC 不同組別之間有效的協調。

六個優先議題之工作團隊從 2007 年開始發展數位儀控相關之臨時工作導則 (Interim Staff Guidance)：

(1) TWG #1“數位儀控網路資通安全”，2007 年 12 月發行 DI&C-ISG-01 網路資通安全。

(2) TWG #2“數位儀控多樣性與深度防禦”，2007 年九月發行 DI&C-ISG-02 多樣性與深度防禦。

(3) TWG #3“透視數位儀控之風險”，2008 年八月發行 DI&C-ISG-03 透視風險。

(4) TWG #4“數位儀控通訊”，2007 年九月發行 DI&C-ISG-04 通訊議題。

(5) TWG #5“高整合控制室人因工程”，2007 年九月發行 DI&C-ISG-05 人因工程。

(6) TWG #6“數位儀控申照程序”，DI&C-ISG-06 申照程序 (研擬發展中)。

爲了將法規審查的不確定性降到最低，美國核管會採取較保守的立場，因此 ISG 爲保守性的導則，另外 NRC 高階人員期望有一些多樣性，故其他的解決方法經由額外的審查亦可以被接受；ISG 導則並非最終的法規文件，NRC 計畫持續與業者溝通，以加強法規標準的一致性，長程目標爲透過機構的程序發展標準審查計畫、分部技術立場 (Branch Technical Positions)、法規指引與法律條文等。

目前在通訊的獨立性、多樣性與深度防禦分析、及人因工程等重要議題，已發展出有效的導則指引；但在某些議題上仍待持續加強努力：例如定義可被接受的網路資通安全最低需求，針對低機率事故提供一個分級的多樣性與深度防禦分析方式，定義多樣性與深度防禦分析中使用的風險評估方法，及定義數位更新申照程序的資訊需求等。

3. 走向成功之路

針對 TXS 平台技術，AREVA 與 NRC 發展數位儀控法規全面性符合計畫，將 TXS 使用於美國 EPR™ 反應器特有的專題報告作爲 TXS 專題報告之補充資料。AREVA 從 2006 年中開始與 NRC 開會釐清主要的申照議題，並提供 NRC 人員 TXS 訓練課程，及贊助支持 NRC 與大學合作之 TXS 技術研究。

2006 年十月 AREVA 與 NRC 舉辦 TXS 應用前會議，提出主要的申照議題，包括 IEEE-603 之符合性、系統設計的多樣性引動機制、設備更新的申照需求、技術規範、網路資通安全、與申照審查等重要主題。2008 年元月 31 日 Oconee 電廠向 NRC 提出變更需求申請。

NRC 第一次引用新的 ISG 導則審查 Oconee 變更申請案，法規審查包括通訊的獨立性、網路資通安全的威脅、與網路資通安全監測/記錄的需求，但 NRC 在數位儀控與網路資通安全符合性的審查經驗有限。NRC 引用的 ISG 導則如下：

- DI&C-ISG-01 網路資通安全：針對安全系統程序的存取控制、較低安全層級的界面與惡意程式碼的預防等 NRC 有興趣的議題，處理審查的導則卻有限。ISG-01 將法規指引 RG 1.152 匹配到 NEI 04-04 工業網路導則，並以程序爲導向；將 TXS 在核能安全的歷史發展活動，匹配到網路資通安全，以符合 NRC 關注的生命週期程序。網路資通安全的重點集中在閘道單一方向硬體設施之設計，而 TXS 軟體開發程序、通用性的平台設計、再加上電廠特定的項目，成功地引用至 Oconee 變更案中。
- DI&C-ISG-02 多樣性與深度防禦：針對運轉員限制時間 30 分鐘內的手動操作，審查歷史紀錄的安全分析。使用相同的程序控制，對 RPS 與 ESFAS 系統沒有影響，Oconee 核電廠使用原有存在的感測元件與引動器，與其他數位儀控系統沒有連結，將系統範圍最小化。ISG-02 定義軟體共因模式失效的影響，共因失效具備可測試與多樣性，並須澄清單一故障與多層防禦的顧慮。

- DI&C-ISG-03 透視風險：提供 12 項特定的審查導則，使用於新設機組，Oconee 設備變更案不適用。
- DI&C-ISG-04 通訊議題：提供訊號控道間通訊及與服務單元之雙向通訊的導則，針對不同區間的通訊，定義 20 項特定的審查標準，優先指令則定義 10 項審查標準，多區間的控制與顯示站應注意獨立性與隔離、人因工程、及多樣性與深度防禦等；針對訊號通訊議題，Oconee 核電廠重新評估 TXS 專題報告之結論如下：

  ①針對不同控道間訊號正確性驗證採用有利的結果；及

  ②將服務單元永久連接至人機界面執行系統監測與記錄。
- DI&C-ISG-05 人因工程：提供電腦化程序書、最少設備、多樣性與深度防禦分析中運轉員手動操作等議題之導則。
- DI&C-ISG-06 申照程序 (研擬中)：提供設備改善申照的適當指引，例如：明確的數位儀控更新指引，明確的申照程序 (包括提交、稽查、檢查作業)。

NRC 原已經認定 Oconee 變更案符合 IEEE 7-4.3.2-2003，由於 NRC 引用 BTP 7-14 執行軟體工具開發之審查，在驗證測試之前，模擬測試工具必須通過審查與核准，這項新立場影響 Oconee 電廠的申照時程；NRC 新立場要求 TXS 模擬驗證測試工具之專題報告核准後，才接受使用 SIVAT 軟體驗證工具執行 V&V 驗證計畫，因此 Oconee V&V 計畫修改爲不使用 SIVAT 工具，而是在工廠允收測試時執行三部機組之軟體整合測試。

NRC 核准的 TXS 專題報告可應用於安全保護系統數位化更新計畫，TXS 通用系統的申照作業，各項重要議題之技術報告送給 NRC 的時程與內容詳如下表：

報告編號	報告內容	日期
EMF-2110 R1	TELEPERM XS 數位反應器保護系統	2000 年五月核准
EMF-2267	西門子電力公司多樣性與深度防禦方法論	2000 年五月核准
ANP-10272	TELEPERM XS 安全系統軟體計畫手冊	2006 年 12 月提交，第 2 版於 2010 年五月提交至 NRC
ANP-10303	TELEPERM XS 模擬驗證測試工具	2009 年六月送給 NRC 審查

TXS 技術是 NRC 第一個核准的安全數位儀控平台專題報告，也是第一個使用數位平台在核能安全系統的大型計畫，Duke 能源公司收到的 Oconee 變更案的安全評估報告草稿，NRC 沒有任何附帶的負面意見。TXS 技術建立了工具開發與驗證的基準，澄清模擬工具如何使用於支援驗證測試，並降低測試作業相關法規的不確定性。針對訊號控道間的通訊及與服務單元之雙向通訊，未來類似變更計畫 NRC 核准的先備條件，必須依據 DI&C-ISG-04 導則，Oconee 變更案已驗證 TXS 系統通訊技術的堅實可靠性。

包括變更計畫、程序書、設計結果、程序證明文件等，均與 DI&C-ISG-06 申照程序有關，Oconee 申照經驗可建立 NRC 安全有關軟體開發週期審查的案例。從 Oconee 經驗中，發現缺乏現代化開發工具與安全相關平台發展改善議題之法規經驗，與應用軟體開發週期程序的細節與標準化，在未來使用 TXS 之數位化更新計畫，須特別注意以降低額的外風險；同時，上述經驗可以直接轉換給其他現代化更新案件使用。

AREVA 於 2006 年 12 月提交 TXS 安全系統軟體計畫手冊專題報告，經過 NRC 兩次稽查會議審查，並到德國 Erlangen 檢查支援文件，五個回合審查共提出 98 個問題，五次技術會議討論並提出待解決問題，經由無數次的電話與 NRC 連絡確認並解決問題。由於 NRC 變更審查人員，加上新設反應器組與核能法規組之間的協調不容易，因此審查的困難度比預期的還難。NRC 不允許 Duke 公司參考尚未核准的 TXS 軟體計畫手冊，而軟體手冊的目的僅是說明與 Oconee 變更案相關特定的應用軟體開發程序，AREVA 因此另外提交應用軟體開發程序書給 NRC，以支援軟體開發之平行審查，NRC 終於核准 Oconee 變更申請。

雖然 NRC 於 2005 年已經知道模擬驗證測試工具 SIVAT，但在 Oconee 變更申照報告中並未詳細說明，因此 NRC 於 2008 年八月決定 SIVAT 需要分開審查，NRC 要求測試工具亦須經過核准才能使用，若 Oconee 變更案使用 SIVAT 工具，NRC 審查時間將會延後，若不使用則維持兩年之審查時間，因此 Duke 公司取消 SIVAT 在 Oconee 變更案之應用，改爲在 Oconee 三個機組的 FAT 允收測試時執行所有軟體測試。

因應未來的數位化計畫，AREVA 於 2009 年 12 月提交 SIVAT 模擬驗證測試工具專題報告，NRC 審查共提出 22 個問題，並執行一次稽查會議審查文件。NRC 關心的是驗證工具的合格使用：包括 SIVAT 開發與驗證合格的作業、正確的使用 SIVAT、並能證明 SIVAT 對 TXS 安全系統沒有直接或間接之負面影響。NRC 尚未發行 SIVAT 工具之安全評估報告草案。

AREVA 提交軟體計畫手冊第二版的專題報告，包括所有從 Oconee 變更案中所學習到的經驗，與所有待解決事項之說明文件，NRC 已完成技術審查，但尚未發行軟體計畫手冊之安全評估報告草案。

降低風險的主要改善：澄清 NRC 審查 Oconee 變更案時所提出之需求，並因應未來美國核電廠設備修改計畫，針對軟硬體與開發程序書修改，定義變更的管控程序 (10CFR 50.59)。

美國 EPR™機組使用優先模組 (Priority Modules) 的設計，爲了檢定這些優先模組，NRC 審查 AREVA NP 的測試方法論，優先模組提供 100%可測試性，並採用簡單的設計，以達到不需共因失效的處理措施。

多樣性與深度防禦方法論，以 NUREG CR-6303 爲基準，可符合 NRC BTP 7-19，NRC 接受 EMF-2267“西門子多樣性與深度防禦方法論”之專題報告。多樣性與深度防禦方析包含共因失效/多樣性、影響後果與人員可靠度等三項特定的分析；其中，影響後果分析的結果，發現廠外電源喪失與其他事件不會同時發生，單一故障亦不會同時發生，正常的控制系統均能正常動作；人員可靠度分析則是要求於 30 分鐘內可以手動操作降低事故之嚴重性。

針對多樣性與深度防禦，從 Oconee 變更案可得到下列經驗；

(1) 多樣性與深度防禦考量的因子：受限於原有或新增儀器、受限於原有設備位置或新增盤面、使用積極的最佳評估分析或現有的分析方法、類比或數位多樣性引動儀控系統、多樣性數位儀控的可用性、與整體數位系統整合的策略、申照的解決方法等。

(2) 多重選擇：選用最少的類比或數位多樣性引動系統，使用現有的感測元件與引動器，最佳評估分析，不與其他數位儀控系統連結。

(3) 數位多樣性引動系統：使用現有的感測元件與引動器，使用設計基礎使分析範圍最小化，使用其他功能性較寬廣的數位儀控系統。

4. TELEPERM XS 技術架構

驗證測試步驟的先後順序：概念審查→軟硬體元件測試→整合與系統測試→規範的驗證→軟硬體生產測試→工廠允收測試→安裝測試；驗證測試步驟可由 TXS 專題報告與軟體計畫手冊兩大部份來涵蓋，概念審查、軟硬體元件測試、整合與系統測試包含在 TXS 專題報告中，規範的驗證、軟硬體生產測試、工廠允收測試、安裝測試則在軟體計畫手冊中。

(1) TXS 專題報告分爲系統軟體與系統硬體兩部份，系統軟體包括功能方塊資料庫、TXS 執行環境、操作系統、特定硬體專用軟體；系統硬體包括通訊系統、輸出入模組、及其他程序模組。軟體計畫手冊主要是應用軟體：包括功能圖形模組與一般性的軟體界面。

(2) 針對訊號控道間的通訊議題，TXS 系統採取下列解決方案以符合法規：

- 設備分佈於不同盤面，以驗證合格的光纖隔離、採用雙重埠隨機存取記憶體 (Dual Port Random Access Memory) 緩衝電路，在實體上、電氣與通訊的獨立性，TXS 系統可符合 IEEE-603 與 IEEE-384。
- TXS 設計架構包括應用軟體嚴謹來回的程序、不同步的操作系統、靜態記憶體定位、訊息轉換控制、無程序岔斷、固定負載、與看門狗 (Watchdog) 計時器等，可確保安全控道間的資料傳輸不會抑制安全功能的執行，符合 IEEE 7-4.3.2 與相關的法規指引。
- TXS 擁有阻擋錯誤傳遞的屏障、無單一故障之弱點、額外之故障檢測及調整能力，TXS 訊號驗證技術可符合 IEEE-603 與 IEEE-379，並能改善系統的效能。

(3) 針對系統與服務單元的通訊議題，TXS 採取下列解決方案以符合法規：

- 採用驗證合格的光纖隔離、雙重埠隨機存取記憶體 (Dual Port Random Access Memory) 緩衝電路，在實體上、電氣與通訊的隔離，TXS 系統可符合 IEEE-603 與 IEEE-384。
- TXS 設計架構包括監測與服務界面之隔離點、應用軟體嚴謹來回的程序、不同步的操作系統、靜態記憶體定位、訊息轉換控制、無程序岔斷、固定負載、看門狗計時器等，可確保安全控道間的資料傳輸不會抑制安全功能的執行，符合 IEEE 7-4.3.2 與相關的法規指引。
- 所有設備位於控制存取區域，設定密碼並以鑰匙操作控制，TXS 系統多層存取管控以避免未經授權經由監測或服務界面存取，可符合 IEEE-603、IEEE 7-4.3.2 與相關的法規指引。

(4) 針對 TXS 與閘道的通訊議題，採取下列解決方案以符合法規：

- TXS 系統將監測與服務界面充當邏輯屏障、閘道 TXS 端使用 TXS 通訊原則、閘道與服務單元分開使用通訊程序器，可符合 IEEE-603、IEEE 7-4.3.2 與 D&IC-ISG-04。
- 依據 DI&C-ISG-01，在外圍安全層之閘道界面，要求額外的網路資通安全管控，TXS 系統設置防火牆與單向通訊控制硬體。

(5) TXS 應用軟體：

- 開發程序採用特別設計的架構來改善應用軟體的可靠度：使用標準方塊資料庫提供大型的經驗基礎，並利用 NRC 已核准的程式開發工具 SPACE (Specification and Coding Environment Engineering Tool) 自動產生程式碼。SPACE 工具可消除程式碼轉換錯誤及工程人員試圖加入的複雜程式碼，藉以降低人為疏失。
- SIVAT 的特別設計乃為了在模擬環境中驗證儀控功能之應用碼，SIVAT 使用 SPACE 工具從計畫工程資料庫自動產生模擬程式碼，模擬驗證工具已提交 NRC 審查，並列在 TXS 軟體計畫手冊專題報告中。透過 SIVAT 工具，可提早在開發階段偵測到應用軟體的錯誤，降低計畫風險。

(6) 軟體的生命週期分成計畫 (Planning)、需求 (Requirements)、設計 (Design)、實施 (Implementation)、整合 (Integration)、驗證 (Validation)、安裝 (Installation)、運轉維護 (Operation & Maintenance) 等階段，各階段 TXS 應用軟體開發的作業程序已載明於軟體手冊中：

- 計畫階段的各項作業計畫：軟體管理、軟體開發、軟體品保、整合、安裝、軟體安全、軟體驗證與確認 (V&V)及開發階段的軟體構型管理 (運轉階段的軟體構型管理由業者負責)；
- 需求階段的各項作業：需求規範 (來自儀控設計與 FSAR 的功能需求)、需求的安全分析、V&V 需求的分析報告、構型管理的需求報告；
- 設計階段的各項作業：設計規範、軟硬體架構、設計安全分析、V&V 設計的分析報告、構型管理的設計報告；
- 實施階段的各項作業：程式碼列表、程式碼安全分析、V&V 實施分析與測試報告、構型管理的實施報告；
- 整合階段的各項作業：系統建置文件、整合安全分析、V&V 整合分析與測試報告、構型管理的整合報告；
- 驗證階段的各項作業：驗證安全分析、V&V 驗證分析與測試報告、構型管理的驗證報告。

(7) TXS 計畫網路資通安全的審查乃依循美國核管會法規 RG 1.152 及 RG 5.71，其中 RG 1.152 關注的兩個領域：第一是確認安全架構可以實現網路資通安全之需求，而且對安全功能無負面效應；第二爲在開發階段執行管控，以保證沒有不需要之程式碼插入安全相關軟體。RG 5.71 則著重在技術架構與開發管控，以避免網路資通安全被攻擊破壞。

二、 Oconee 變更案安全評估報告摘要

1. 報告目錄

- 6.0 ENVIROMENTAL CONSIDERATION
- 7.0 CONCLUSION
- 8.0 REFERENCES
- 9.0 ACRONYMS

2. 簡介說明
   - Oconee 電廠有三個核能機組，使用 TELEPERM XS 數位電腦平台進行安全反應器保護系統更新，以取代原 Bailey Meter 公司的類比系統。
   - 數位 RPS/ESPS 系統將提供訊號處理、訊號驗證及保護邏輯等功能。
   - 處理現行感測器訊號、確保可靠運轉、提供線上自我測試及診斷功能，提升系統可用性並降低維護負擔。
   - 此執照變更申請包含詳細的描述、技術評估、法規評估及環境考量。NRC 於 2008 年 3 月 18 日公開會議中，提出 LAR 一些應用上不足及仍有疑慮的問題：
     - 多樣性與深度防禦；
     - 雙向溝通 (Bi-directional Communication)；
     - 軟體計畫手冊；
     - 已核准之 TXS 平台於 Oconee 變更案被修改的部份；
     - 軟體驗證與確認，及例外項目；
     - SIVAT 軟體模擬驗證測試工具。
   - Oconee 於 2008 年 4 月 3 日提出問題解決之答覆時程，NRC 於 2008 年 4 月 24 日接受 Oconee 變更案申請，同意審查 LAR；並開始執行稽核作業：
     - 2008 年五月，美國 AREVA Alpharetta 辦公室；
     - 2008 年九月與 2009 年四月，德國 Erlangen；
     - 2008 年 11~12 月，數位 RPS/ESPS 系統 FAT 允收測試。

3. ISG-04 通訊議題

- Oconee 核電廠 RPS/ESPS 更新案費時五年，才取得 NRC 核准。DI&C-ISG-04 包括 (1) 控道間通訊，(2) 優先指令，(3) 多區控制與顯示工作站等三個章節，其中第 2、3 節不適用於 Oconee 變更案。NRC 第一次以 ISG-04 審查數位儀控系統更新案，此案例有助於釐清 ISG-04“通訊議題”的審查重點。
- ISG-04 涉及安全控道間及安全與非安全間的訊號通訊，重點爲控道間通訊功能需具備確定性，且在任何情況下不能影響安全功能的執行。設計上要求須具備專用通訊處理器、光纖、點對點、專線，使用類似雙重埠隨機記憶體架構與安全功能處理器交換資料，訊號從安全至非安全設備單向傳輸。
- NRC 對 Oconee 核電廠更新案審查，進行 ISG-04 控道間通訊議題共 20 點要求之符合度評估，結果發現第 3、10 點不符合 ISG-04，但符合法規要求，NRC 認爲可以接受；第 11 點不符合 ISG-04，但以行政管制與操作程序書進行改善，NRC 同意接受；其餘 17 點皆符合。20 點要求敘述如下：
  (1) 安全控道需能獨立運作，不能因爲等待外部資料而延誤。NRC 檢視程式碼與功能方塊圖，確認安全控道即使喪失通訊無法收到其他控道資料時，不會影響安全功能之執行。
  (2) 安全控道需具備防護外部干擾能力，外部傳入資訊不能禁止或延遲控道執行安全功能。TXS 系統以鑰匙開關決定其工作模式，不會影響安全功能，NRC 檢視系統設計，確認控道內通訊不會受到外部的影響。
  (3) 安全控道不能接收外部資訊，除非此資訊可加強或支援安全功能。TXS 系統安全控道需要經由通道間的通訊，取得其他控道感測器量測值並進行判斷，此爲非必要的流程；安全控道執行中需與非安全設備服務單元進行雙向通訊，違反安全控道不能接收外部資訊的原則，有潛在危機。基於上述兩點及 Oconee 系統很複雜，NRC 認定不符合 ISG-04 第三點要求。

NRC 現場稽核，詳細檢視通訊流程與第二大/第二小程式碼與功能圖，要求提供通訊功能失效之 FMEA 分析結果，並提供各種劇本測試，NRC 認爲通訊設計雖不符合 ISG-04 第三點要求，但符合 IEEE 603-1991，因此可符合本項要求。NRC 認爲 AREVA 未能於 LAR 變更申請時提供詳細資料，使審查時間延長。

(4) 專用程序處理器來執行通訊功能，通訊與安全功能之程序處理器須非同步執行，兩者只透過專用雙埠記憶體交換資訊。NRC 人員檢視 TXS 通訊設計，確認可符合要求。

(5) 考慮存取記憶體所需之最長通訊時間，執行安全功能所需時間要能確定，NRC 審查 TXS 安全功能程序處理器執行一個週期的時間，確認系統以嚴謹的週期性方式執行，符合第五點要求。

(6) 執行安全功能的程序處理器不能使用握手方式或由外部訊號中斷，NRC 審查 Oconee RPS/ESPS 系統相關通訊協定，發現所有握手方式皆由通訊程序處理器負責，不會影響安全功能程序處理器，符合要求。

(7) 要求：通訊格式與內容需事先定義，不能任意改變。NRC 審查 Oconee RPS/ESPS 系統相關通訊協定，確定所有通訊格式與內容均事先定義，實際測試結果亦顯示通訊程序處理器可排除非事先定義的通訊資料，符合要求。NRC 希望廠家能於變更案申請文件中，詳細定義通訊格式的每個位元。

(8) 要求：通訊不能影響執行安全功能。Oconee RPS/ESPS 系統採通訊專用與安全功能專用程序處理器，且系統固定週期執行，NRC 審查結果符合。

(9) 要求：通訊傳入資料必須定義在共享記憶體的固定位址，這些位址不能移爲他用，NRC 審查相關設計文件，確認所有通訊相關記憶體均事先定義，即使重新編譯程式也不會改變記憶體位址。

(10) 安全控道執行中，其程式不能被任意更改，必須以硬體方式與維護設備隔離。Oconee 電廠僅有一個參數改變設定鑰匙，改變此鑰匙會改變相對記憶體的狀態，NRC 認定 Oconee 電廠 RPS/ESPS 系統不符合 ISG-04 第十點要求，因此 AREVA 提供保護機制，NRC 接受這項改善措施。但 AREVA TXS 平台若應用於其他系統仍須重新評估，NRC 希望廠家能於 LAR 變更申請階段，提出與 ISG-04 的符合度評估，並對不符合處提出說明與改善方案。

(11) 要求：安全控道執行中，不能接受外部軟體指令改變其程式執行流程。無論 Oconee RPS/ESPS 系統處於旁通或跳脫狀態，參數設定鑰匙會改變相對記憶體的狀態，導致服務單元改變安全程序處理器工作模式，因此 NRC 認定 Oconee RPS/ESPS 系統不符合 ISG-04 第 11 點要求。Oconee 電廠以行政管制與操作程序書改善。

(12) 在任何通訊狀況下，不能影響安全功能執行，AREVA 提供 ISTec 執行 12 種通訊條件下的測試報告後，NRC 審查後同意接受。

(13) 爲確保傳輸資料的正確性，針對重要通訊例如四個控道間資料的傳送，對接收資料必須有錯誤檢查機制。NRC 檢視相關通訊設計文件，確定對接收資料有 16 位元 CRC 循環冗餘檢查 (Cyclic Redundancy Check) 與傳輸資料序號檢查機制，確保錯誤資料不會送交安全程序處理器。

(14) 安全區間彼此的重要通訊需爲點對點專線連接，而且要用光纖隔離。AREVA RPS/ESPS 系統使用 PROFIBUS 通訊協定，此 BUS 上只有兩點訊號，可視爲點對點，而且 PROFIBUS 連接光纖模組，可符合 ISG-04 第 14 點要求。

(15) 重要通訊需採固定資料長度與定時傳送的方式，依據 SER 3.1.1.6.1.7 節所述 Oconee RPS/ESPS 系統通訊格式與內容均事先定義，NRC 評估結果可符合 ISG-04 第 15 點要求。

(16) 網路通訊與外界無連線時，需證明不會因 RPS/ESFAS 系統通訊失效，導致安全功能執行拖延或跳入死結無法執行，。NRC 依據 TXS 專題報告 SER 2.2.1.1 節所述，TXS 的通訊計數功能可用來評估通訊的工作狀態，而且系統有通訊專用程序處理器處理一切通訊問題，在任何通訊異常下，不會導致系統安全功能無法執行。

(17) 重要通訊控道必須通過環境驗證，確保異常事故後仍能正常工作，NRC 檢視廠家提供的 TXS 儀控平台環境測試報告後同意符合。

(18) 通訊架構需進行危害與功能異常分析，NRC 檢視廠家提供的 FMEA 分析報告後同意接受。FMEA 報告包括系統對內對外通訊異常的分析結果。

(19) 要求：通訊頻寬需保留餘裕給突發狀況；NRC 檢視 RPS/ESPS TXS 系統架構，認爲系統採週期性執行，且有通訊專用程序處理器與特定記憶體位址的設計，同意符合 ISG-04 第 19 點要求。

(20) 要求通訊時間的確定性，控道反應時間計算應涵蓋設計與驗證中的通訊失誤率，NRC 審查 AREVA 編號 32-9009296-005 “Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Response Time Calculation” 文件後同意符合。

- NRC 審查方式：①由 AREVA 提供訓練，增進 NRC 人員對 TXS 系統之了解程度；②審查設計、測試報告與相關評估報告；③執行現場稽核，評估程式碼與功能測試。
- NRC 深入審查 TXS 程式碼，並假設各種情況（劇本）評估 TXS 通訊議題。NRC 認爲 AREVA 提供佐證資料不全，導致審查進度緩慢。
- AREVA 提供更新案與 ISG-04 的符合度評估報告“Alignment of Oconee RPS/ESPS Project with NRC DI&C-ISG-04 - Task Working Group NO.4 ”。
- NRC 安全評估報告提到 Oconee 核電廠 RPS/ESPS 更新案符合法規要求，但日後應用 TXS 數位平台於核電廠時，仍須依據電廠實際需求與設計，重新進行 ISG-04 評估。

4. 軟體計畫手冊 (Software Program Manual)

- LAR 執照變更申請文件中提及應用軟體之發展乃依照軟體計畫手冊執行，但是 NRC 尚未正式核准軟體計畫手冊，所以要求 Duke 公司提供其他補充文件說明軟體品質的評估。
- 軟體計畫手冊之需求文件，包括功能需求規範、軟體需求規範、軟體設計規範、軟體需求可追溯性矩陣 (traceability matrix) 之應用、驗證與確認 (V&V) 計畫等。Duke 公司檢討後發現，上述文件已於 PRS/ESPS 執照變更申請時提交，故不需再額外參考軟體計畫手冊，所以刪除執照變更申請內參照軟體計畫手冊之內容。

5. 已核准之 TXS 平台於 Oconee 變更案被修改的部份

- NRC 曾核准過一些核電廠安全系統之數位應用，例如，2003 年核准 Palo Verde 核電廠使用 Common Q 進行 RPS 系統爐心保護計算器 (Core Protection Calculator) 之數位化更新。NRC 要求申照者必須提出新系統與已核准過系統的差異，這些差異爲電廠特定事項須能符合已核准平台之法規要求。
- 當申照者應用 TXS 平台時，NRC 成員在審查過程或專題報告中發現差異，都應該於安全評估報告中提出。爲了解決已核准專題報告與實際應用上的差異，安全評估報告應確認限制條件，並比照適當的法規標準來評估差異，具體解釋爲何差異是可以被接受的。
- 由於 Oconee 變更案之數位平台設計，和已被 NRC 核准之 TXS 專題報告不完全相同，而 LAR 並沒有提出足夠的資訊，因此 NRC 要求 Duke 公司提供更多的附加資訊，讓 NRC 來接受這些差異。
- NRC 審查著重於基本運轉原理、生命週期作業、驗證測試方法、構型管理與設計變更程序，其稽核範圍包括充分審查及品保程序的有效性。
- Duke 公司於 2008 年 5 月 15 日針對 TXS 設計原則及發展方法、構型管理與設計變更程序之審查及稽核、Oconee 先前提交給 NRC 的文件等各方面提出補充解釋。Oconee 核電廠提交給 NRC 的一些特定文件，可用來證明其軟硬體使用以及程序變更是符合已被核准的程序，Duke 公司相信其設計及資格皆能符合 NRC 核准之專題報告。

- LAR 第 2.7 節中敘述 TXS 專題報告與 Oconee TXS 數位平台之差異性，TXS 專題安全評估報告第 6.0 節，提出 Oconee 核電廠在進行安裝時必須要符合下列之 17 項電廠特定項目，Oconee 於 LAR 表 1-1 中回應說明，NRC 亦於 Oconee RPS/ESPS 變更案安全評估報告第 3.1.1.7 節作評估回應。
  (1) 申照者在安裝 TXS 平台設備時，必須考慮電廠特定條件 (例如：溫度、溼度、地震及電磁相容性)，且須符合 EPRI TR-107330 與 TR-102323-R1 之驗證要求。SER 3.31 節：LAR 3.3.4 節中描述 TXS 系統設備資格，符合 EPRI TR-107330 與 TR-102323-R1 之驗證要求與電廠特定條件 (溫度、溼度、地震及電磁相容性)。
  (2) 電廠特定軟體發展驗證作業與構型管理程序要符合工業標準與 NRC 認可的做法，並符合 SRP BTP HICB-14 (儀控系統數位電腦軟體審查指引)。LAR 3.4.3 與 3.6.4 節：描述軟體發展驗證作業與構型管理程序。SER 3.2.1.10、3.2.1.11、3.2.2.2 節：NRC 評估若正確的執行驗證計畫，確信可產生高品質的軟體產品。評估軟體構型管理流程，認爲在電廠運轉 (包括系統測試、修改及維護) 時提供了必要的高水準指引。
  (3) 若申照者要發展輔助飼水控制系統，必須包含自動引動與流量指示，並確認此應用可符合 10 CFR 50.34 (f)(2)(xii)之要求。SER 5.0 節：此數位變更案不更換輔助飼水控制系統，本項目不適用。
  (4) 若申照者要更換現行之事故監測儀器系統 (包含旁通及無法使用之狀態資訊)，必須確定新系統能提供同等之取樣與分析能力，並符合 10 CFR 50.34 (f)(2)(xvii)之要求。SER 5.0 節：此數位變更案不更換事故監測儀器系統，本項目不適用。
  (5) 若申照者要安裝爐心冷卻不足監測系統，必須確定新系統符合 10 CFR 50.34 (f)(2)(xviii)之要求。SER 5.0 節：此數位變更案不安裝爐心冷卻不足監測系統，本項目不適用。

(6) 若申照者要安裝 TXS 圍阻體隔離系統，必須確認此應用能符合 10 CFR 50.34 (f)(2)(xiv)之要求。　　SER 3.1 節：說明圍阻體功能，NRC 評估後認爲可接受此應用，並且符合三浬島行動計畫待辦事項 II.E.4.2 要求(必須提供圍阻體隔離系統)。

(7) 爲了監視電廠狀態，防止核心損傷，因此申照者必須確認 TXS 系統能符合 10 CFR 50.34(f)(2)(xix) 處理與顯示之要求。SER 5.0 節：此數位變更案不更換此系統，本項目不適用。

(8) 若申照者要安裝 TXS 事故後監視反應爐水位系統，必須提供電廠特定檢查範圍，並確認符合 10 CFR 50.34(f)(2)(xxiv) 之人因疑慮。SER 5.0 節：此數位變更案不更換此系統，本項目不適用。

(9) 若申照者要安裝 TXS 反應爐保護系統，必須確認系統是多樣性的，能符合 10 CFR 50.62 之要求，以降低預期暫態未急停(ATWS)事故之風險。LAR 2.4 節：Oconee 提供電廠控制系統、手動控制與 ATWS 系統及多樣性相關資訊。SER 3.9 節：NRC 評估後，確認 Oconee TXS 保護系統之多樣性急停系統與預期暫態未急停緩和系統致動電路(AMSAC)是獨立與多樣性的，可符合 10 CFR 50.62 要求。

(10) 設定點必須評估。LAR 3.3.16.8 節中，Oconee 電廠提供修改儀器設定點不確定性分析，設定點允許值不會改變任何跳脫功能。SER 3.4.3.8 節：NRC 審查不確定性分析，確定 RPS/ESPS 設備可依設定值自動引動保護邏輯，並經 FAT 測試驗證。

(11) 申照者必須進行電廠特定事故分析評估，並與電廠安全分析報告第 15 章之事故分析一致。LAR 3.3.16.8、3.4.5、3.5.3、3.5.4 節，針對反應時間，LAR 3.4.5 節中於設計階段計算安全系統反應時間，並於 FAT 測試驗證符合電廠特定事故分析之接受標準。SER 3.7 節：UFSAR 第 15 章之事故分析，假設安全功能儀器設定值、設定值不確定性及反應時間等三個參數，只要新系統不會改變設定值，不會導致不確定性大於假設值，不會導致反應時間大於假設值，原來的分析依然可以涵蓋及有效。NRC 已於第 10 項評估儀器設定點、設定點的不確定性及反應時間計算，並評估 FAT 測試報告，確認數位 RPS/ESPS 保護系統可符合反應時間的要求。

(12) 申照者必須確認 TXS 平台之應用可預防數位儀控系統共因模式失效。LAR 3.2.3 節：Oconee 電廠提供多樣性與深度防禦方法及工程研究來預防軟體共因模式失效。SER 3.9 節：NRC 評估後，認爲多樣性保護系統之軟硬體不會受到共因模式失效及電力喪失的影響。

(13) 申照者必須提出電廠特定的運轉技術規範，包含定期測試週期。LAR 3.6.5 節：於 LAR 補充文件中，Oconee 電廠提出運轉技術規範修改，包含控道查驗、控道功能測試及控道校正測試週期修改。SER 3.4.2.7.1、3.4.2.7.2、3.4.3.5、3.10 節：NRC 評估後，認爲可以接受。

(14) 申照者必須證明 TXS 系統電源可符合 EPRI TR-107330 之要求。LAR 3.3.18 節：RPS/ESPS 數位設備使用多重的 Absopulse 120 VAC/24 VDC 電源供給器，經測試符合 EPRI TR-107330 之要求。SER 3.1.1.2.8、3.4.5 節：NRC 評估後確認 Oconee 電廠使用之 Absopulse 電源供給器可符合 EPRI TR-107330 負載共享及熱插拔能力的要求。

(15) 申照者必須驗證隔離元件可符合 EPRI TR-107330 之要求。LAR 3.3.4 節：Oconee 電廠表示測試樣本成功完成隔離測試，並符合 EPRI TR-107330 之要求。SER 3.3 節：NRC 評估後，認爲驗證測試符合 EPRI TR-107330 之要求。

(16) 申照者必須證明 Siemens TXP 與其他廠家控制系統符合專題報告 SER 4.1 節“TXS 系統多樣性與深度防禦評估”之接收指引規定，(TXP 系統不使用於 Oconee 控制系統)。LAR 2.4.1.1 節：Oconee 電廠提供控制系統與 RPS/ESPS TXS 之評估，來確認符合 LAR 3.2.3 節所述系統多樣性與深度防禦。SER 3.9 節：NRC 評估後，確認數位 RPS/ESPS 保護系統多樣性與深度防禦評估方法符合 SRP BTP 7-19，可被接受。

(17) 在應用軟體的整個生命週期中，申照者必須符合需求追蹤表的要求，特別在未來如果有修改時，須列舉並追蹤系統的需求。SER 3.2.2.5 節：NRC 審查 Oconee 電廠之需求追蹤表，認爲追蹤的過程提供了可接受的方式來確保全部需求皆能正確實現於 RPS/ESPS 應用軟體中。

6. 軟體驗證與確認 (V&V) 及例外項目：

- NRC 認爲 Oconee 電廠依照 IEEE-1012 所執行之軟體驗證與確認工作，測試計畫書由開發或是測試部門來執行，有違背軟體驗證與確認工作 (V&V) 之獨立性要求。
- Duke 及 AREVA 公司決定修改軟體驗證與確認之方法，提出 IEEE-1012 之例外項目，藉由軟體開發人員的支援，協助產出測試計畫與執行測試，包括準備測試規範、程序書、測試報告，並將這些人員納入 V&V 部門，接受 V&V 部門之指揮，以符合獨立性之要求。

7. SIVAT 軟體模擬驗證測試工具

- LAR 文件指出使用 SIVAT 工具執行測試，可忽略元件測試與整合測試兩個測試階段。NRC 認爲此方法並不符合業界標準或是法規要求，而且其測試之程式碼並非爲最後控制器之執行程式，SIVAT 工具也尚未被認可。所以要求需對控制器上的實際程式執行測試，或是補充 FAT 的測試執行個案，以符合元件測試與整合測試之要求。
- Duke 回應，於 Oconee 變更案放棄使用 SIVAT 工具，而於 FAT 執行相關之補充測試。

8. ISG-01 網路資通安全審查

- Oconee RPS/ESPS 數位安全系統更新案之安全評估報告第 3 章“網路資通安全技術評估”審查內容，NRC 依據 RG 1.152 R2 及 ISG-04 需求，審查 Duke 公司提送之網路資通安全相關補充文件及報告，同意 Oconee 電廠更新之 RPS/ESPS 數位安全系統符合 RG 1.152 R2 版本法規立場 2.1-2.5 之要求，而法規立場 2.6-2.9 之要求，NRC 將在安裝前進行稽查。
- 此外從審查 ISG-01 在 Wolf Creek 與 Oconee 之應用，了解到 NRC 進行核電廠數位安全系統保安/資安議題的審查立場與 ISG-01 一致，並無其他新增要求。NRC 進行網路資通安全審查，分成 TXS 平台及 RPS/ESPS 數位系統應用軟體開發兩部份：
  (1) TXS 平台以 2000 年經認可的平台安全評估報告爲主，Oconee 電廠補充網路資通安全需求，若數位平台設計有變更則須提交例如需求規範、設計管制、V&V 報告等相關文件資料；
  (2) RPS/ESPS 數位系統應用軟體開發：數位儀控系統軟體文件係依據 SRP 標準審查計畫 BTP 7-14 進行審查，其中即要求軟體開發過程階段應提交的文件須涵蓋網路資通安全的需求，NRC 依據上述需求審查。
- NRC 於 2000 年 5 月核准 TXS 平台專題報告之安全評估報告，安裝於 RPS/ESPS 系統之應用軟體，亦於幾年後由相同的廠家發展完成，安裝於不同之系統；適用的資通安全法規指引於 2006 年 1 月才發佈，因此 NRC 於審查 TXS 平台專題報告時，並未特別審查資通安全，儘管如此，於 TXS 平台發展階段時，其安全措施已經到位，SER 評估 TXS 平台及 RPS/ESPS 系統應用軟體可符合資通安全規定。
- GDC 21 要求保護系統須設計成安全功能之執行具有高可靠度，預防網路安全攻擊，必須考慮維持安全功能之高可靠度。SER 3.6 節說明 RPS/ESPS 數位系統從設計至系統測試符合資通安全規定，基於以上結果符合 RG 1.152 2.1~2.5 節相關規定，NRC 認爲 Oconee 電廠於網路攻擊時提供安全功能高可靠度之系統設計，符合 GDC 21 之要求。

9. ISG-02 多樣性與深度防禦審查

- RPS 系統四個控道都採用同一儀控系統平台之設計，多樣性與深度防禦安全分析顯示某些安全功能可能受共因模式失效的影響。如果依據 FSAR 第 15 章之分析結果，顯示 RPS 保護動作需於 30 分鐘內動作，以符合 BTP 7-19 要求，因此應增設一多樣性自動備用系統，用以啓動因爲共因模式失效影響之安全功能，此系統可爲非安全系統，但須具有如 ATWS 系統之加強型品質。
- ISG-02 多樣性與深度防禦，D3 議題共包括七個 NRC 立場：

(1) 立場一、足夠的多樣性：

數位儀控系統可能因軟體共因失效而喪失安全系統功能，NRC 認爲軟體共因失效對於核電廠安全的影響已超出設計基準，須保護 RPS 系統免受軟體共因失效的威脅，因此要求持照者或系統供應商應提出多樣性與深度防禦安全分析，並符合 NUREG/CR-6303“Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems”及 NUREG-0800 BTP HICB-19“Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems”。

持照者必須具體指出必要的備份系統與運轉員手動操作，NRC 評估後認爲 Oconee 電廠已詳細評估多樣性與深度防禦，電廠預計安裝 DLPIAS 及 DHPIAS 注水系統，於 RCS 低壓力時引動低壓或高壓注水，緩和大小破口爐水喪失事件，電廠亦提供自動系統 AMSAC (預期暫態未急停緩和系統致動電路) 及 DSS (多樣性急停系統)，降低 ATWS 風險，

(2) 立場二、運轉員手動操作：

反應器保護系統若因軟體共因失效導致安全功能喪失，由於電廠已符合 BTP 7-19 之接受準則，運轉員在 30 分鐘內不須介入手動操作；持照者應在控制室提供足夠的資訊與控制，這些控制系統須與 RPS 系統不相關而且獨立分開，才能不受共因失效影響。

Oconee 電廠於控制棒彈出事故與小破口爐水喪失事故時，運轉員手動操作可以有效減緩事故之嚴重性。控制棒彈出事故 (Control Rod Ejection Accident)，運轉員一小時內手動引動反應器廠房冷卻系統與噴灑系統 (RBCS & RBS)；小破口爐水喪失事故 (SBLOCA) 時，於喪失次冷卻水兩分鐘內手動急停反應器，並於一小時內手動引動 RBCS 與 RBS 系統。

兩分鐘內手動急停反應器之手動操作，與 DI&C-ISG-02 準則要求運轉員在 30 分鐘內不須介入手動操作不符合，而這項操作之由來乃是依據 1979 年三浬島事件之經驗回饋，發現某些爐心暫態下無法跳脫反應爐冷卻水泵，因此要求運轉員必須手動急停反應器並跳脫 RCP，Oconee 電廠 30 多年來也一直訓練運轉員如此操作，NRC 於 2008 年 5 月稽查電廠之運轉員訓練，認定運轉員操作熟練，因此兩分鐘內之手動急停反應器操作，雖成爲 DI&C-ISG-02 準則的例外項目但可被接受。

(3) 立場三、挑戰 BTP 7-19 立場 4：

BTP 7-19 立場 4 重新闡述爲：控制室應配置一組顯示與手動控制系統，以利運轉員操作反應度控制、一次系統爐心冷卻與熱移除、圍阻體隔離與完整性等電廠關鍵性安全功能。如上節所述，這組顯示與控制系統須與 RPS 系統獨立分隔，例如使用硬接線，若軟體元件受到相同的軟體共因失效影響而喪失自動功能時，仍可提供給運轉員手動操作之備用系統。

Oconee 電廠主控制室有一組顯示與控制設備，不受 RPS/ESPS 系統軟體共因失效之影響，提供運轉員手動啓動及控制電廠關鍵安全功能。

(4) 立場四、共因失效的影響：

NRC 認爲造成電廠安全系統功能失效的可能性很多，即使是最輕微的失效模式仍可能耗費運轉員時間去執行判斷及反應，因此 NRC 要求軟體共因失效的 FMEA 失效模式分析應包含部份啓動 (partial actuation)、啓動失效(failure to actuate) 及全部啓動失效 (total failure to actuate)。

可被偵測到的失效或故障都可以提出解決辦法，但是，無法偵測的失效可能會阻礙系統啓動，因此，無法偵測的故障更應受到關注。Oconee 電廠已將 RPS/ESPS 系統 FMEA 失效模式分析列表，NRC 於 SER 3.2.2.7 節評估，同意 Oconee 電廠可符合本立場。

(5) 立場五、共因失效的適用性：

NRC 認爲安全系統設計須具備多樣性與可測試性，則可以減少共因失效對系統的影響。保護系統需存在足夠的多樣性，且系統每一項輸入、內外部初始狀態及訊號可能的組合都應具有可測試性。

NRC 評估 Oconee 電廠 RPS/ESPS 數位系統，認爲多樣性不足，且系統太複雜無法符合可測試性，不能降低共因失效之影響，因此 Oconee 電廠額外增列 DLPIAS / DHPIAS 多樣性系統，這兩個系統的詳細說明列於 SER 3.9.3/3.9.4 節。

(6) 立場六、防禦層級：

NRC 表示有些電廠使用單一數位儀控系統平台，結合 RTS 與 ESFAS 功能，當合併衍生出新的共因失效模式時，應採用本文立場一、二提出說明。NRC 建立 D3 評估接受指引，並指出四個防禦層級：控制系統、反應器跳脫系統 (RTS)、特殊安全設施啓動系統 (ESFAS) 、監測與指示。

控制系統爲電廠正常運轉時操作之非安全設備，防止反應爐暫態趨向於不安全狀態；反應器跳脫系統利用安全設備快速降低反應度；特殊安全設施啓動系統包含數種安全設備，以移除熱能或協助維持燃料包覆、反應器容器、圍阻體等三種屏蔽之完體性，避免放射性物質外洩；運轉員處理反應爐事故所需之監測與指示設備，包括感測器、顯示器、數據傳輸系統以及手動控制。

NRC 評估 Oconee 電廠數位系統整合 RPS 與 ESFAS 功能，RTS 與 ESFAS 兩層防禦措施已結合爲一，依據 SER 3.9.1.1、3.9.1.2 節敘述 Oconee 電廠已符合立場一、二之要求，因此 NRC 認爲亦可符合四層防禦措施之立場。

(7) 立場七、單一故障：

數位系統假設的軟體共因失效可能使安全功能失效，因此系統設計應包括多樣化的方式來執行相同或不同的功能，以減輕事故的嚴重性。若系統在事件狀況下，仍有一定的品質來執行這項功能，則可由非安全系統執行。NRC 評估 Oconee 電廠 RPS/ESPS 系統設計包含這些多樣化的方式，可符合立場七。

10. 多樣性系統

(1) AMSAC 與 DSS 系統

- Oconee 電廠提供 AMSAC (ATWS Mitigation System Actuation Circuitry) 及 DSS (Diverse scram system) 系統降低 ATWS 事故嚴重性，並符合 10 CFR 50.62 “Requirements for Reduction of Risk from Anticipated Transients without Scram Events for Light Water Cooled Nuclear Power Plants.” 之要求。SRP 7.8 節 “Diverse Instrumentation and Control System” 亦提及 SRP 針對多樣性啓動系統可接受的標準。
- AMSAC 及 DSS 系統共享軟硬體，包含兩個 PLC 可程式邏輯控制器及 UPS 不斷電系統，PLC 型號爲 SY/MAX-400 由廠家 Square D 製造，使用 Square D 獨有之階梯程式軟體，確保這系統之獨立性，不會受 RPS/ESPS 系統軟硬體共因模式失效或電源喪失之影響，符合 10 CFR 50.62 之要求。AMSAC 及 DSS 系統於 Oconee 變更案並未修改亦非新增，因此不需要針對這兩個系統進行審查或評估。

(2) DLPIAS 系統

- DLPIAS 低壓注水系統爲必要的設備，以符合多樣性與深度防禦安全分析，與 SRP 7.8 節接受準則。
- 同時發生小破口爐水喪失事件與 ESFAS 數位系統軟體共因失效，反應爐冷卻水低壓力時引動 DLPIAS，提供反應爐低壓力高容量的水源。故障模式如同於 FMEA 分析中描述的，並依 FAT 進行測試，以驗證單一失效之符合性。

- DLPIAS 系統不使用任何軟體，設計包含安全及非安全組件，類比電驛電源爲非安全系統，低壓注水啓動電路與 DLPIAS 開關之隔離則爲安全設備，以電氣隔離器分開安全及非安全組件。
- DLPIAS 系統包含三組傳統類比電器，採三選二跳脫邏輯，若任一壓力傳送器或邏輯電路故障則變成二選二邏輯。DLPIAS 系統有正常與旁通二種運轉模式，另有手動按鈕來超控 (Override) 系統。

(3) DHPIAS 系統

- DHPIAS 高壓注水系統則非原始即被要求之必要設計，乃爲回應 ISG-02 軟體共因模式失效之考慮而安裝。
- 同時發生小破口爐水喪失事件與 ESFAS 數位系統軟體共因失效，反應爐冷卻水低壓力時引動 DhPIAS，提供反應爐低壓力高容量的水源。故障模式如同於 FMEA 分析中描述的，並依 FAT 進行測試，以驗證單一失效之符合性。
- DHPIAS 系統不使用任何軟體，設計包含安全及非安全組件，類比電驛電源爲非安全系統，高壓注水啓動電路與 DHPIAS 開關之隔離則爲安全設備，以電氣隔離器分開安全及非安全組件。
- DHPIAS 系統包含三組傳統類比電器，採三選二跳脫邏輯，若任一壓力傳送器或邏輯電路故障則變成二選二邏輯。DHPIAS 系統有正常與旁通二種運轉模式，另有手動按鈕來超控 (Override) 系統。

三、 國際現況

1. 芬蘭核能安全管制單位 STUK 考慮安全與非安全兩個平台均故障的狀況，因此需要非電腦系統爲額外的備用系統；待澄清解決的問題：①提昇安全系統與非安全系統間的獨立性，②限制從安全系統到控制系統的單方向通訊；TVO 公司已同意相對應的架構文件，目前正由 STUK 審查中。
2. 英國衛生與安全部認爲兩套數位系統仍不符合多樣性，因此初始安全分析 (PSAR) 計算必須考慮共因模式失效，而且需要非電腦系統爲備用系統；待澄清解決的問題：①限制從安全系統到控制系統的單方向通訊，②由於安全分析電腦系統的可靠度不足，因此需要非電腦備用系統，③控制室手動控制與分類顯示；英國衛生與安全部聲明初始的提案建議看起來是合理可行的，預料經過適當的修改後將可被接受。
3. 法國擁有 25 年數位儀控系統的運轉經驗，依據這個基礎，核能安全管制單位認爲使用 TXS 與 SPPA T2000 兩套平台可符合多樣性，因此不需要非電腦的後備系統，但仍須提交 T2000 的驗證基礎給管制單位審查。

四、 法規導引文件

安全系統數位化變更申照程序，最重要的是了解法規的需求。法規標準與重要的法律文件包括聯邦法規與 NRC 法規指引，聯邦法規爲法律要求，需完全符合；NRC 法規指引則定義符合法規的可接受方式，例如定義法規特定的要求、或認可的工業標準 (也可以有例外或增列條款)，而且允許替代方案 (替代方案需要 NRC 更多更詳細的審查)。

Oconee 電廠設計準則乃依據 1967 年 7 月 11 日發佈之 10 CFR 50 一般設計準則，NRC 以 10 CFR 50 以及三浬島行動計畫待辦事項當作審查之適用準則，並依據 RG 1.22、RG 1.47…等 18 個法規指引評估 RPS/ESPS 數位儀控系統。標準審查計畫 (Standard Review Plan) 敘述 NRC 內部審查的責任與審查的方法，並建立審查的結果與發現；針對反應器跳脫系統、特殊安全設施起動系統、多樣性引動系統 (例如 Oconee 電廠 RPS/ESPS 數位系統)，審查之法規需求與接受準則已明列於標準審查計畫 (NUREG-0800 第七章表 7-1) 中，分部技術立場 (Branch Technical Position) 說明審查期間被提出的技術性資料，適用的條文包括 SRP 7.2、7.3、7.8、7.9 節、附錄 7.1-B、7.1-C、7.1-D，與 BTP 7-3、7-9、7-11、7-12、7-14、7-17、7-19、7-21。SRP 與 BTP 提供有用的資訊，但不是法律要求；NUREG 與 NUREG/CR 則是 NRC 研究法規所提供的資訊報告。

IEEE 603-1991 與機械常用之 ASME code 類似，具有法規的地位。依據個別核電廠核准建廠執照的年代，10CFR 50.55a(h)要求核電廠須符合該廠之 Licensing Base(FSAR)或遵循 IEEE Std 279-1971「核電廠保護系統準則」或 IEEE Std 603-1991「核能電廠安全系統準則」（含 1995 錯誤修訂版），其準則說明如下：

- 1971/1/1 之前，符合該廠之 Licensing Base 或 IEEE 603-1991。
- 1971/1/1 ~ 1999/5/13 期間，符合 IEEE 279-1971 或 IEEE 603-1991。
- 1999/5/13 以後，IEEE 603-1991。

1. 法律規章：
   - 10 CFR 50.55a(a)(1) 品質標準
   - 10 CFR 50.55a(h) 保護系統
   - 10 CFR 50.62 ATWS 預期暫態未急停規則
   - 10 CFR 73.54 網路資通安全規則
   - GDC 1 品質標準與紀錄
   - GDC 2 對抗自然現象的保護設計基礎
   - GDC 4 環境與飛射物設計基礎
   - GDC 13 儀器控制
   - GDC 19 控制室
   - GDC 20 保護系統功能
   - GDC 21 保護系統可靠度與可測試性
   - GDC 22 保護系統的獨立性
   - GDC 23 保護系統失效模式
   - GDC 24 保護系統與控制系統之分隔
   - GDC 25 反應度控制異常之保護系統的需求
   - GDC 29 預期運轉操作事件的保護
2. 系統法規指引：
   - RG 1.22 保護系統引動功能定期測試
   - RG 1.28 設計與建造之品保計畫需求
   - RG 1.47 核電廠安全系統旁路與不可用狀態顯示
   - RG 1.53 核電廠保護系統單一故障接受準則之應用
   - RG 1.62 保護措施手動引動
   - RG 1.75 電氣系統實體上之獨立性
   - RG 1.89 對核電廠安全的重要電氣設備之環境驗證
   - RG 1.105 安全相關儀器的設定點
   - RG 1.118 電源與保護系統定期測試
3. 數位硬體法規指引：
   - RG 1.152 核電廠安全系統中的數位電腦之接受準則
   - RG 1.153 安全系統的電源與儀器控制之接受準則

- RG 1.180 安全儀控系統電磁干擾評估導則
- RG 1.209 核電廠數位電腦安全儀控系統環境驗證導則

4. 數位軟體法規指引：
   - RG 1.168 核電廠安全系統之數位電腦軟體驗證、確認、審查與稽核
   - RG 1.169 核電廠安全系統之數位電腦軟體構型管理計畫
   - RG 1.170 核電廠安全系統之數位電腦軟體測試文件
   - RG 1.171 核電廠安全系統之數位電腦軟體單元測試
   - RG 1.172 核電廠安全系統之數位電腦軟體需求規範
   - RG 1.173 核電廠安全系統之數位電腦軟體生命週期發展程序
   - RG 5.71 核能工業之網路資通安全計畫

5. 法規指引認可之工業標準：

硬體

RG 1.53	IEEE 379-2000 核電廠安全系統單一故障接受準則之應用
RG 1.75	IEEE 384-1992 1E 設備與電路的獨立性之接受標準
RG 1.89	IEEE 323-1974 核電廠 1E 設備 IEEE 標準驗證
RG 1.105	Part 1 of ISA-S67.04-1994 核能安全相關儀器設定值
RG 1.118	IEEE 338-1987 核電廠安全系統定期偵測試驗接受準則
RG 1.153	IEEE 603-1991 核電廠安全系統接受準則

軟體

RG 1.168	IEEE 1012-1998 軟體驗證與測試
	IEEE 1028-1997 軟體審查與稽查
RG 1.169	IEEE 828-1990 軟體構型管理計畫
	IEEE 1042-1987 軟體構型管理導則
RG 1.170	IEEE 829-1983 軟體測試文件
RG 1.171	IEEE 1008-1987 軟體單元測試
RG 1.172	IEEE 830-1993 針對軟體需求規範，IEEE 建議執行項目
RG 1.173	IEEE 1074-1995 軟體生命週期發展程序

設備驗證

RG 1.180	IEEE 1050-1996 電廠儀控設備接地準則
	MIL-STD-461E, 1999 控制次系統與設備之電磁干擾特性的需求
	IEC 61000 (Parts 3, 4 and 6) 電磁干擾耐受度

IEEE C62.41-1991 針對低壓交流電路中之突波，IEEE 建議執行項目

IEEE C62.45-1992 連接低壓交流電路之設備突波測試導則

RG 1.209　IEEE 323-2003 核電廠 1E 設備驗證標準系統需求

RG 1.152　IEEE 7-4.3.2-2003 核電廠安全系統之數位電腦接受標準

因應 ISG 臨時工作導則增列的要求，法規面仍待挑戰的領域：第一項爲網路資通安全應注重程序導向而非結果導向，第二項爲通訊獨立性的接受標準仍不明確。

6. 標準審查計畫 (SRP)
   - Section 7.0 儀器控制審查程序
   - Appendix 7.0-A 數位儀控審查程序
   - Section 7.1 儀器控制介紹
   - Appendix 7.1-A 重要安全儀控系統接受標準與導則
   - Appendix 7.1-C IEEE 603 符合性之評估導則
   - Appendix 7.1-D IEEE 7-4.3.2 符合性之評估導則
   - Section 7.2 反應器跳脫系統
   - Section 7.3 重要安全保護系統
   - Section 7.7 控制系統
   - Section 7.8 多樣性儀控系統
   - Section 7.9 資料通訊系統
7. 分部技術立場 (BTP)
   - BTP 7-8 RG 1.22 應用導則
   - BTP 7-11 隔離裝置之應用與驗證導則
   - BTP 7-12 儀器設定值之建立與維持導則
   - BTP 7-14 數位電腦儀控系統軟體審查導則
   - BTP 7-17 自我測試與偵測試驗規定導則
   - BTP 7-18 數位電腦儀控系統 PLC 可程式邏輯控制器使用導則
   - BTP 7-19 數位電腦儀控系統多樣性與深度防禦評估導則
   - BTP 7-21 數位電腦即時性能導則

五、 其他安全儀控數位平台

1. 英維思公司 Tricon 平台：

Tricon 平台專題報告於 2001 年經 NRC 核准，但尚未有主要的安全保護系統更新計畫經 NRC 核准，於 2009 年九月重新提交專題報告的修訂版本給 NRC 審查。

Diablo Canyon 核電廠屬 Pacific Gas & Electric 公司所有，共有兩部西屋 PWR 機組，裝置容量各爲 1120MW，商轉日期分別 1985 年 5 月 7 日、1986 年 3 月 13 日。Diablo Canyon 核電廠於 2009 年十月告知 NRC 將使用 Tricon 平台更新 RPS/ESFAS 安全保護系統，NRC 於 2010 年五月開會決定 Diablo Canyon 電廠之設計變更申請需參照核准後的 Tricon 平台專題報告，因此 Diablo Canyon 電廠已將變更申請延後至 2011 年五月。

Tricon 平台目前待解決的議題，包括 ①缺少應用軟體開發程序的專題報告，②無法定義計畫特定的生命週期與管控，③欠缺與計畫特定相關的申照核准經驗，④不具有多樣性與深度防禦之能力與方法，⑤尚未執行模擬測試工具的申照作業等。

2. 西屋公司 Common Q 平台：

Common Q 平台專題報告於 2000 年經 NRC 核准，但尚未有主要的安全保護系統更新計畫經 NRC 核准，西屋公司將重新提交專題報告的修訂版本給 NRC 審查。NRC 於 2003 年核准 Common Q 之軟體計畫手冊，同年亦核准 Palo Verde 核電廠使用 Common Q 進行爐心保護計算器 (Core Protection Calculator，CPC 系統爲反應器保護系統之一部份) 之數位化更新，但於 2005 年 8 月 22 日 Palo Verde 電廠#2 號機發現 Common-Q 軟體錯誤，造成 RPS 系統不可用，依據運轉技術規範機組停機。

NRC 於 2009 年稽核報告中發現 AP-1000 軟體開發程序有瑕疵，西屋公司將重新提交軟體計畫手冊的修訂版本給 NRC 審查。Common Q 平台目前待解決的議題，包括 ①缺少 NRC 核准的通用方法去執行多樣性與深度防禦分析，②尚未執行模擬測試工具的申照作業。

3. Mitsubishi MELTAC 平台

MELTAC 平台專題報告與軟體計畫手冊於 2007 年提交給 NRC 審查，但 NRC 於 2009 年稽核報告中發現 AP-1000 軟體開發程序有瑕疵，NRC 將審查限制在 ABWR 之設計驗證，審查過程發現有關 IEEE 標準的符合性、測試的獨立性、使用的控制架構等問題。MELTAC 平台目前待解決的議題，包括 ①缺少 NRC 核准的通用方法去執行多樣性與深度防禦分析，②尚未執行模擬測試工具的申照作業。

4. Rolls Royce SPINLINE 3 平台

SPINLINE 3 平台專題報告於 2009 年提交給 NRC 審查，平台專題報告中已包括軟體計畫手冊，NRC 於 2010 年提出九個審查問題。SPINLINE 3 平台目前待解決的議題，包括 ①缺少 NRC 核准的通用方法去執行多樣性與深度防禦分析，②尚未執行模擬測試工具的申照作業。

5. DRS +32 平台

DRS +32 平台專題報告尚未提交給 NRC 審查，因爲仍然存在技術性問題，NRC 於 2009 年 11 月開會建議，DRS +32 平台之專題報告獲准的機率很低。

6. Doosan HFC-6000 平台

HFC-6000 平台專題報告於 2008 年提交給 NRC 審查，NRC 於 2010 年要求額外的資料說明，並將執行審查稽核作業。

7. 西屋進步型邏輯系統 (ALS) 平台

2009 年 NRC 核准 Wolf Creek 主蒸汽與隔離系統 (MSFIS, Main Steam and Feed Isolation System) 使用 ALS FPGA (Field Programmable Gate Array) 平台變更申請，Diablo Canyon 核電廠於 2010 年告知 NRC 將使用 ALS 平台更新 RPS/ESFAS 安全保護系統，NRC 於 2010 年五月開會決定 Diablo Canyon 電廠之設計變更申請需參照核准後的 ALS 平台專題報告，目前 ALS 平台之專題報告尚未提交給 NRC 審查，因此 Diablo Canyon 電廠已將變更申請延後至 2011 年五月。

肆、建議事項

一、 本公司核三廠 7300 電子卡片、SSPS、ESF、SSILS 等安全儀控系統，預計於民國 106、107 年更新爲數位化系統，由於原能會依循美國核管會法規，基於 Oconee 電廠申照過程冗長，本公司應及早因應。爲了避免國外廠商得標後，原能會審照時間過長或規範不符原能會要求等不確定性，造成合約執行上之困擾，擬建議核三廠分成兩階段辦理：第一階段先成立 SSILS 等安全儀控系統 DCR 改善案，並完成 DCR 文件中之系統規範、安全評估、失效模式分析、適用法規等 (必要時請國內研究機構協助完成)，完成之申照需求文件先送至原能會審查，待原能會核准後，再依據核准內容與原能會要求事項，訂定採購規範發包與施工。

二、 目前 NRC 已核准之安全儀控數位平台專題報告包括 AREVA TELEPERM XS、英維思公司 Tricon、西屋公司 Common Q，而已提交專題報告至 NRC 審查者有 Mitsubishi MELTAC、Rolls Royce SPINLINE 3、Doosan HFC-6000；目前只有 AREVA TELEPERM XS 實際應用於核能電廠反應器保護系統之更新，Common Q 則使用於 CPC 計算器，其餘平台尚未獲得 NRC 核准使用於核電廠反應器保護系統之運轉實蹟，本公司應持續關注各項平台申照之進度，以利核三廠安全儀控數位化更新時之選擇參考。

三、 NRC 審查 Oconee 變更修改案，提出之疑慮包括：多樣性與深度防禦、訊號間之雙向溝通、軟體計畫手冊、TXS 平台 Oconee 電廠特定修改的部份、軟體驗證與確認 (V&V)、軟體模擬驗證測試工具等，針對這些疑慮，核三廠未來於制定規範時應列爲參考重點，並應針對 ISG 之符合度列表評估送交原能會審查。

四、 美國國內航空對於境內班機行李托運需收取美金 25 元之托運費，來回兩趟至少須支付 50 元美金，這筆費用目前無法報銷，而出國人員有 120 元美金之返國公務資料運費，由於目前多數公務資料已轉成光碟或電子檔，使用此項費用之機會已不大，建議行李托運費用可以從此項費用下報支。

伍、縮寫

AMSAC = ATWS Mitigation System Actuation Circuitry

ATWS = Anticipated transients without scram

DHPIAS = Diverse High Pressure Injection Actuation System

DLPIAS = Diverse Low Pressure Injection Actuation System

DPRAM = Dual Port Random Access Memory

DSS = Diverse scram system

ESF = Engineered Safety Feature

ESFAS = Engineered Safety Feature Actuation System

ESPS = Engineered Safeguards Protection System

FPGA = Field Programmable Gate Array

GDC = General Design Criterion

GSM = Graphical Service Monitor

GW = Gateway

HW = Hardware

ISG = Interim Staff Guidance

LAR = License Amendment Request

MSFIS = Main Steam and Feed Isolation System

MSI = Monitoring & Service Interface

NI = Nuclear Instrumentation

NRC = Nuclear Regulatory Commission

NRC-NRO = NRC New Reactor Organization

NRC-NRR = NRC Nuclear Reactor Regulation (Operating Reactors)

PLD = Programmable Logic Device

RCPPM = Reactor Coolant Pump Power Monitor

RPS = Reactor Protection system

SAS = Safety Automation System

SBLOCA = Small Break Loss of Coolant Accident

SICS = Safety Information and Control System

SIVAT = Simulation Validation Test Tool

SPACE = Specification and Coding Environment Engineering Tool

SPM = Software Program Manual

SRP = Standard Review Plan

SSILS = Solid State Interposing Logic System

SSPS = Solid State Protection System

TWG = Task Working Group

V&V = Verification and Validation

陸、參考資料

1. Oconee, Units 1, 2 & 3, Issuance of Amendment Nos. 366, 368, and 367, Reactor Protective System and Engineered Safeguard Protection System Digital Upgrade. January 28, 2010 (ADAMS Accession No. ML100220016).
2. Duke Energy Carolinas, LLC Oconee Nuclear Station, Units 1, 2, and 3, Docket Numbers 50-269, 50-270, and 50-287, License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change (TSC) Number 2007-09, Supplement 2, April 29,2008 (ADAMS Accession No. ML081260167).
3. Duke Energy Carolinas, LLC Oconee Nuclear Station, Units 1, 2, and 3, Docket Numbers 50-269,50-270, and 50-287, License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change (TSC) Number 2007-09, Supplement 3, May 15, 2008 (ADAMS Accession No. ML081430003).
4. Duke Energy Carolinas, LLC Oconee Nuclear Station, Units 1, 2, and 3, Docket Numbers 50-269,50-270, and 50-287, License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change (TSC) Number 2007-09, Supplement 4, May 28,2008 (ADAMS Accession No. ML081550145).
5. Acceptance Review of January 31,2008, License Amendment Request (LAR) for a Digital Upgrade to the Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) at Oconee Nuclear Station, Units 1, 2, and 3 (OCONEE) (TAC Nos. MD7999, MD8000, AND MD8001), April 24, 2008 (ADAMS Accession No. ML081070521).