行政院原子能委員會

委託研究計畫研究報告

運轉自動化與控制室人因評估技術研發

The Development of Evaluation Technique for Automation Operation and HFE of MCR

計畫編號：**992001INER003**

受委託機關**(**構**)**：私立中原大學

計畫主持人：林久翔

核研所聯絡人：楊智偉

聯絡電話：**03-2654411**

E-mail address：**hsiang@cycu.edu.tw**

報告日期：**99** 年 **11** 月 **24** 日

目　錄

圖　目　錄

表　目　錄

中文摘要

目前核能電廠進步型主控制室已經採用高度自動化與系統資訊整合化的設計，並且使用影像顯示器作為主要的人機介面，讓運轉員透過選單選擇想要監控的系統資訊，但是這種方式可能會造成運轉員花費較多的時間在選擇需要的系統，而這個影響可能會導致緊急事故發生時，運轉員無法及時的做出反應，所以在現行先進型主控制室的設計議題「最小清單」，就是希望找出除了運轉員經常使用的影像顯示器之外，還需要額外設計哪些人機介面用以增加運轉員對核電廠狀態的掌握以及縮短反應時間。本研究探討最小清單的定義與準則，以工作分析法建立最小清單的架構與流程，並且以核電廠的設計基準事故「冷卻水流失事故以及喪失場外電源」模擬情境作為案例探討，對本研究提出建立最小清單之方法進行驗證。期望本論文對於未來核能電廠設計最小清單可做為參考資料。

關鍵字：最小清單、工作分析法、核能電廠、主控制室

Abstract

In a modern control room employing digital technology, the digital instrumentation and controls are automatic and the system is highly-integrated, and video display units become the main human-system interfaces. The operator selects system information which he wants to monitor by selecting from the menu. But this method will let operator to take more time to search and choose what is needed from the system. This effect may make the operator hard to take actions in time during the emergency accident. Therefore, “minimum inventory” becomes an important design issue in a modern control room. Among the displayed information, a minimum set of human-system interfaces can be defined to provide the operator enough information to complete the required tasks. This study looks into the regulatory body and available guidelines about minimum inventory and develops a procedure to establish the minimum set of human-system interfaces. The study then verifies the procedure with a case study in which the step by step usage of the procedure is illustrated using a design based accident “Loss of Coolant Accident with Loss of Off-Site Power”. The results show that the procedure is valid and further research is recommended to consider the approach in the human system interface verification and validation process.

Keyword: Minimum Inventory, Task analysis, Nuclear Power Plant, Main Control Room

壹、計畫緣起與目的

一、研究背景與動機

日趨嚴重的溫室效應使得人們愈來愈重視溫室效應氣體排放等相關議題，而在環境保護、經濟發展、降低成本等諸多因素的考量下，核能發電成為了在眾多限制因素考量下的首選，因此目前已有許多國家再度開始興建核能電廠以供給足夠的電力，台灣目前已有三座核能發電廠正在運轉，其所供給的電力約佔總體發電量的兩成，大部分的供電仍是以火力發電為主，然而火力發電卻會因其碳排放造成嚴重的空氣污染，進而使溫室效應加劇，故目前台灣已積極地興建第四座核電廠來替代火力發電的供電量，然而，歷史上曾經發生的核安事故 (如：三浬島核能電廠事故、車諾比核能電廠事故)所造成的影響也讓人們在使用核能電廠發電時對安全產生疑慮。

在一般的情況下，核能電廠的整體運作皆是由主控制室的運轉人員在掌控，運轉人員透過儀控介面監控、維持電廠的運作狀態，因此，為了要確保核能電廠運轉時的穩定與安全，隨著過去事故發生後的檢討，核能電廠主控制室儀控設備的介面設計已有了相當程度的改善，其設計已被要求需符合人因工程 (Human Factor Engineering, HFE)與人機互動 (Human System Interaction, HSI)的理論、原理與準則，此外，隨著電腦技術的發展，目前新建置核能電廠主控制室中皆是使用數位式的儀控設備，相較於過去傳統的類比式儀控設備，數位式儀控設備期望能透過提供運轉人員較為清楚、且經過整合的系統資訊，以有效地降低運轉人員的工作負荷並維持其情境知覺，進而能大幅減低人為失誤發生之

機率，故自動化儀控設備的使用基本上是有助於提升核能電廠運轉的安全性。而台灣目前在興建的第四座核能電廠之主控制室即是採用自動化的數位式儀控系統，亦即在操作上具有高度資訊化與自動化之特性。

由於系統高度自動化，因此在一般的正常運作狀態 (Normal Condition)下，運轉人員除了依照標準操作程序進行常規性的系統啟動操作外，主要的工作是監視系統資訊，隨時掌握反應爐的運轉狀態，而當系統發生異常事故 (Incidents and Accidents)時，運轉員除了要持續關注系統狀態外，亦要在最短的時間內診斷事故的類型及發生的原因，接著再根據事故類型找出對應的緊急異常操作程序書 (Emergency Operation Procedures, EOPs)，之後便可遵循程序書的處理流程妥善地將事故排除。

雖然國外對於自動化主控制室的使用已行之有年，但無論是在實務或學術領域，其對於數位儀控系統與運轉人員的互動關係上仍持續地探索與驗證，例如：美國核能管制委員會 (Nuclear Regulatory Commission, NRC)自 1999 年美國第一座進步型核電廠建置完成後，便針對主控制室的數位儀控設備與控制相關之人因議題，提出了許多人因相關的設計規範與準則 (如：NUREG/CR 6838、NUREG 0711、NUREG1791 等)，而這些規範與準則皆有助於維持運轉人員在進行儀控系統操作時的作業績效，且使其情境知覺與心智負荷達到最佳的平衡狀態，因此，進步型核電廠在正式運轉之前，若能將儀控系統與運轉人員的配置按照相關規範進行驗證，即能有效確保核電廠未來的運轉安全與績效。

核電廠主控制室乃是一種複雜動態系統，隨著資訊技術的進步，數位儀控 (Digital Instrumentation and Control, DI&C)設備成為核電廠主控室核能運轉系統之設計主流，目前核能電廠主控制室設有大型顯示看板 (Wide Display Panel, WDP)、主操控台(Main Control Console, MCC)與值班主任台 (Shift Supervisor Console, SSC)，而主要的數位式儀控人機介面為影像顯示器(Video Display Units, VDU)。與傳統型核電廠不同，進步型核電廠將以往傳統型主控制室內多達上千個系統經過數位化以及系統整合，將需要的硬體空間從大量固定位置的人機介面轉化為選單式的選項，並且透過影像顯示器讓運轉員獲知電廠運轉資訊、維持電廠正常運作。

傳統型主控制室內每個系統皆有固定的人機介面，儘管需要較多的空間，其優點在於運轉員透過訓練可以快速搜尋並且控制所需的系統且不會有缺乏系統資訊的問題，而進步型主控制室使用影像顯示器作為主要的人機介面，讓運轉員透過選單選擇想要監控的系統資訊，但進步型主控制室內配備的影像顯示器與核電廠的系統數目並不相符，運轉員雖然可以透過選單切換所需的系統資訊，但是這種方式可能會造成運轉員花費較多的時間在選擇需要的系統，而這個影響可能會導致緊急事故發生時，運轉員無法及時的做出反應，所以在現行先進型主控制室的設計議題「最小清單」(Minimum Inventory, MI)，就是希望找出除了運轉員經常使用的影像顯示器之外，還需要額外設計哪些人機介面用以增加運轉員對核電廠狀態的掌握以及縮短反應時間。

而美國核能管制委員會對於人機介面最小清單制訂暫訂行

則(Interim Staff Guidance, ISG)用以審查最小清單應該具備的功能，例如：要能夠監控裂變物屏障、能夠支援緊急操作程序裡的要求、能夠穩定核電廠反應爐在安全狀態、人機介面的形式上要屬於空間固定式 (Spatially Dedicated and Continuously Visible, SDCV) 讓操作人員易於尋找、或是屬於一次動作即可完成(accessible by taking only one action)，儘管對於最小清單該有的功能有了初步的規範，但是目前對於最小清單的建構流程尚未明確，所以本研究想要發展一套建立最小清單的流程，期望對於未來核能電廠設計最小清單時可做為參考資料。

二、研究目的

基於前述之研究動機，本研究想要探討最小清單的定義與準則，發展一套適合建立最小清單的流程與方法，並且對核電廠發生緊急事故時運轉員的操作流程進行案例探討，驗證本研究提出之最小清單的建立流程與方法可以符合緊急事故發生時所需之人機介面。本研究目的整理如下：

1. 本研究探討進步型核電廠主控制室最小清單的定義與準則，並建立設計最小清單的流程與架構。
2. 針對本研究所提出之設計最小清單的流程與架構提出一驗證方法，並以核電廠緊急事故模擬演練時運轉員動作分析作為驗證案例探討。

貳、文獻探討

一、國內外進步型核電廠現況分析

世界上第一座進步型核能電廠於 1996 年在日本正式開始運轉，而我國台電公司於 1993 年起啟動核能四廠興建計畫 (今以改名為龍門電廠)。而此龍門電廠即將成為台灣第一座進步型核能電廠，進步型核能電廠的特徵之一在於其主控制室儀控系統採取全數位化設計，在操作上具有高度資訊化與自動化之特性，自動化的意義是在適當的時候將原先屬於人員所執行的功能轉由機械或電腦執行，讓人員能在工作時更加地迅速、方便，提升系統運轉的效能，此定義也意謂當系統導入自動化時，原先的人機功能的分配將受到改變 (Sanders & McCormick, 1992)。數位化儀控系統改善了許多過去類比式儀控系統的問題，然而，也產生了一些與過去類比式儀控系統截然不同的潛在問題。Chuang & Chou (2006)認為核電儀控系統採取數位化的設計使得運轉員的角色與功能全盤改變，其中包括：資訊呈現、運轉員與系統互動、系統資訊需求以及監控作業等。另一方面，Lee & Seong (2006)也認為儀控作業自動化所導致的問題之一，便是人員與自動化系統誰負責最後的決策，除此之外，其研究也認為高度自動化也可能降低運轉人員的情境知覺。O'Hara, Persensky, & Szabo (2006)提出儀控系統數位化將產生一些人因的新議題，包括：人員與自動化系統的角色、人員選用與訓練、正常操作管理、擾亂與緊急作業管理以及維護與變更管理等。因此針對數位化與類比式儀控系統的特性進行比較與說明，由表 2-1 的敘述可知，主控制室的儀控介面由類比式轉變為數位式後，高度自動化與系統整合化所

帶來的影響，其相關的軟硬體改變是否能被運轉人員所適應將攸關未來龍門電廠的運轉安全，本研究認為其改變可能會影響核電廠運轉的議題，包括：由於主控制室儀控設備數位化後，運轉人員作業方式改變，然而在緊急狀況發生時，從原本固定式的儀控介面轉變為高度整合化的儀控介面，此種轉變對於人員進行危機處理的心智負荷及其對系統的情境知覺是否足夠，甚至發生人機介面失效的情況時，我們應該確保提供哪些儀控介面用以維持操作人員的情境知覺、降低人員心智負荷，使人員能夠更快速的進行狀況排除，回復電廠安全狀態，均應納入考量。

表2-1 類比式與數位化儀控系統比較表

	類比式儀控系統	數位化儀控系統
控制室整體設計	大多由類比式控制與顯示裝置所構成，因此有大量的按鈕、顯示燈等，在傳統類比式的核能電廠控制室中，儀表與控制裝置約有 3000 個以上，因裝置眾多，故所需空間較大。	具電腦化設計之特性，大多由鍵盤、滑鼠、觸控式螢幕、觸控式面板等所構成，因大部分顯示與控制裝置已經過數位化之整合，故所需空間較少。
系統軟體需求分析	基本上，人員從指針及顯示燈等獲得系統狀況，因此對軟體需求不大。	需完整並經過驗證之軟體系統以進行有效益且有效率地操作。
運轉人員工作負荷	以過去之操作而言，類比式系統裝置繁多且彼此間的交互作用複雜，但若人員配置安排得宜，操作應可維持一定之安全性與績效。	由於數位化系統為近年來逐漸使用，以目前之研究而言，發現在特定情況下並不適合應用，譬如加速儀表之判別 (Wickens and Hollands, 2000)。而對於人員負荷之影響也尚待人因相關學者進行評估。
運轉資訊顯示方式	以類比方式進行呈現，故以大量不同色彩的燈泡代表系統狀態，且配置大量的指針量表，以類比而連續之方式呈現相關資訊。	以數位方式呈現相關資訊，故將原本以燈泡或量表呈現之資訊整合至選單、訊息方塊中，人員可以透過電腦取得所有需要資訊，然而，因大量的資訊被整合在單一螢幕中，因此人員必須對系統選單與相關資訊的位置相當熟悉，方能取得適當資訊。
運轉人員操控方式	類比式的操控方式具有一對一的特性，也就是，一個操控裝置進行一項作業，因此需要相當多的旋鈕、按鈕等操控元件，因此，人體計測的思考在類比式的操控設計中相當重要。	數位式控制設備的操控方式與一般家用或辦公用電腦非常類似，最主要的操控介面是鍵盤、滑鼠與觸控螢幕，由於操控作業由直接操作轉為選單式操作，此時人員的工作負荷，大幅的由生理負荷轉為心智負荷，因此人為失誤的種類也將產生改變。

二、最小清單

(一)緣由

現在設計的進步型主控制室採用數位化技術，將各個系統的資訊與控制整合在一個離散式控制平台 (Distributed Control System, DCS)，在正常工作時主控制室運轉員可以使用運轉員工作站的人機介面進行監視與控制，然而當緊急狀況發生時，有可能會發生運轉員工作站人機介面失效的狀況，所以在核電廠主控制室的設計除了運轉員平常使用的人機介面需求之外，也必須考慮當緊急狀況發生時，哪些重要系統以及其相關設備必須要維持有效是目前進步型主控制室設計的重要議題，而這些重要系統的人機介面清單即稱為「最小清單」，即為確保核能電廠運轉安全所需滿足人機介面之最小集合。

(二)相關法規與規範

電廠的人因工程方面之發展、設計與評估應該根據可接受的人因工程準則來使用一個有架構的分析方法，NUREG-0711 HFE PRM (Human Factors Engineering Program Review Model) 為一系統化之安全評估準則，目的是確保整體設計能夠符合人因工程的標準，其是一個從上至下的架構，這架構的頂端起始於高層級的目標，之後將目標解析，得到達成這些目標所必須包含的功能，這些功能再分配至人員與系統且分散至各項作業中，人員的作業會被分析來確認作業績效需要的警報、顯示與控制，作業被安排至各種目的之工作中，而人機介面、作業程序與訓練這三項將設計來給予最好的支持，而這三項的細節設計則為此由上至下的架構中的底層，人因工程安全評估的範圍廣泛，包含一般與緊急的操作行為、維護、測試、檢測與監視

行為，然而，在進步型核能電廠的設計驗證階段中，在確認控制室設計與進步型儀控設備時，可能會無法獲得詳細的設計資訊，所以發展了兩部分的方法來檢視控制室的人因工程，第一部分牽涉到建立最小清單的詳細流程與實際必須要的人機介面清單，第二部分之美國核能管制委員會人員的檢視，所使用的接受標準是確認於完成控制室的設計時，系統化的流程之執行有人因工程準則的協同，譬如設計警報、控制與顯示，由此可知，最小清單能提供進步型主控制室最基本的人因需求項目。

目前關於最小清單的相關議題，國外研究機構，如：美國核能管制委員會、電力科學研究院 (Electric Power Research Institute, EPRI)都有釋出關於最小清單的相關的規定以及規範可供核能電廠設計人員在設計初始階段參考，美國核能管制委員會所編制的數位儀控之暫訂行則針對數位儀控設備的最小清單有以下主要的定義：要能夠支援緊急操作程序書裡的工作執行，並且把電廠回復到穩定的狀態，除了上述的要求之外，還需要考慮到運轉員在操作系統時的動作進行可能性風險評估 (Probabilistic Risk Assessment, PRA)把容易造成操作失誤的人機介面進行審查。

在 ISG-05 裡對於主控制室最小清單的要求有以下幾點：

1. 要提供監視裂變物屏障的功能 。
2. 能夠確認以及執行反應爐停爐動作。
3. 提供保護裂變物屏障安全系統的控制功能。
4. 能夠支援緊急操作程序書裡的要求。

5.將核電廠反應爐穩定在安全狀態。

對於遠距遙控停爐設備也有以下幾點要求：

1.能夠確認以及執行反應爐停爐動作。

2.將反應爐維持在安全的狀態。

上述要求的人機介面皆需要符合運轉員易用性(accessibility)設計，從 ISG-05 的內容可以清楚了解到審查人員在進行審查時，對於人機介面最小清單提供的功能要求有哪些部分。

另一項由電力科學研究院 (EPRI)提出的 1015089 文件對於人機介面最小清單的設計有更為詳細的指導原則，將 EPRI-1015089 所描述的內容整理成圖 2-1 的心智圖，EPRI-1015089 提供之文件由相關規範以及準則開始探討哪些系統與人機介面是安全相關，從中發現內容多為人機介面設計的指導原則，EPRI-1015089 提供的是一個關於人機介面的設計矩陣，首先是找出需要的功能，如：執行手動動作，接著找出完成這項功能所需之人機介面，如：迅速的指示器、警報器，以及人機介面應該要符合哪些法規的要求，進而去定義出一個符合法規需求的設計矩陣給設計人員參考，表 2-2 為其中一小部分的設計矩陣概念。

然而這兩份關於最小清單的要求文件，都是對於系統功能以及硬體設備進行規範與要求，例如最小清單的人機介面應該要與運轉員工作站的系統獨立，而且要為空間固定式(SDCV)，然而在文件中並沒有發現要如何去建立最小清單的流程，所以本研究將依循此兩份文件敘述的內容，發展一套制定人機介面最小清單的流程。

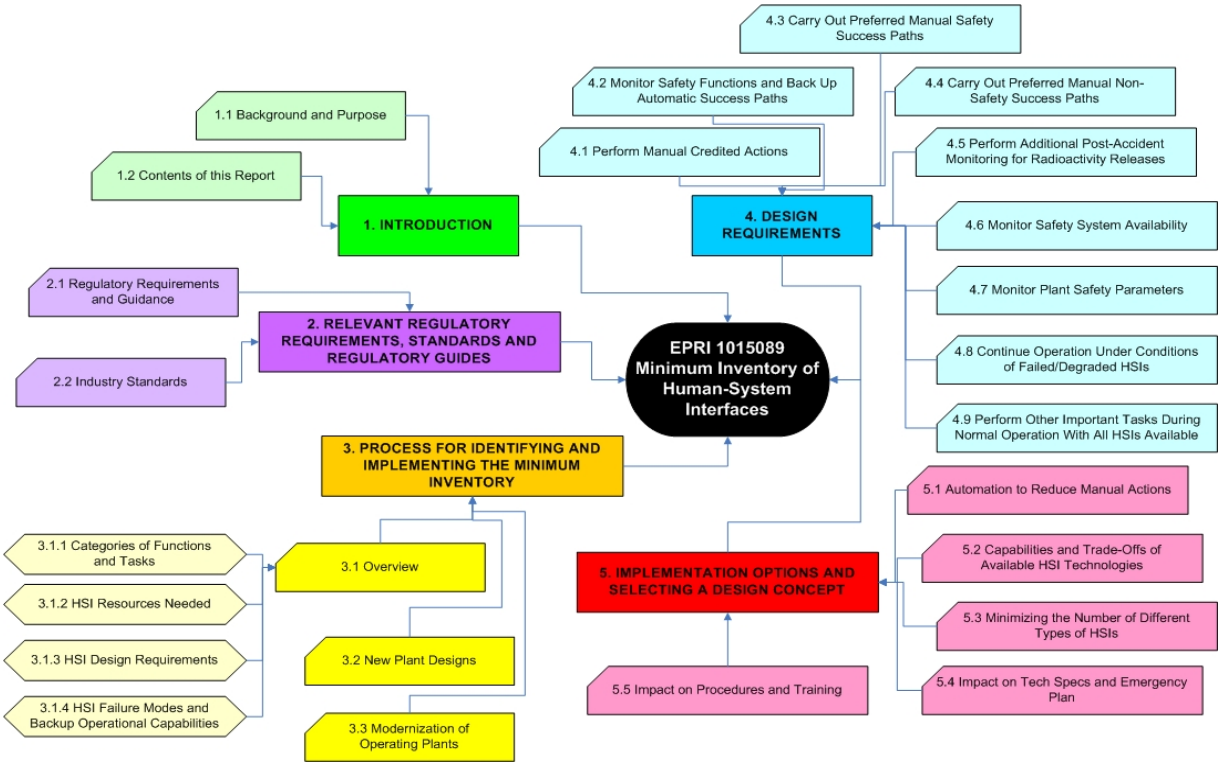


圖2-1 EPRI-1015089 心智圖

表2-2 最小清單人機介面的設計需求矩陣

功能、任務/相關的人機介面	人機介面設計需求		合適的準則規範以及工業設計要求
	安全層級分類	易用性	
1.執行手動動作 (**Perform Credited Manual Actions)**			
迅速反應的指示器 (Prompting indications)	安全相關	至少要有一個固定位置的顯示器	IEEE 603 (§5.8.1, §5.8.4) Reg. Guide 1.97 Rev. 3 (Type A; Category 1) Reg. Guide 1.97 Rev. 4 (Type A)
迅速反應的警報器 (Prompting alarms)	已經在運轉中的電廠屬於 NSR 層級 新設計的電廠屬於 SR 層級用以支援手動動作	固定位置的顯示器	None
控制器以及立即回饋的指示器 (Controls & immediate feedback indications)	屬於安全相關層級	固定位置的顯示器 SDCV 必須要 One-step accessible is acceptable if supported by appropriate HFE analyses	IEEE 603 (§6.2)

三、工作分析法

作業分析主要用在調查現有情況，而不是去規劃新的系統或設備，其透過蒐集及分析使用者與系統間互動的資訊，以評估作業配置、人機互動等過程優缺點的技術。在作業分析中，所獲致的結果除了能夠預測系統或模式的優缺點，以進行設計上的評估與選擇外，更可進一步分析使用者在進行該項任務時的心智工作負荷，以預測其執行績效。工作分析法所產生的資訊可建立現有實際情形的基礎，可為新工作設計或需求的參考資料。

工作分析包含調查操作人員的認知程序及實際行動，具備高度的抽象化及細節。實際上工作分析技法混合了各種方法，最常被使用的是層級工作分析法 (Hierarchical Task Analysis, HTA)。

層級工作分析法最初是為了訓練需求所制定 (Annett and Duncan, 1967)。它包含了將工作打散成數個小工作，再深入成更小單元的作法。將這些將這些小單元聚集成計畫，用以規範工作在實際情形可能的執行方式。層級工作分析法專注在實際可觀察的行為，而且也包含了注意毫不相關的軟體或互動裝置。起始點是使用者的目的，檢驗使用者目的，並確認主要工作和達成目標的聯結關係，在適當處將工作 (Task)細分成小單元的次工作 (Subtask)。

另一種工作分析法將介紹的是操作流程圖 (Operational Sequence Diagram, OSD)，操作流程圖屬於圖形化的工作分析方法，操作流程圖被開發用來描述每個情境。操作流程圖提供了一個圖形化的工作分析方法，清楚的描述整合所有潛在硬體需求的系統功能 (Walley & Sheherd, 1992)。操作流程圖使用標準的操作

圖示，對於完成工作或工作流程中，一個描述資訊、決策及操作流程的方法。除了描述工作完成過程外，操作流程圖還有其他的功用 (Backer, Johnson, Malone, & Malone, 1979)：

1. 評估人機界面和功能分配
2. 定義主要工作的狀況
3. 定義超過負荷和不足的狀況
4. 定義主要決策及操作重點
5. 開發工作區的設計及評估標準
6. 定義高錯誤可能發生點
7. 發展操作的流程

本研究欲使用上述兩種分析手法，探討人員在執行作業流程所需之人機介面時，進而發展一套人機介面最小清單的建立流程。

參、研究方法與過程

一、人機介面最小清單建立與驗證方法

由美國核能管制會提出的 ISG-05 對於最小清單的定義描述中提到，人機介面 (如：警報器、控制器、顯示器)的最小清單要能夠支援緊急操作程序書的執行，並且把核能電廠回復到安全的狀態，所以如何找出重要的系統，並且驗證這些系統的人機介面在事故發生時可以支援運轉員執行緊急操作程序書的內容，即為本研究想要提出之方法。

依照上述對於最小清單的要求發現，人機介面的最小清單的建立流程必須先從選定緊急事故作為開始，透過探討緊急事故發生時對於核電廠的影響，並且依照緊急操作程序書進行事故排除以及傷害減緩的步驟，對於每個程序書進行工作分析，藉此可以得知運轉員在每個程序書的流程中所需操作的系統以及相關的人機介面，搜集整理這些人機介面，進而得到設計端的人機介面清單。

本研究主要以核電廠設計基準事故「冷卻水流失事故以及喪失場外電源」 (Loss of Coolant Accident with Loss of Off-Site Power, LOCA with LOOP)為探討案例，進行最小清單建立與驗證流程，所謂設計基準事故是指電廠在執照申請時必須於安全分析報告中分析的各種假想事故，以作為緊急安全系統設計的參考，在冷卻水流失事故以及喪失場外電源中，必須對於反應爐(Reactor Pressure Vessel)進行補水以及壓力管控，以及一次圍阻體 (Primary Containment)相關設備的管控，所以我們挑選緊急操作程序「反應爐控制」(Reactor Pressure Vessel Control)、「一次圍

阻體控制」(Primary Containment Control)的控制串進行分析，進而找出可以達成減緩事故危害之相關系統與人機介面。

接著透過核電廠模擬事故發生時，運轉員實際演練事故排除以及傷害減緩的流程，紀錄運轉員在事故發生時依照緊急操作程序書以及自身經驗進行事故排除時使用到的人機介面，並且詢問運轉員於過程中是否有缺乏需要的人機介面，將上述的人機介面整理成驗證端的人機介面清單。所以本研究也會分析運轉員在冷卻水流失事故以及喪失場外電源發生時，運轉員使用哪些人機介面達成事故排除，以驗證設計端的人機介面清單是否符合人員操作需求。

將一個從設計端得到的人機介面清單與後端驗證得到的人機介面清單進行比對，如果人機介面需求相符，則定義人機介面清單即是目前緊急事故發生時所需持續維持有效的人機介面最小清單，如果分析驗證端所需的人機介面多於設計端所需之人機介面，則需將驗證端多出的人機介面請核能工程專家進一步透過功能性分析以及重新審視最小清單的定義，符合則加入最小清單需求，反之則剔除，反覆的驗證直到最小清單的完善。經由以上所述將建立最小清單的流程繪製如圖 3-1。

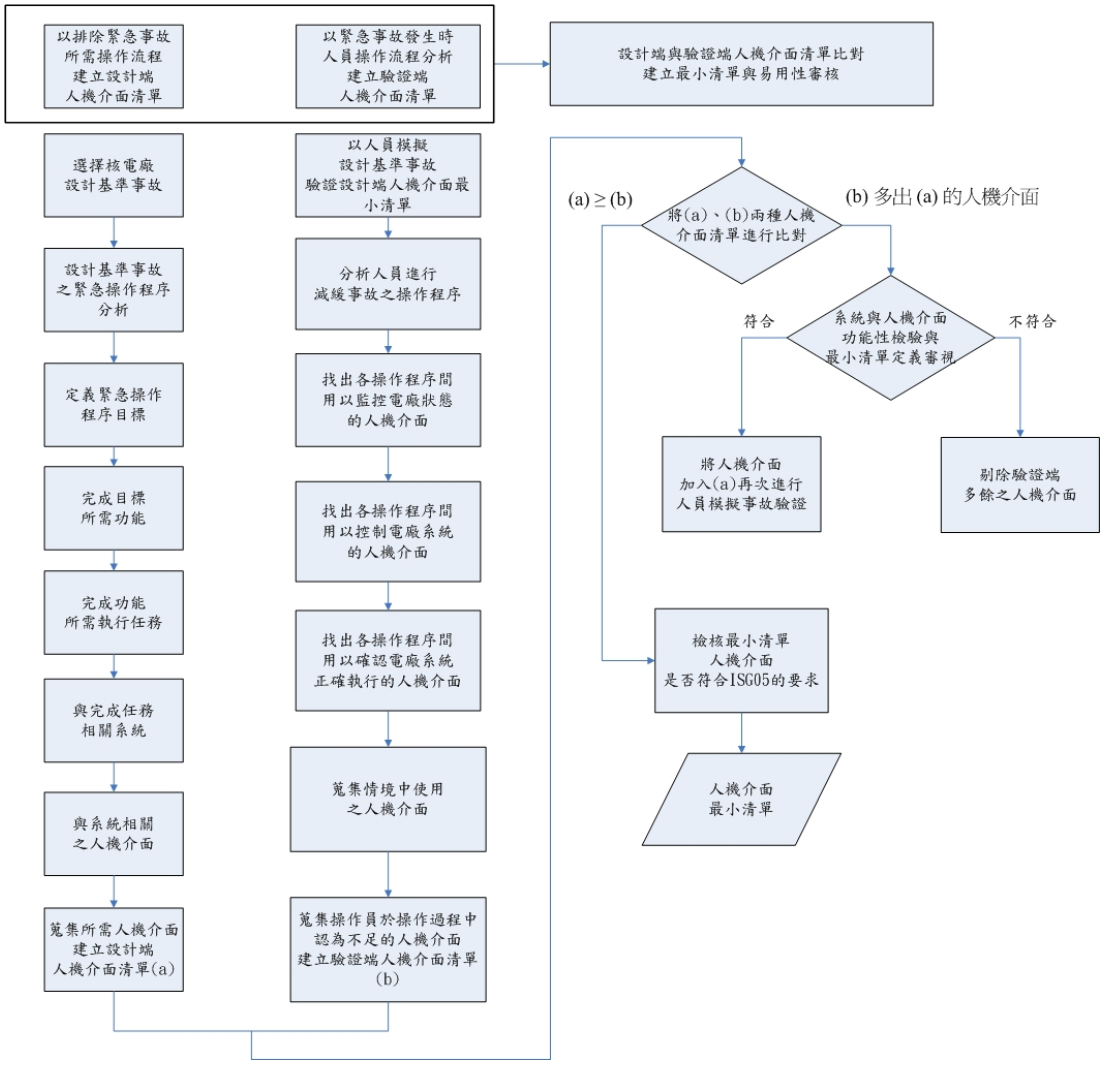


圖 3-1 考慮人因之最小清單建立方法流程圖

二、緊急操作程序流程分析方法

緊急程序導則/嚴重事故導則(Emergency Procedure Guideline/Severe Accident Guideline, EPG/SAG)即為在發生緊急事故時提供給運轉員執行動作所參考的依據，運轉員必須根據緊急程序導則/嚴重事故導則(EPG/SAG)上之指示，來緩和事故並且確保電廠之完整性。而每個緊急操作程序都有各自需要應對的狀況以及完成的目標，主要可分為以下幾部分：

1. 反應器控制 (Reactor Pressure Vessel Control)：主要針對反應器爐心水位及壓力之控制程序。
2. 一次圍阻體之控制 (Primary Containment Control)：共分為圍阻體壓力、乾井 (Drywell)壓力、抑壓池溫度與水位以及氫氣量等項目之控制程序。
3. 二次圍阻體之控制程序 (Secondary Containment Control)。
4. 放射性物質釋放之控制程序 (Radioactivity Release Control)。

以反應器控制為例，反應器控制目標即是在進行停爐時，維持爐心的水位及壓力在安全的狀態下，以避免燃料防護套燒毀導致反應爐熔融或是壓力過大導致反應爐崩毀的一序列程序。

為了在緊急狀況發生時可以正常執行上述緊急操作程序，必須先界定出所需之人機介面，並且確保所需之人機介面在緊急情況發生時可以正常操作，所以在此選用層級工作分析法分析運轉員在進行緊急操作程序時所需之人機介面，檢驗運轉員目的，並確認主要工作和達成目標的聯結關係，依照層級分析法的特性並結合本研究所欲探討之最小清單建立方法，建構圖 3-2 符合最小清單之流程層級分析法分析圖。

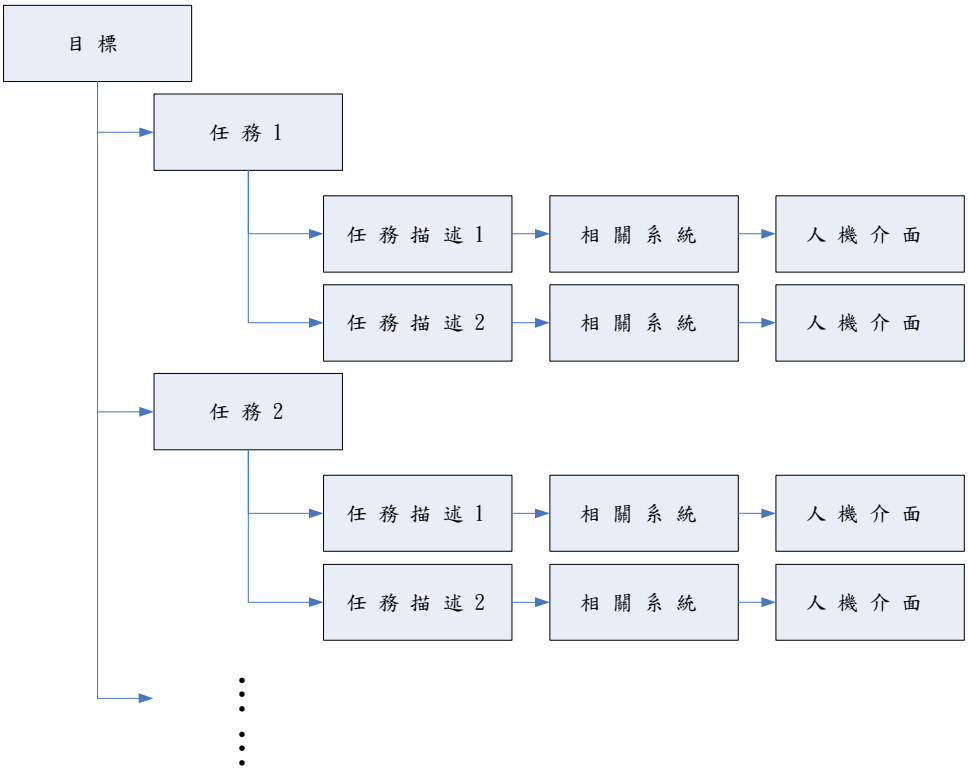


圖3-2 建立最小清單層級分析圖

目標的定義就是各個緊急操作程序要進行控制的部份，例如反應器控制，而圖中分支下來的功能就是為了要達到目標所需要的功能，如反應器控制的其中兩個分支;爐心壓力控制 (Reactor Control/Pressure)以及爐心水位控制 (Reactor Control/ Level)，而任務描述就是要讓功能正常執行的一連串操作程序之敘述，相關系統則是在執行一連串操作程序所需用到的系統，將上述之步驟簡略敘述如下：

1. 一開始是定義目標，以本研究的想要探討的案例來說目標就是進行反應器的管控。
2. 接著找出完成目標所需要的功能，如：確認電廠狀態需不需

要進行反應器管控、進行反應爐水位控制。

3. 將緊急操作程序書對完成功能所需的程序進行整理，得到各個步驟的任務描述。
4. 進而從每個步驟的任務描述中找出所需要之系統與相關人機介面。

經過一連串的執行動作之後，蒐集這些系統相關的人機介面即完成設計端的人機介面清單。

三、以反應器控制為範例進行最小清單流程分析

從圖 3-3 反應器控制導則中得知，反應器控制主要的任務有三個，分別是進入爐心壓力控制、爐心水位控制、爐心功率控制，而且只要核電廠狀況滿足進入條件的其中一項條件，就必須要執行反應器控制的相關內容，例如：當反應器水位低於 378.6 cm、反應器壓力高於 7.24 MPaG、乾井壓力高於 11.2 KPaG 或是爐心功率高於 5%或是無法偵測到爐心功率以及反應爐需要被停爐的時候，就必須執行反應器控制，而一個緊急操作程序與別的緊急操作程序也有相關，甚至是另一個緊急操作程序的進入條件，以反應器控制控制串「反應爐水位控制 (RC/L)」的操作來說，如果一開始就發生反應器水位偵測不到的情況，則離開 RC/L 操作程序然後進入緊急應變程序反應器注水的程序，這在進行 RC/L 的時候是需要重複確認執行，另外在緊急指導原則的描述中會參雜著圖表，這些圖表是用來提供運轉員執行動作的依據，如圖 3-4 一次圍阻體水位限制圖，當抑壓室的壓力以及一次圍阻體的水位無法維持在白色區域內的時候，運轉員此時應該停止從外部繼續注水進入反應器。

在 RC/L 的部份會先要求運轉員利用主要的補水系統恢復爐心水位。而緊急應變程序 1 進入條件主要是在 RC/L 部分無法將水位維持在爐心燃料之上時，則必須利用更多輔助補水系統將爐心水位維持在（中文）爐心燃料水位之上，若是主要補水以及輔助補水系統皆失效的情況下，則跳出 RC/P 而進入（中文）緊急應變程序 3，控制壓力利用蒸汽以延長對燃料做冷卻的時間。RC/P 主要目的是要穩定爐心壓力同時藉此輔助爐心水位控制，若有需求時會透過洩壓的動作使爐心壓力降低並且冷卻爐心至冷停機狀態。

RPV CONTROL GUIDELINE

PURPOSE

The purpose of this guideline is to:

- Maintain adequate core cooling,
- Shut down the reactor, and
- Cool down the RPV to cold shutdown conditions ([Avg. RPV water temperature £93.3 °C (cold shutdown conditions)]).

ENTRY CONDITIONS

The entry conditions for this guideline are any of the following:

- RPV water level below [380.8 cm (low level scram setpoint)]
- RPV pressure above [7.35 MPaG (high RPV pressure scram setpoint)]
- Drywell pressure above [0.012 MPaG (high drywell pressure scram setpoint)]
- A condition which requires reactor scram, and reactor power above [5% (APRM downscale trip)] or cannot be determined

圖3-3 RPV Control Guideline (Applicant's Design Control Document, 2010)

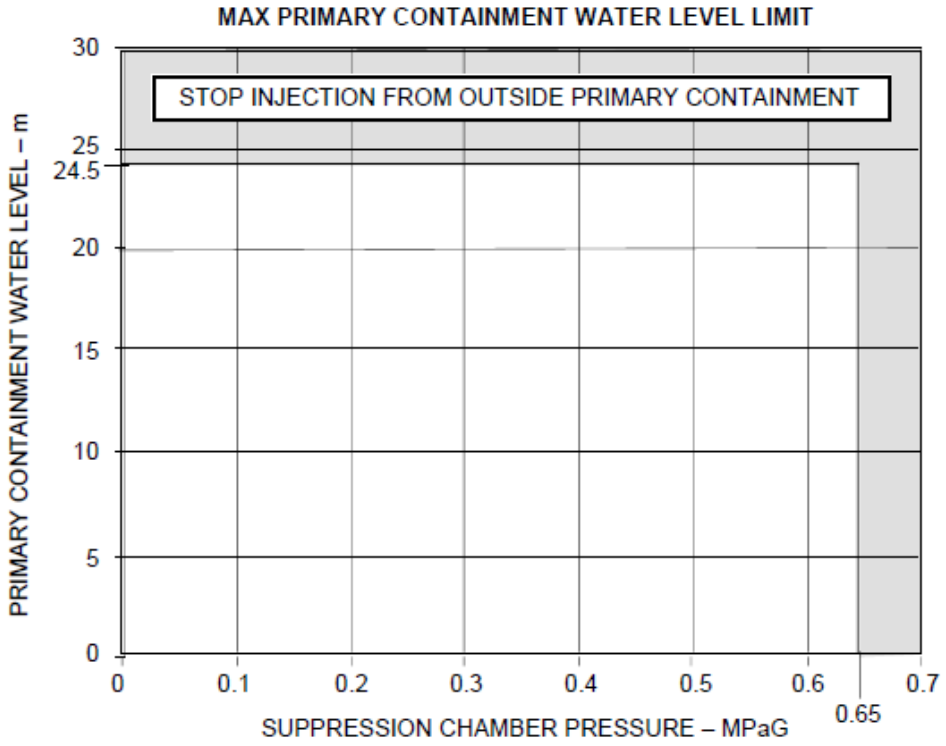


圖3-4 一次圍阻體水位限制圖 (Applicant's Design Control Document, 2010)

從反應器控制的進入條件開始進行建立最小清單層級分析法，一開始必須注意反應器的水位以及壓力、乾井壓力、以及爐心功率或是爐心需要開始停爐，只要以上某一個進入條件符合，則開始進行反應器控制的操作程序，在執行反應爐水位以及壓力控制之前，還需要判斷反應爐是否開始停爐，如果反應爐尚未開始停爐則啟動停爐，接著要確認反應爐內全部控制棒是否插入，如果沒有或是有偵測不到的狀況，則需要進一步的確認反應爐是否在爐內完全沒有硼液注入的狀態下停爐，如果反應爐已經注入硼液或是無法確定是否注入硼液的狀況發生，則進入緊急程序5，反之，則進入反應爐水位 (RC/L)以及壓力 (RC/P)控制程序，將上述之程序使用建立最小清單層級分析法，找出其相關人機介

面，將其圖像化為圖 3-6。

在圖 3-6 中可以看到整個進入條件被劃分成了三個部份，依照緊急操作程序指導原則，在判斷進入條件時有約三個步驟需要檢查，首先是判斷整個核電廠的狀態是否需要開始進入反應器控制，在緊急操作程序指導原則中指出此時需要監看反應器的水位以及壓力、乾井壓力、以及爐心功率或是爐心需要開始停爐，將上述任務描述定為「監控電廠狀態」，在任務描述的下一個步驟即是找出可以完成此任務的相關系統，如：根據 ABWR Tier1 設計文件中得知，核能沸水系統(Nuclear Boiler System) 提供監控乾井壓力、反應器水位及壓力的相關設備。

接著依照緊急操作程序指導原則，還需要判斷反應器是否開始停爐，如果還沒開始停爐，則需要透過控制器將反應器轉為停爐狀態，所以此時需要的相關系統為反應器保護系統，因為該系統提供了關於反應器資訊的顯示器以及控制器。

最後則是判斷反應器開始停爐之後，反應器停爐需要的相關設備是否開始啟動，如控制棒是否全部插入，或是已經注入硼液，而上述所需要注意的事項，將其整理成任務描述，在透過任務描述去尋找相關的系統，在這個任務描述中必須注意控制棒的狀態以及硼液的狀態，所以透過 ABWR 的設計文件得知相關的系統是控制棒驅動系統(Control Rods Driven System)、棒位控制與資訊(Rod Control & Information System)、備用液體控制系統(Standby Liquid Control System)，接著再去搜尋相關的人機介面。

ENTRY CONDITIONS

The entry conditions for this guideline are any of the following:

- RPV water level below [380.8 cm (low level scram setpoint)]
- RPV pressure above [7.35 MPaG (high RPV pressure scram setpoint)]
- Drywell pressure above [0.012 MPaG (high drywell pressure scram setpoint)]
- A condition which requires reactor scram, and reactor power above [5% (APRM downscale trip)] or cannot be determined

OPERATOR ACTIONS

RC-1 If reactor scram has not been initiated, initiate reactor scram.

If while executing the following step:

- Any control rod cannot be determined to be inserted to or beyond [4.2%* (Maximum Subcritical Banked Withdrawal Position)] and it has not been determined that the reactor will remain shutdown under all conditions without boron, enter [procedure developed from Contingency #5].
- RPV water level cannot be determined, enter [procedure developed from Contingency #4].

圖3-5 RPV Control condition控制串 (Applicant's Design Control Document, 2010)

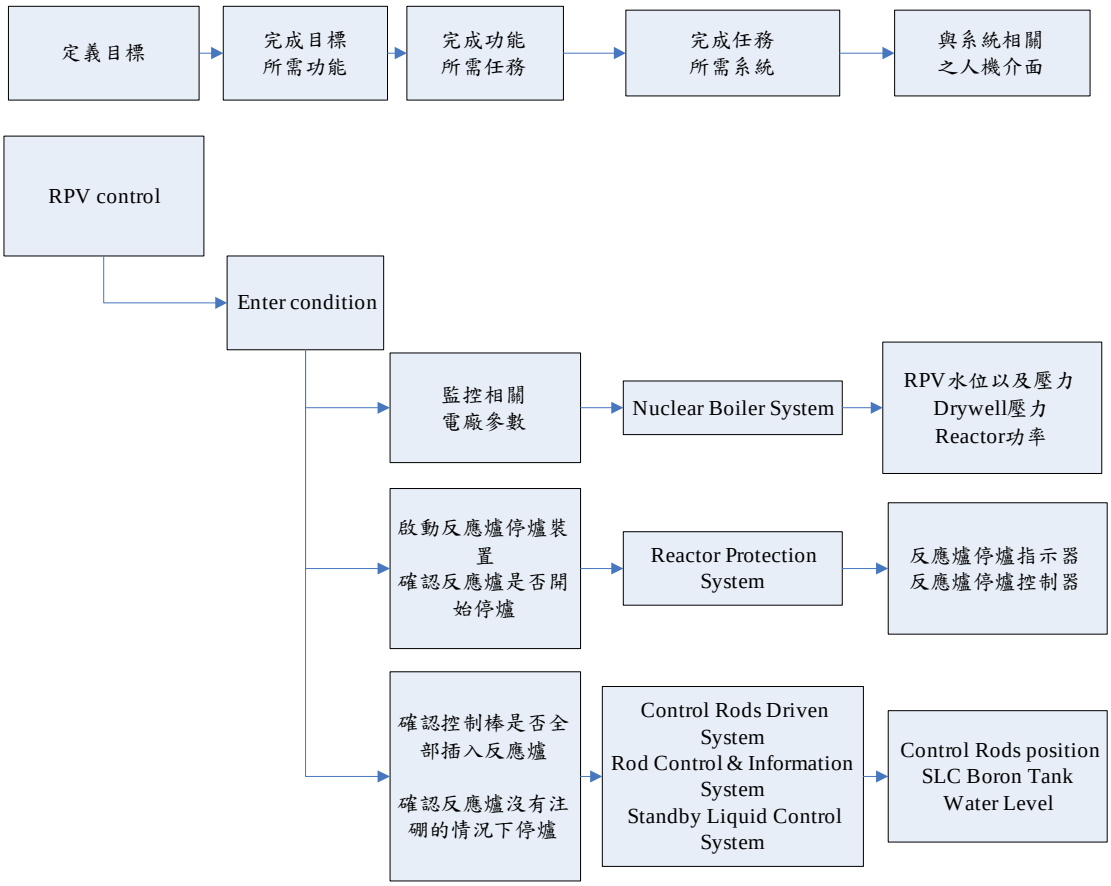


圖 3-6 RPV Control enter condition 層級分析圖

了解反應爐狀況以及確定反應器控制的先決條件之後，為了達到安全停爐，所以需要同時進行反應爐水位 (RC/L)以及反應爐壓力 (RC/P)管控。

反應爐水位管控 (RC/L)方面，根據圖 3-7 RC/L 控制串，在 RC/L-1 的部分要求運轉員先啟動以下設施：

- Isolation (ESP-590.1)
- Emergency Core Cooling Systems (ECCS)
- Emergency Diesel Generators (EDG)

此時運轉員必須要根據 ESP-590.1 將必須的隔離閥門關閉，並且啟動 ECCS 以及緊急柴油發電機 (EDG)。

接著在 RC/L-2 重覆確認事項的部份會要求重複確認兩件事項：

1. 如果反應器水位無法確定則進入反應爐水位覆蓋。
2. 如果乾井水位以及濕井壓力無法保持在一次圍阻體之下而且爐心能夠得到有效的冷卻，則停止所有除了做爐心冷卻必須以外的外注水源，第二點的確認事項是避免外注水源不斷注入會造成圍阻體額外的負荷，所以在爐心能夠得到有效冷卻時可以停止不必要的外注水源。

確認事項結束之後 RC/L-2 要求運轉員操作以下系統維持爐心水位在 378.6 到 473.9 cm 之間：

- Condensate/Feedwater
- Control Rods Drive System
- Reactor Core Isolation Cooling
- High Pressure Core Flooder
- Residual Heat Removal in Low Pressure Core Flooder mode

在進行爐心補水的時候，需要檢查下列事項：

1. 如果爐心水位沒辦法維持在 378.6 cm 以上，則開啟下列子系統 (Detail E)以維持爐心水位在 0.0 cm 以上。
   - AC power source independent water addition (RHR Division C)
   - Condensate Storage & Transfer System
   - ECCS Keep-Fill Systems
   - Standby Liquid Control System (test tank)
   - Standby Liquid Control System (Boron tank)
2. 如果自動洩壓裝置(Automatic Depressurization Systems, ADS)計時器開始啟動，則預防自動洩壓裝置自動啟動。

3. 如果爐心水位無法維持在 0.0 cm 上，則離開 RC/L 近入緊急應變程序 1

將上述之 RC/L 工作描述依照建立最小清單流程分析法進行分析整理，可將其圖像化為圖 3-8，在此必須重複執行並檢查 RC/L 條件，直到反應爐完全停爐。

在圖 3-8 的任務描述分為四個區塊，而這些分類大致上是依據緊急操作程序指導原則而來，在指導原則的描述中都有各自需要監看的資訊以及控制的系統，所以依照指導原則的分類進行各個任務描述的整理，這邊分類的原則是一個監看資訊的動作結合對應的控制動作，例如：如果爐心水位沒辦法維持在 378.6 cm 以上，則開啟下列子系統 (Detail E)以維持爐心水位在 0.0 cm 以上。照此敘述將其整理為「確認反應器水位並使用下列子系統維持反應器的水位。」依照此原則進行圖 3-8 的建構。

RC/L Monitor and control RPV water level. ☞ #1

RC/L-1 Initiate each of the following which should have initiated but did not:

- Isolation
- ECCS
- Emergency diesel generator

RC/L-2 Restore and maintain RPV water level between [380.8 cm (low level scram setpoint or shutdown cooling RPV water level interlock, whichever is higher)] and [484.4 cm (high level trip setpoint)] with one or more of the following systems:

- Condensate/feedwater
- CRD
- RCIC with suction from the condensate storage pool, defeating low RPV pressure and area high temperature isolation interlocks and high suppression pool water level suction transfer logic if necessary. ☞ #3,4
- HPCF; control and maintain pump flow less than [the HPCF Vortex Limit]. ☞ #5

圖3-7 反應爐水位部份控制串 (Applicant's Design Control Document, 2010)

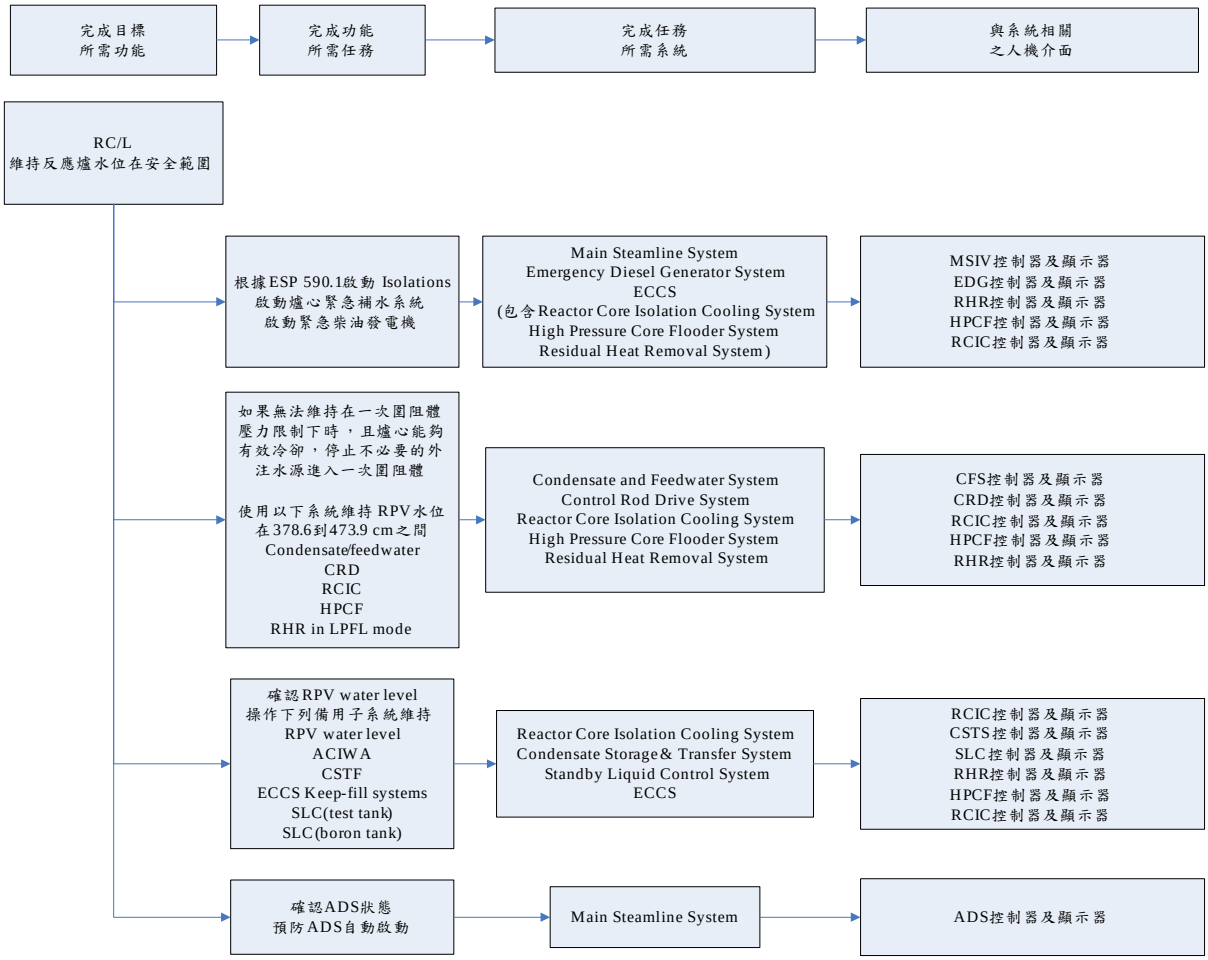


圖3-8 反應爐水位控制串層級分析圖

另外一個主要任務是關於反應爐的壓力控制 (RC/P)部份，進入爐心壓力控制(圖 3-9)後會先遇到重複執行項，要求運轉員確認以下四件事：

1. 如果乾井壓力過高 (11.6kPaG)而觸發 ECCS 啟動信號，除非為了冷卻爐心，否則避免 LPFL 注水系統注入爐心直至爐心壓力降至 1.55MPaG 以下。
2. 如果預期需要進行反應器洩壓，則使用主蒸汽旁通進行洩壓。
3. 如果爐心需要進入緊急洩壓，則跳出 RC/P 壓力控制轉為緊

急洩壓程序(Emergency Depressurization)。

4. 如果爐心水位無法確定，則跳出爐心壓力控制轉為反應爐灌水程序。

接著在 RC/P-1 的部份詢問 SRV 有沒有重複開關 (cycling) 的現象，如果 SRV 已經有 cycling 的現象，則必須手動開啟 SRV 做爐心降壓，避免 SRV 在重複開關的情況下有可能會卡住或受損。在經過初步降壓之後，會進入 RC/P-2 OR，確認三件事：

1. 如果 Suppression pool 溫度無法保持在 Heat Capacity Temperature Limit (Fig. M)之下，則要設法把壓力槽的壓力維持在其之下
2. 如果 Suppression pool 水位無法保持在 SRV Tail Pipe Level Limit (Fig. N)之下，則要設法把壓力維持在其之下。
3. 如果需要 Steam Cooling，則離開 RC/P 程序後，進入 Contingency 3。

接著在 RC/P-2 的部份，要求運轉員使用 Turbine Bypass Valve 將爐心壓力穩在 7.24 MPaG，目的是避免壓力的震盪會造成爐心功率的不穩定，除了使用 Turbine Bypass Valve 控制爐心壓力之外，反應器壓力也會因為以下系統造成上升：

1. Safety/Relief Valve
2. Reactor Core Isolation Cooling (injection or test mode)
3. Turbine-driven feedwater pumps
4. Reactor Water Cleanup System (recirculation mode)
5. Main SteamLine drains
6. Reactor Water Cleanup System (blowdown mode)

在 RC/P-3 的部份，程序書要求運轉員持續進行反應器的洩

壓動作，並且注意反應器的溫度下降速度要維持低於 55°C/h，並且如果反應器需要洩壓則打開 SRVs 進行洩壓動作。而 RC/P-4 的部份當到達反應器的冷卻溫度以及壓力的解除互鎖限制時 (0.931 MPaG)，只使用 RHR in LPFL mode 維持水位，並保持溫度下降速度為 55°C/h，如果無法成立 shutdown cooling，則使用上述之洩壓系統維持反應器壓力低於 0.931 MPaG。

將上述之 RC/P 工作描述依照建立最小清單流程分析法進行分析整理，並且依照圖 3-8 的建構原則，可將其圖像化為圖 3-10。

RC/P Monitor and control RPV pressure.

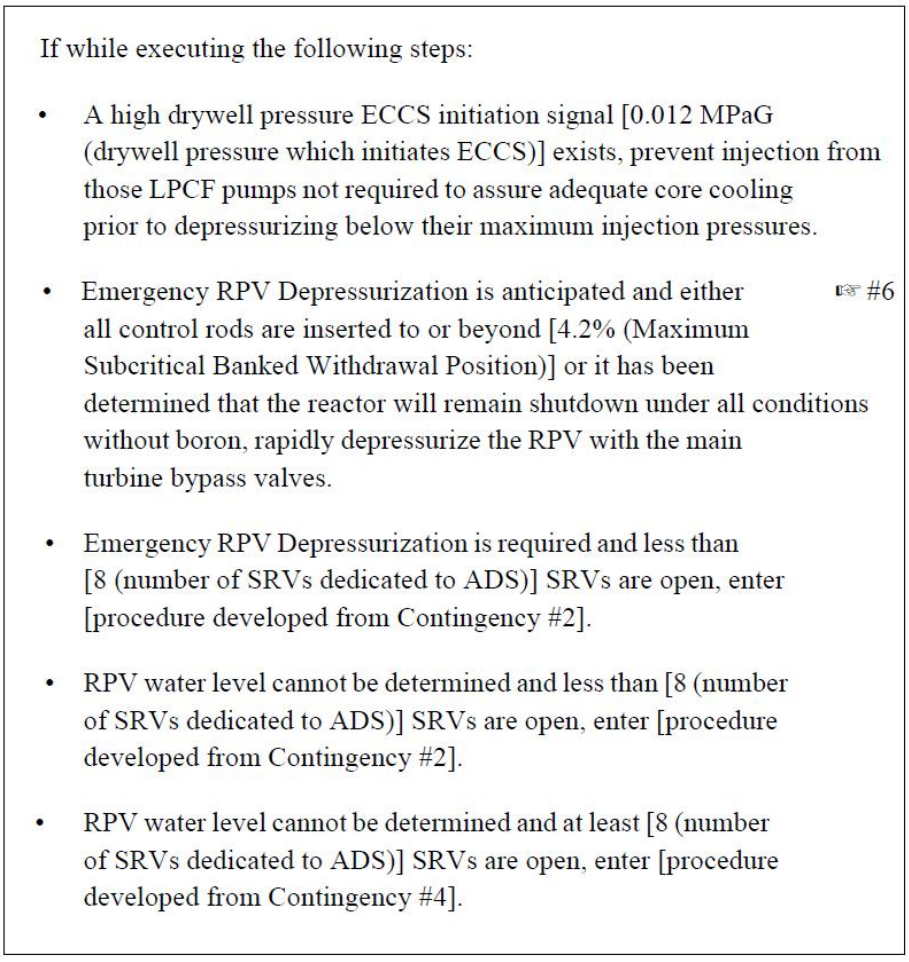


圖3-9 反應爐壓力部分控制串 (Applicant's Design Control Document, 2010)

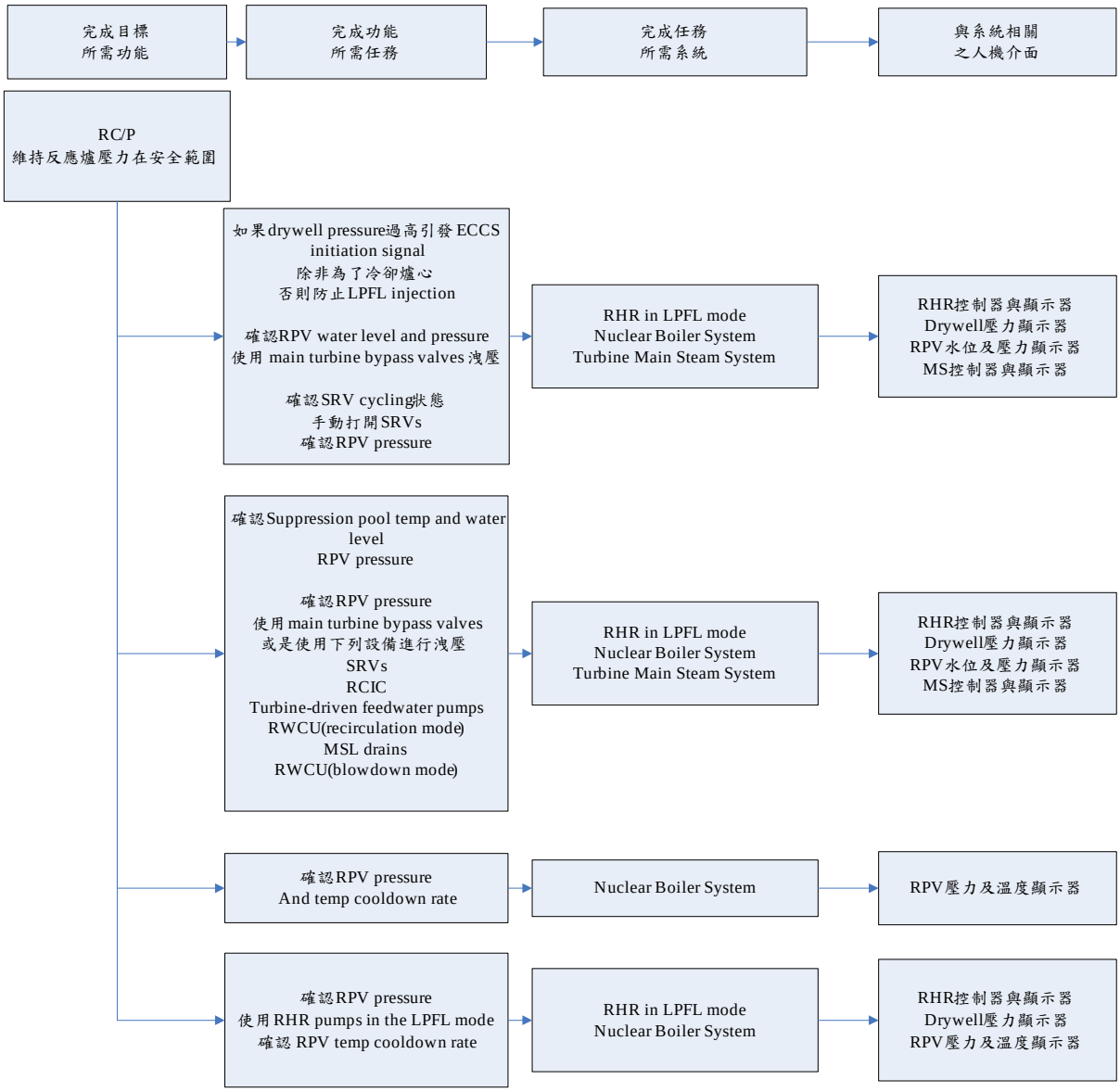


圖 3-10 反應爐壓力控制串層級分析圖

四、人機介面清單初步建立

以上為使用反應器控制為例，進行建立最小清單流程分析法進行分析整理之流程所得到的部份功能，依照緊急操作程序的控制串發展一系列的任務描述，進而找出可以達成任務之相關系統與人機介面，圖 3-11 即是完整的反應器控制分析圖，放大版本

請參閱附件 D，以同樣的方式進行一次圍阻體之控制的分析並且依照 ISG-05 的需求提供易用性的審查表格，如人機介面的設計是否為固定位置且持續可見、是否一個動作即可完成的控制，將上述之需求整理成 A-1、A-2 即為人機介面最小清單初步清單。

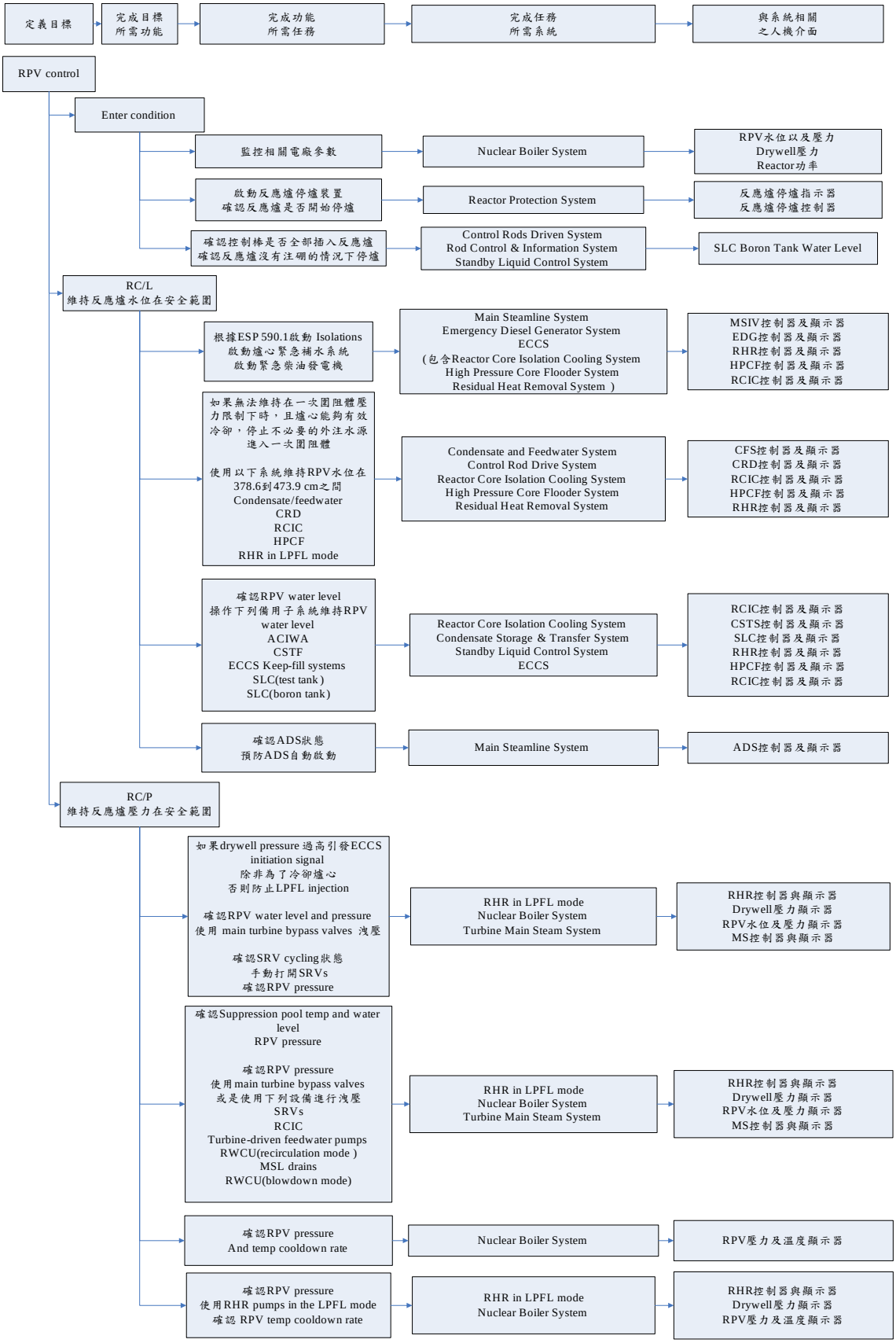


圖 3-11 RPV Control 層級分析圖

肆、驗證分析

一、龍門電廠人因工程確認與驗證 2.5 簡介

目前核四廠主控制室人機介面系統的開發正進入人因工程確認與驗證 (Human Factors Engineerng Verification and Validation, HFE V&V)階段。此階段的工作包含：人機介面支援作業的確認 (HSI Task Support Verification)、人因工程設計確認 (HFE Design Verification)、整合的系統驗證 (Integrated System Validation) 與人因問題的解決 (Human Factors Engineering Discrepancies Resolution)等部分。

龍門電廠的 V&V 2.5 主要是針對下列五個人機介面的進行人因工程驗證分析，其中包含了：

1. 主控室面板 (Main Control Room Panels)
2. 主控室圖像化顯示器 (Main control Room Operator Graphics Displays)
3. 遠端停爐系統面板 (Remote Shutdown System Panels)
4. 主控室警報器與通報器系統 (Main Control Room Alarm and Annunciator Subsystem)
5. 主控室安全相關參數顯示系統 (MCR Safety Parameter Display Subsystem)

人因工程確認與驗證目的在驗證主控制室、遠端停爐系統、現場控制盤的設計符合人因工程設計原則，以及確認電廠的人機介面設計能夠充分支援人員在各種運轉情境下之作業績效。V&V 作業要項包括：(1)人機介面作業支援確認 (HSI Task Support Verification)，將功能與作業分析需求中確定的事項和人

機介面設計組件做比對，確認人員作業需求的組件均已齊備。(2)人因工程設計確認 (HFE Design Verification)，將詳細的人機介面設計來和人因工程指引做比對，確定每個人機介面組件的設計都已考慮人員的能力與限制。(3)整合系統的驗證 (Integrated System Validation)，透過由作業、風險以及工程分析來界定績效標準，確認整合的人機介面設計可以讓人員進行安全的運轉而不會有過高的工作負荷。

自個別介面的靜態驗證開始，然後是整合後的動態作業效能評估，其中動態評估涵蓋正常、異常、緊急、暫態、設備故障之情節。下列為 V&V2.5 定義的九個模擬情節：

1. Process Instrumentation, Alarms and Control System Failure
2. LOCA With Loss of Off-Site Power
3. Anticipated Transient Without Scram (ATWS)
4. Shutdown from Outside MCR
5. Loss of Normal and Emergency Feedwater
6. Inadvertent SRV Opening
7. Pressure Regulator Failure - Open
8. Trip of All RIPs
9. Startup to rated Power (Control Rod Withdrawal for Criticality, Generator Synchronization and Initial Loading

以上情節是以核能電廠的設計基準事故 (Design Base Accident, DBA)發展而成，所謂設計基準事故是指電廠在執照申請時必須於安全分析報告中分析的各種假想事故，以作為緊急安全系統設計的參考。而在設計基準事故發生後，各項緊急操作系統需依電廠原來的設計而動作，且不會對環境以及公眾的健康及安全造成威脅，否則電廠就無法獲得運轉執照。所以經由設計基

準事故的情境模擬訓練人員，除了確保系統在緊急狀況事件發生時可以發揮原有的功能，也可以發現人員在情境模擬操作人機介面時所遭遇到的問題，如：常用的人機介面無法短時間內找到或是操作，藉由改善人機介面縮短運轉員反應時間，可以在事故惡化之前，將電廠回復到穩定的狀態，避免對環境以及公眾的健康及安全造成影響。

二、最小清單人員操作順序分析法

為了找出人員進行事故排除時所使用的人機介面，在此使用操作程序圖的概念進行人員任務流程分析，核電廠運轉員的決策制定模式包含以下三類：

1. 監控資訊與確認回饋 (Monitoring and Feedback)，如：滿足任務目標、程序執行成效。
2. 計畫 (Planning)，如：選擇可行的方案。
3. 系統控制 (Control)，如：程序的執行、終結、調整。

將此決策制定模式結合運轉員任務流程，呈現如圖 4-1，以了解運轉員進行事故傷害減緩時的作業流程。

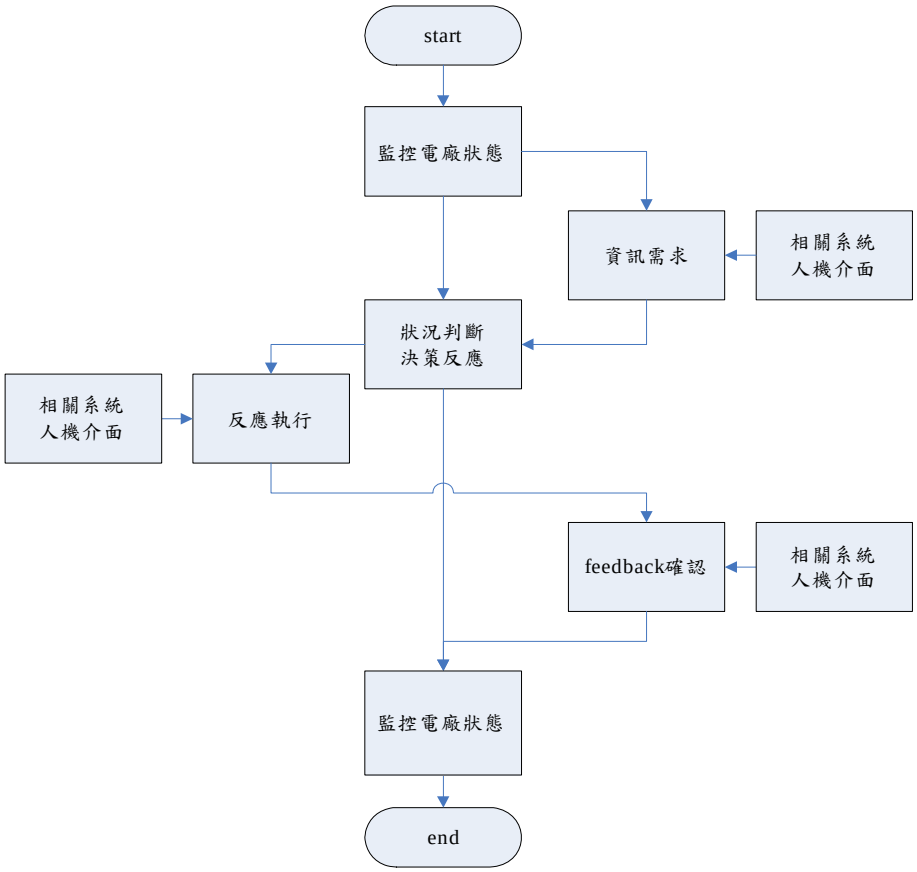


圖4-1 人員操作順序分析圖

舉例來說在平常運轉任務時，運轉員需要隨時注意電廠內的安全相關參數以及警報系統，此時的動作屬於「監控資訊」，運轉員依照自身經驗或是標準作業程序書進行場內參數監控，此時運轉員注意到主控制室內警報響起，運轉員決定先將警報器靜默(Silence) 鍵並回報給值班主任，此時的動作屬於「計畫」，接著運轉員按下警報靜默鍵並將警報內容回報給值班主任，此時的動作屬於「系統控制」，然後確認警報器已經靜默並且接受到值班主任的指示，此時的動作屬於「確認回饋」，最後回到監控系統參數或是執行值班主任的指示進行系統監控、系統控制、回報資訊等動作。

以此任務流程分析法對運轉員進行 V&V 2.5 的情境的操作行為分析，並且在各操作行為產生時記錄所需之人機介面，進一步的定義出完成任務所需之人機介面最小清單。

三、以冷卻水流失事故以及喪失場外電源 (LOCA with LOOP)為例

冷卻水流失事故 (Loss of Coolant Accident, LOCA)，是核能電廠的設計基準事故之一，所謂設計基準事故是指電廠在執照申請時必須於安全分析報告中分析的各種假想事故，以作為緊急安全系統設計的參考。一般而言所謂冷卻水流失事故乃指反應器冷卻系統 (Reactor Coolant System)破裂，喪失完整性，爐心冷卻水大量從破口流入低壓的圍阻體內。冷卻水由兩端破口大量且急速流失，爐心內燃料棒在短時間內及不再為水所覆蓋，但燃料棒內的衰變熱持續產生，燃料護套溫度持續升高，此時緊急爐心冷卻系統 (ECCS)將自動動作注入冷卻水冷卻爐心。失水事故大多數是在地震發生後，冷卻水管路被震斷裂而引起，故評估模式分析中需加入喪失廠外電源的假設，所以在冷卻水流失事故以及喪失場外電源情境中，值班主任以及運轉員需要設法對爐心補充冷卻水、維持反應爐壓力、並且在事故造成更嚴重的影響之前停爐。

V&V2.5 冷卻水流失事故以及喪失場外電源情境一開始電廠立即發出停爐的信號，同時全部的 RIP 跳機，以下為資料觀測內容：

(一)在情境開始後 0~10 分鐘之間人員動作以及系統狀態

反應爐心操作運轉員 (Reactor Operator；RO)偵測到訊號並且把反應爐的模式轉換為停爐狀態，接著 RO 查看 WDP 並

且宣佈以下系統已經自動執行還有其相關狀態：全部的控制棒插入、緊急柴油發電機啟動、C 組緊急柴油發電機啟動失敗、RCIC 開始、而輔助運轉員 (Assistant Reactor Operator；ARO)確認飼水管線 A 破裂。在接收到 RO 以及 ARO 的資訊回報之後，值班主任 (Shift Supervisor；SS)準備進行反應器控制，同時 RO 確認反應爐水位趨勢以及電廠層級的警報系統警告 HPCF 在反應爐水位 L1.5 的狀態下作業，而 ARO 此時在監控飼水系統的狀況並且嘗試關閉飼水管線 A。

RO 確認 RHR 獨立控制系統組 I、II，SS 要求 ARO 查看目前的反應器水位，接著 RO 查看警報系統，了解場內狀況並且將警報靜默，ARO 接受 SS 指令 「查看目前的反應器水位」而使用 SPDS 查看反應器水位，並且回報反應器水位以及飼水系統管線 A/B 皆無法關閉。

SS 要求 ARO 查看緊急柴油發電機的狀態，ARO 接受 SS 指令並且確認緊急柴油發電機 C 失效，此時 RO 使用 FWC 查看反應爐水位趨勢，然後使用手動按鈕啟動自動洩壓系統。RO 再次的確認反應爐水位趨勢，並且回報 S/P 溫度在 59°C、水位在 726cm，SS 要求 ARO 搜尋 LOCA 的程序書，此時電廠內 HPCF C 以及 RHR C 開始自動啟動。

RO 檢查反應爐水位還維持在有效範圍，ARO 回報無法找到 LOCA 的程序書給 SS，ARO 接著將 RHR C 模式轉為 S/P 冷卻，RHR B 模式轉為 LPFL 冷卻，RHR A 轉為 standby，RO 察看了水位並且詢問 SS 是否應該把水位控制在 L8，SS 回覆將反應器水位控制高於 L8，此時電廠內的 DW 壓力到達

52KPaG、溫度達 113°C，RO 確認反應爐水位趨勢並且與 SS 討論。

(二)在情境開始後 10~20 分鐘之間人員動作以及系統狀態

RO 確認 HPCH 的狀態，而 ARO 透過監看 WDP 了解到在上次切換 RHR A 的模式時發生錯誤，重新把 RHR A 模式切換回 LPFL 模式，此時 S/P 溫度升為 60°C，RO 持續的注意反應爐水位趨勢並且跟 SS 討論，並且透過 WDP 重新確認一次主要的參數跟系統狀態。　接著 RO 確認 ACS 狀態、反應爐溫度上升速率並且與 SS 討論，ARO 試著啟動 RCIC 並且回報 SS，SS 認為 RCIC 會因為低壓力的關係而無法啟動。

(三)在情境開始後 20~30 分鐘之間人員動作以及系統狀態

RO 確認 RHR 與 HPCF 狀態並且與 ARO 討論如何啟動 HPCF，但是因為系統控制邏輯的設計，操作行為出現遲疑，因為水位高於 L8 所以 ARO 無法啟動 HPCF。RO 確認 ACS 狀態並且與 SS 討論，接著確認反應爐水位趨勢，RO 確認 HPCF 狀態並且與 SS 討論，RO 檢查關於 HPCF 的警報，ARO 檢查 AAS，RO 檢查 Main Turbine 狀態回報給 SS，確認電廠狀態，冷卻水流失事故以及喪失場外電源情境結束。

上述為 V&V 2.5 操作人員在冷卻水流失事故以及喪失場外電源情境中所執行的相關動作以及他們之間的互動，將其使用最小清單人員任務分析法整理成下圖 4-2，圖內容若太小請參閱附件 E，藉此方法可以找出任務執行的時候需要哪些人機介面協助操作人員了解電廠現況、控制電廠系統，接著將模擬

內容所需之人機介面整理成附件 B-1、B-2。

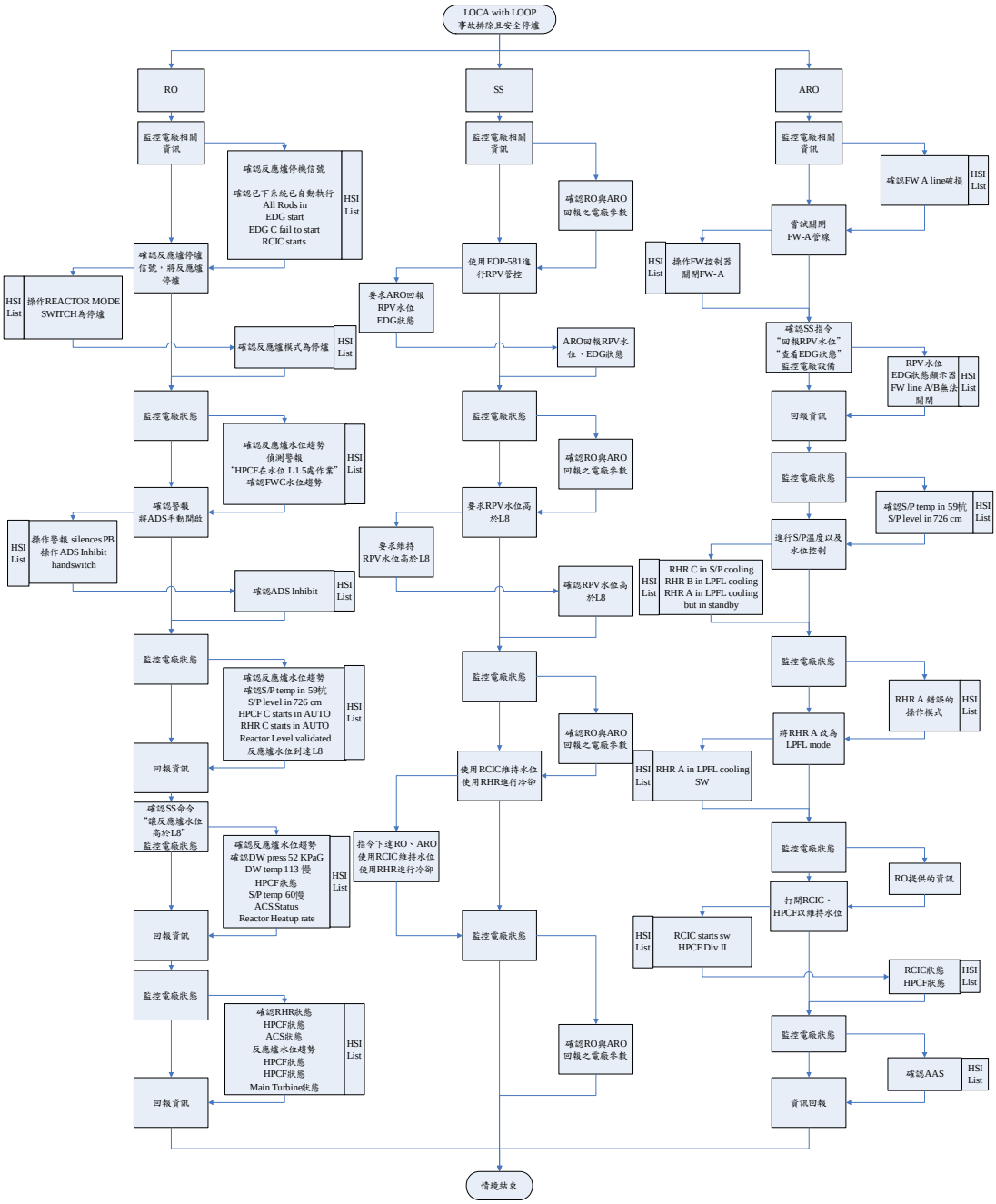


圖4-2 人員操作流程分析圖

四、比對結果

將驗證端與設計端的人機介面清單比對，發現其中爐內泵(Reactor Internal Pumps, RIP)狀態顯示器，設計端提供之人機介

面清單並未包含，應是冷卻水流失事故以及喪失場外電源整個事件包含了多種程序書的操作，可能包含標準操作程序書、異常作業操作程序書、緊急操作程序，而本研究是針對緊急操作程序進行分析，而反應器控制、一次圍阻體之控制裡並未提到需要監控RIP。

至於其他關於反應器以及一次圍阻體的人機介面比對的結果皆符合，可以說設計端獲得之清單，能夠支援冷卻水流失事故以及喪失場外電源事件發生時，運轉員監控反應器以及一次圍阻體狀態。

伍、主要發現與結論

一、討論

(一)兩種分析手法討論

本研究使用兩種手法進行最小清單流程的建立與驗證，一種是在初始階段建立人機介面最小清單使用的層級分析法，另一種是在驗證階段分析人員動作進而找出人機介面最小清單的人機互動流程分析法，以下將對兩種方法進行討論。

1. 層級分析法

在第三章使用的分析手法是藉由分析緊急操作程序指導流程，進而得到人機介面的最小清單，手法分為四個部份：

(1) 一開始是定義目標，例如：反應器控制。

(2) 接著找出完成目標所需要的功能，如：確認電廠狀態需不需要進行反應器管控、進行反應爐水位控制。

(3) 將緊急操作程序對完成功能所需的程序進行整理，得到任務描述。

(4) 進而從每個部份的任務描述找出所需要之系統與相關人機介面，例如：反應器控制的 RC/L-2 要求運轉員操作以下系統維持爐心水位在 378.6 到 473.9 cm 之間：Condensate/Feedwater、Control Rods Drive System…等系統，我們可以將其整理為監控反應器水位，並操作 Condensate/Feedwater、Control Rods Drive System…等系統維持水位，根據 ABWR tier 1 的設計文件找到相關的系統以及相關的人機介面。

而這種分析方法的好處在於可以對於流程分歧時，也可

將它整合在同一個任務描述裡，例如圖 5-1 裡的其中一個控制串 C1-4，從圖中可看出在 C1-4.1、C1-4.2 的部份，因為判斷條件不同而導致兩種決策的產生，經由第三章提出的方法可以將其分歧的部份整理成圖 5-2，進而找出相關的系統以及人機介面。

然而此方法並不適用於分析運轉員操作流程，因為運轉員在實際進行情境模擬時是一連串緊湊的任務執行，在一段時間內需要操作許多不同功能的系統，而層級分析法是透過目的、功能、任務描述等層層關係找出相關的人機介面，在分析運轉員操作動作上並不是十分的直觀，需要透過一層轉換的手續，而且因為必須將運轉員操作過程依照目標、功能、任務描述進行拆解，無法直接的判斷出運轉員在哪個時段的負荷較高以及介面的使用頻率次數多寡。

C1-4 When RPV pressure drops below [1.37 MPaG (highest RPV pressure at which the shutoff head of a low-water-quality alternate injection subsystem (excluding SLC) is reached)]:

C1-4.1 Line up for injection, start pumps, and irrespective of pump NPSH and vortex limits, increase injection flow to the maximum with all systems and injection subsystems.

C1-4.2 When RPV water level drops to [0 cm (top of active fuel)], EMERGENCY RPV DEPRESSURIZATION IS REQUIRED; line up for injection, start pumps, and increase injection flow to the maximum with all alternate injection subsystems.

If RPV water level cannot be restored and maintained above [0 cm (top of active fuel)], PRIMARY CONTAINMENT FLOODING IS REQUIRED; enter [procedure developed from Contingency #6].

圖5-1 Contingency #1 Alternative Level Control部分控制串

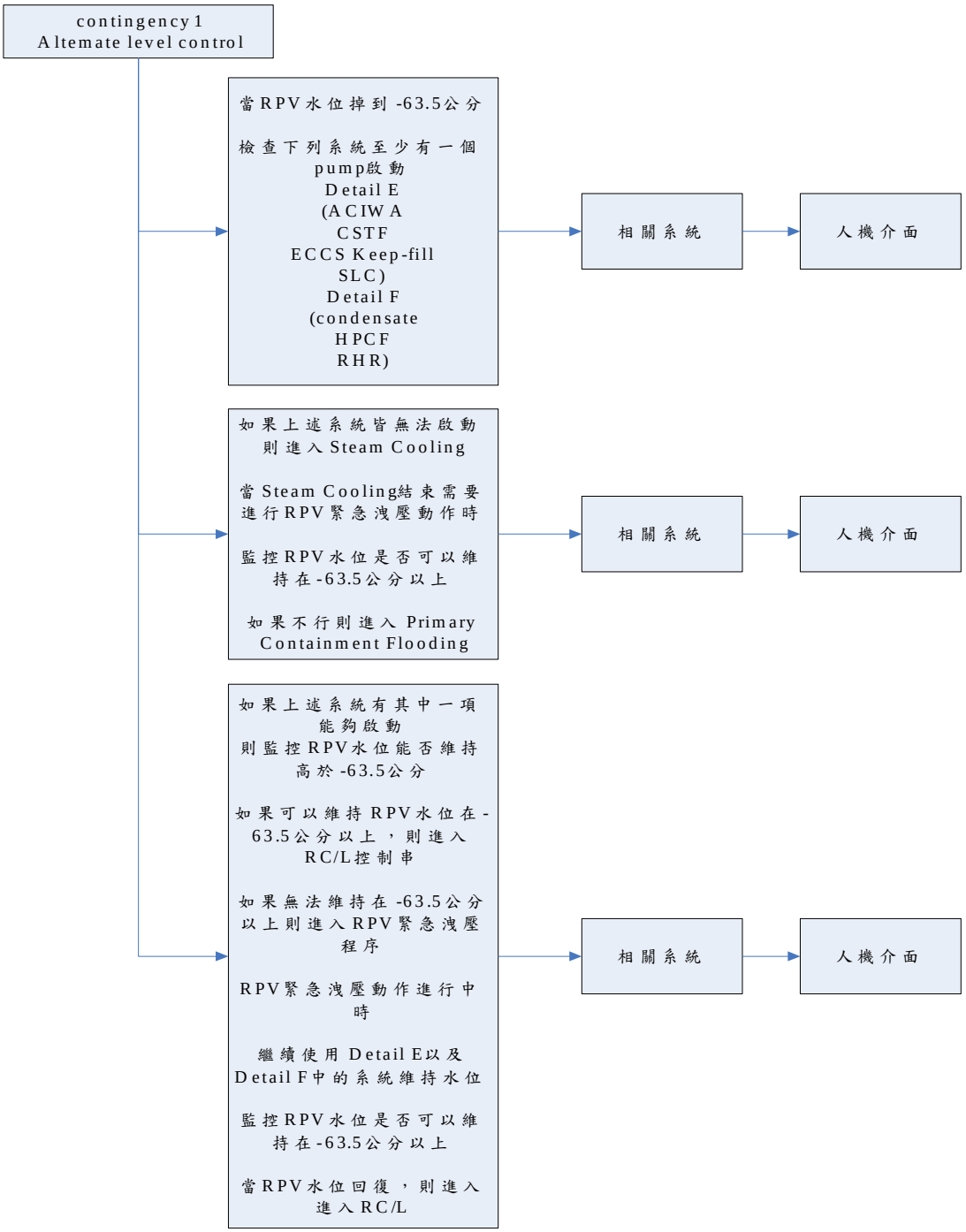


圖5-2 Contingency #1 Alternative Level Control 控制串層級分析圖

2. 人機互動流程分析法

第四章使用的人機互動流程分析法，使用操作程序圖的概念進行運轉員在 V&V2.5 情境模擬中操作流程的分析，下

圖 5-3 是節錄 V&V2.5 運轉員處理異常事故時的部分作業情形，事故剛開始發生時運轉員需要掌握電廠狀況，所以運轉員檢視了顯示電廠相關參數的人機介面，發現部分系統為了減緩事故危害已經自動啟動，接著運轉員接收到反應爐停爐信號，而將反應爐運轉模式切換為停爐狀態，然後經由相關的指示器確定反應爐運轉模式切換為停爐狀態。

使用此種分析方法的好處在於它可以了解運轉員進行此操作動作的目的，是接收到值班主任的指示或是注意到顯示器上異狀，再者，此種分析方法是依照時間次序的特性進行，故可以了解到在模擬情境的各個階段運轉員需要哪些人機介面來完成任務指示，並且在高工作負荷時需不需要額外的人機介面輔助運轉員了解電廠狀況。

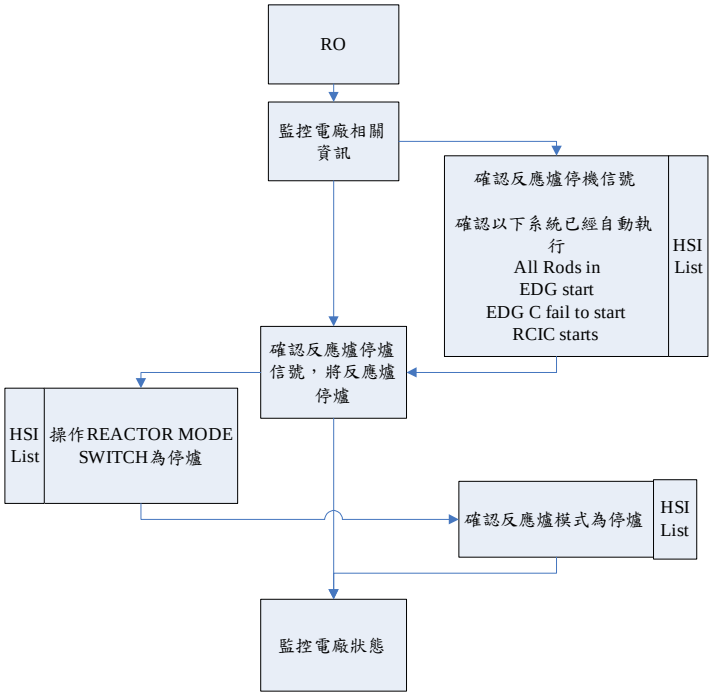


圖5-3　V&V2.5情境中運轉員操作流程圖

(二)人機介面最小清單

本研究依循緊急操作程序指導原則找出人機介面最小清單，並且透過核電廠 V&V2.5 情境模擬驗證方法是否有效，經過人機介面清單的比對，發現從設計端找出之人機介面清單多於驗證端之人機介面清單，且設計端的人機介面清單包含了驗證端所需的人機介面，也就是說在冷卻水流失事故以及喪失場外電源的情境中，設計端提供的人機介面可以讓運轉員在事故發生時，即時監控反應爐以及一次圍阻體的狀態。

但是本研究從緊急操作程序指導原則找出之人機介面清單是屬於系統顯示器以及控制器的清單，還缺少警報器的清單，而主控制室的設計裡有警報系統 (Alarm and Annunciator System, AAS)，且 ABWR Tier 1 的設計文件裡也包含警報器的設計，故如何定義出警報器的設計標準，而哪些警報器又視為必需，在整個緊急操作過程中應該針對哪些情況設立警報器，以提升運轉員的情境知覺，還需進一步的探討。

二、結論

本研究根據現行的法規與準則，發展一套關於核電廠主控制室儀控設備最小清單的建立方法，以緊急操作程序指導原則內容進行分析找出儀控設備的最小清單，並且透過核電廠人因工程 V&V2.5 的情境模擬資料，將操作人員在模擬情境中所使用的人機介面進行驗證，經過兩者人機介面清單的比對，發現本研究第三章提出之層級分析法所得到的人機介面清單可以包含並支持 V&V2.5 作業內容所需之人機介面，由設計基準事故冷卻水流失事故以及喪失場外電源的事故排除流程可說明，從緊急操作程序

「反應器控制」以及「一次圍阻體之控制」找出之人機介面最小清單可以支持解決緊急事故，確立了本研究之想法的可行性。

此外，有關最小清單的人因驗證結果顯示，藉由層級分析法所得執行 EOP581 的最小清單，較現行電廠人機介面清單多了一個 RIP 顯示，本研究認為此結果的主要原因為所選擇的進行人機互動流程分析的緊急異常事故案例為冷卻水流失事故以及喪失場外電源，當運轉人員在處理此事故時雖然會先檢視 EOP-581 與 EOP-582，但隨著事故狀況的演進，則可能會再需要其他的 EOP (如：EOP-583、EOP-584)來輔助事故的處理，甚至所有的 EOP 皆可能會使用到，但本研究僅針對 EOP-581 與 EOP-582 進行層級分析，因而產生驗證端的最小清單分析結果項目會多餘設計端分析結果之情形，此外，分析結果亦能證明現階段進步型核電廠主控制人機介面最小清單是達到「足夠維持核能電廠安全」的目標，原因即在於現實所具備的人機介面已包含緊急異常操作程序書所提及之項目，因此運轉員在處理緊急異常事故時便可以在最快的時間內獲得所需參考之資訊，進而有效地完成系統之操作。雖然結果未如預期般理想，不過問題的癥結並非無法解釋，故本研究所提出之最小清單分析與驗證方法仍具實用價值。

三、未來研究與建議

最小清單係指當進步型核能電廠發生緊急狀況時，主控制室內能輔助運轉人員處理異常事故的最基本、最重要之人機介面項目之清單，換言之，最小清單的完整性將攸關於核能電廠運轉之安全。而核能電廠在正式商轉前必需先向政府管制單位 (如：行政院原子能委員會)確保其運轉之安全性，進以避免發生危及人

員生命財產之重大事故，因此，與運轉安全息息相關之人機介面最小清單即是審查的重點之一，本研究所提出之結合層級分析與人機互動流程分析的最小清單分析與驗證方法將能提供給管制單位有系統地依據作業流程將人機介面的最小清單進行檢核，藉由檢核結果便可了解目前主控制室內的最小清單是否具備輔助運轉員處理緊急異常事故之要求，進以有效管控核能電廠整體運作之安全。

然而，核電廠主控制室還有其他安全相關的處理程序以及輔助運轉員監控的警報系統，而這些人機介面在緊急狀況發生時是否一定要保持持續有效，還有賴於其他分析手法，如：人員的可能性風險評估 (Probability Risk Assessment, PRA)，探討人員在關鍵動作時可能需要額外的人機介面輔助其做決策。透過對運轉員作業流程進行更詳細的探討，設計能夠輔助運轉員進行事故排除的人機介面，藉此將人機介面最小清單設計更加完善。

參考文獻

1. Applicant's Design Control Document. (2010). *NRC: Issued Design Certification – ABWR.* Retrieve June 16, 2010, from http://www.nrc.gov/reactors/new-reactors/design-cert/abwr/dcd/tier-2/ch-18.pdf
2. Annett, J. & Duncan, K. D. (1967). Task analysis and training design, *Occupational Psychology*, 41, 211-21.
3. Baker, C. C., Johnson, J. H., Malone, M. T., & Malone, T. B. (1979). *Human factors engineering for Navy weapons systems*. Alexandria, VA: Essex Corporation.
4. Chuang, C. F. & Chou, H. P. (2006). Investigation on the Design of Human-System Interface for Advanced Nuclear Plant Control Room. *5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology (NPIC&HMIT 2006)*, November 12-16, 2006, Albuquerque, New Mexico.
5. DI&C-ISG-05. (2007). Interim Staff Guidance on Highly-Integrated Control Rooms-Human Factors Issues (HICR-HF).
6. EPRI 1015089. (2007) Minimum Inventory of Human-System Interfaces, Draft Report. ML071490407. U.S. Nuclear Regulatory Commission.
7. Lee, S. J., & Seong, P. H. (2006). Human-Centered HMI Design to Support Cognitive Process of Operators in Nuclear Power Plants. *5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology (NPIC&HMIT 2006)*, November 12-16, 2006, Albuquerque, New Mexico.
8. Meister, D. (1985). *Behavioral analysis and measurement methods* (pp. 66-68). New York: John Wiley & Sons.
9. O'Hara, J., Higgins, J., Persensky, J., Lewis, P. M., & Bongarra, J. P.

(2004). *Human Factors Engineering Program Review Model*. US Nuclear Regulatory Commission, Washington DC, NUREG-0711 Rev. 2

10. O'Hara, J., Persensky, J., & Szabo, A. (2006). Development of Human Factors Engineering Guidance for Safety Evaluations of Advanced Reactors. *5th international Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology (NPIC & HMIT 2006)*, November 12-16, 2006, Albuquerque, New Mexico
11. Persensky, J., Szabo, A., Plott, C., Engh, T., & Barnes, V. (2005). *Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.54(m)*. US Nuclear Regulatory Commission, Washington DC, NUREG-1791.
12. Plott, C., Engh, T., & Barnes, V. (2003). *Technical Basis for Regulatory Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.54(m)*. US Nuclear Regulatory Commission, Washington DC, NUREG/CR-6838.
13. Sanders, M. S. & McCormick, E. J. (1992). *Human factors in engineering and design*, Seventh Edition. McGRAW-HILL, INC.
14. Walley, S. P. & Shepherd, A. (1992). The task analysis process. In B. Krwan, & L.K. Ainsworth (Eds.), *A guide to task analysis*. Washington, DC: Taylor & Francis, Inc.
15. Wickens, C. D. & Hollands, J. G., (2000). *Engineering Psychology and Human Performance*, 3rd ed. Prentice Hall, Saddle River, NJ.

附件 A-1　RPV Control HSI list

RPV control HSI list				
任務描述	相關系統	人機介面	SDCV	take only one action
RC-enter condition	NBS	RPV 參數顯示器 Drywell 參數顯示器 反應爐功率顯示器		
RC-1	RPS	反應爐停爐顯示器 反應爐停爐控制器		
RC-2	RCIS	控制棒全入顯示器		
	SLC	注硼顯示器		
RC/L-1	MS	MSIV 狀態顯示器 MSIV 控制器		
	FW	FW 狀態顯示器 FW 控制器		
	EDG	EDG 狀態顯示器 EDG 控制器		
	ECCS	RCIC 狀態顯示器 RCIC 控制器 HPCF 狀態顯示器 HPCF 控制器 RHR 狀態顯示器 RHR 控制器		
RC/L-2.1	NBS	RPV 參數顯示器		
	CFS	CFS 狀態顯示器 CFS 控制器		
	CRD	CRD 狀態顯示器 CRD 控制器		
	RCIC	RCIC 狀態顯示器 RCIC 控制器		
	HPCF	HPCF 狀態顯示器 HPCF 控制器		
	RHR	RHR 狀態顯示器 RHR 控制器		
RC/L-2.2	NBS	RPV 參數顯示器		
	CSTF	CSTF 狀態顯示器 CSTF 控制器		
	SLC	SLC Test Tank water level SLC Boron Tank water level SLC 控制器		

附件 A-1　RPV Control HSI list (續)

RPV control HSI list				
任務描述	相關系統	人機介面	SDCV	take only one action
RC/L-2.3	MS	ADS 狀態顯示器 ADS 控制器		
RC/P-1	NBS	RPV 參數顯示器 Drywell 參數顯示器		
	RHR	RHR 狀態顯示器 RHR 控制器		
	MS	SRVs 狀態顯示器 SRVs 控制器		
RC/P-2	NBS	RPV 參數顯示器		
	MS	MSL drain 控制器		
	RCIC	RCIC 狀態顯示器 RCIC 控制器		
	RWCU	RWCU 狀態顯示器 RWCU 控制器		
	MFTP	Turbine-Driven water pump 顯示器 Turbine-Driven water pump 控制器		
RC/P-3	NBS	RPV 參數顯示器		
RC/P-4	NBS	RPV 參數顯示器 Drywell 參數顯示器		
	RHR	RHR 狀態顯示器 RHR 控制器		

附件 A-2　Primary Containment Control HSI list

primary containment control HSI list				
任務描述	相關系統	人機介面	SDCV	take only one action
Enter condition	NBS CMS	Drywell 參數顯示器 Suppression Pool 參數顯示器 Wetwell 氫氣顯示器 Drywell 氫氣顯示器		
PC/P	NBS	Drywell 參數顯示器		
	SGTS	SGTS(B、C) 控制器 SGTS 狀態顯示器		
	RBHVAC	RBHVAC System 控制器 RBHVAC System 狀態顯示器		
	NBS	Wetwell 參數顯示器 Drywell 參數顯示器		
	ACS	Suppression Pool 參數顯示器		
	RHR	RHR(B、C) 控制器		
	NBS ACS	Wetwell 參數顯示器 Suppression Pool 參數顯示器 drywell 參數顯示器		
	RHR	RHR(B、C) 控制器 RHR(B、C) 狀態顯示器 Drywell Cooling System fan control (other control)		
	ACS	ACS controls for venting and purging of the containment (other controls) ACS 狀態顯示器		
DW/T	NBS	Drywell 參數顯示器		
	SGT	Drywell Cooling System fan control(other control) SGT 狀態顯示器		
DW/T-1	NBS	Drywell 參數顯示器		
	ACS	Suppression Pool 參數顯示器		
	SGT	Drywell Cooling System fan control(other control) SGT 狀態顯示器		
	RHR	RHR(B、C) 控制器 RHR(B、C) 狀態顯示器		

附件 A-2　Primary Containment Control HSI list (續)

primary containment control HSI list				
任務描述	相關系統	人機介面	SDCV	take only one action
SP/T	ACS	Suppression Pool 參數顯示器		
	RCIS	Reactor power 顯示器		
	RPVS	RPV 參數顯示器		
	RHR	RHR(A、B、C) 控制器		
SP/L	ACS	Suppression Pool 參數顯示器		
	SPCU	SPCU 控制器 SPCU 狀態顯示器		
	RCIC	RCIC 控制器 RCIC 狀態顯示器		
	HPCF	HPCF 控制器 HPCF 狀態顯示器		
	RHR	RHR 控制器 RHR 狀態顯示器		
PC/G	CMS	Wetwell 氫氣顯示器 Drywell 氫氣顯示器		
	ACS	Suppression Pool 參數顯示器 ACS 控制器 ACS 狀態顯示器		
	FCS	FCS 控制器 FCS 狀態顯示器		

附件 B-1　LOCA with LOOP 人機介面

LOCA with LOOP HSI Inventory				
時間	相關系統	人機介面	SDCV	take only one action
情境開始後 0 min	NBS RPS	RIP 狀態顯示器 反應爐停爐顯示器 反應爐停爐控制器		
1 min	RCIS EDG FW	控制棒狀態顯示器 EDG 狀態顯示器 FW 狀態顯示器		
2 min	NBS Plant alarms FW	RPV 水位顯示器 HPCF 警報器 FW 狀態顯示器 FW 控制器		
3 min	RHR	RHR 控制器		
4 min	NBS Plant alarms FW	RPV 水位顯示器 警報靜默鍵 FW 狀態顯示器		
5 min	EDG FWC MS	EDG 狀態顯示器 EDG 控制器 RPV 水位趨勢圖 ADS 控制器		
6 min	MS	ADS 控制器		
7 min	FWC NBS HPCF RHR	反應爐水位趨勢圖 S/P 溫度水位顯示器 HPCF 狀態顯示器 RHR 狀態顯示器		
9 min	C91 RHR	RPV water validation RHR 控制器		
9 min	NBS	RPV 水位顯示器 Dw 溫度壓力顯示器		
10 min	FWC	反應爐水位趨勢圖		
11-12 min	HPCF RHR NBS	HPCH 狀態顯示器 RHR 狀態顯示器 RHR 控制器 S/P 溫度顯示器		
14 min	FWC	反應爐水位趨勢圖		
18 min	ACS	ACS 狀態顯示器		

附件 B-1　LOCA with LOOP 人機介面 (續)

LOCA with LOOP HSI Inventory				
時間	相關系統	人機介面	SDCV	take only one action
21 min	APR RCIC	反應爐溫度速率 RCIC 控制器		
23 min	HPCF RHR	HPCF 狀態顯示器 HPCH 控制器 RHR 狀態顯示器 RHR 控制器		
25 min	ACS FWC HPCF	ACS 狀態顯示器 反應爐水位趨勢圖 HPCF 狀態顯示器		
30 min	Alarm System AAS TURB	HPCF 警報器 AAS 狀態 Main TURB 狀態顯示器		

附件 B-2　RPV Control 以及 Primary Containment Control 與 LOCA with LOOP 人機介面比較

設計端人機介面清單			驗證端人機介面清單
	RPV Control HSI List	Primary Containment Control HSI List	LOCA with LOOP HSI List
displays	RPV 參數顯示器 Drywell 參數顯示器 反應爐功率顯示器 反應爐停爐顯示器 控制棒全入顯示器 注硼顯示器 MSIV 狀態顯示器 FW 狀態顯示器 EDG 狀態顯示器 RCIC 狀態顯示器 HPCF 狀態顯示器 RHR 狀態顯示器 CFS 狀態顯示器 CRD 狀態顯示器 CSTF 狀態顯示器 SLC Test Tank water level SLC Boron Tank water level ADS 狀態顯示器 SRVs 狀態顯示器 RWCU 狀態顯示器 Turbine-Driven water pump 顯示器	Drywell 參數顯示器 Suppression Pool 參數顯示器 Wetwell 氫氣顯示器 Drywell 氫氣顯示器 SGTS 狀態顯示器 RBHVAC System 狀態顯示器 RHR(B、C) 狀態顯示器 ACS 狀態顯示器 SGT 狀態顯示器 RCIC 狀態顯示器 HPCF 狀態顯示器 Reactor power 顯示器 RPV 參數顯示器 FCS 狀態顯示器	RIP 狀態顯示器 反應爐停爐顯示器 控制棒狀態顯示器 EDG 狀態顯示器 FW 狀態顯示器 RPV 水位顯示器 S/P 溫度水位顯示器 HPCF 狀態顯示器 RHR 狀態顯示器 Dw 溫度壓力顯示器 ACS 狀態顯示器 Main TURB 狀態顯示器

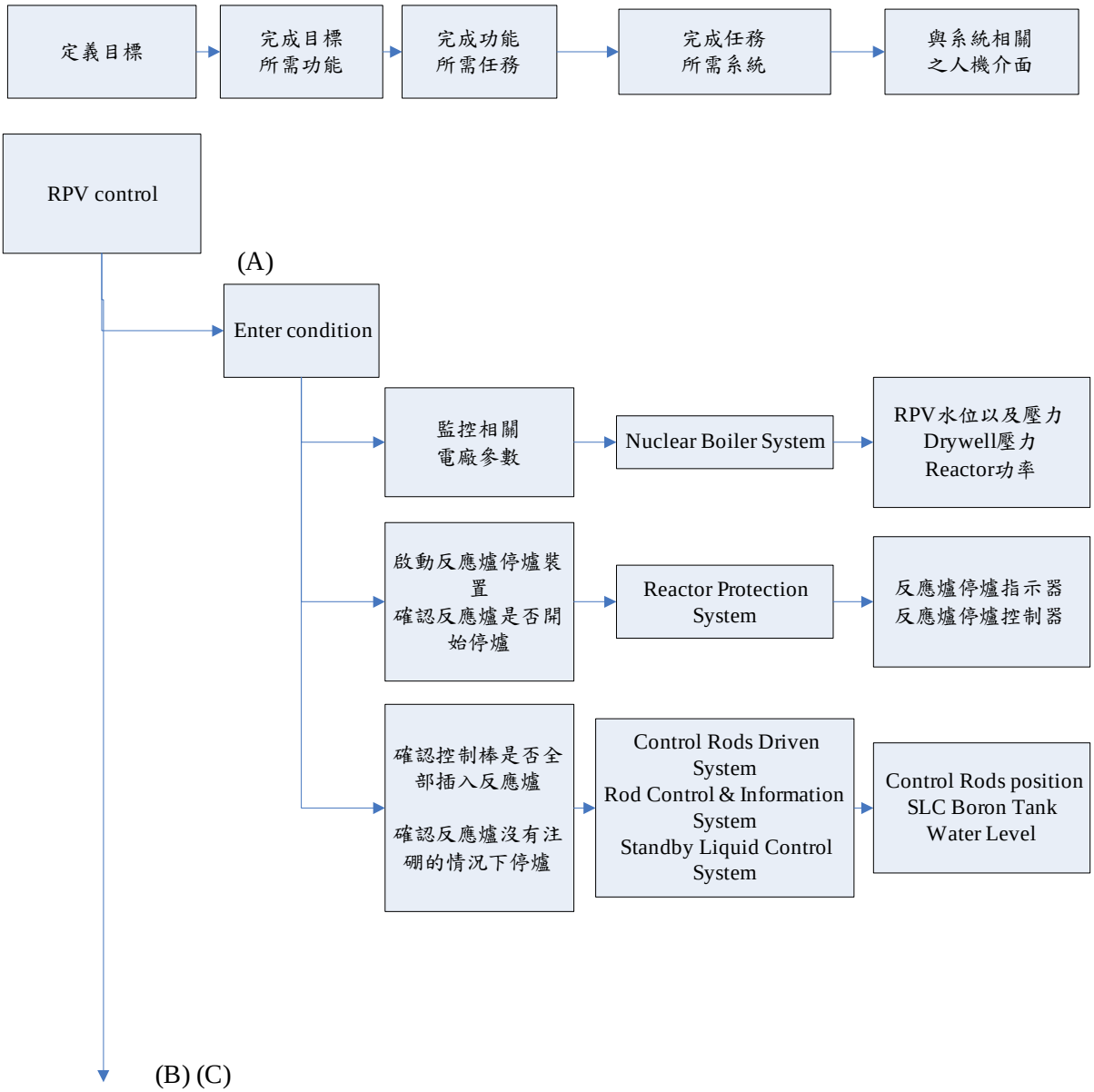
附件 B-2　RPV Control 以及 Primary Containment Control 與 LOCA with LOOP 人機介面比較(續)

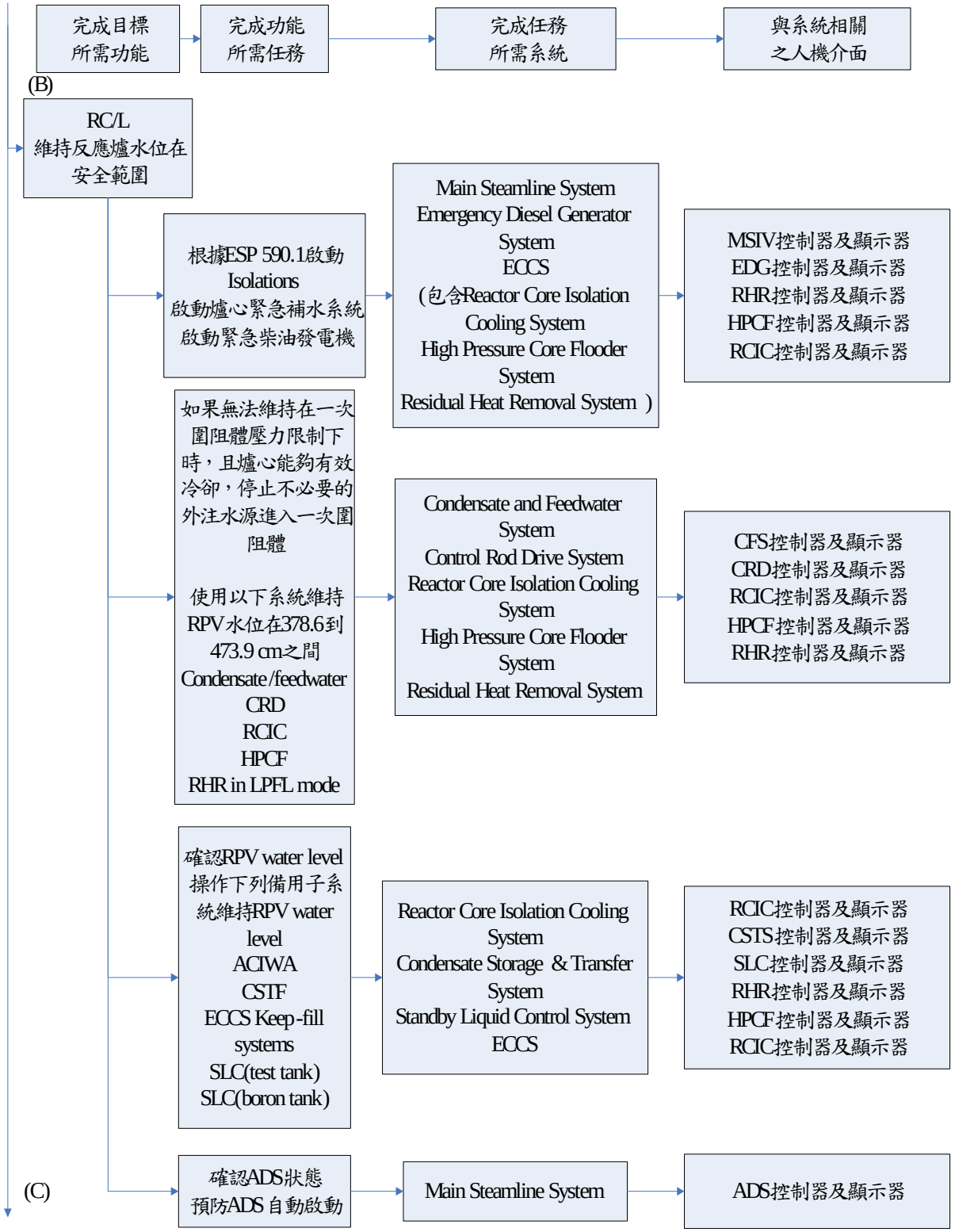
設計端人機介面清單			驗證端人機介面清單
	RPV Control HSI List	Primary Containment Control HSI List	LOCA with LOOP HSI List
controls	反應爐停爐控制器 MSIV 控制器 FW 控制器 EDG 控制器 RCIC 控制器 HPCF 控制器 RHR 控制器 CFS 控制器 CRD 控制器 CSTF 控制器 SLC 控制器 ADS 控制器 SRVs 控制器 MSL drain 控制器 RWCU 控制器	SGTS(B、C) 控制器 RBHVAC System 控制器 RHR(B、C) 控制器 ACS controls for venting and purging of the containment (other controls) Drywell Cooling System fan control(other control) SPCU 控制器 RCIC 控制器 HPCF 控制器 FCS 控制器	反應爐停爐控制器 FW 控制器 EDG 控制器 ADS 控制器 RHR 控制器 RCIC 控制器 HPCH 控制器

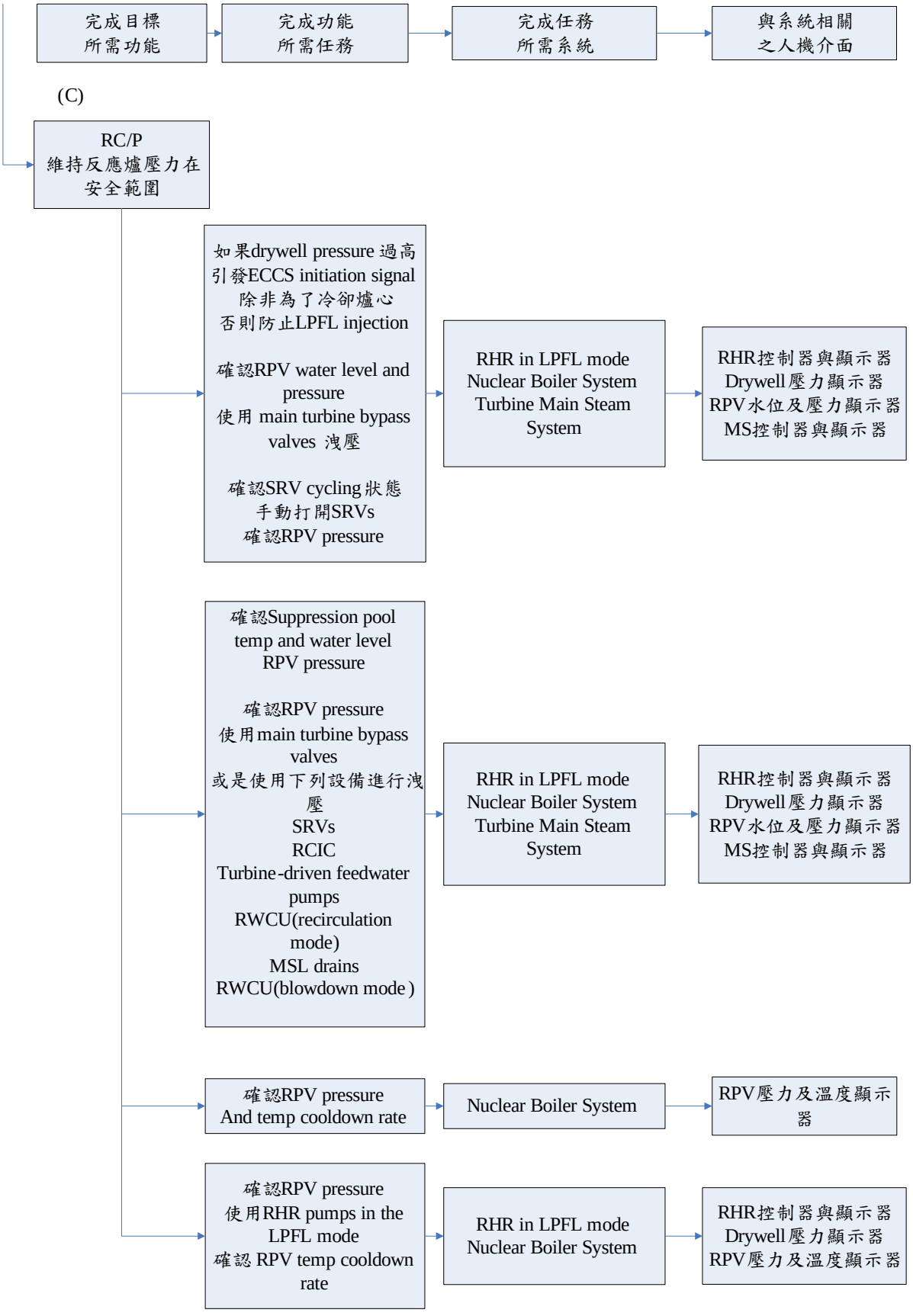
附件 C　核電廠系統英文縮寫對照表

縮寫	字義	中譯
AAS	Alarm and Annunciator System	
ABWR	Advanced Boiling Water Reactor	進步型沸水式反應
ACS	atmospheric control system	
ADS	automatic depressurization system	
CMS	containment monitoring system	
COPS	Containment Overpressure Protection System	圍阻體過壓保護系統
CRD	control rod drive	控制棒驅動系統
DCIS	digital control and instrumentation system	
ECCS	Emergency Core Cooling System	緊急核心冷卻系統
ECW	emergency chilled water	
EDG	emergency diesel generator	緊急柴油發電機
FW	Feedwater Control System	
FWLB	feed water line break	飼水破管
HPCF	high pressure core flood	高壓爐心灌水系統
HVAC	heating ventilating and air conditioning	
LOCA	loss of coolant accident	冷卻水流失事件
LOOP	loss of off-site power	失去外電源
LPFL	low pressure flooder mode	低壓灌水模式
MCC	main control console	
MS	Main Steam System	
MSL	main stream line	主要流動管線
RBCW	reactor building cooling water	
RBHV	reactor building heating ventilating and air conditioning	
RCIC	reactor core isolation cooling	反應爐爐心隔離冷卻系統
RCIR	Reactor Recirculation System	再循環水流量控制系統
RCIS	Rod Control and Information System	控制棒和資訊系統
RFC	Recirculation Flow Control System	再循環流量控制系統
RHR	residual heart removal	餘熱移除系統
RIP	Reactor Internal Pump	反應爐內部再循環水泵
RPV	reactor pressure vessel	反應爐爐心
RWCU	Reactor Water Cleanup System	
SGT	standby gas treatment system	
SGTR	steam generator tube rupture	
SLC	Standby Liquid Control	
SPDS	Safety Parameter Display System	
SRV	Safety Relief Valve	
SSLC	Safety System Logic and Control System	
VDU	Video display units	影像顯示單元
WDP	wide display panel	大型展示盤

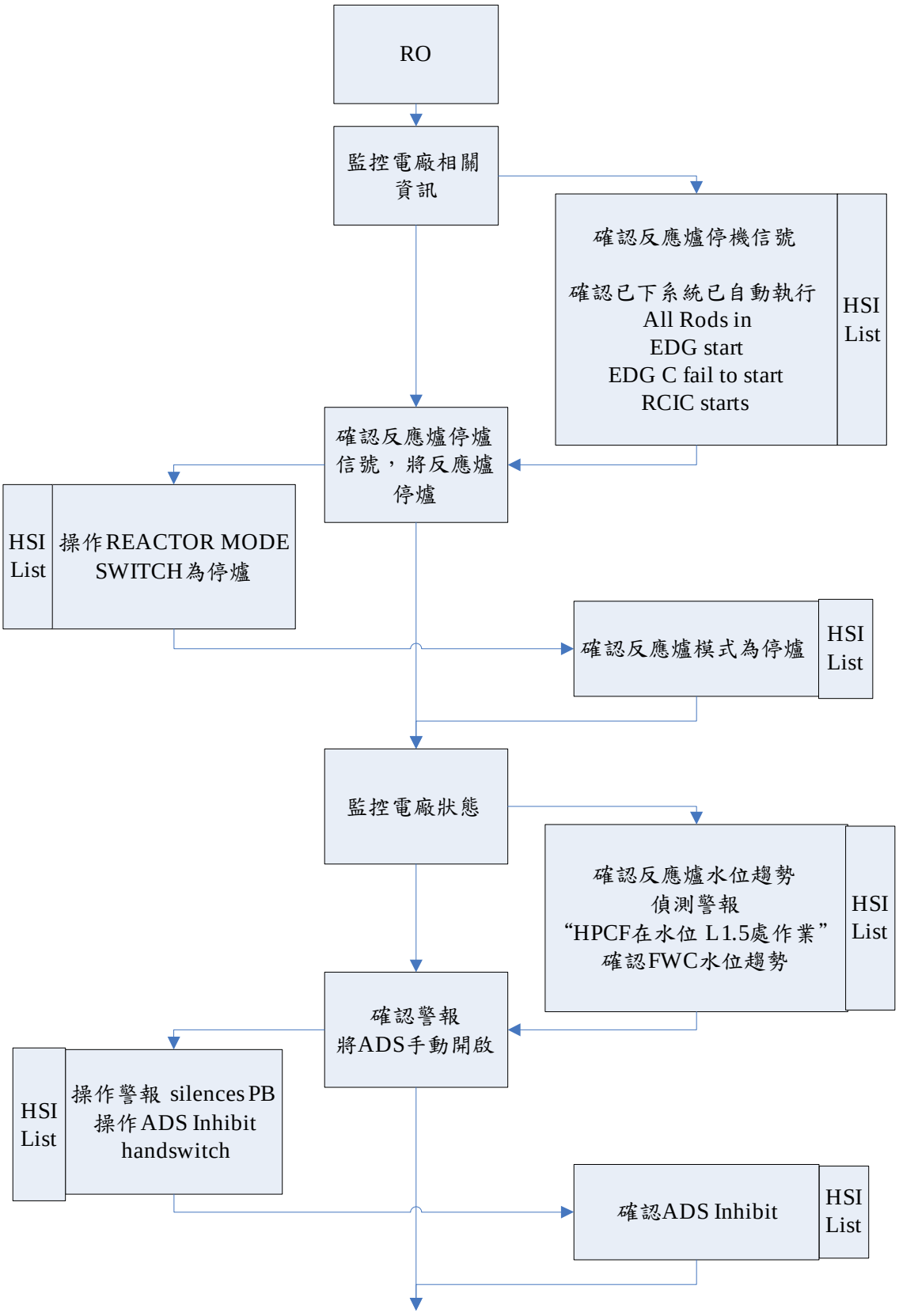
附件 D　RPV Control 層級分析圖

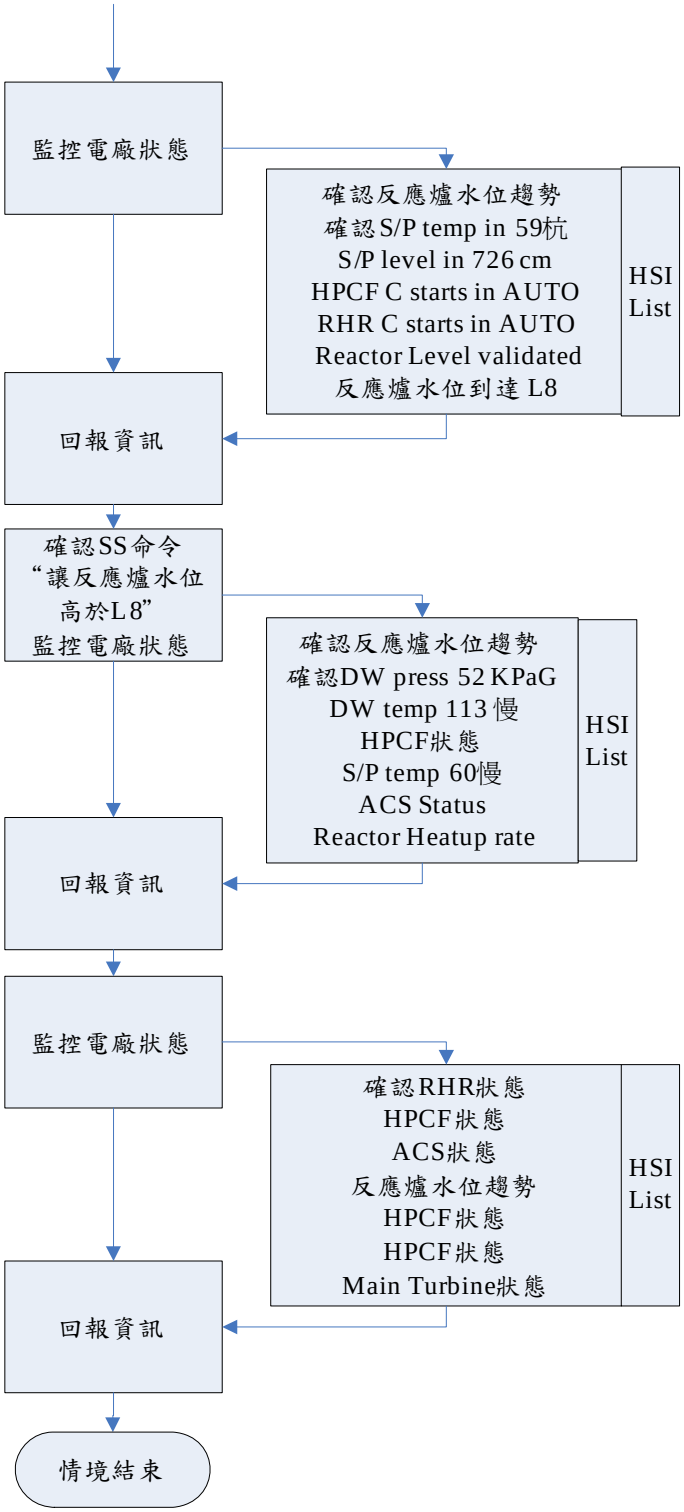


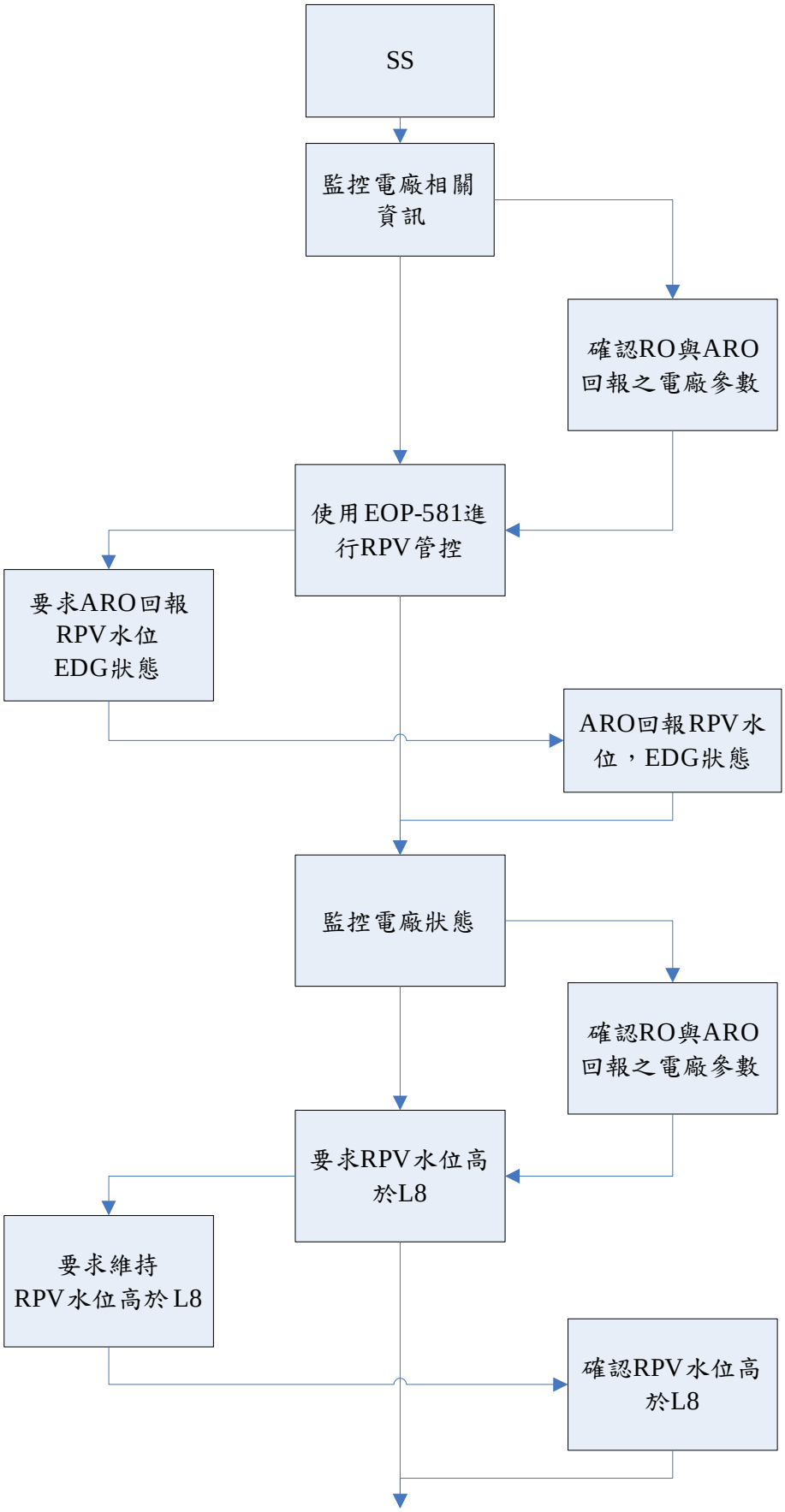

完成目標
所需功能
完成功能
所需任務
完成任務
所需系統
與系統相關
之人機介面
(B)
RC/L
維持反應爐水位在
安全範圍
根據ESP 590.1啟動
Isolations
啟動爐心緊急補水系統
啟動緊急柴油發電機
Main Steamline System
Emergency Diesel Generator
System
ECCS
(包含Reactor Core Isolation
Cooling System
High Pressure Core Flooder
System
Residual Heat Removal System)
MSIV控制器及顯示器
EDG控制器及顯示器
RHR控制器及顯示器
HPCF控制器及顯示器
RCIC控制器及顯示器
如果無法維持在一次
圍阻體壓力限制下
時，且爐心能夠有效
冷卻，停止不必要的
外注水源進入一次圍
阻體
使用以下系統維持
RPV水位在378.6到
473.9 cm之間
Condensate/feedwater
CRD
RCIC
HPCF
RHR in LPFL mode
Condensate and Feedwater
System
Control Rod Drive System
Reactor Core Isolation Cooling
System
High Pressure Core Flooder
System
Residual Heat Removal System
CFS控制器及顯示器
CRD控制器及顯示器
RCIC控制器及顯示器
HPCF控制器及顯示器
RHR控制器及顯示器
確認RPV water level
操作下列備用子系
統維持RPV water
level
ACIWA
CSTF
ECCS Keep-fill
systems
SLC(test tank)
SLC(boron tank)
Reactor Core Isolation Cooling
System
Condensate Storage & Transfer
System
Standby Liquid Control System
ECCS
RCIC控制器及顯示器
CSTS控制器及顯示器
SLC控制器及顯示器
RHR控制器及顯示器
HPCF控制器及顯示器
RCIC控制器及顯示器
(C)
確認ADS狀態
預防ADS自動啟動
Main Steamline System
ADS控制器及顯示器

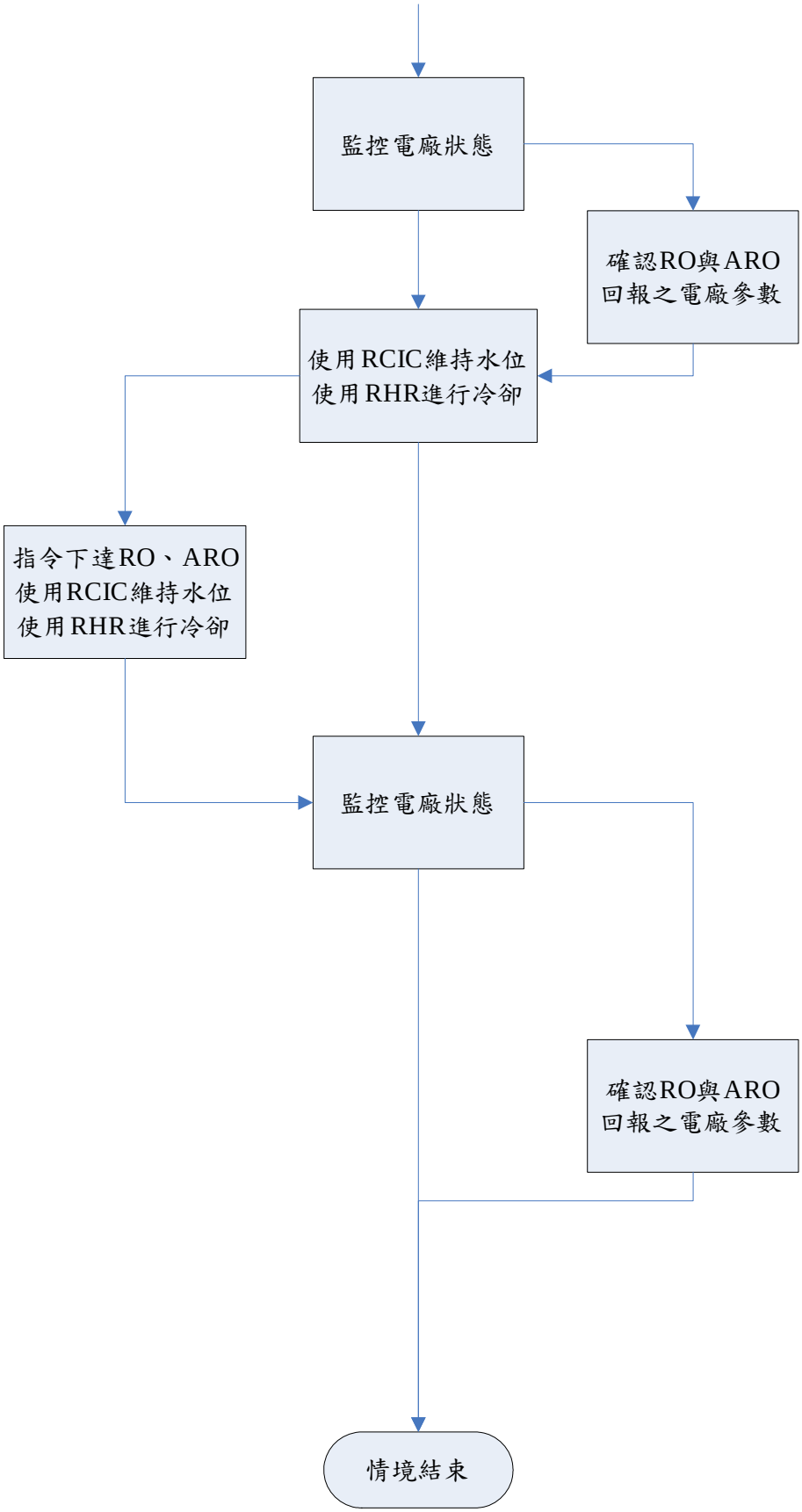

完成目標
所需功能
完成功能
所需任務
完成任務
所需系統
與系統相關
之人機介面
(C)
RC/P
維持反應爐壓力在
安全範圍
如果drywell pressure 過高
引發ECCS initiation signal
除非為了冷卻爐心
否則防止LPFL injection
確認RPV water level and
pressure
使用 main turbine bypass
valves 洩壓
確認SRV cycling 狀態
手動打開SRVs
確認RPV pressure
RHR in LPFL mode
Nuclear Boiler System
Turbine Main Steam
System
RHR控制器與顯示器
Drywell壓力顯示器
RPV水位及壓力顯示器
MS控制器與顯示器
確認Suppression pool
temp and water level
RPV pressure
確認RPV pressure
使用main turbine bypass
valves
或是使用下列設備進行洩
壓
SRVs
RCIC
Turbine-driven feedwater
pumps
RWCU(recirculation
mode)
MSL drains
RWCU(blowdown mode)
RHR in LPFL mode
Nuclear Boiler System
Turbine Main Steam
System
RHR控制器與顯示器
Drywell壓力顯示器
RPV水位及壓力顯示器
MS控制器與顯示器
確認RPV pressure
And temp cooldown rate
Nuclear Boiler System
RPV壓力及溫度顯示
器
確認RPV pressure
使用RHR pumps in the
LPFL mode
確認 RPV temp cooldown
rate
RHR in LPFL mode
Nuclear Boiler System
RHR控制器與顯示器
Drywell壓力顯示器
RPV壓力及溫度顯示器

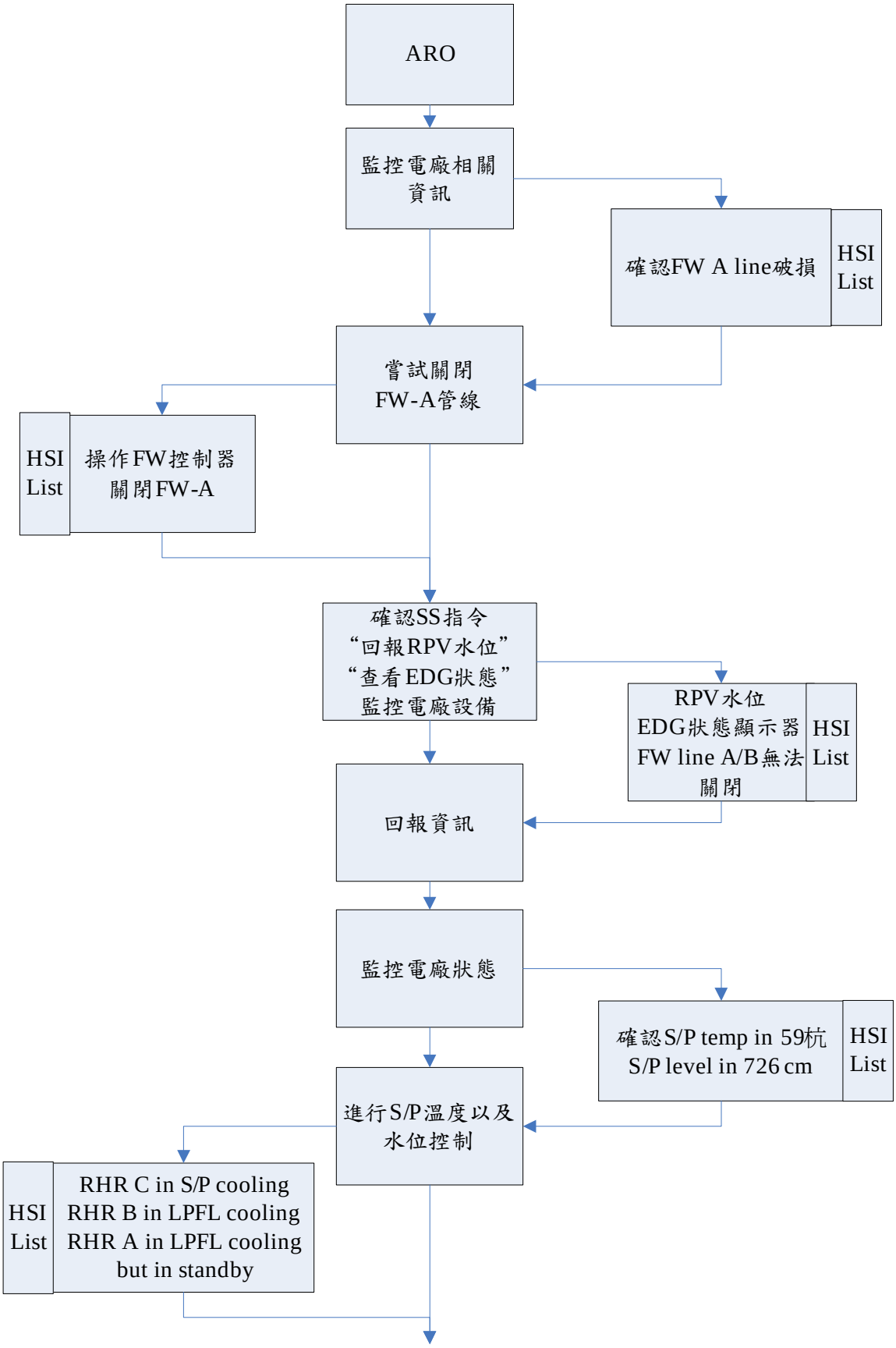
附件 E　LOCA with LOOP 人員操作流程分析圖

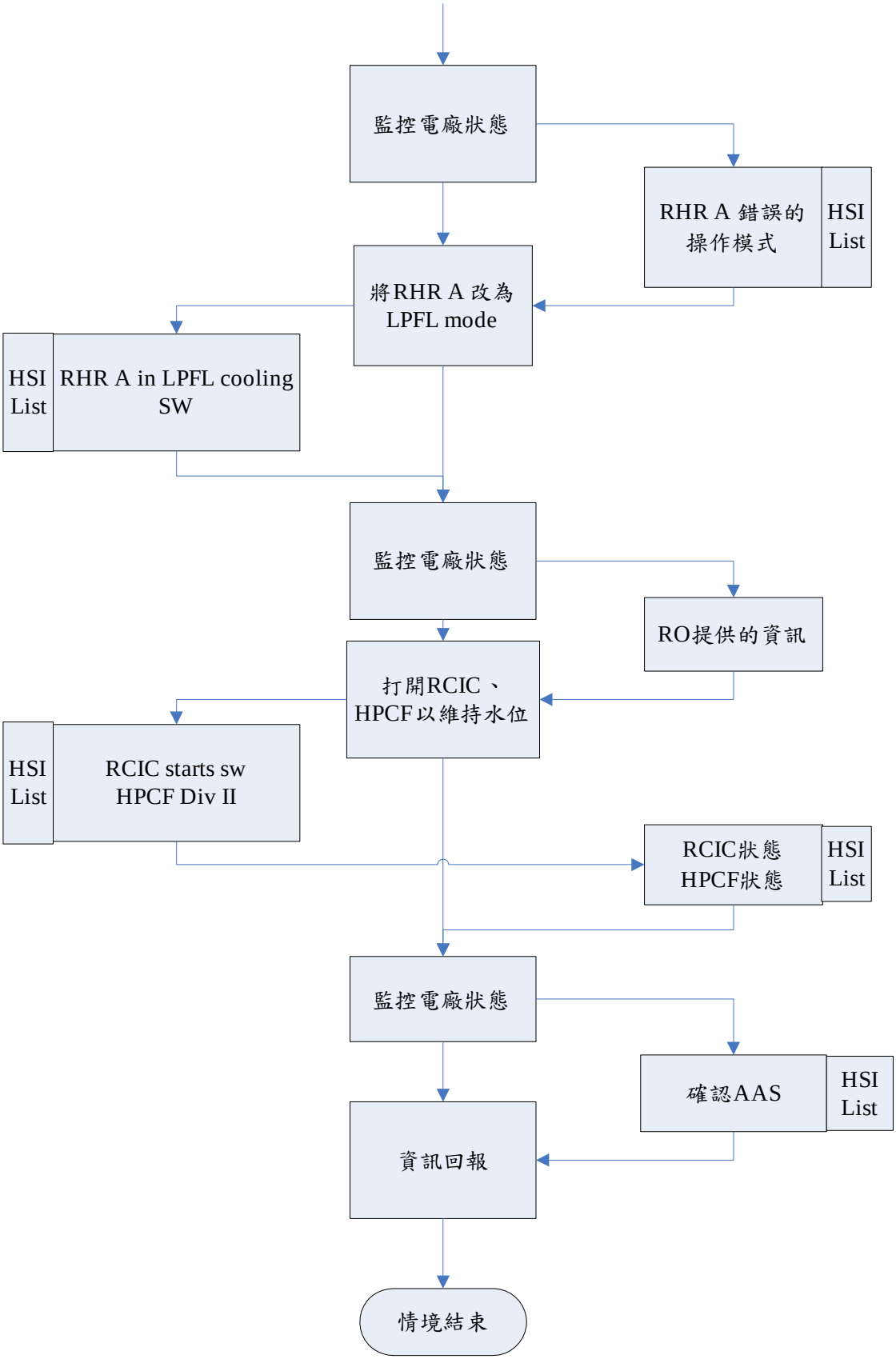



監控電廠狀態
確認反應爐水位趨勢
確認S/P temp in 59杭
S/P level in 726 cm
HPCF C starts in AUTO
RHR C starts in AUTO
Reactor Level validated
反應爐水位到達 L8
HSI List
回報資訊
確認SS命令
“讓反應爐水位
高於L8”
監控電廠狀態
確認反應爐水位趨勢
確認DW press 52 KPaG
DW temp 113 慢
HPCF狀態
S/P temp 60慢
ACS Status
Reactor Heatup rate
HSI List
回報資訊
監控電廠狀態
確認RHR狀態
HPCF狀態
ACS狀態
反應爐水位趨勢
HPCF狀態
HPCF狀態
Main Turbine狀態
HSI List
回報資訊
情境結束


SS
監控電廠相關資訊
確認RO與ARO回報之電廠參數
使用EOP-581進行RPV管控
要求ARO回報RPV水位EDG狀態
ARO回報RPV水位，EDG狀態
監控電廠狀態
確認RO與ARO回報之電廠參數
要求RPV水位高於L8
要求維持RPV水位高於L8
確認RPV水位高於L8


監控電廠狀態
確認RO與ARO
回報之電廠參數
使用RCIC維持水位
使用RHR進行冷卻
指令下達RO、ARO
使用RCIC維持水位
使用RHR進行冷卻
監控電廠狀態
確認RO與ARO
回報之電廠參數
情境結束


ARO
監控電廠相關資訊
確認FW A line破損
HSI List
嘗試關閉FW-A管線
HSI List
操作FW控制器關閉FW-A
確認SS指令
“回報RPV水位”
“查看EDG狀態”
監控電廠設備
RPV水位
EDG狀態顯示器
FW line A/B無法關閉
HSI List
回報資訊
監控電廠狀態
確認S/P temp in 59杭
S/P level in 726 cm
HSI List
進行S/P溫度以及水位控制
HSI List
RHR C in S/P cooling
RHR B in LPFL cooling
RHR A in LPFL cooling
but in standby


監控電廠狀態
RHR A 錯誤的操作模式
HSI List
將RHR A 改為LPFL mode
HSI List
RHR A in LPFL cooling SW
監控電廠狀態
RO提供的資訊
打開RCIC、HPCF以維持水位
HSI List
RCIC starts sw HPCF Div II
RCIC狀態 HPCF狀態
HSI List
監控電廠狀態
確認AAS
HSI List
資訊回報
情境結束