行政院及所屬各機關出國報告
（出國類別：實習　）

核能儀控系統數位化更新驗証測試技術研習

服務機關：台灣電力公司核能發電處
出 國 人　職　　稱：十一等核工監
　　姓　　名：柳克和
出國地區：美國
出國期間：自92年12月16日至92年12月27日
報告日期：93年1月20日

行政院及所屬各機關出國報告提要

出國報告名稱：核能儀控系統數位化更新驗証測試技術研習

頁數：18 附件: □有■否

出國計畫主辦機關/聯絡人/電話

台灣電力公司／陳德隆／（02）23667685

出國人員姓名/服務機關/單位/職稱/電話

柳克和/台灣電力公司/核能發電處/核工監/(02)23666595

出國類別：□1 考察□2 進修□3 研究■4 實習□5 其他

出國期間：自92年12月16日至12月27日　　出國地區：美國

報告日期：93 年 1 月 20 日

分類號/目

關鍵詞：儀控設備的確認與驗證

內容摘要：（二百至三百字）

1. 國內核能電廠運轉已逾十餘年，營運中的核能電廠之類比式儀控系統漸趨老舊，且備品取得不易，由於數位化技術的進步，於工業上的應用已相當成熟，其設計彈性較大，又可進行自我測試、診斷及自動校正等功能，且數位化儀控之通訊介面較易標準化，承建核四廠核島儀控部分的奇異公司採用數位儀控設計建造，設計過程需求，包括硬體/軟體發展與整合、驗証與確認（V&V）等，由於奇異公司具有上述之技術與經驗。
2. 大致來說，硬體設計與採購程序完全依照 GE 的 Engineering Operating 程序進行.這樣的程序包括概括設計控制與文件， 確認，測試，設計審核，紀錄與設計變更管制.。更進一步來說，對 PRNM 而言，除一般工程程序外還包含一些特殊，額外的硬體定義及統合需求.。
3. 依據軟體完成所有的工作及最後基準的審查和結案，最後軟體是安裝在擷取管制圖書館帳戶，包括所有編輯，聯結，組合或其他指令必須清楚地再製設計編碼，對於產品設備實際上安裝在 EPROMs.

目　　錄

一、目的：

國內核能電廠運轉已逾十餘年，營運中的核能電廠之類比式儀控系統漸趨老舊，且備品取得不易，由於數位化技術的進步，於工業上的應用已相當成熟，其設計彈性較大，又可進行自我測試、診斷及自動校正等功能，且數位化儀控之通訊介面較易標準化，承建核四廠核島儀控部分的奇異公司採用數位儀控設計建造，設計過程需求，包括硬體/軟體發展與整合、驗証與確認（V&V）等，由於奇異公司具有上述之技術與經驗。

大致來說，硬體設計與採購程序完全依照 GE 的 Engineering Operating 程序進行.這樣的程序包括概括設計控制與文件， 確認，測試，設計審核，紀錄與設計變更管制.。更深一步來說，對 PRNM 而言，除一般工程程序外還包含一些特殊，額外的硬體定義及統合需求.。

依據軟體完成所有的工作及最後基準的審查和結案，最後軟體是安裝在擷取管制圖書館帳戶，包括所有編輯，聯結，組合或其他指令必須清楚地再製設計編碼，實際上係安裝在 EPROMs 產品.

二、過程：

(一) 行程：

時　間	地　點	工作摘要
12/16~12/16	台北→舊金山→聖荷西	往程
12/17~12/25	奇異公司	研習核能儀控系統數位

化更新驗証測試技術

12/26~12/27　聖荷西→舊金山→台北　返程

(二) 訪問奇異公司：

1. 奇異公司(NYSE:GE)是一個結合科技與製造並朝向多元性發展的世界級企業集團，在全世界一百多個國家設有分公司，同時擁有超過三十萬名的員工。奇異電力系統的發電機組在大小電廠裡二十四小時不間斷的工作著。追求發電機組的極致效率、強化電力供應的穩定程度，是奇異電力系統在同業間始終保持領先地位的重要依據。目前在聖荷西市的奇異公司著重在核能部門，這裡有核能訓練中心，NUMAC 儀控設備開發研製中心，以及核四廠核島部分的設計部門，核四廠模擬器的設計，組裝和測試中心。

2. 因此次至奇異公司研習目標為核能電廠儀控設備行數位化改善時，有關數位軟體的確認與驗證執行，以保証經過設備的更新仍可確保機組的安全與可靠。目前核一廠已完成 TIP,WRNMS,RMS 等系統，核四廠安裝相同之設備，此為奇異公司之產品，故研習期間至該公司研製 NUMAC 工廠瞭解 PRNMS 並討論核電廠有關系統數位化之架構及設備，並瞭解該系統執行數位軟體的確認與驗證測試之現況。

三、內容：

(一) 儀控設備軟體品保計畫

USNRC 接受 GE 可以利用 NUMCAC PRNM 計畫來執行 GE 的品保方案。這方案必須符合下列條件

-10 CFR 50 Appendix
- ANSI/ ASME NQA-1
- ISO 9001

大致來說，硬體設計與採購程序完全依照 GE 的 Engineering Operating 程序進行.這樣的程序包括概括設計控制與文件， 確認，測試，設計審核，紀錄與設計變更管制.。更深一步來說，對 PRNM 而言，除一般工程程序外還包含一些特殊，額外的硬體定義及統合需求.。

特殊的硬體文件，使用者手冊與維護要求在操作和維護手冊都有說明。

(二) 儀控設備軟體確認與驗證

PRNMS 軟體係採用在先前經 USNRC 審查過 NEDO-31439-A(NUMAC-WRNMS)及最近電廠規範用於 NUMAC Leak Detection Monitor and Reactor Building Vents Radiation Monitor 的確認與驗證計畫（Verification & Validation Program）。本計畫特別論及 USNRC RG 1.152 所述例如設計控管，改變控管，文件，紀錄保存，獨立查証，以及軟體開發特別的需求。確認與驗證方法論的基本方法有（1）設計過程分成若干邏輯步驟，每個步驟總結成一項文件。（2）對於設計過程的每一步驟執行獨立的技術確認審查，包括確認的方法及結果。（3）設計步驟分成若干邏輯群組，每一群組組成為下一設計步驟的基準。（4）每一設計步驟群組要保証係遵守該程序，涵蓋技術確認審查，問題獲得解決後，並經獨立程序審查。（5）在硬體執行軟體完整性的最後綜合驗證測試，以及（6）所有步驟

過程都有文件可查。所有的 PRNMS 設計過程分成若干設計小組，每一小組皆是組成後續作業的基準。所有的 PRNMS 軟體包括 386SX 電腦模組作業系統，顯示和自我測試功能皆涵蓋在確認與驗證(V&V)計畫內。

1. 定義及規畫

本設計階段係由定義和以適合實務上作業之上層需求的確認書所組成。包括本部分適用於 the Standard Software V&V program 之確認書。

2. 成果績效的定義

本設計階段涵蓋基本儀器設計，包括硬體設計，硬/軟體的功能配置，使用者的介面設計以及 PRNMS 內部微電腦與外部設備間通訊聯結之通訊協定定義。

3. 高階軟體設計

本設計階段提供高階軟體設計，包括其設計風格和結構，個別軟體組件，軟體模組功能配置和運算的優先次序。PRNMS 硬軟體的基本風格係為基本的 NUMAC 標準設計濃縮版，本設計階段其特點為主要著重於功能分割和配置。

4. 細部設計/編碼/模組測試

本設計階段涵蓋細部軟體設計，編碼和模組測試。在本設計階段包括所有軟體的編碼的審查都做過查証。在此層次的所有模組都測試過，或先前完整的測試都有文件保存。

5. 整體測試/最後設計

本設計階段提供軟體功能，軟體的顯示和硬體的整

體性。如 PRNMS 在 NUMAC 機櫃完成最後測試。採用多競爭者測試，以及在個別軟體程序確認書中准許其他特殊儀器工具。所有必要的設計變更在此設計階段完成。

6. 確認與軟體問題

本設計階段包括正式確認測試。本測試試驗所有有關硬體介面或使用者介面之間的 PRNMS 功能。整體測試則在 PRNMS 機櫃上執行。

7. 設計變更

對於未來設計變更，上述的各階段將會一再的重覆，但是每一階段的範圍可以減少至涵蓋僅已經變更的設計單元。

8. 基準審查

在結束每一設計部分要做上述各節的基準審查。正式文件審查如下：

＊確定所有的設計步驟已完成並且已查証。

＊針對低於定義與畫基準（the Definition and Planning Baseline）的任何基準，確定對批准的過去基準文件已經執行設計和查証。

＊確定查証範圍和方法是合理的，所有的意見都做成文件，查証待決案件已結案。

＊所有的決議都做成文件，包括對使用在下一個設計階段的批准文件（基準文件）。

同樣的，基準審查係檢定並提示文件証明所有的待決案件和問題，所提示文件証明的基礎或假設，對於任何後續設計階段工作，常做為更重要待解決案件的結案

依據。所提示文件証明同時視為，依據在過去設計階段的假設，在目前階段執行任何設計工作一項待決案件。所有的待決案件在後續設計階段前結束，並且審查內容要涵蓋設計階段期間在輸入需求任何變更或確定的問題。

對所有設計階段的首務，要審查確認下列各項：

＊結束過去審查中開出的待決案件，包括狀況的假設，以及確定由於以前的假設而作必需的任何變更的合併。

＊解決在設計工作期間依據以前批准基準所確定的任何問題。

＊確定由於以前的基準的變更而作必需的任何變更的合併，或以前的基準尚未變更的。

（三）儀控設備軟體建構管理

1. 設計期間軟體建構管理

設計過程期間，軟體的儲存在工作電腦帳戶直到它準備成為基準為止，一則是最後版或是一個中間定點。一般將是使用後者的選擇，期望在過程或中間點執行審查，以釐清何版本文件已被審查。

暫時的定點（frozen）或基準軟體安裝在具有擷取管制的電腦帳戶，在原始碼形式加上任何必要的編輯，聯結或組合指令必須清楚地再製一致目的編碼。對設計而言，這些儲存位址仍是"在進行處理中"。

依據軟體完成所有的工作以及最後基準的審查和結

案，最後軟體是安裝在擷取管制圖書館帳戶，包括所有編輯，聯結，組合或其他指令必須清楚地再製設計編碼，對於產品設備實際上安裝在 EPROMs.

此外電腦帳戶儲存的原始檔案，實際目的編碼載入 EPROM 記憶元件，對於影印文件（hard copy documents）和長期性的微縮影片則視作硬體產品。

2. 設計完成後軟體建構管理

EPROM 的製造係藉各種電子方法和批准的手冊所完成。副本文件的定義為其編碼可以下載，但是實際上 EPROM 程式是從控制的電子檔案經過校正電子檔案之副本文件的確認後才能執行。

PRNMS 的所有軟體包裝在 386X 電腦，顯示控制器模組（Z180 或 64180 微電腦處理器）以及 ASP 模組（數位信號處理器）的 EPROM 晶片裡。軟體版本管制是藉 EPROM 零件編號來維持。將藉由硬體零件編號版本附隨體版本，並且要求提供 Engineering Chang Notice。EPROM 的確認是標示在實體元件上。

電廠可經由建立硬體建構程序進行的軟體管控，除非電廠選擇軟體的更新版。

四、心得與建議：

1.軟體驗證與確認(Verification and Validation, SV&V)工作是儀控系統數位化更新工作中相當重要也是一般較為不熟悉的項目，本附錄針對電廠進行儀控系統數位化更新中所必須規劃之工作項目進行探討，以為相關工作之參考。

2.此次出國研習期間雖短，但在出國研習前已陸續研閱一些相關資料，在研習期間之研討驗証，致對儀控系統確認與驗證計畫（Verification & Validation Program）架構有進一步之認識，對日後有關核能電廠儀控系統數位化更新相關業務處理必有所助益。

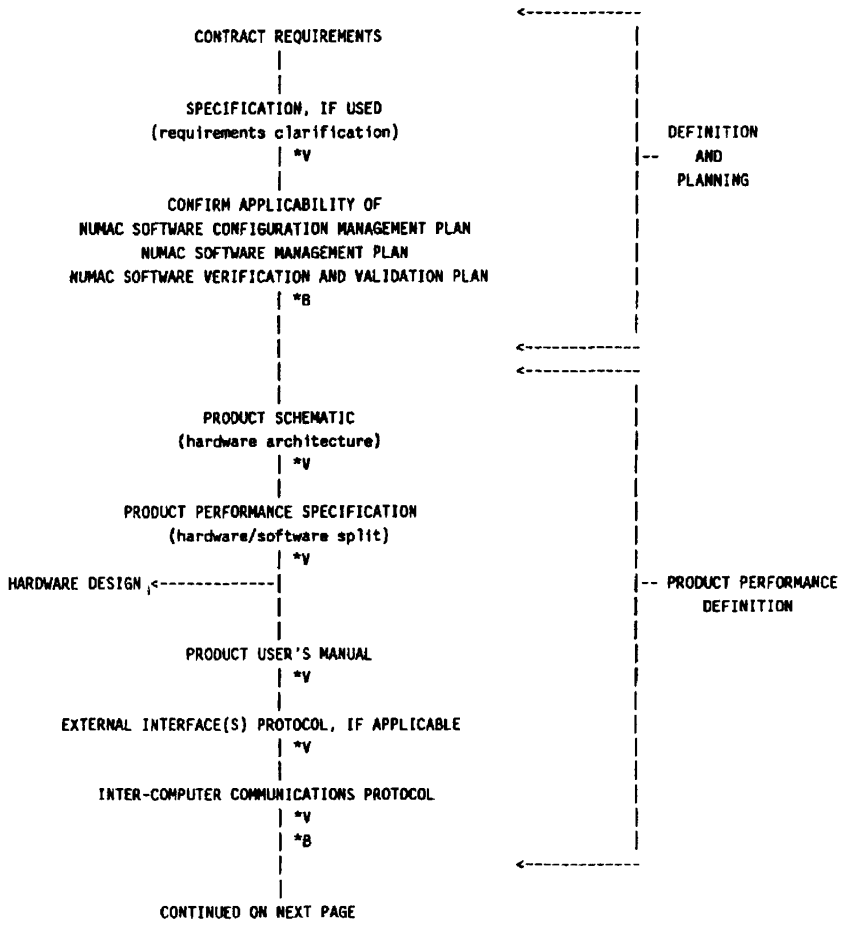


Figure 1
Software Development Tasks

NEO 807 (REV 4/88)

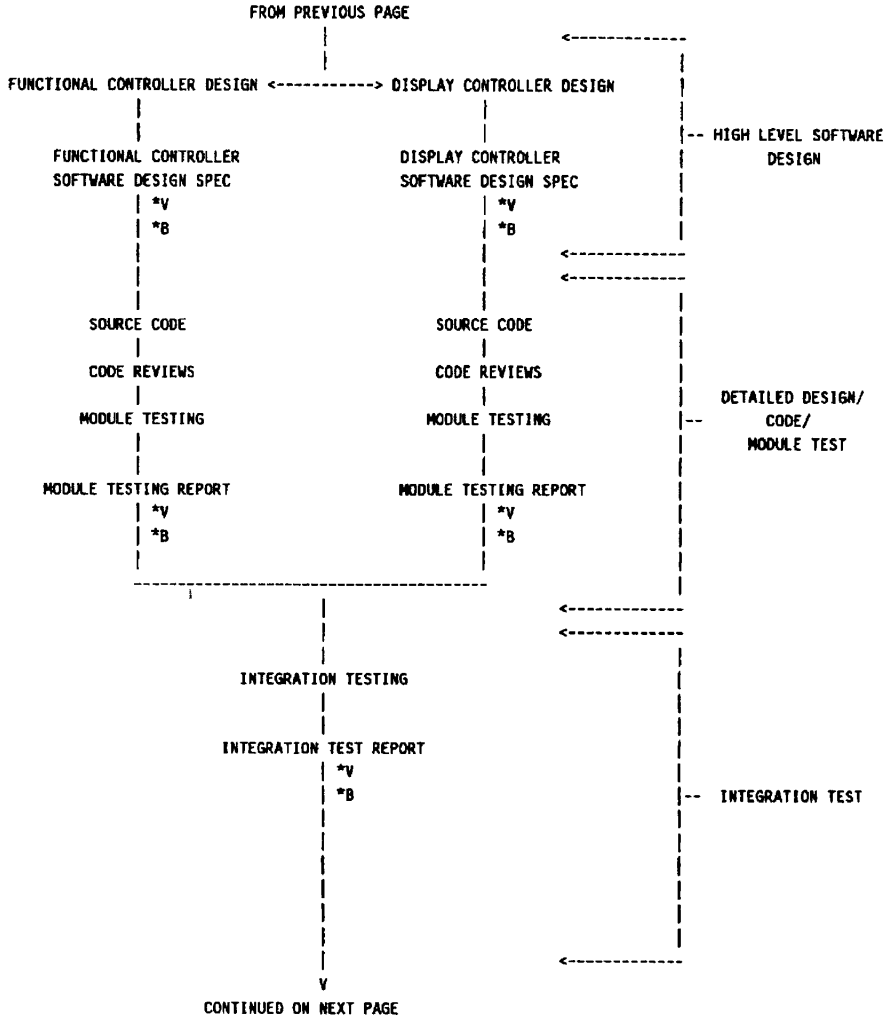
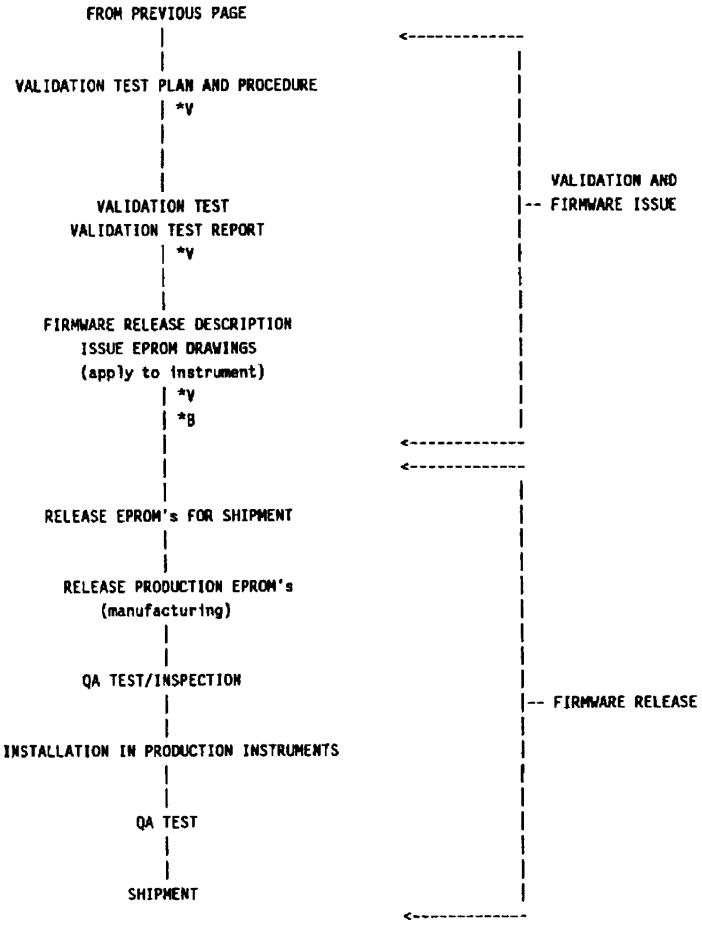


Figure 1 (continued)



NOTES:

V = Design Verification
B = Baseline Review

Figure 1 (continued)

儀控設備軟體之確認與驗證程序計畫

Verification and Validation Process Plan

- Management Process
- Acquisition Process
- Supply process
- Development Process
- Operation Process
- Maintenance Process

1. Management Process
   - Task, which may be employed by any party that manages its respective processes.
   - The management tasks:
     - Prepare the plans for execution of the process
     - initiate the implementation of the plan
     - Monitor the execution of the plan
     - Analyses problems discovered during the execution of the plan
     - Report progress of the processes
     - Ensure products satisfy requirements
     - Assess evaluation results
     - Determine whether a task is complete
     - Check the results for completeness
2. Acquisition Process
   - Begins with the definition of the need to acquired a system, software product, or software service.
   - Continues with the preparation and issuance of a request for proposal, selection of a supplier, and management of the acquisition process through to acceptance of the system, software product, or software service.
   - Plan interface with the supplier, and acquirer, and review the draft system requirements contained in the request for proposal.
   - Acquisition Support Task:
     - Scoping the V&V Effort
       - Define the project V&V software criticality(e.g., safety, security, mission critical, technical complexity)
       - Assign a software integrity level to the system and the software
       - Establish the degree of independence

        - Estimate of the V&V budget
    - Planning the interface between the V&V effort and supplier
        - Plan the V&V schedule for each V&V task.
        - Identify the preliminary list of development processes and products to be evaluated by the V&V processes
        - Describe V&V access rights to proprietary and classified information
    - System requirements review
        - Review the system requirements (e.g., system requirements specification, feasibility study report, business rules description) in the RFP .

3. Supply Process
    - The supply process is initiated by either a decision to prepare to answer an acquirer's request for proposal of by signing and entering into a contract with the acquirer to provide the system, software product, or software service.
    - Supply Process Task:
        - Planning the interface between the V&V effort and supplier
            - Review the supplier development plans and schedules to coordinate the effort with development activities
            - Establish procedures to exchange V&V data and results with the development effort.
        - Contract verification
            - Verify system requirements (from RFP, contract) satisfy and are consistent with user needs.
            - Verify procedures are documented for managing requirement changes and for identify the management hierarchy to address problem.
            - Verify procedures for interface and cooperation among the parties are documented, including ownership, warranty, copyright, and confidentiality.
            - Verify acceptance criteria and procedures are documented in accordance with requirements

4. Development Process
    - The development process contains the activities and tasks of the developer.
    - The process contains the activities for requirements analysis, design, coding, integration, testing, and installation and acceptance relate to software products
    - The V&V activities verify and validate these software products.
    - The V&V activities organized into Concept V&V, Requirements V&V, Design V&V, Implementation V&V, Test V&V, and Installation and Checkout V&V.
    - Activity: Concept V&V
        - Address:

        - System architectural design and system requirements analysis
    - Objectives:
        - Verify the allocation of system requirements, validation the selected solution, and ensure that no false assumptions have been incorporated in the solution
- Task:
    - Concept documentation evaluation
    - Criticality analysis
    - Hardware/Software/User requirements allocation analysis
    - Traceability analysis
    - Hazard analysis
    - Risk analysis

5. Operation Process
    - Address:
        - Operational testing
        - System operation
        - User support
    - Objectives:
        - Evaluate new constraints in system, assess proposed changes and their impact on the software, and evaluate operating procedures for correctness and usability.
6. Maintenance Process
    - Address:
        - Problem and modification analysis
        - Modification implementation
        - Maintenance review/acceptance
        - Migration
        - Software retirement
    - Objectives:
        - Assess proposed changes and their impact on the software, evaluate anomalies that are discovered during operation, assess migration requirements, assess retirement requirements, and re-perform V&V tasks.
    - Task:
        - SVVP revision
        - Proposed change assessment
        - Anomaly evaluation
        - Criticality analysis
        - Migration assessment
        - Retirement assessment

- Hazard analysis
- Risk analysis
- Task iteration

7. Software V&V reporting
   - V&V activity summary reports
   - Task reports
     - Document V&V task results and status
     - Summarize the results of V&V tasks performed for each of the following V&V activities: Acquisition, support, planning, concept, requirements, design, implementation, test, and installation and checkout.
   - Anomaly report
     - Document each anomaly detected by the V&V effort
   - V&V final report
     - Issued at the end of the installation and checkout activity or at the conclusion of the effort
   - Special studies reports
     - Describe any special V&V studies conducted during the software life cycle.
   - Other reports
     - Describe the results of tasks not define in the SVVP.

8. Software V&V Administrative requirements
   - Task Iteration
     - The SVVP shall describe the criteria to determine the extent to which a V&V task shall be repeated
   - Deviation
     - The SVVP shall describe procedures and criteria used to deviate from the Plan.
   - Control Procedures
     - The SVVP shall describe control procedures applied to V&V effort. These procedures shall describe how software products and V&V results shall be configured, protected, and stored
   - Standard, Practices, and Conventions
     - Including internal organizational Standard, Practices, and Policies
   - Anomaly Resolution and Reporting
     - The SVVP shall describe the method of reporting and resolving anomalies.

9. Software V&V Documentation requirements
   - V&V Test documentation
   - SVVP documentation
     - The SVVP shall define the purpose, format, and content of test document: (IEEE Std 829-1983)

- Test Plan
- Test Design
- Test cases
- Test Procedures
- Test Results

10. Software V&V plan outline
    - 1. Purpose
    - 2. Referenced Documents
    - 3. Definitions
    - 4. V&V Overview
    - 4.1 Organization
    - 4.2 Master Schedule
    - 4.3 Software integrity Level Scheme
    - 4.5 Responsibilities
    - 4.6 Tools, Techniques, and Methods
    - 5. V&V Processes
    - 5.1 Process: Management
    - 5.1.1 Activities: Management of V&V
    - 5.2 Process: Acquisition
    - 5.2.1 Activities: Acquisition support of V&V
    - 5.3 Process: Supply
    - 5.3.1 Activities: Planning V&V
    - 5.4 Process: Development V&V
    - 5.4.1 Activities: Concept V&V
    - 5.4.2 Activities: Requirement V&V
    - 5.4.3 Activities: Design V&V
    - 5.4.4 Activities: Implementation V&V
    - 5.4.5 Activities: Test V&V
    - 5.4.6 Activities: Installation and Checkout V&V
    - 5.5 Process: Operation
    - 5.5.1 Activities: Operation V&V
    - 5.6 Process: Maintenance
    - 5.6.1 Activities: Maintenance V&V
    - 6. V&V Report Requirements
    - 7. V&V administrative Requirements
    - 7.1 Anomaly Resolution and Reporting
    - 7.2 Task Iteration
    - 7.3 Deviation
    - 7.4 Control Procedures

- 7.5 Standard, Practices, and Conventions
- 8. V&V Documentation Requirements