核能電廠人員作業安全管理系統之建立
完成報告

計畫編號：NSC 88-TPC - H- 009- 001

執行時間：87 年 8 月 1 日至 88 年 7 月 31 日

計畫主持人：許尚華教授

共同主持人：吳壽山教授

行政院國家科學委員會
八十八年度電力科技產業學術合作研究計畫

核能電廠人員作業安全管理系統之建立

中華民國 88 年 7 月

中文摘要：

人員作業績效攸關核電廠之安全。綜觀核能事故與安全事件多與人員作業有關。雖然這些與人員作業有關之事件，其肇因並非人員本身，而是源由於影響人員作業之系統因素，然而研究發現作業人員通常在不知、不察覺、或心理負荷狀況下造成疏失。因此，在降低人為疏失之方法中，提昇作業人員之安全意識、改善作業方式、查核其安全作業行為，不失為有效之方法。

國內核電廠的安全作業，在「安全文化」運動、自我查證、保守決策等措施的推動之下，廠內人員作業績效已大為提昇。然而，有關包商人員之作業行為之改善尚可研究提昇，尤其是包商在維修作業中所扮演的角色日益重要。

本研究之目的是研發包商作業人員安全行為查核系統。此系統結合人因工程與品質管理之理論與做法，發展以計畫（plan）-執行（do）-驗證（check）-改善行動（action）為架構之安全行為查核表。此系統可應用於在作業前瞭解包商是否具備安全意識，是否知道有那些潛在危險因子（hazards）的存在以及減少危險因子的作業方法；在作業中，如何辨認危險狀態、如何評估執行方法是否正確；在作業後，審查所有危險因子是否解決、如何改善目前作法。

本計畫的進行分為以下幾個階段：(1)瞭解包商作業內容，(2)確認危險因子，並將之歸類，(3)建立作業人員安全行為查核系統，(4)測試，(5)技術移轉給核電廠人員。並且將來朝人員安全行為查核電腦化，便於資料監控與記錄，以符合 ISO 之要求。

本計畫預期的具體成果有兩項：(1)作業人員安全行為查核系統，與(2)技術移轉之教案，可有效提昇包商作業稽查品質，以增進核能安全。

關鍵詞：人為疏失、作業安全稽查、核能安全

英文摘要：

Human performance is very important to nuclear safety. Most of accidents and incidents were related to human error. Therefore, it is imperative that human performance be improved. The purpose of this study has two folds: (1) to develop an audit system for safe performance, and (2) to transfer the human performance audit system to Taipower personnel.

The human performance safety audit system was developed on the basis of human error theories, human error data of nuclear power plants, and task analysis. It contains a checklist of good practice of safe behavior performed during maintenance tasks. These good practices include: thorough planning, efficient resource management, pre-job reviewing and briefing, risk assessment, conscious checking, situation awareness, memory reminders, usage of feedback information, communication and coordination, housekeeping, post-job evaluation and improvement.

To effectively transfer the human performance safety audit system to Taipower personnel, course material associated with the audit system was also developed. It consists of eight modules: (1) introduction to system safety, (2) the safety management plan, (3) hazard analysis, (4) basic concepts of human performance and human error, (5) causes for human error, (6) techniques to reduce human error, (7) management of safe performance, and (8) the use of audit system.

Keywords: human error, human performance safety audit, nuclear safety

第一章　緒　論

人員作業績效影響核能安全甚鉅。綜觀核電廠事故與安全事件大約有 40% 與人員作業有關。因此，近年來無論是管制單位或者核電業者對於提昇人員作業績效的努力不餘遺力。但是一般對於人為疏失的調查與責任歸屬都直指當事者，因此人為疏失的矯治措施也多偏向：用自動化來取代人員作業，以降低人員負荷；加強訓練來彌補其知識技能的不足；與處罰當事者來減少疏失的再發生。但是，這些措施的成效卻不如預期：自動化增加了系統複雜度並且自動化的運作缺乏透明化，而使得作業人員在察覺異樣以及介入監控更加困難；加強訓練僅對作業者因欠缺相關知識與技能所造成的疏失有效，至於對熟練的作業中所犯的疏失卻無效；還有，對當事者的懲罰也僅能對那些有動機問題的違規事件有效，對於作業規畫的不當或執行的疏忽並無所助益，而且懲罰也常引起情緒反應，造成組織管理的問題。因此，為了要有效地防治人為疏失，吾人需對人為疏失是如何產生的以及它的本質要有所瞭解。

要瞭解人為疏失的本質，首先必須瞭解人員可能犯那些疏失。Rasmussen（1982）將人為疏失的型態依作業者對於作業的熟悉度和作業時的意識狀態分為三類：（1）技巧行為的疏忽(或遺忘)（skill-based slips or lapses）-作業者在執行非常熟稔的作業，通常處於無意識狀態，只是偶而注意一下作業的進行而已。此時如果注意力不當、記憶遺忘或知覺錯誤，就會發生此類疏失；（2）規則行為的錯誤（rule-based mistakes）-作業者在進行作業，遇到熟悉的問題，就會將儲存在腦中之應變法則取出。此時如果他將問題情境辨認錯誤，錯用了不適用「好」的規則或者應用了「壞」的規則，就會發生此類疏失；（3）知識行為的錯誤-作業者面臨不熟悉的問題時，他必須利用所擁有的知識，來分析與解決問題。由於人們工作記憶的限制與應用不完整的心智模型，而牽強附會(Confirmation bias)，過度自信(Overconfidence)，大一統(Similarity bias)，和祇考慮到常發生的跡象(Frequency bias)，導致決策錯誤。

至於人為疏失發生的機制是如何？由事故分析發現：1.大多數的事故是由一連串小疏失衍生而成—錯誤鍊(error chain)；2.這些疏失是後果，而非原因；真正原因乃是當事者受系統的潛在問題的影響而觸發的。而這些系統的潛在問題是由於系統元素（亦即，人員、硬體、軟體、作業）間互動不良或元素與環境之間不協調所產生的。因此，Maurino, Reason, Johnson 與 Lee（1995）將人員的失效分為活動的失效（active failures）和潛在的失效（latent failures）兩種。活動的失效是與系統直接接觸的人（如運轉人員、維修人員）產生不安全行為，改變了設備、系統的狀態，立即對系統顯現的不良後果；而潛在的失效是管理階層、設計工程師造成組織相關的弱點或層層防禦的瑕疵，蟄伏在系統中有一段期間。進而 Reason 等人對於事故的發生歷程提出了「病原論」。他認為組織的制度上的缺失促成了工作情境的不良與系統層層防禦系統的漏洞，而工作情境的不良增加活

動的失效（不安全行為）的可能性，防禦的漏洞也導致潛在的失效。若在作業當時，如果兩種失效結合互動起來就會產生意外事件。由於系統事故大多由活動的失效所觸發，以往對事故的分析與防制僅限於活動失效，因此，事故的防範成效有限，如要正本清源，就必須將事故的分析與防制延展至潛在失效，先從組織程序著手改善，進而改善工作情境因素，以防制不安全行為的發生，並且彌補防禦設施的瑕疵，以減緩不安全行為所造成的後果。

由上述之人為疏失發生機制可以發現，這些與人員作業有關之事件，人為疏失只是結果而非原因，也就是說，事故與事件的肇因並非完全在於作業人員本身，而有近因與遠因。近因乃影響人員作業之前置因素（error precursors），包括：作業要求、作業情境、人們能力與極限、與人們行為傾向，它直接觸發活動失。遠因乃組織內的弱點（organizational weaknesses），包括組織文化、制度與程序、與溝通協調。因此，人為疏失有關的事故防治，應以人們能力與行為傾向為基礎，改善組織、作業、與情境。

在發展人為疏失防制方法，回溯有關人為疏失的研究文獻，指出大多數的技能基礎疏失是在作業人員不知、不察覺、或心理負荷過重的狀況下所造成。因此，在降低人為疏失之方法中，提昇作業人員之安全意識、改善作業方式、查核其安全作業行為，不失為有效之方法。

國內核電廠的安全作業，在「安全文化」運動、「自我查證」、「保守決策」等措施的推動之下，廠內人員作業績效已大為提昇，安全事件大為減少。然而，有關包商人員之作業行為之改善尚可研究提昇，尤其是包商在維修作業中所扮演的角色日益重要。

提昇核能安全的方法，首重於事前的預防與事後的改善。目前與國內核電廠人員作業績效分析相關系統有：「台電版人員作業績效增進系統」。此一系統使用於事件發生後，對人為疏失作肇因分析，分析結果作為日後改善之依據。它於事先防範的應用，有所限制。因此，有必要發展一套著重於人員作業疏失事前預防的系統。

本研究之目的是研發包商作業人員執行有關安全作業的作業行為稽查系統。此系統結合人因工程與品質管理之理論與作法，發展以計畫(plan)-執行(do)-驗證(check)-改善行動(action)為架構之安全行為查核表。此系統可應用於：在作業前，瞭解包商是否具備安全意識，是否知道有那些潛在危險因子(hazards)的存在、瞭解相關作業以及減少危險因子的作業方法；在作業中，如何辨認危險狀態、如何評估執行方法是否正確；在作業後，審查所有危險因子是否解決、如何改善目前作法。

第二章 研究詳細內容

本計劃之研究方法與步驟主要分為兩部分來說明：(1)有關安全作業之作業行為稽查系統之建立，與(2)作業行為稽查之技術移轉。茲分述於下：

第一節　安全關鍵作業之作業行為稽查系統之建立

壹、研究方法及步驟

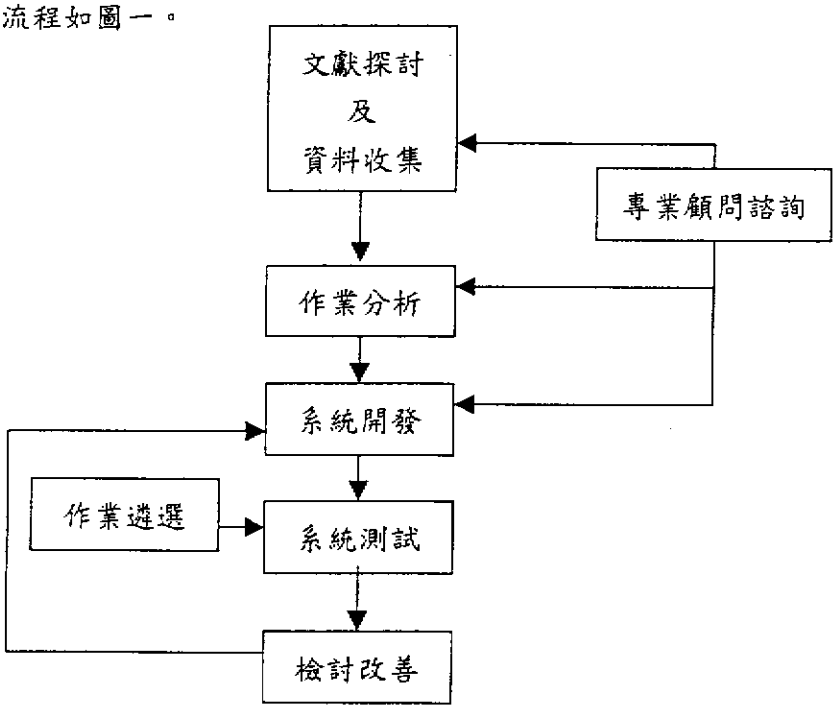
此部份之研究方法與步驟如下：

(1) 文獻探討：探討有關人為疏失、安全稽查、與品質管理之理論與作法。

(2) 瞭解包商有關安全之作業：進行作業分析，確認潛在危險因子、辨認危險狀態、危險狀態之處置方式，相關之作業，溝通、之協調需求等。

(3) 發展安全作業之作業行為稽查查核表：以品管 PDCA 為架構，作業分析結果為內容，發展作業行為稽查查核表。

本部分的流程如圖一。



圖一　稽查系統建立流程

貳、研究結果

一、文獻探討與資料收集

文獻探討著重於人為疏失與安全稽查，茲將結果分述於下：

I. 人員作業疏失模型

Reason（1995）將人員造成複雜系統故障的方式分為兩類：

（1） Active failure-會立即有不好的效應，如按錯鍵，

（2） Latent failure-會蟄伏一段時間，直至它們和局部的觸發情境相結合才會彰顯出來。這些觸發情境包括：active failure、技術差錯、或系統的不尋常狀況。作業者承襲因設計不良、目標相衝突、組織有缺陷、和管理決策錯誤所造成的系統缺陷。這些 latent failure 是由與人機介面時、空遠離的人所造成，例如，設計師、高階決策者、管制者、經理、和維修人員。

因此，人為疏失的肇因分析與防制範圍不應止於活動失效而且還需包含潛在失效。

至於人為疏失的分類，可分為下列幾個模型：

A.行為表徵模型

依外在表徵將疏失分為 omission（沒作）、commission（作錯）、沒認知到危險的情境、對問題作錯的決策、對一個情境作不適當的反應、和時機不對。但是，此種分類方式對於要瞭解疏失是怎麼發生的以及如何消除它，並無任何幫助。

B.作業與環境模型

傳統人因工程理論著重於機器設計、環境、與作業結構對人為疏失發生機率的影響。這些模型考慮到影響作業績效的因素（performance-shaping factors）例如，作業的結構和工作負荷、身體與心理壓力、以及顯示器與控制器的設計。這些模型的基本原則乃是作業。作業可以活動（activity）和所牽涉的行為種類來分類：

1.活動分類法

例如，協調、執行程序、掃瞄、辨認、問題解決、調節、駕駛、溝通、計畫、記錄、和維持。

此種模型的缺點是人們很少只從事一個作業，而且它的績效可能受別的作業所影響。

2.行為分類法

Lees 將它分為五類：

- 簡單作業：由不複雜的動作序列所組成，牽涉很少決策。錯誤的頻率受到壓力的程度、人因工程的品質、訓練與練習的品質、書面指示與使用方法的品質、人員動作間的相關性、和人員的重複性（personnel redundancy）。
- 警戒作業（vigilance tasks）：信號的偵測。影響因素有：感官型態（sensory modality）、信號的本質、強度、頻率、預期性、監視的時間、動機、和需要作的動作。
- 緊急反應作業（emergency response tasks）：影響因素是壓力。壓力低，造成不小心、不注意；壓力高，降低績效。
  - ➡兩種緊急反應：
    - ✧ 懷疑（incredulity response）-運轉員相信儀表或警報所呈現的是錯誤或假的訊號。當運轉員面臨許多假警報之後，很可能如此相信。
    - ✧ 回到舊有行為模式（revert to stereotype）
- 複雜作業（complex tasks）

C.認知機制模型

考慮到運轉員在執行作業時所用的認知機制。

1. **Norman 的疏忽模型**

在 Norman 的 Activation Trigger Schema 模型中，「基模」定義為貯存在事實或技能記憶中一個有組織架構的知識。一個意向使幾個基模變得活躍起來，每一基模皆有其啟動值（activation value）與一些觸發的狀況（trigger conditions）。外在的觸發物會引起內部的啟動，而且基模的選擇是基於此基模是否需要滿足觸發狀況。

Norman 將疏忽分為三種：

(1) 在意念形成時所犯的疏失-

(a) 模式疏失（mode error）：發生在當狀況被解釋、分類時發生錯誤，也就是說，雖然所做的動作是如同初衷，它適合所假定的狀況，但非真正的情境。此種疏失發生在系統不提供有關目前狀況清楚的回饋資訊。

(b) 描述疏失（description error）：意向的敘述不完整或模糊。它發生在下列的情況—

(i) 要形成適當的意向時，缺乏所有需要的資訊。

(ii) 雖然適當的意向已形成，但是缺乏描述所要

進行的動作，因而在從記憶中選擇資訊時常造成混淆，而造成誤動作。總之，當不同的動作有類似的描述，常發生描述疏失。例如，在控制面板上，當操作方式很像時，常誤動作。

(2) 基模啟動時所造成的疏失—又分：

(a) 不經意地啟動不屬於目前動作序列的基模，而造成疏忽。

(i) 捕獲疏失（capture error）-當一個熟悉而且類似正在做的動作序列的習慣取代了所意想動作的順序。

(ii) 資料導向的啟動疏失（Data-driven activation）—發生在當環境啟動錯誤的基模。例如，Stroop effect。也就是說，當外界的事件或狀況干擾到運轉員對環境或系統的狀態的解釋時，此種疏失就發生。

(iii)關聯性的啟動（Associative activation）-不需要動作順序的相似性，只要有很強的關連性就會發生。意向啟動了適當的基模，而後又啟動其他相關的基模。

(b) 曾經被啟動的基模在適當的控制行為的時機之前沒被啟動發生在當記憶失敗或受干擾而使得合適的動作被漏掉。沒被啟動或干擾會導致動作順序錯亂、跳過某些步驟、或重覆某些步驟。

(3) 基模觸發時所造成的疏失—

基模可能適當地被選擇和啟動，但是由於觸發不當（時機不對）而造成疏忽。例如，顛倒、合併、思想引發不意想的動作、和過早觸發基模。這種疏失很難被偵察到。

2. **Rasmussen 的人與作業不搭調（Human-Task Mismatch; Human-System Mismatch）**

- 故障的外在模型（External Model of malfunction）—由於人員動作所引起的不能接受的狀態。
- 故障的內在狀態（Internal Mode of malfunction）—進行認知決策過程中發生的問題，這種人員失效可能由於這些認知決策過程的不妥或因習慣性的抄捷徑所導致。
- 人員故障的機制（Mechanisms of Human Malfunction）

  <u>技能層次</u>

  - 動作變異性（Motor variability）：感覺動作控制的時間與

空間精確度不足，而造成偶而的不協調。

- 方位迷失（Topographic misorientation）：內部的模型與外部的世界不一致。
- 習性佔奪（Stereotype takeover）：高度學習的基模干擾到要做的動作的基模，而造成捕獲疏失。

規則層次

- 規則與程序回憶錯誤：
  - 某個單獨而且不一定屬於主要工作的序列項目忘掉或漏掉，例如，在修理或校正之後，忘掉要恢復正常運轉。
  - 對某個獨立項目回憶錯誤，例如數字。此層次的變異性可能包括選擇不同方案時選擇錯誤，例如，左右上下顛倒。
- 對系統改變的適應不良：

  環境內產生改變通常會將目前的基模更新。不過，這種更新常常到發生了不協調後才更新。這種感覺動作基模的更新依賴最佳的調整不協調，也就是說，合適的微調（fine tuning）只發生在如果它被勝過，因此，Rasmussen 認為不協調是不可避免的，唯有讓系統能夠忍受且不會對不協調產生無法挽救的反應。
- 習性固著（Stereotype fixation）與習性佔奪（Stereotype takeover）：

  習性固著發生在當感覺動作的基模在不適當的情境中被啟動，而當事者在事後知道應該怎麼做。習性佔奪則發生在人們意識到應使用特別的程序，但是卻再度墜落到熟悉的例行動作。

  當人們和複雜系統互動時，他們所控制的程序或多或少是看不見的，因此他們必須從組物理測量所提供的線索去推測現況並且選擇適當的控制動作。這些線索通常只是和某個狀態有關，而非狀態的所有特質。運轉員通常把正常事件典型的徵狀，包括一些非正式的訊號如馬達的噪音，當作所熟悉狀態方便的指標。這種策略在正常和熟悉的情境相當省力又有效。但是當系統狀態發生改變，而這種改變雖不會影響指標的量度但使得相關動作不合適時，就會將運轉員掉入陷阱。例如，運轉員可能下結論認為儀表讀數的異常是由於缺乏校正所造成，事實上是由於漏油所造成。
- 熟悉關連的捷徑（familiar association shortcut）

知識性

- 所有因果條件沒被考慮
- 副作用沒被考慮

- 人員故障的原因（Causes of Human Malfunction）—人員故障不僅起因於人員的變異性，而且也由於環境中先前事件所導致。
- 影響作業績效的因素（Performance-Affecting Factors）—除了人員的認知、體型特性、生理功能、主觀價值，還包含：工作環境、人機介面設計、訓練、等等。

3. Reason 的人為疏失模型

不安全動作(Reason,1990)

A. 未意向的動作(Unintended Action)

- 疏忽（Slip）-注意力的失效
  - 介入
  - 遺漏
  - 順序錯誤
  - 時機不對
- 遺忘（Lapse）-記憶的失效
  - 遺漏預定的項目
  - 遺忘位置
  - 忘記意圖

B.意向的動作（Intended Action）

- 錯誤
  - 規則基礎的錯誤
    - 誤用好的規則
    - 應用壞的規則
  - 知識基礎的錯誤
- 違規：
  - 例行的違規
  - 例外的違規
  - 破壞的動作

總之，主要疏失類型具備下列主要特性：

- 疏忽：技能基礎行為；動作不是如預想的；作業人員沒察覺；執行作業失效。

- 遺忘：技能基礎行為；無意識的心智疏失；作業人員在後來才可能察覺到 ；資訊貯存階段的失效。
- 錯誤：規則基礎或知識基礎；除非是故意的（違規），否則作業人員不太可能察覺；規畫階段的失效。
- 違規：故意偏離標準作業程序。

另外，Reason 認為基本的疏失趨勢（basic error tendency）與資訊處理機制（information processing domains）互動，而產生主要的疏失群（primary error groupings）。

基本的疏失趨勢：

(1) 生態的限制（Ecological constraints）—對特定的環境產生進化性的調整而產生的結果。

(2) 增進改變的偏差（Change-enhancing biases）—由神經系統偵測到改變而產生，因為心理機制要有系統地改變以適應變化的狀況。

(3) 資源的限制（Resource limitations）—源由於人類資訊處理的限制。有限的處理確保僅有幾個認知結構能在同一時間有最大的活動力。如果沒有此限制，人們無法從感覺資料抽取意義，無法將我們的思想、語言、和動作組織成有一貫性、目標導向的序列。

(4) 基模特性（Schema properties）—造成往熟悉、期待的方向發生錯誤，如（a）誤以為資料符合錯誤的基模；（b）雖然用對基模，但是用猜想來填下刺激架購的空隙；（c）太依賴顯著的基模。

(5) 策略與經驗法則（Strategies and heuristics）—當處理基模時，策略可幫忙克服資源的限制，但是不合適的或過度使用的策略與經驗法則會導致疏失。

這五種疏失的趨勢影響到人們資訊處理的階段（感覺記入、輸入選擇、暫時記憶、長期記憶、辨認、判斷、推理、動作控制）或運作而產生主要的疏失。因此，主要的疏失群分為：

(1) 錯誤的感覺：對外在世界的主觀經驗與客觀事實不吻合。

(2) 注意力失敗：發生在(a)克服分心；(b)處理同時進來的輸入；(c)焦注在兩個同時進來訊息之一；(d)將注意力分配在兩個同時進行的作業；(e)執行監督、保管、和驗證的作業。

(3) 記憶疏忽：包括忘掉表上的項目、忘掉意向、和忘掉對以前的動作的追蹤。

(4) 不預想的字和動作：心不在焉而使用字、標示、與動作偏離預想。這種偏離是因執行的失敗所引起。

(5) 辨認失敗：對於感覺資料的知覺錯誤，例如，錯誤地辨認出事實上不存在的東西或者沒辨認初已存在的東西。這種疏失發生在當感覺

的證據不完整和當存在有知覺到某個刺激存在或不存在的期待。

(6) 不正確和被阻礙的回憶：包括記錯或不記得句子、故事、地點、面貌、或事件。

(7) 判斷錯誤：心理物理和時間的判斷、風險的判斷錯誤、診斷錯誤、對機會和共變項瞭解錯誤、概率判斷的誤失、社會評估錯誤。

(8) 推理錯誤。

此八種疏失群依作業者的意向（intention），亦即，一個想要做的動作，又可分成兩種：疏忽（slips）和錯誤（mistake）。

4. Reason 計畫的錯誤（mistakes in planning）

計畫的過程可分為（1）設定目標，（2）尋找方案，（3）比較與評估方案，（4）決定合適的方案。他提出計畫的心理歷程模型：

- 工作資料庫（working database）：

  目前在規畫過程中所用的資訊貯存於工作資料庫。此資料庫有容量的限制並且持續地改變其內容。至少有三種資訊存在於內：

  - 透過輸入的功能從環境中所衍生的資訊。
  - 從基模資料庫所取出的資訊。
  - 從活動的但是不一定相關的基模自然發生的資訊。

- 心理運作（mental operations）：

  包括選擇、判斷、與決策。其中有兩種決策：

  - 設定目標：各種想要的結果都加以考慮而後根據所能達成的可能性給予權重。
  - 達成目標：同樣的方法應用到達成目標的方法。

- 基模：

  基模將和計畫相關的以及未索取的資訊送達工作資料庫。所謂未索取的資訊是指被那些高啟動性的基模推出來的片段影像和文字：充滿情緒的材料，被環境的情境或相關的計畫元素所觸發的資訊，或最近或常用的基模的輸出資訊。心理運作操弄基模而產生計畫。

工作資料庫所產生的錯誤：

- 只含括部份和計畫相關且可獲得的資訊。
- 在同一時段，不超過兩或三個因素同時存在此資料庫。這種限制使得無法考慮和搜尋所有的方案。
- 內容持續改變。
- 計畫受過去經驗的影響。
- 受到可利用性（availability）影響而限制了解決方案的搜尋。
- 內容偏向過去成功經驗：計畫較可能含括在過去證明是成功的方案。

- 資訊可能受局部環境因素所引發，因此越受矚目的的資訊越可能納入計畫中。

心理動作與基模產生的錯誤：

- 不太會去計畫可能發生的偶發事件因為受到過去事件而低估了未期待干預的可能性。
- 較優先考慮那些生動、情緒化的資訊而低估了它們在規畫過程中的主觀價值。
- 無意識地填滿不足證據的空隙來符合他們的理論。而後，它們又無法分辨資料是真的存在或由基模提供的。
- 不擅長由抽樣值來評估參數。
- 不擅於偵測到共變關係。
- 大一統效果（halo effect）：把兩個不同順序減合而一。
- 將因果關係過於簡化：常依因與果相似性，而可能判斷其有因果關係。
- 對他們知識的正確性過於自信。著重於符合他們所選的動作的證據而忽略反證。
- 受限於對統計的瞭解，不擅長做預測。
- 急欲瞭解所有內部與外部產生的資訊。
- 依合適性而非理想性來選擇目標，因此選擇短程目標重於長程目標。
- 基模的應用可能導致應用了過於僵硬、受限於規則、和保守的程序，或者不適合情境的經驗法則。

當計畫規畫好之後，計畫者會尋找證明其有效性的證據而無法去吸收那些估計計畫會失敗的資訊。

D.社會心理學模型

Reason 認為還需考慮人為疏失環境的特定狀況以及人員的狀況的原由。存在人員的疏失原因有暫時的（如情緒）也有長久的（如信念、價值、和氣質）。

Taylor 也強調個人價值系統和責任感對運轉員行為的重要性。那些避免疏失的安全保護系統若沒考慮這些因素則效果會有所限制。

II. 疏失的偵測

技能基礎疏忽的偵測

- 自我監督或依賴回饋資訊：

  用知覺分析和回饋檢查來偵測疏失。疏忽和遺忘比錯誤可能偵測得到，但是有些疏失（如遺漏步驟）就很難偵測。

- 他人發現：此法對於診斷錯誤與作業人員在壓力之下特別有效。
- 利用系統對疏失的反應：
  - 牽制：避免使用者表達不能實現的意圖。
  - 警告。
  - 不作任何事：對不合理的輸入不反應。
  - 自我更正：就照我的意思作。
  - 讓我們談一下。
  - 教教我：系統要求使用者教它。
- 利用 forcing function：

  所謂「forcing function」就是除非疏失已被更正，否則會避免動作能夠持續進行的設計。它是用以避免某些技能基礎疏失發生的標準作法。例如，螺絲只能符合一邊，如此螺絲才不會裝錯。當疏失的後果會嚴重的話，就有理由去設置 forcing function。

規則基礎錯誤的偵測

- 誤用好的規則—很難自我偵測，必須仰賴他人
- 應用壞的規則—定期有系統地審查程序書。但是如果一個複雜系統擁有非常多的法則與程序且這些程序時常更改的話，此法工作量浩大。因此必須先確定問題的嚴重程度，以決定是否需要審查法則與程序。

III. 降低疏失的策略

- Sanders and McCormick 提出下列方法—
  - 設計
    - 排除設計（exclusion design）：使疏失無法發生。
    - 避免設計（prevention design）：使疏失很困難發生。
    - 失效但仍安全（fail-safe design）：降低疏失的後果。
  - 人員選擇
    - 確認所需之技能與能力，但是需要可靠與有效的測驗。
  - 訓練
  - 程序查核表（procedural checklist）：避免記憶遺忘。
- Lourens
  - 改善設備與工作的設計以減少疏忽（slips）。

- Mason
  - 減少疏忽與遺忘
    - 改善設計，再加上訓練。
  - 減少錯誤的潛在性
    - 訓練-團隊與個人，透過過度學習，複習來維持技能。
    - 設計-資訊重複，清楚的標示，顏色加碼。
  - 減少知識基礎錯誤
    - 危險察覺（hazard awareness）課程。
    - 監督。
    - 工作計畫的檢查。
    - 訓練後測驗。
  - 減少違規
    - 增強工作與守紀律動機。
    - 進行風險評估，確認風險知覺與益處間之平衡。
    - 監督，建立團體行為的常模，同時管理階層對於安全承諾。

- 組織內確認與控制疏失的方法

  1.設置一個事件報告系統，匯集固定期間內所有的事件。

  2.對事件進行肇因分析。

  3.召集組織內所有層級的人員參與進行問題解決的活動，著重安全文化的提昇-建立共同的願景與目標，推動有效的溝通。

  4.管理階層持續監督與控制所產生的改變，因此組織對安全議題會發展出正面效應。管理階層對於安全的承諾會透過決策的過程而發酵。

設置安全計畫的步驟：

（1）創置事件與事故之人因資料庫。

（2）定期重估作業人員的績效。

（3）改善資訊顯示以提供清楚的跡象。

（4）在團隊作業時，知覺到互動過程中增加風險的因素（如，傾向風險、團隊思考偏差）。

IV. 安全管理系統

所謂「安全管理系統」就是組織透過管理過程來控制風險。建立安全管理系統的三種方法：

1.系統方法。

2.安全文化與態度的孕育。

3.實施安全稽查，查核一些管理功能，如：規畫、組織、執行、控制。

這三種方法將人與風險管理面結合在一起，強調：

- 管理階層承諾的重要性。
- 設定清楚的安全目標。
- 妥當地溝通所需要的資訊。

系統方法

系統含括：

- 結構的元素—主要崗位、報告的關係、委員會與其他團體、安全文件。
- 過程-動作、問題解決、資訊的提供與溝通。
- 連結點—回饋迴路。
- 外在影響—政府、立法機關、經濟、科技、改變的速度、與公眾意見
- 次系統—控制（決策、政策、策略規畫），監督，執行（運轉、維護），溝通

因此，安全管理有以下六個元素：政策、組織、規畫與執行、測量績效、審查績效、與稽查。這些元素靠員工的參與、持續的改善、資源的提供、與風險控制等過程來支援。元素間靠回饋迴路來連結。一個有效的安全管理系統需要有功能面（包括管理控制、監督、執行、與溝通）與人性面（領導力、政治與安全文化等次系統）。

安全文化與態度

文化乃是一個群體共有之特徵，它包括：信念、價值觀、態度、意見、動機、動作、儀式、符號等。它表達於五個層面：

- 人造物-可觀察的，如團體標示。
- 行為型態-可觀察的動作。
- 行為常模-可以從觀察到的行為推測。
- 價值觀。
- 基本假設-中心價值。

安全態度的三大元素：

- 組織規則。
- 態度的安全目標物。
  - ■被動-如檢驗設備、穿帶合適的個人防護設備、內務。
  - ■主動-如知道安全檢查的結果、提出建議、尋找安全資訊。
- 安全行為。

美國核電廠安全文化研究，確認出四個安全文化指標：

- 有效的溝通。
- 良好的組織學習，能夠因應改變。
- 著重於健康與安全。
- 外在因素，如公司財務、經濟環境、管制法規。

V. 安全稽查

至少有六種安全稽查：

1. 對特定的議題（如人為因素、危險物質、或環境）稽查。
2. 工廠技術稽查（plant technical audit）—深度審查所有工廠和技術人員所執行的過程。
3. 定點技術稽查（site technical audit）—定期檢驗所有特定的工作。
4. 確認稽查（compliance audit or verification audit）—用於檢驗這個組織是否符合安全的要求。
5. 有效性稽查（validation audit）—著重於檢驗是否採納了正確的次系統和組件，是否進行正確的監督，是否設置了合適的次系統。
6. 管理安全稽查（management safety audit）—每年進行一次，包含一般安全議題。

執行安全稽查之原則：

- 採取正面態度，而非一心想找錯誤。
- 確認出偏離準則點。
- 促進對造成偏離的事件分析。
- 強調好的實施方法。
- 要有專業態度、公正、與客觀。
- 將稽查整合入安全與風險管理系統。
- 盡量客觀、準確地評估一個管理功能。
- 提供一個風險狀態的測量方法。
- 指認出重要區域的優缺點。
- 提供一個清楚改善的準則。
- 成為一個監督改善的方法。

發展安全稽查的階段：

1. 訪問與熟悉所要稽查的場地。
2. 設計問卷。
3. 稽查安全的前題基準與活動。
4. 確認回答與稽查的分數。
5. 分析結果。
6. 確定問題點。

7. 準備並遞交報告。
8. 執行建議事項。
9. 監督改善過程。

安全稽查其他技術：

- 行為抽樣（Behavior Sampling）：

  適用於評估例行的低風險、高可能性的作業。它用以確定在工作場所之不安全行為。需要在隨意的時機對行為作一連串的觀察。需要至少一個觀察員進行觀察。觀察員要熟悉所要觀察的行為。工作人員在觀察時不改變其行為。每次觀察要區分出安全與不安全行為。抽樣的樣本需要至少 600 次。計算出不安全行為的百分比。

- 工作場所的檢視（Workplace Inspections）：

  用於評估不安全行為的程度與結果。檢視範圍不僅包括工作場所，還包括工作方法、工作環境、與員工的設施。檢視需要相當的知識與技能，不可盲目的仰賴查核表。

  檢視的類型有：

  - 正式的檢視—每年一次，最詳細；用於確認所有的安全狀態。
  - 重複檢視—用於監督在偵測出特定危險後的改進成效。
  - 找出危險—每日調查以評估工作場所的風險。
  - 對特定事件的檢視—用於收集特定事件的資訊。

  執行原則：

  - 必須作觀察，不僅是看而已。
  - 深入檢驗每個細節。
  - 花時間慢慢檢視。
  - 要有耐心與小心。
  - 問兩個主要問題：什麼出了錯？為何出錯？
  - 問「如果這些事發生，會導致什麼後果？」

二、作業分析：瞭解包商有關安全之作業

本研究以核二廠為例，將其八十七年全年之包商作業項目依單位別作統計，發現大多作業之主辦課乃修配與電氣兩單位（如表 1），作業性質屬檢測、修理、與拆裝。另外，將「包商與安全有關之工作項目」挑選出來，（部份項目如表 2）做作業分析，並對歷年來包商人員作業不當資料（部份項目如表 3）與各核電廠大修期間包商違規事項（見表 4）作初步檢討，發現大多之疏失屬技能型疏忽（skill-based slips），而這些疏忽又很多是注意力、辨識、遺忘、溝通協調。另外有些疏失屬於知識型錯誤，這些錯誤與風險認知有關。

有關核電廠營運程序書內之「包商工作人員施工前重點講習記錄表」（如表 5）的適用性也作了初步的探討，發現應將安全行為模式的學習納入重點講習，以強化其安全行為。

作業分析將作業依順序分解至作業之組成動作單元步驟，確認出每一步驟所需之資訊與控制，還有人為疏失可能發生點。本研究對包商進行之維修作業進行分析，將作業項目依序分為：作業交待、作業計畫、前置作業、工作協調、工作執行、工作復原、驗收、復原。這些作業項目再細分為作業行為單元，而各行為單元之可能疏失也可隨之確認出來（見表 6），另外，作業相關之危險也可由檢視工作場所來發掘。分析結果可以作為安全作業行為查核之基準。

表 1　八十八年核二廠包商作業統計表

主辦單位	廠　內	廠　外
化　　學	5	1
電　　氣	84	21
修　　配	88	23
機　　械	63	9
供　　應	3	4
改　　善	36	86
北 展 館	2	8
核　　技	4	0
儀　　控	21	4
檢 測 隊	6	0
工　　安	6	2
大修小組	1	1
儀　　器	2	0
訓　　中	1	3
廢　　料	7	6
電　　算	1	0
保　　健	2	1

表 2　包商與安全有關之工作部份項目

工　　程　　名　　稱
1.反應器再循環幫浦檢修工程
2.再循環系統隔離閥檢修工程
3.壹號機 EH 系統管路拆檢工程
4.膨脹接頭內外檢配合工程
5.冷凝水幫浦大修工程
6.管閥拆除及薄化管件更新工程
7.緊急幫浦室電氣盤面及管線修繕工程
8.氣渦輪機廠房消防管路更新工程
9.燃料填換大修相關工程
10.反應器安全釋放閥（SRV）檢修工程
11.配合一號機停機 MOV 電氣檢修
12.反應器 MSIV FCV 檢修工作
13.液壓控制器單元 HCU 檢修
14.增設 RHR 彎道 Drain Tank 管路
15.再循環系統隔離閥檢修工程
16.反應器再循環泵浦檢修工程
17.減震器拆裝檢修工程
18.第四組空氣乾燥器安裝工程

表 3　歷年來包商人員作業不當資料部份案例

	事　　件
案例一	86.5.6 電氣課包商人員進行一號機 1EJ-HV-223 之馬達操作閥診斷測試過程中，因疏忽不慎將使用之線夾金屬裸露部份碰觸 HB-225 閥之開啟控制回路，致造成 HV-225 閥在非正常運轉模式下異開啟，而使爐水噴灑至圍阻體，造成在該區工作人員之污染。（**注意力、操作方式**）
案例二	86.5.13 包商人員於二號機輔助廠房四樓進行廠房塗裝工程時，未通知主辦課負責人申請掛指示卡，導致控制室值班人員不知情下起動 SGTS A 串進行測試。（**溝通協調**）
案例三	87.5.4 包商工作人員在監工不在場之下誤將應補入 DIV III 儲油槽之油加入 DIV I 儲油槽。（兩種油等級不同）（**注意力、辨識**）
案例四	87.5.1 包商人員執行 2AD-2P-72 之維修作業時，鬆開泵浦進口法蘭準備檢修，發現管內積水不停洩出，未即時通知檢員處理造成該區積水。（**風險認知**）
案例五	87.7.30 執行項廢液系統之加壓空氣上浮槽浮渣刮除器之檢修時，包商人員逕行操作閥門，導致疏忽未將沖洗水閥關閉，使得廠用水持續入系統集水池，並溢流至廠房外排水溝及廠外環境。（**風險認知、遺忘**）
案例六	87.9.11 安全小組人員赴現場巡視時，發現某包商人員未經申請與核准，即逕行研磨二氧化碳之消防管閥，經安全小組及時阻止而避免工安事故之發生。（**風險認知**）

表 4　各核電廠大修期間包商違規事項

營運期間測試（ISI/IST）

編號	案例編類	公佈日期	違規內容摘要	改正措施摘要
一	檢測注意事項	1995/11/10	1.防護布帽未捆綁，於反應爐水下目視檢測時掉落地面。 2.置放 CRB 於存放架內繩子未繫牢吊鉤以致掉落反應爐。	➡輻安 ➡工安、核安
二	測試結果與判讀	1991/6/14	閥 packing 調整後未留記錄證明是否執行過 F/T，不符程序書 1102.01 之規定，閥控制機構調整後，未填相關記錄，不符 ASME IWV-3200 之規定。	
		1992/10/1	檢查 Snubber 發現多項缺失，顯示檢測及維護不確實。(EF-007-7)	
		1995/3/31	1.水壓試驗完成，未依程序書 650-M-IST 規定恢復安全閥功能。 2.閥(AL-V009)未完成檢修即交回副卡，致灌水時漏水，違反程序書 1104.01 規定。	1.將 Gagged 型式之安全閥列入儀器隔離查核表，及完成試驗程序書(650-M-IST-113)內加列 PSV 裝拆 Gag 螺栓步驟查核程序。 2.已修訂程序書(700-M-068)，現場施工實施雙重確認法蘭包封(Gland Packing)已鎖緊及所有檢修工作皆已完成才交還副卡

停機安全（Shutdown Safety）作業

編號	案例編類	公佈日期	違規內容摘要	改正措施摘要
一	安全系統電動閥測試	1997/5/8	包商人員進行馬達操作閥診斷測試過程中，因疏忽造成圍阻體噴灑閥誤開啟，爐水噴灑至圍阻體內，致使該區地面，機件及部份工作人員之衣服及鞋底污染。	已將「安全有關電動閥接點連鎖資料表」增列於程序書以供執行診斷測試時閥門隔離之參考；另依原能會要求再詳細檢討那些閥進行診斷測試時，必須執行隔離措失並明訂於程序書中，預定 86 年 9 月底完成。

設計變更作業

編號	案例歸類類別	公佈日期	違規內容摘要	改善矯正措施摘要
一	DCR 採購品質文件	1996/11/2	設計修改案 DCR-1280（廣域中子偵測器）乾管更換工程，承包商（奇異）未能提供完整文件以供證明品質，驗收部門未確實管制相關作業品質。	1.已請奇異補附相關文件，並於起動前獲原能會視查員審查同意。 2.DCR-1280 施工時，已確實執行到貨時附有相關文件，且待相關文件審查合格及會同開箱驗收合後才允許安裝。
二	DCR 施工管制	1997/5/5	汽機廠房執行電纜托網托架焊接補強工程時，因防火布鋪設不當，致施工中掉落之焊渣熔毀覆蓋在電纜上方之防火布，造成焊接處約 1 米下方電纜托網內之 98 條電纜悶燒受損。	1. 修訂動火許可證申請程序書： a. 訂定各種金屬熔點溫度及防火布耐火溫度作為工作人員執行及複查人員檢查之依據。 b. 明確規定防火布鋪設方法及增列動火作業檢查表。 2. 將程序書規定檢查事項拍攝成教學錄影，作一般訓練宣導用。

大修掛卡及系統恢復作業

編號	案例歸類類別	公佈日期	違規內容摘要	改善矯正措施摘要
一	掛卡隔離管制	1994/3/9	1.抑壓池執行 DCR-591 承包商未經監工確認已完成掛卡手續前，即進行集水池出水管鑽孔工作，致抑壓池地面走道污染。 2.低壓汽機兩處扶梯前之電纜鐵管因被踩踏呈現斷裂情形。	1.已對承包承商依規定懲處，並要求各承攬商負責人務必取得紅卡後才可進行施工。 2.已加裝角鐵支撐保護。
		1989/2/24	輔助鍋爐之 MV-B29 未依程序書 105 規定掛卡，包商即自拆修，造成工作人員受傷。	
二	操作紅（禁止操作）卡	1994/10/2	#1 HI-V075 副卡指示為 close，測試完成後，未消卡即開閥洩水、洩壓，違反程序書 162 及 1104.3 規定。（EF-192）	

維護／測試作業

編號	案例歸類	公布日期	違規內容摘要	改正措施摘要
一	維護前未開立檢修工作連絡書	1995/6/13	包商執行儀器校正造成反應器半急停，且事前未與主控室連絡，未開工作連絡書，致運轉員無法迅速查知故障所在，使反應爐保護系統（RPS）再次動作。	1.已修訂程序書 763.12 共管儀器列入合併校正，防止相互干擾。 2.已修訂程序書當日若工作未完成，次日需與值班主任連絡確認可執行方可開始工作，當日之工作亦須先行復原。
		1994/11/1	執行飼水流量校正試驗，未提檢修工作聯絡書。	
		1994/10/2	#1 BM-V006 未依程序書 1102.01 規定開 SWP 即進行拆修。	
		1995/12/2	電驛之校驗測試未依程序書 1102.01 規定開設備請修單（SWP）及掛卡，且無校驗程序書，即進行檢測。	1. 已發備忘錄（運 85005）要求遵守開立請修單規定。 2. 已在氣渦輪機控制室加裝維護管理電腦系統（MMCS）終端機，使值班主任能迅速開單檢修。 3. 已將起變、主變及輔變的保護電驛列入程序書 700-E-124，其校驗工作配合大修列入大修工作許可單（OWP）內。
二	維護人員劑量管制	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書 105 相關規定：因兩串 RHR 停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於 Refueling Floor 鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用 Tie 之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。
三	電焊作業	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書 105 相關規定：因兩串 RHR 停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於 Refueling Floor 鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用 Tie 之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。

維護／測試作業（續頁）

編號	案例類別	公佈日期	違規內容摘要	改正措施摘要
四	工安及動火管制	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書 105 相關規定：因兩串 RHR 停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於 Refueling Floor 鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用 Tie 之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。
		1992/5/10	包商擅自切割閥架，致 CTMT Spray PUMP A Room 消防系統動作。值班人員未確實依程序書 105 規定簽結動火管制。	
五	閥維修不符合 ASME Code	1991/6/14	閥 packing 調整後未留記錄證明是否執行過 F/T，不符程序書 1102.01 之規定，閥控制機構整後，未填相關記錄，不符 ASME IWV-3200 之規定。	
六	反應爐爐穴工作	1995/11/10	1.防護布帽未捆綁，於反應爐水下目視檢測時掉落地面。 2.置放 CRB 於存放架內繩子未繫牢吊鉤以致掉落反應爐。	
七	不良工作習性	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書 105 相關規定：因兩串 RHR 停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於 Refueling Floor 鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用 Tie 之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。

維護／測試作業（續頁）

編號	案例類別	公佈日期	事件現象內容摘要	改善措施摘要
八	接線錯誤	1997/5/30	輔助廠房進行塗裝工程，因未依程序先申請，致控制室人員不知情而起動備用氣體處理系統進行測試。	1.a.缺失之個案已改善完成。b.圍後已屆預定完成日期而未完工 EMR 案件，由品質課逐項檢討，改善課定期追蹤。c.EMR 程序書將配合修訂。 2.a.承包商負責人應每日向龍廠承辦人聯繫當日工作內容及地點，變更時需先報備，已列入程序書 1226 修訂。b.已訂定廠房塗裝施工須知，並將其列入員工及包商工具箱會議。
九	安全有關 MOV 測試	1997/5/8	包商人員進行馬達操作閥診斷測試過程中，因疏忽造成圍阻體噴灑閥誤開啟，爐水噴灑至圍阻體內，致使該區地面，機件及部份工作人員之衣服及鞋底污染。	將「安全有關電動閥接點連鎖資料表」增列於程序書以供執行診斷測試時閥門隔離之參考；另依原能會要求再詳細檢討那些閥進行診斷測試時，必須執行隔離措失並明訂於程序書中，預定 86 年 9 月底完成。
十	未遵守測試程序書	1996/4/24	未依程序書步驟執行 600-O-038.1（停機時馬達驅動輔助飼水泵測試），因誤解程序書拆除連線之含意，造成喪失電壓（LOV）信號。	1.已提報三廠防制人為疏失改善方案，並列入核管案件 30-8501 管制。 2.程序書不詳盡時，應立即提出討論，並查閱相關圖面確認，已列為異常事件報告（RER-85-32-004）訓練重點。
十一	測試後未依規定復原	1995/3/31	1.水壓試驗完成，未依程序書 650-M-IST 規定恢復安全閥功能。 2.閥（AL-V009）未完成檢修即交回副卡，致灌水時漏水，違反程而書 1104.01 規定。	1.已將 Gagged 型式之安全閥列入儀器隔離查核表，及完成試驗程序書（650-M-IST-113）內加列 PSV 裝拆 Gag 螺栓步驟查核程序。 2.已修訂程序書（700-M-068），現場施工實施雙重確認法蘭包封（Gland Packing）已鎖緊及所有檢修工作皆已完成才交還副卡。（已獲原能會同意結案）
十二	其他類案例	1989/2/23	1.MOV 維修工作人員訓練不足，易造成設備損壞。 2.第二次大修 Snubber 失效率甚高，據現場工作人員反應，係包商不填踩壞，顯示管理及監工不周。	

人員資格與訓練

編號	案例歸類	公佈日期	違章規範內容摘要	改善矯正預防措施摘要
一	承包商掛卡管制訓練、踩踏電纜管路	1994/3/9	抑壓池執行 DCR-591 承包商未經監工確認已完成掛卡手續前，即進行集水池出水管鑽孔工作，致抑壓池地面走道污染。	已對包商依規定懲處，並要求各承攬商負責人務救取得紅卡後才可進行施工。
二	承包商訓練與資格檢定	1995/3/31	控制棒導引管支梢超音波檢測及蒸汽產生器二次側上部組件檢查，外籍包商有多項缺失，台電未確實審查其資格等。	爾後於執行蒸汽產生器二次側上部組件檢查時，將檢測員檢測資格、視力體檢及儀器有關校驗等證明列為人員資格審核與終期報告之必備文件。
		1989/2/23	1.MOV 維修工作人員訓練不足，易造成設備損壞。 2.第二次大修 Snubber 失效率甚高，據現場工作人員反應，係包商不填踩壞，顯示管理及監工不周。 3.電廠未訂定包商工作人員及監工訓練，資格規定。	
		1991/2/8	1.重要馬達由同一包商負責內檢，但包商維修品質可議。 2.電廠監工經驗不足，未及時糾正或給予包商訓練及檢定。	

輻防作業

編號	案例歸類	公佈日期	違章規範內容摘要	改善矯正預防措施摘要
一	防護面具使用	1993/10/1	大修期間發生防護面具濾罐未依規定安裝確實掉落反應爐中，燃料主吊車剎車手拉桿掉落反應爐池中。	濾罐已分別於 82 年 9 月及 10 月尋獲，另一只燃料吊車剎車拉桿歷經四次大修均未尋獲，研判當初剎車並未安裝拉桿或拉桿並未掉入池內。

廠房管理作業

編號	案例歸類	公佈日期	違規內容摘要	改正措施摘要
一	管制區內塗裝用料管理	1997/8/16	廠房地面塗裝工程有諸多不符程序書823規定，且程序書823對塗料之管制亦須一併檢討改善。	1.負責塗裝承包商以停工處罰，自86.9.18復工後，已無違規情形發生。 2.塗料管制已就程序書823修訂： (1)建立「化學品使用許可查證聯」文件。 (2)防火評估及管制。 (3)化學品防火評估依據及存放地點、數量等之管制。
二	反應爐穴工具管理	1996/6/17	大修期間美商奇異公司承包爐心側板修理工程發生物件掉落事件。及中子偵測系統（LPRM）更換工程發生LPRM掉落事件。	奇異公司將以本案經驗回饋其公司內部之設計、安裝部門。
		1993/10/1	大修期間發生防護面具濾罐未依規定安裝確實掉落反應爐中，燃料主吊車剎車手拉桿掉落反應爐池中。	濾罐已分別於82年9月及10月尋獲，另一只燃料吊車剎車拉桿歷經四次大修均未尋獲，研判當初剎車並未安裝拉桿或拉桿並未掉入池內。
三	動火管制	1997/5/5	汽機廠房執行電纜托網托架焊接補強工程時，因防火布鋪設不當，致施工中掉落之焊渣熔毀覆蓋在電纜上方之防火布，造成焊接處學1米下方電纜托網內之98條電纜悶燒受損。	1.修訂動火許可證申請程序書： a. 訂定各種金屬熔點溫度及防火布耐火溫度作為工作人員執行及複查人員檢查之依據。 b. 明確規定防火布鋪設方法及增列動火作業檢查表。 2.將程序書規定檢查事項拍攝成教學錄影，作一般訓練宣導用。
		1992/5/10	包商擅自切割閥架，致CTMT Spray PUMP A Room消防系統動作。值班人員未確實依程序書105規定簽結動火管制。	
四	安全護具使用	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書105相關規定：因兩串RHR停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於Refueling Floor鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用Tie之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。

爐心作業

編號	案例歸類	公佈日期	違規內容摘要	改正措施摘要
一	反應爐穴作業工具物品管理	1995/11/10	1.防護布帽未捆綁，於反應爐水下目視檢測時掉落地面。 2.置放 CRB 於存放架內繩子未繫牢吊鉤以致掉落反應爐。	

化學與廢料管制作業

編號	案例歸類	公佈日期	違規內容摘要	改正措施摘要
一	測試不當引發污染	1997/5/8	包商人員進行馬達操作閥診斷測試過程中，因疏忽造成圍阻體噴灑閥誤開啟，爐水噴灑至圍阻體內，致使該區地面，機件及部份工作人員之衣服及鞋底污染。	將「安全有關電動閥接點連鎖資料表」增列於程序書以供執行診斷測試時閥門隔離之參考；另依原能會要求再詳細檢討那些閥進行診斷測試時，必須執行隔離措失並明訂於程序書中，預定 86 年 9 月底完成。

機組起動作業

編號	案例歸類	公佈日期	違規內容摘要	改正措施摘要
一	未遵守程序書規定	1994/5/16	大修期間，工作人員執行工作時，未遵守程序書 105 相關規定：因兩串 RHR 停用，造成燃料更換樓層蒸汽凝結，地面嚴重積水。污染區研磨未戴防護面具。包商執行管路安裝時，以重要設備之管路當支撐，焊條未保溫，人員未戴安全帽。	1. 大修期間，於 Refueling Floor 鋪塑膠布，請保健物理人員於其滴水處偵測，燃料池盡量使用 Tie 之海水即運轉機組之海水冷卻。 2. 設備/管路維修屬長期性工作，將於適當地點安裝吊耳。

表 5　包商工作人員施工前重點講習記錄表

表格 1151G~11　15

包商工作人員施工前重點講習記錄表

廠別：核　　廠　　機組別：　　號機　　大修別：EOC-

工程名稱：

品質等級：　□Q　　□R1　　□NON-Q AND NON-R1

1.0 訓練課程：_____

2.0 訓練時間：_____年_____月_____日_____時_____分起計_____小時

3.0 訓練地點：_____

4.0 講　　師：_____

5.0 參加人員：公司名稱：_____

簽到人員：_____

_____

6.0 講訓內容：_____

6.1 工程內容：_____

6.2 施工範圍：_____

_____

6.3 作業程序：

6.3.1 依核二廠營運作業程序書#_____執行。

6.3.2 遵守核二廠營運作業程序書品管及行政管理要求。

6.3.3 品質檢查：接受台電人員之檢查/抽驗工程品質（含停留點查證點檢查，應於施工前通知品管人員到場查證）。

6.3.4 工作現場應懸掛發包工作標示牌（填妥標示內容）。

6.3.5 工作前自我查証與五分鐘哲學概念，對設備維修之人員與設備安全性說明。

表 5　包商工作人員施工前重點講習記錄表（續）

表格 1151G~2

6.3.6 作業程序書重點及注意要點說明：

A. _____
B. _____
C. _____
D. _____
E. _____
F. _____
G. _____
H. _____

6.4 現場環境說明：

廠房：_____號機：_____廠房　　標高：EL_____呎_____吋

環境狀況：_____
_____
_____

6.5 工作安全及保健物理：

6.5.1 重視工作安全之要求，未經許可禁止操作、攀登、踐踏或掉掛任何設備管路。

6.5.2 遵守「勞工安全衛生法規」及「保建物輻射防護」之規定。

6.6 其他：_____
_____
_____

課長：　　股長：　　承辦人：

表 6　維護作業分析與可能人為疏失之確認

活動	作業項目	行為內容	可能人為疏失
1.工作安排	1.1 作業交代	1.1.1 工作指派	未指派、指派不清、指派不當
		1.1.2 瞭解工作內容	誤解、不瞭解
	1.2 作業計畫	1.2.1 規畫工作內容	無計畫、內容錯誤、人員指派不當、時間不當、地點不當
		1.2.2 準備工具及器材	未準備、準備錯誤
		1.2.3 評估與演練	未進行、無法進行、評估（演練）錯誤
2.作業實施	2.1 前置作業	2.1.1 檢視工作條件	未檢視、檢視錯誤
	2.2 工作協調	2.2.1 協調	未協調、協調不良
	2.3 執行	2.3.1 檢查/核對	沒作、無法作、作錯
		2.3.2 故障診斷	鑑別錯誤、研擬對策錯誤
		2.3.3 移除/安裝/替換/修理/拆線/連接/焊接/跨接	沒作、作錯、順序不當、時機不當、誤觸
		2.3.4 校正/調整/設定	沒作、無法作、操作量不適當、時機不當、順序不當、多餘操作、反向操作
3.工作會驗	3.1 稽查	3.1.1 觀察比較	沒作、無法作、作錯
		3.1.2 核對	沒作、無法作、作錯
		3.1.3 確認	沒作、無法作、作錯

三、安全作業行為稽查查核表之發展

基於人為疏失之文獻探討，安全作業行為的稽查不能只對行為的結果作稽查，它還要涵蓋人員之認知決策歷程，始能確認出作業人員失效的發生點，進而能追溯出人為疏失之前置原因。另外，由電廠包商人為疏失與違規案例分析，發現大多人員作業績效問題乃屬疏忽與風險察覺的錯誤。疏忽乃由於注意力、遺忘、與知覺錯誤所引起。因此，安全作業行為的稽查也就著重於（1）作業前的計畫與安全知識的獲取；（2）作業中的檢查機制（不論是自我檢查或同儕檢查）與回饋控制機制的存在與運用、提示物與資訊的提供、狀況與風險察覺；（3）作業後之評估與檢討；（4）管理階層對改善案的評估、決策、與追蹤。

安全作業行為稽查查核表乃依上述之重點，以包商作業程序為架構來發展，如此查核表能夠與作業過程結合，使得查核表易於使用。茲將查核表表列於下：

A. 包商作業人員報到

1.是否具備作業相關知識與技能？

2.是否瞭解工作內容？

3.是否瞭解相關之安全規定與準則？

4.此作業與非核電廠相同之作業是否有差異點？
這些差異點何在？對安全有何影響？

B. 作業前之規畫

1.作業計畫是否可行？

- 作業時間是否有足夠？
- 人力是否符合作業需求？
- 分工作業負荷是否合理？

2.本作業是否會影響機組安全與工安？若會，計畫有評估其風險並演練過？

3.本作業與其他作業、其他部門、或系統設備有無關聯？

- 若有關聯，在進行何步驟前需要與其他人員與部門作溝通、協調？
- 溝通、協調需要用何種方式？
- 如何確認溝通、協調對方已獲得訊息且完成相關應對作業？

4.本作業有那些設備管路禁止操作、攀登、踐踏或掛掉？

5.本作業需要那些工具設備？

- 這些工具是否備妥？是否符合安全規範？
- 工具應如何正確使用？

6.作業前之簡報是否進行？每位作業人員是否瞭解其任務要求、作業內容、每一步驟的細部動作與關鍵安全步驟、以及安全規定？

- 在進行每一步驟時需要那些資訊？這些資訊如何獲取？
- 在進行每一步驟時需要操作那些控制器或工具？如何進行操作？如何確認操作動作的完成？

■ 關鍵安全作業步驟是否瞭解？是否模擬演練並標明於程序書上？

7.作業過程中有那些停留查證點？是否在施工前有通知品管人員查證？

8.本作業之作業環境與作業本身是否容易引起人為疏失？

■ 這些疏失在進行那些步驟時會發生？（應將這些作業點標明為檢查點）

■ 那些疏失會牽涉那些潛在危害（hazards）？

9.那些動作和情況會觸發這些危害的發生？

10.這些危害的發生應如何辨識、偵測與控制？

■ 發生時，應如何及時將狀況向廠方報告？向誰報告？

11.危害相關之防護器具是否攜帶並知道如何使用？

12.危害發生應如何應變？

■ 應變時，應如何及時將狀況報告？向誰報告？

■ 應變程序書是否熟悉並且攜帶？應變程序是否演練過？

■ 是否知道如何將危害侷限於局部？

■ 是否知道緊急疏散程序與路線？

C.作業進行階段

1. 是否有掛卡？

2. 是否攜帶程序書與相關文件和圖面？

3. 合適的工具與輔助器材是否具備？會使用？

4. 是否攜帶輔助工具與防護器具？防護器具是否配戴完整？是否有作業的提醒物（reminder）？

這些提醒物是否具備以下特性：

- 必須能夠在緊要時刻引起注意（醒目）
- 在時間與空間上與要記住的作業步驟相接近（接近性）
- 能夠提供足夠的資訊告訴在何時、何地執行所要記住的步驟（情境）
- 告知作業者需要作什麼（內容）
- 讓作業者能夠檢查有多少個別的動作與項目應包含在正確的作業中（檢查）
- 它可有效地應用於範圍廣的要記住的步驟（廣博的）
- 直至所需之前步驟已完成，否則會阻礙此一步驟的進行（強迫性）
- 幫忙作業者知道所需之步驟已完成（確認）
- 當動作已檢查完畢，此提醒物很容易移開（結束）

5. 是否作業前先檢視工作條件？

6. 作業是否與原先計畫相符合？

■ 若不符合，則有何改變？

■ 對於改變，有何因應措失？此因應措施是否被廠方允許？

7. 是否存在有阻礙作業進行的因素？若有，是否能排除？若不能排除，

有何因應措施？

8. 作業人員是否正確地瞭解風險與嚴重優先順序？

9. 此步驟如須與別單位協調，是否進行協調？協調完成後，始進行此步驟。

10.進行每一步驟前，是否有足夠的資訊以完成作業？

11.進行每一步驟前，是否核對所要作業的設施是正確的？

12.進行步驟時，是否擷取到所需的資訊？

■這些資訊顯示出設備的狀態為何？

13.如對此步驟有所疑慮或對狀況不甚了解，是否停止作業並請求他人支援與協助？

14.進行的步驟動作結果是否合乎作業要求？

15.關鍵動作完成後，是否有請同伴或廠方品管人員檢查？

16.動作完成後，系統狀態是否與預期相符合？

- 如非與預期相符合，發生了什麼問題？
- 這問題若持續下去，會對系統安全產生什麼後果？
- 應如何處置（應用那些法則）以解決此問題？
- 這些法則有無副作用而對系統安全產生影響？

17.此步驟如屬檢驗點，是否停止並立即請求廠方品管人員檢查？

D.作業結束

1.是否有觀察比較、核對、確認作業如預期結果？

2.復原作業前是否先知會相關單位？

3.是否將原設備復原並清除作業現場？

4.是否執行重置作業，並確認所有相關組件介面恢復正常？

5.是否進行系統檢測，以確認系統恢復正常？

6.是否將檢查點彙整驗收？

E.作業檢討

1.在作業中有何意料之外的事發生？

2.在進行那些步驟時容易發生疏失？監工是否知道這些狀況？

3.有那些情境容易造成這些疏失？

4.訓練是否涵蓋所需之知識與技能？

5.程序書是否正確、能用、易懂？

6.作業的計畫是否合理？時間是否足夠？

7.工作場所的資源與資訊是否足夠？

8.工作流程是否有效率？

9.有那些經驗可以承傳？這些經驗是否有正式記載於文件中？

10.監工是否提供所需的支援與指導？

F.作業改善

1.改善的提案是否考慮到有效性、顯著性、持續性、難易度、經濟性、及時性？

2.各提案的評估是否就有效性、顯著性、持續性、難易度、經濟性、及時性等項有指標得以綜合量化評價？

3.提案的決策是否以安全為優先考量？

4.改善案的效果是否持續地追蹤？

第二節： 作業行為稽查之技術轉移

壹 研究方法及步驟

此部份之研究方法及步驟如下：（流程如圖 2）

一、資料收集：收集國內外稽查觀念與作法之相關文獻。

二、技術移轉教案之開發：選用適當之教學編輯輔助器材，編寫教案。

三、試教：選取未來稽查人員，移轉稽查相關技術。

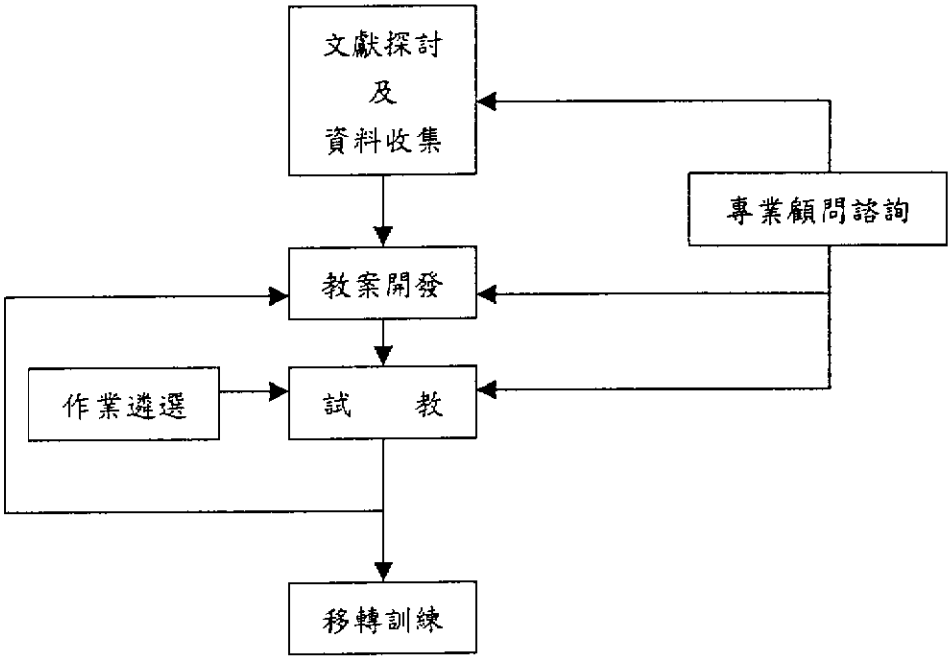


圖 2 技術移轉流程

貳 研究結果

此部份之研究結果如下：

一、資料收集：收集及探討國內外稽查觀念與作法之相關文獻執行本研究所將開發出來之稽查系統之技術轉移時，有必要將國內外相關之稽查觀念與作法一併納入教案內，以利學員對稽查有個全面性的概念，從而了解本研究所將開發出來之稽查系統的殊勝。進而能充分善用此系統使其成為核電廠員工及包商作業事故之最佳終結者。

國外諸多稽查觀念與作法中，以經濟部工業局所引進之現代安全管理（Modern Safety Management；MSM）較完整該系統並歷經多年來的推廣，以為國內多數大型企業所知曉，但是，該系統並未被有效落實在前述企業。現代安全管理課程表如表，其各主題的主要內容如後。

表 5：現代安全管理課程表

第一天	
● 簡介	
● 災害的影響及其解析方法	1
● 損失控制管理	2
● 定期檢查	3
第二天	
● 複習	
● 小組會議	4
● 安全規章推行	5
● 財產損失控制	6
● 有效安全宣導	7
第三天	
● 複習	
● 個人溝通	8
● 作業環境健康管理	9
● 事故調查	10
● 事故推演	11
第四天	
● 複習	
● 下班後安全	12
● 績效量測	13
● 作業分析與步驟	14
● 作業觀察	15
第五天	
● 複習	
● 激勵技巧	16
● 獲取高階主管的支持	17
● 課後測驗	
● 討論	

「災害的影響及其解析方法」介紹災害結果比例分析、災害損失費用冰山模型，損失發的骨牌模型，損失控制的三階段，及每個階段的控制範例。

「損失控制管理」介紹管理的功能，損失控制管理的目標，降低風險的方法，管理的基本原則，管理控制的內容，達成損失控制的管理工作，及管理控制的十項安全要點。

「定期檢查」介紹檢查的好處，類型，檢查前準備，檢查順序的設定，補救設施的發展，追蹤行動的執行，及檢查報告的準備。

「小組會議」介紹溝通定義、原則、有效的會議領導技巧，及安全談話的原則：(1)事前準備(2)針對重點(3)針對對象，(4)具體化及(5)具體指示等。

「安全規章推行」介紹安全規章之執行與落實，個人防護設備之使用，良好

內務整理之鼓勵，物料節約觀念之增強，及物料節約計畫指引。

「財產損失控制」介紹財產損失之災害被忽視之原因，財產損失事故與人員傷失亡之關係，財產損失之鑑認方法，關鍵性財產損失項目之放量因素，及財產損失之控制技術。

「有效安全宣導」介紹推銷第一定律，有效安全宣導需具備：特質，宣導安全的方式，安全活動指引，安全宣導之定則，及安全作動十項守則（即美軍十點計畫）。

「個人溝通」介紹個人溝通應用範圍，個人工作引導步驟定期訪談的好處，是個人訪談的步驟，重點指示的基本指引，工作績效教導，及認知權定律。

「作業環境健康管理」介紹健康危害分類及其變數，危害物進入人體的途徑，健康危害的辨識、評估、與控制，及物質安全資料表。

「事故調查」介紹調查的目的、調查的人員，調查的步驟不提報事故的十大原因，事故現場所需採取的初期行動、面談指南，可提供訊息之零件檢測及記錄及其他文件證據，事故分析，及系統化的原因分析技術。

「事故推演」介紹關鍵性虛驚事故的辨識，虛驚事故的檢討，災害事故的推演，災害事故推演應用，及災害事故推演的利益。

「下班後安全」介紹家庭意外事故對工作場所損失控制的影響，下班後安全計劃注意事項，計劃成效的評估方式，管理上可採行之推行方式（時機）及典型的社區團體活動。

「績效量測」介紹良好量測工具的特性，量測的方式，獲得潛在損失數據的方法，量測"控制"的優點，量測"控制"的方法，量測的型態及提高評斷準確性的原則。

「作業分析與步驟」介紹作業(TASK)，作業程序(PROCEDURE)，與常規(PRACTICE)的定義，訂定有效作業程序(常規)的步驟，關鍵性作業的辨認，及潛在危害因素的確認。

「作業觀察」介紹作業觀察的功用，看與觀察的差別，作業觀察之型式，計劃性作業觀察之步驟，作業之選擇，員工之選擇，部份或重點觀察，及作業觀察之利益。

「激勵技巧」介紹何謂員工工作榮譽之激發，管理推行的三階段，合作參與的管理／領導方式，有效的行為增強步驟，工作生涯品質，組織氣氛，工作調度，工作榮譽之原動力及發展工作榮譽之益處。

「獲取高階主管的支持」則介紹十一項主管重視的項目。

如上所述，現代安全管理課程講義確實包含了諸多安全管理所需的觀念與作法，應該可以作為本研究所將開發出來之教案的重要參考，但需特別注意以下兩點：

1. 講義係為五天之訓練內容，在觀念上與作法上似有過猶不及的現象，本研所將開發出來的教案應以簡明、扼要、中肯為原則，訓練時間以不超過十二時為原則。
2. 如同前所述，此現代安全管理系統並未被有效地落實在國內企業裡，自有其潛在的問題，因此在參考的同時，應特別避免陷入同樣的問題。

至於國內的諸多稽查關念與作法中，如同 2.1.1 一節所述眾多選擇，唯有相關技術之轉移部份，較欠缺一套完整的作為或許確實存在相關教案可供參考，將在接下來的幾個月裡，繼續進行此一方面資料之收集與參考，俾使本研究之成果品質能有進一步的提昇。

二、教案開發：

I. 選用適當的教學編輯輔助器材，編寫教案

教案開發主要目的係尋求一有效溝通方式，將本研究所開發出來的稽查系統之相關知識與執行技術傳授給學員，為達有效溝通的目的，相關的教學法包括成人教育原等，及可用的教學輔助器材均應進一步的探討，尤其是逢臨科技媒體蓬勃發展的現代，下列工具應考慮納入本研究之教案設計過程裡。

(一) 學員可自行依自我能力調整自我進度的電腦多媒體稽查系統教案軟體之劃。

(二) 可克服時空，節約學員時間與經費的遠距離稽查系統教學設計之規劃。

(三) 可提供學員快速查詢相關稽查知識與技術的電腦查詢系統之規劃，可考慮電腦查詢軟體設計及網路相關資訊聯結等方向規劃。

(四) 網路互動系統設計之規劃，以隨時解決不同地點學員的問題，可能的話也可規劃談天網站，交流各地學員彼此的心得與感情，提昇彼此的稽查技術與能力。

教案初期書面資料應以適當的文書處理軟體設計，如 WORD、POWERPOINT 等，設計出易於閱讀活潑有趣的手冊，加以適當的紙張品質的選擇及親和性包裝，並提供講員恰當的教學投影片資料，電腦多媒體化之教學用簡報程式，及教學評量問卷等，以提昇及改善整個技術移轉的品質。

為了執行教有訓練計畫，除應訂定訓練目標外，還要編製或選定適當之教材，來指導員工學習。教材教法是訓練上傳授員工工作知能或協助員工發展潛能時所必須講究的。教材是訓練的內容，有了充實的內容，訓練才不致空疏；教法是訓練的方法，有了良好的方法，才可以有效地達成教育訓練的目的。教材與教法兩者能密切配合，教材才顯得有用，教法才不致落空。

藉由教學理論與學習理論的探討，我們瞭解到企業教育訓練之本質，及執行訓練時所應用之理論及技巧。適當的運用各種理論及技巧，增加學習成效及訓練效果。

成人學習的特點：

1.成人以往的經驗為其教育的始點，並關係到吸收新知識的能力，如何充分利用就有經驗來進行新的學習是非常重要。

2.成人具有自發性動機，大都是問題導向或工作導向來進行學習，而且由於成人多餘的時間不足，所以傾向立即可用的學習。

3.成人學習的動機多來自於內在因素，且學習過程中重視回饋，以確定是否學到實際可用的技能。

4.成人自主性高，容易受到學習環境的干擾，故必須在一個愉快的環境中進行學習活動。

5.成人仍有可塑性的存在，而基於需要的前提、興趣的前提及發展的前提，成人必須再學習或重新學習以應付生活的需要。

教案為教學的具體方案，其範圍以一個單元或一個課程為內容，時間不限，通常以一小時為一個單位。教師在教學之前，將教學時師生的活動、教學目的、教學方法及教學器材等詳細的計畫，以便施教。這種詳細的計畫稱

之為「教案」。教案應包含之要素有：1.學生分析；2.環境佈置；3.教材分析；4.教學目標；5.教學過程；6.流程圖；7.教案格式；8.教學資料；9.單元教學；10.考核方法；11.時間控制。

教案的編製方式如下：

1.編製步驟：a.確立目的；b.了解情境（包括對象及環境）；c.選編教材；d.定教學方法；e.準備教具；f.計劃過程；g.整理繕寫。

2.注意要點：a.內容詳簡得宜；b.綱舉目張；c.了解教學原理；d.熟悉教學方法；e.想像教學情境；f增加活動；g.準備充分；h.以一頁為宜。

II.教案內容

本教案分為下列幾個單元：1.系統安全之基本概念，2.系統安全管理計畫，3.危險分析，4.人為疏失之本質與基本觀念，4.5.促成人為疏失的因素，6.人為疏失的防治，7.安全行為的管理，8. 稽查查核表的使用。茲將每一單元之內容剛要分述於下：

1.系統安全之基本概念

本單元闡述安全的定義，安全與風險之關係，系統的定義，系統方法的介紹，以及引用系統方法來解決安全問題的動機。

2.系統安全管理計畫

本單元介紹管理的理論以及如何用系統方法來建立安全管理計畫，還有敘述安全管理計畫應涵蓋之項目。

3.危險分析

本單元介紹各種危險分析的方法。

4.人為疏失之本質與基本觀念

本單元闡述人為疏失之本質與分類。

5.促成人為疏失的因素

本單元介紹促成人為疏失的近因（TWIN 模型）與遠因（亦即，組織因素）

6.人為疏失的防制

本單元介紹人為疏失的防制方法

7.安全行為的管理

本單元介紹安全行為的管理以及安全稽查的發展原則

8.稽查查核表的使用

本單元介紹稽查查核表的內容、項目之評估方法與標準、查核報告之彙整。

教案的詳細內容編錄於附錄一。

第三章　結論與建議

本研究主要分為兩部分，第一部份為有關安全作業之作業行為稽查系統之建立，第二部份為作業行為稽查之技術轉移。前者的主要工作項目有：(1)文獻探討，(2)瞭解包商有關安全之作業，及(3)發展安全作業之作業行為稽查查核表，等;後者的主要工作項目有：(1)資料收集，(2)技術移轉教案之開發，及(3)試教等。

在有關安全作業之作業行為稽查系統之建立的文獻探討方面，對於人為疏失與安全稽查部份的相關理論進行深入探討。在人員作業疏失模型部份，檢討了行為表徵模型、作業與環境模型、認知機制模型等相關文獻；其中認知機制模型方面，Norman 的疏忽模型、Rasmussen 的人與作業不搭調（Human-Task Mismatch; Human-System Mismatch）、Reason 的人為疏失模型、及 Reason 計畫的錯誤（mistakes in planning），指出人員作業之心智歷程在人為疏失發生機制中扮演重要角色，因此安全行為的稽查應涵蓋作業之認知歷程。此外，在降低疏失的策略方面檢討了 Sanders and McCormick 方法、Lourens 方法、Mason 方法、及組織內確認與控制疏失的方法等，認為人為疏失的防範不僅應著重於作業人員的安全行為的塑造與增強、安全意識的提昇，而且也應涵蓋組織運作、作業程序、作業環境缺陷的改善。

在安全稽查部份檢討了稽查種類、稽查原則、稽查階段、及其他安全技術等。此外，在安全管理系統檢討了建立安全管理系統的三種方法，強調：(1)管理階層承諾的重要性，(2)設定清楚的安全目標，及(3)妥當地溝通所需要的資訊。因此，安全稽查系統的推展必須獲得管理階層的支持，制訂獎勵制度，以加強其安全行為，由此建立安全文化。

在有關安全作業之作業行為稽查系統之建立的作業分析方面，主要為瞭解包商有關安全之作業。本研究檢討了「包商與安全有關之工作項目」與歷年來包商人員作業不當和違規資料，這些資料指出包商之人為疏失大多屬技能行為的疏忽與安全意識的不足。因此，包商工作人員施工前重點講習實應加強（1）安全行為模式之訓練和潛在風險的知覺與評估-安全行為包含：規畫、執行、檢查、評估、修正改善等五個階段，每個階段有其最佳化的作法以確保安全。演練這些作法可以將安全行為內在化成為作業習性，取代其以前之不合適的作業習性；（2）講授系統與設備的知識，建立其正確的心智模型，以減少知識基礎的錯誤；（3）獎懲制度的宣導，以降低違規、抄捷徑。

基於理論的探討與電廠人為疏失案例的分析，安全作業之作業行為稽查系統的重點在於：將安全行為作法成為正式化（formalize）的作業模式，把無意識的例行動作，提昇至意識層次，以降低技能疏忽；將狀況察覺、風險評估成為作業流程的必要步驟，以掌握現況，降低規則錯誤。因此，安全作業之作業行為稽查系統的發展乃以作業分析為基準，將安全行為之具體作法納入查核表。建議未來可將查核表轉換為安全行為宣導與訓練的工具。

在作業行為稽查之技術轉移的資料收集方面，主要探討經濟部工業局所引進之現代安全管理 (Modern Safety Management ; MSM)。認為現代安全管理課程講義確實包含了諸多安全管理所需的觀念與作法，應該可以作為本研究所將開發出來之教案的重要參考，但需特別注意以下兩點：

1.講義係為五天之訓練內容，在觀念上與作法上似有過猶不及的現象，本研所將開發出來的教案應以簡明、扼要、中肯為原則，訓練時間以不超過十二時為原則。

2.此現代安全管理系統並未被有效地落實在國內企業裡，自有其潛在的問題，因此在參考的同時，應特別避免陷入同樣的問題。

在國內的諸多稽查觀念與作法中，有相關技術之轉移部份，較欠缺一套完整的作為，未來應繼續進行此一方面的研究，俾使作業行為方面的安全稽查更能發揮其功效。

在作業行為稽查之技術轉移的教案開發方面，為將本研究所將開發出來的稽查系統之相關知識與執行技術有效的傳授給學員，相關的教材，教法之設計所應用到之理論、原則包括成人教育原理等，及可用的教學輔助器材等均做了進一步的探討，目前教案運用 POWERPOINT 為媒體來傳遞，建議未來將最新的一些科技媒體工具考慮納入本研究之教案設計過程裡。

誌　　謝

謝謝行政院國家科學委員會經費支援，此一研究才得以進行，希望能繼續支援此一計劃至年度結束時，並適度支援後續的相關研究計劃，以使此計劃的效益能充份發揮出來。

參 考 文 獻

[1] Endsley, M. R.. Toward a theory of situation awareness in dynamic systems. Human Factors, 37, 32-64, 1995。

[2] Jensen, R. S.. The boundaries of aviation psychology, human factors, aeronautic decision making, situation awareness, crew resource management. The International Journal of Aviation Psychology, 7, 259-267, 1997 。

[3] Maurino, D. E., Reason, J., Johnson, N., & Lee, R. B. Beyond Aviation Human factors. Hants, UK: Avebury Publishing Limited, 1995。

[4] Sarter, N. E. & Woods, D. D.. Team play with a powerful and independent agent: Operational experiences and automation surprises on the Airbus A-320. Human Factors, 39, 553-569, 1997。

[5] Rasmessen, J.. Human errors: A taxonomy for describing human malfunction in industrial installation. Journal of Occupational Accidents, 4, 311-335, 1982。

[6] Wiegmann, D., & Shappell, S.. Human factors analysis of postaccident data: Applying theoretical taxonomies of human error. The International Journal of Aviation Psychology, 7, 67-81, 1997。

[7] 經濟部工業局，現代安全管理，1993。

[8] 中華民國工業安全衛生協會，勞工安全衛生教材-安全管理師訓練，1994。

[9] 王文科譯，學習心理學，五南圖書，1989。

[11] 吳明清，教材教法的問題與趨勢，師大書苑發行，1996。

[12] 吳幸宜譯，學習理論與教學應用，心理出版社，1996。

[13] Gagne', R. M. The conditions of learning theory of instruction (4th ed.). New York: Holt, Rinehart & Winston, 1985。

[14] Hayes, A., Assisting Adult Students on Award-bearing, 1996。

附錄一

作業安全行為稽核技術移轉教案

台灣電力公司
安全作業行為稽核課程

許尚華
國立交通大學
工業工程與管理學系

第一單元

系統安全之基本概念

一、何謂「系統安全」？

「安全」：免於意外事故的發生與所造成的損失。

沒有一個系統是沒有風險的。因此，較實際的作法是：如何降低風險，同時也能確保系統所帶來的利益。所以，我們必須去了解風險、控制風險，將風險降低至我們所能接受的程度。

「系統安全」涵括了風險管理所有的範疇。它包括了系統發展與運作過程中技術層面與社會層面的議題。它應用了科學、工程、與管理學的原則，以便在系統的生命週期中，在運作的效率、時間、經費的限制下，能夠確保適當的安全、及時確認出危險的風險、並且進行一些措施來避免或控制這些危險。

二、我們為什麼要談【系統安全】？

- 安全是系統所衍生的特性，因此決定是否能接受一個系統的安全並不能端看其組件。組件層次是可靠度的議題；而安全性乃取決於組件間之關係，也就是，整體的情境。
- 早期 "Fly-Fix-Fly" 的方法，頭痛醫頭，效果不彰，且花費過多，難為接受。
  - ■調查意外事故，重建事故肇因
  - ■採取行動以避免或減低同一原因之事故發生，並將這些措施納入準則、規範

●事故的發生是由一連串疏失衍發而成—錯誤鍊（Error Chain）。這些疏失大多發生於系統組件間的介面，受科技、生態、社經政治、和文化之間的互動所影響。所以，事故的防治並不能單靠科技的修正就能解決，必須要多管齊下才能正本清源。

因此，必須採用系統的方法來解決問題

三、系統方法

A.系統觀

1.Reductionism V.S. 系統理論

Reductionism：

將問題切割成幾個部分，然後對於每個部分分別加以檢驗。

它基於以下幾個假設：

(1)將問題分割並不會扭曲問題的全貌

(2)當對每個組件分別單一檢驗時，這些組件就如同在整體中運作

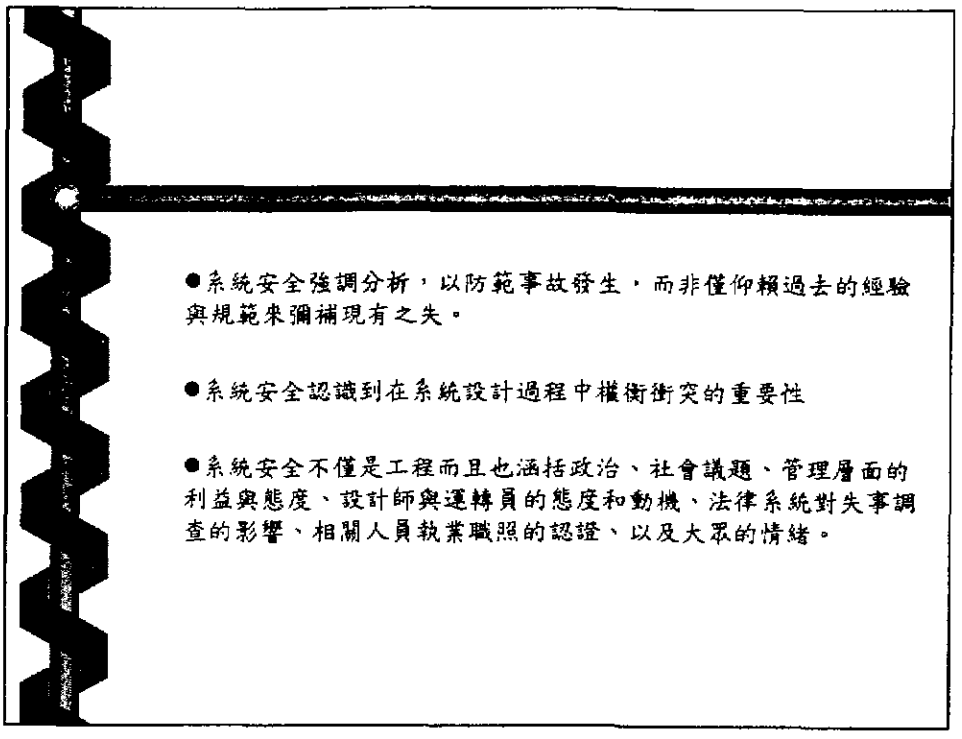
(3)將組件組合成整體的原理是非常直接

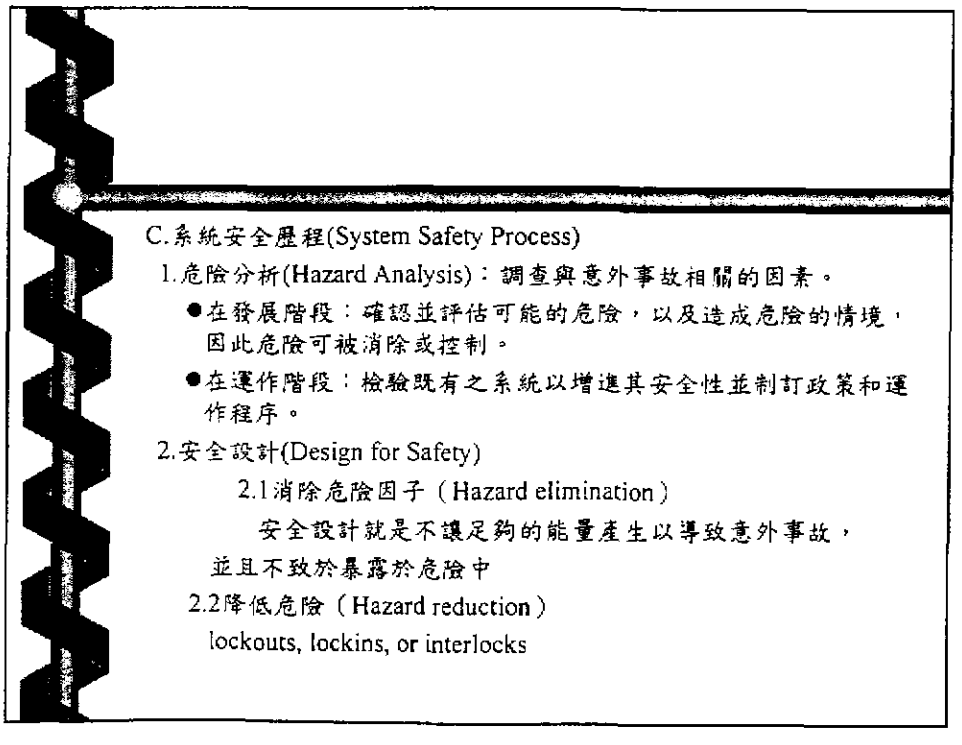
– 系統理論：

- 系統（System）：一群組件一起運作成一個整體，以達成某個共同目標。這些組件互有相關並且直接或間接地互相連結。
- 它認為系統的一些特性必須整體來處理；需要考慮所有層面和所有變數，並且將社會層面與技術層面相關連起來。由於這些系統特性是由系統組件間的關係衍生出來的，因此需要考量組件間是如何互動與結合。
- 必須界定（1）系統的目標，（2）系統範圍，（3）結構，（4）組件，（5）輸入/輸出，和（6）組件間之互動以及系統如何維持其整體性

–B.系統安全的重點-危險的管理：確認、評估、消除、和控制

- 系統安全是在系統發展的過程中建立出來的，而非附加到已完成的系統上去的
- 系統安全將系統整體處理，而非僅片面針對某個次系統或者組件
- 系統安全以較廣的觀點來看危險，而非祇針對失效；非失效系統也會產生危險。並且失效是可靠度的問題，而危險是安全的問題，兩者常互相抵觸


●系統安全強調分析，以防範事故發生，而非僅仰賴過去的經驗與規範來彌補現有之失。
●系統安全認識到在系統設計過程中權衡衝突的重要性
●系統安全不僅是工程而且也涵括政治、社會議題、管理層面的利益與態度、設計師與運轉員的態度和動機、法律系統對失事調查的影響、相關人員執業職照的認證、以及大眾的情緒。


C.系統安全歷程(System Safety Process)
1.危險分析(Hazard Analysis)：調查與意外事故相關的因素。
●在發展階段：確認並評估可能的危險，以及造成危險的情境，因此危險可被消除或控制。
●在運作階段：檢驗既有之系統以增進其安全性並制訂政策和運作程序。
2.安全設計(Design for Safety)
2.1消除危險因子（Hazard elimination）
安全設計就是不讓足夠的能量產生以導致意外事故，並且不致於暴露於危險中
2.2降低危險（Hazard reduction）
lockouts, lockins, or interlocks

2.3控制危害（Hazard control）

- 被動（passive）-利用物理原理，如地心引力
- 主動（active）-需要某些動作以避免或減輕危險的效果。這些動作包括危險的偵測與回復或fail-safe的程序（例如：火煙偵測與灑水系統）

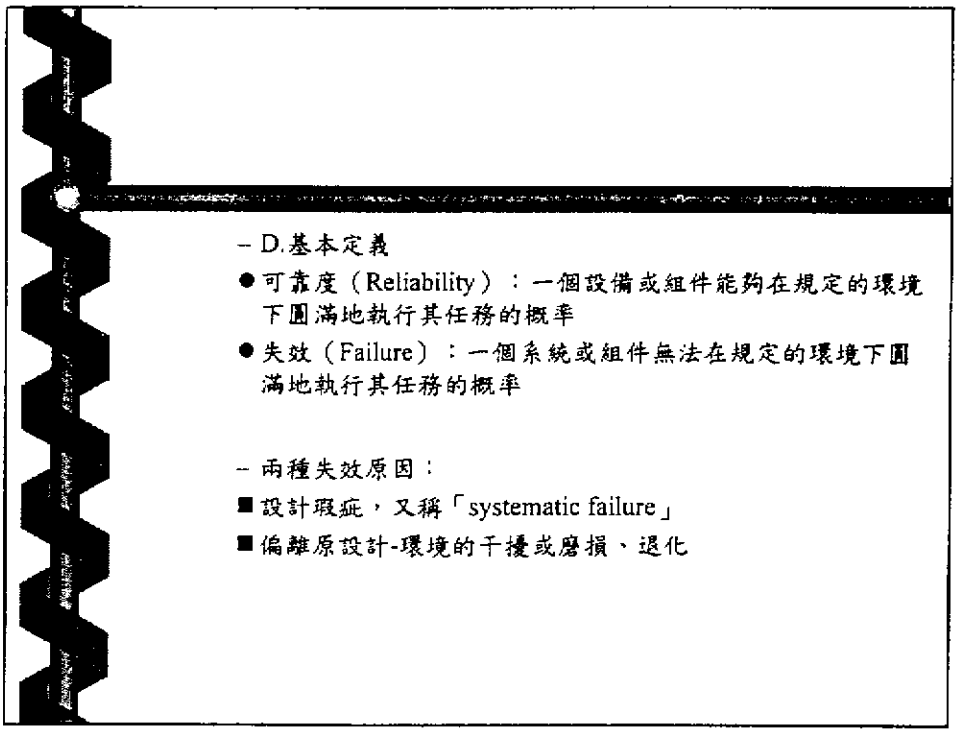
2.4減少損害（Damage reduction）

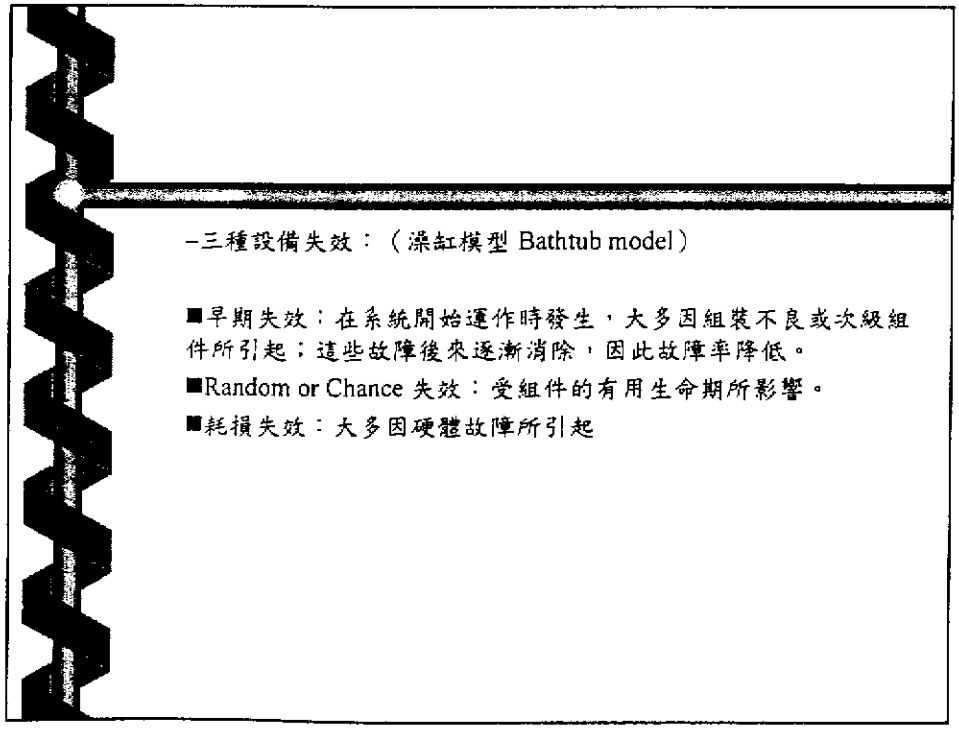
(1)提供緊急狀況的警告設備、緊急訓練、與緊急應變程序,

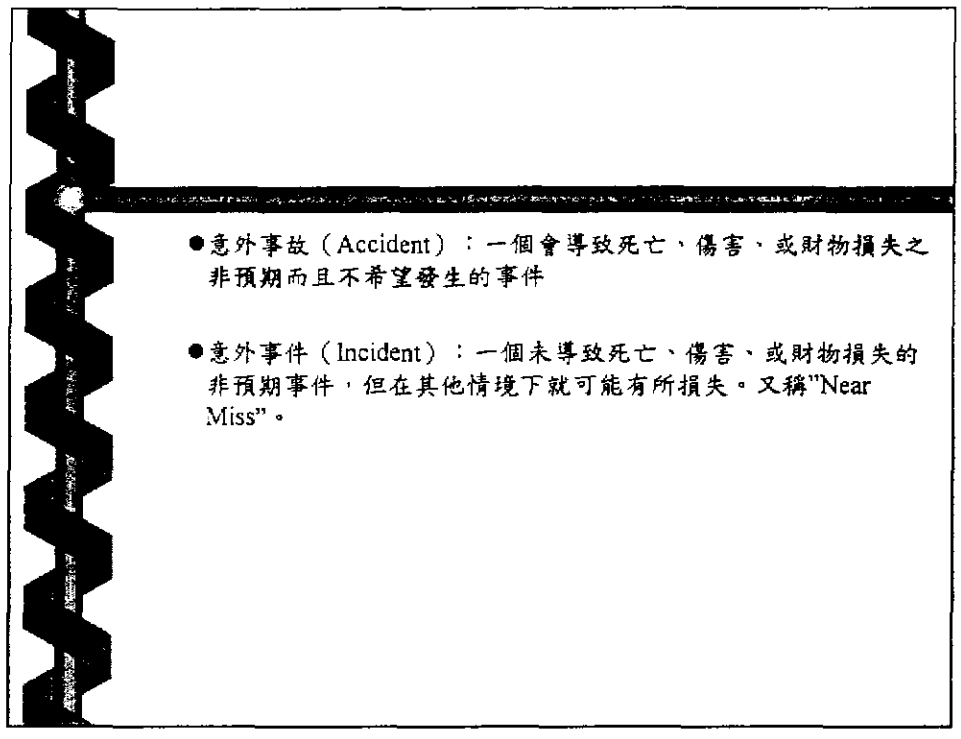
(2)將危險系統與人口密集點隔離

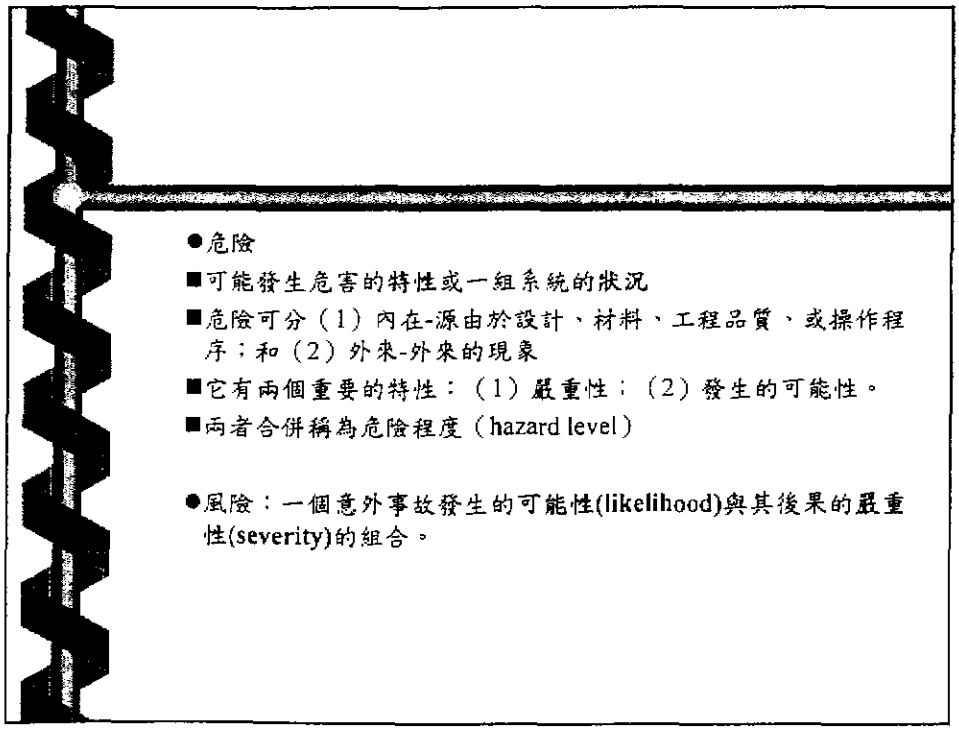
3.安全管理(Management)

- 界定目標和制訂政策
- 規畫作業與程序
- 界定職務，授予權力，和委予責任
- 記載與追蹤危險和解決方案
- 保持安全資訊系統和相關文件


– D.基本定義
● 可靠度（Reliability）：一個設備或組件能夠在規定的環境下圓滿地執行其任務的概率
● 失效（Failure）：一個系統或組件無法在規定的環境下圓滿地執行其任務的概率
– 兩種失效原因：
■ 設計瑕疵，又稱「systematic failure」
■ 偏離原設計-環境的干擾或磨損、退化


–三種設備失效：（澡缸模型 Bathtub model）
■早期失效：在系統開始運作時發生，大多因組裝不良或次級組件所引起；這些故障後來逐漸消除，因此故障率降低。
■Random or Chance 失效：受組件的有用生命期所影響。
■耗損失效：大多因硬體故障所引起


●意外事故（Accident）：一個會導致死亡、傷害、或財物損失之非預期而且不希望發生的事件
●意外事件（Incident）：一個未導致死亡、傷害、或財物損失的非預期事件，但在其他情境下就可能有所損失。又稱"Near Miss"。


●危險
■可能發生危害的特性或一組系統的狀況
■危險可分（1）內在-源由於設計、材料、工程品質、或操作程序；和（2）外來-外來的現象
■它有兩個重要的特性：（1）嚴重性；（2）發生的可能性。
■兩者合併稱為危險程度（hazard level）
●風險：一個意外事故發生的可能性(likelihood)與其後果的嚴重性(severity)的組合。

◉ 四、事故模型

- 要設計一個有效的安全計畫並選擇一套合適的程序和技術，我們必須了解事故的模型及其假設。
- 使用事故模型有兩個目的：（1）了解以前的事故；和（2）學習如何避免未來可能事故。
  （1）事故調查：確認出顯著的因素；在資訊的收集過程中過濾不相關的調查；總之，在事故的調查中模型幫忙設定先後順序並且組織資訊。
  （2）預測事故的發生：決定有那些因素與未來事故有關，以消除或控制它們。

一I.能量模型（Energy Models）

- 早期的模型：
  » 將事故視為未控制的能量釋放出來。因此，在預測或解釋所預期的危險或事故的後果時，能量的種類是非常重要的變項。另外，設置屏障或改變、控制能量流動的路徑是避免事故發生的主要方法。
- MacFarland的模型：
  » 事故是由於（1）所應用的能量超過結構所能抵擋，或（2）有機體與環境間的能量交換受到干擾所引起的。因此，控制能量的來源或能量抵達身體的攜帶物，就可避免事故的發生。

●General Energy Model:

–將事故分為兩種：

(1)能量轉換：當能量轉換成會損壞財物或傷害人員。例如，爆炸。能量轉換的事故需要能量的來源以及相關的轉換機制。避免事故的發生必須控制兩者或其一。

(2)能量不足：當需要能量來執行某個重要功能，例如引擎失去動力。這類的事故需要某種能量來執行安全相關之功能（例如，汽車的煞車油）和讓能量不足的情境或事件（例如，煞車油漏）。

II.骨牌與單一事件模型（Domino and Single Event Models）

– 最早的工安事故模型著重於不安全的情境，後續的模型將重點轉變到人們不安全的動作。

1.骨牌模型

●Heinrich模型：假設人們是事故的原因。事故發生的順序是五個骨牌：

（1）先前或社會環境，導致

（2）個人的疏失，成為第三骨牌的近因

（3）不安全的動作與情境，進而造成

（4）事故，導致

（5）受傷

-當第一個骨牌開始倒時，其餘陸續被擊倒，直至有傷害發生。將其中之骨牌搬離，則可避免傷害發生。Heinrich認為最容易搬除的骨牌是第三個。

●Bird和Loftus將管理決策納入：

（1）缺乏管理上的控制，而讓

（2）基本原因（人員與工作因素）導致

（3）立即原因（低於標準的作業實施/情境/疏失），而成下一項的近因，

（4）事故或事件，

（5）損失

●Adams的模型

（1）管理架構（目標、組織、和運作）

（2）作業疏失（管理階層或監督者的行為）

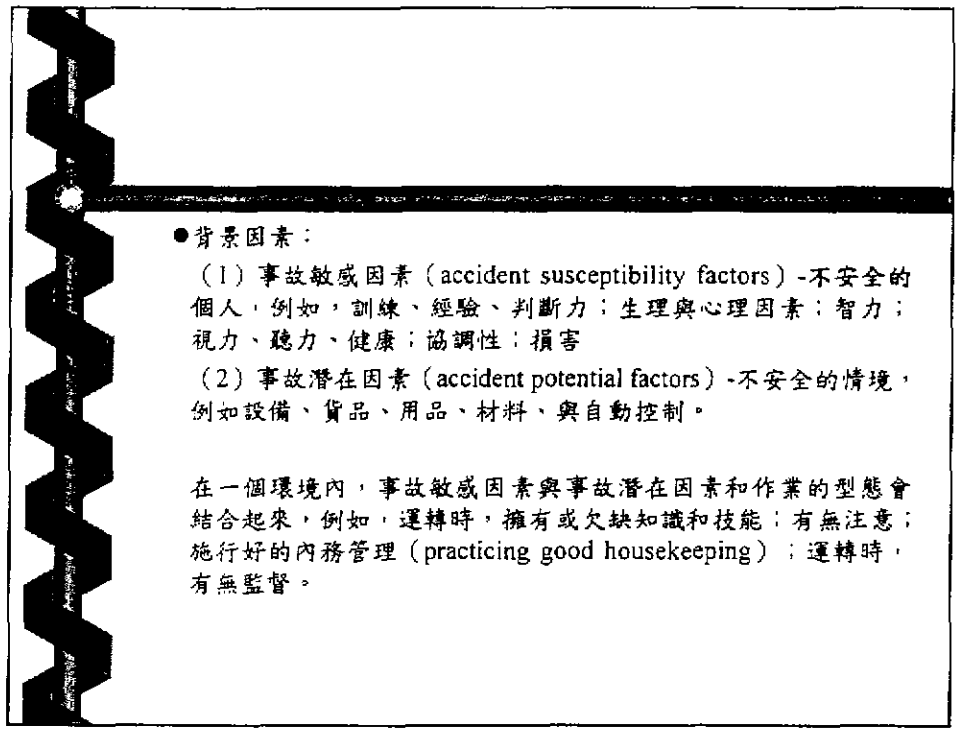
（3）戰術上的疏失（由員工行為和工作狀況）

（4）事故或事件

（5）人員傷害或財物損失

2.美國國家安全委員會模型（National Safety Council Model）

含括背景因素、原始因素、中間因素、立即因素、和可測量的結果

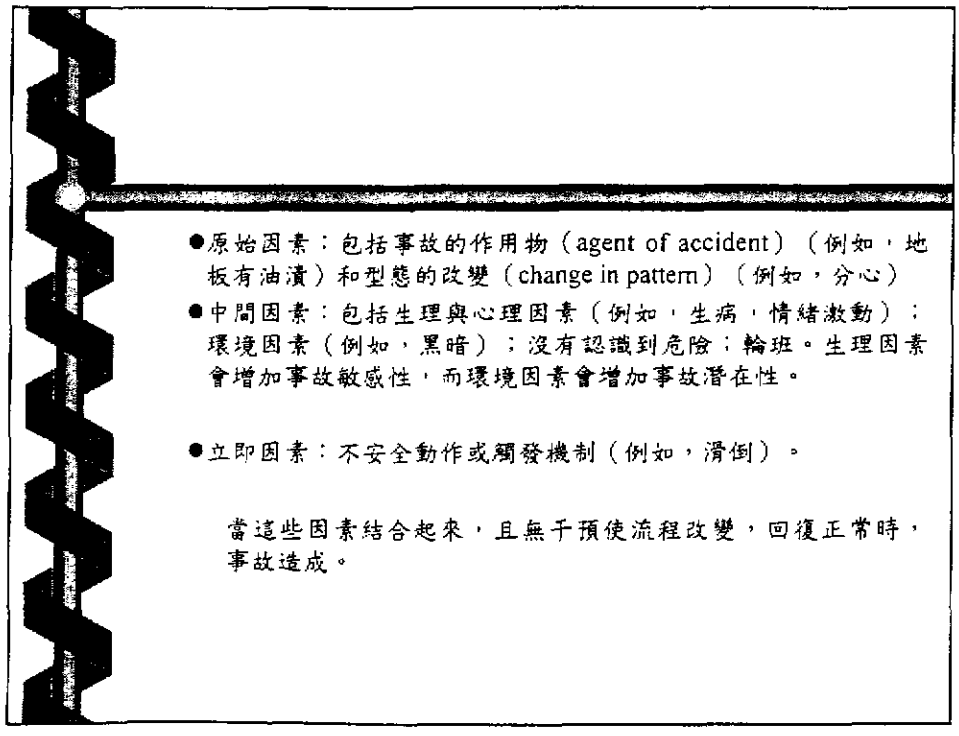


●背景因素：

（1）事故敏感因素（accident susceptibility factors）-不安全的個人，例如，訓練、經驗、判斷力；生理與心理因素；智力；視力、聽力、健康；協調性；損害

（2）事故潛在因素（accident potential factors）-不安全的情境，例如設備、貨品、用品、材料、與自動控制。

在一個環境內，事故敏感因素與事故潛在因素和作業的型態會結合起來，例如，運轉時，擁有或欠缺知識和技能；有無注意；施行好的內務管理（practicing good housekeeping）；運轉時，有無監督。



●原始因素：包括事故的作用物（agent of accident）（例如，地板有油漬）和型態的改變（change in pattern）（例如，分心）

●中間因素：包括生理與心理因素（例如，生病，情緒激動）；環境因素（例如，黑暗）；沒有認識到危險；輪班。生理因素會增加事故敏感性，而環境因素會增加事故潛在性。

●立即因素：不安全動作或觸發機制（例如，滑倒）。

當這些因素結合起來，且無干預使流程改變，回復正常時，事故造成。

III.事件鍊模型（Chain-of-Events Models）

將多個因果因素組織成事件鍊，如果事件鍊斷了，事故就不會發生。事故防治的方法就著重於如何消除某個事件或將事件間作干預。

在這些模型中，以時序來將所發生的事件串聯起來，將事件與狀況標示為近、原始、基本、造成的、系統的、根本的。不安全的動作與狀況祇是要研究為何發生的起點。這個方法的問題是當在回朔事件時無終止點，而且有些前置事件與設計防治措施無關。

1.事故的混亂論（The Perturbation Theory of Accident）

Benner的Multilinear Event Sequence model：事故是一連串事件，而一個事件定義為一個動作者（actor）加上一個動作（action）。事故的過程是幾個特定的動作者互動，每一動作者動作有其時空關係而連成一個順序。因此，事故可用平行進行事件的軌道，用交叉線表達其關係，而且用時序來表示。

這種連續的事件需要動作者對於外界的紛擾作出適應性行為以使事件朝預期的結果進行。祇要動作者能夠適應紛擾，不致於使適應、恢復的能力受過度壓力，能維持平衡，則事故不會發生。

由於此模型提供事件序列中事件間的中介原則以及重新排序以檢驗其它可能性，它能夠增加選擇防治措施的能力。

2.INRS model

-此模型著重於改變的重要性。改變可依人員、機器、環境、和作業來分類。事故可視為正常成功作業的變異性所促發一連串是件鍊的後果。在此模型中，事故對應到變異性的樹狀結構，將對可用於未來改善的點確認出來。因此，重點在於找出截斷事故順序的方法；也就是說，找到能夠改進目前決策或動作或引進新決策的重要決策點。

用事件鍊圖來表達兩種關係：（1）事件鍊關係（Event Chain Relationships），表示如X事件未發生則Y事件也不會發生；（2）群集關係（Confluence Relationships），表示如兩獨立事件不發生，則第三事件不會發生。

3.The National Transportation Safety Board Model of Accidents

用直接事件與因果因素來描述。而因果因素由造成因素產生；造成因素又由系統因素所產生。

4.Johnson's MORT model

- Johnson加入目的、目標、績效、監控與干預。用故障樹向原委會提出「管理疏忽與風險樹」（Management Oversight and Risk Tree）。它是一個查核表。
- 此模型認為所有的事故損失是由於缺乏屏障或控制促成了不需要的能量轉換所造成。損失的來源有二：（1）特定的工作失察和遺漏；和（2）控制工作的管理系統。
- 由於事故通常有許多成因且其疏失與改變順序冗長，MORT提供一個方法將事故的順序分解成一系列個別事件。它考慮到下列的因素：技術資訊系統、設計與規劃、維護、檢驗、當場監督與高階管理、屏障、不需要的、能量流程、政策、和管理系統。

IV. 系統理論模型（Models based on Systems Theory）

系統工程模型著重於探討到底系統運作與組織出了那些問題而讓事故發生。它們認為事故起源於系統組件間的互動違反了一些限制。

系統模型用下列幾個觀念來描述事故：

1.互動功能不良（Dysfunctional Interactions）

互動功能不良有兩種型態：（1）次系統劃分不清、協調不足；和（2）系統的元素之間缺乏連結，例如，團對內之資訊流通不良，個人的能力與工作要求之間欠缺協調

2.控制理論

此類模型將安全認為是控制的問題。系統是由相關的元素所組成，這些元素依靠資訊與控制的迴路來維持動態平衡的狀態。當干擾沒被控制系統適當的控制，故障就發生了。控制模型著重在改變；這些改變由於對系統的瞭解不完整而可以有未預見的後果。

3.偏離常軌（deviations）與決定因素（determining factors）

當系統的變項值落於常模之外時，偏離就發生。所謂常模乃指計畫中、預期的、所要的生產程序。當對偏離有適應不良的反應時，事故就發生。這些偏離可能發生在人們的動作、材料、資訊、指示、設備、環境、能量屏障、和活動間的關係。

第二單元

系統安全計畫

I.管理階層在系統安全所扮演的角色

系統安全的目標唯有靠管理階層的支持使能達到。

管理階層負責：（1）界定安全目標和制訂安全政策；（2）界定權責；（3）建立溝通管道；和（4）設置系統安全機構。

1.界定安全目標和制訂安全政策

管理階層可以透過安全目標與政策的制訂，定義相衝突目標間的先後順序，設置程序以偵測和解決目標間的衝突，和建立誘因的架構。

1.1安全目標與政策

- 安全政策應該界定安全與其他組織目標間的關係並且提供裁決、制訂、和判斷在特定的情境中必須做些什麼。
- 安全政策包含：安全計畫的目標；用於評估短、長期績效的效標；用以做權衡決策的價值觀；權責規定與活動範圍的條文。另外，必須有問題回報的程序。
- 安全政策可分為兩部份：（1）清楚地敘述一般政策與組織的文件；（2）描述規則與程序的詳細文件，包括標準（standards）、手冊（manuals）、與指南（handbooks）。

1.2定義相衝突目標間的先後順序，設置程序以偵測和解決目標間的衝突

- 安全政策需要被宣傳與遵守。管理階層必須確保安全在組織的決策中受重視。進度需要被監督，並且要確認出改進措施，將它們依輕重緩急排序、實施。對於安全問題的彈性反應（如時間具有彈性以應付不確定性和可能的耽擱）也應納入組織的程序中。

1.3必須有誘因和獎勵的結構以促使安全和其他目標之間的權衡能夠處理得當。不僅需要正式的獎勵與規章，而且也要組織文化中非正式的規則（如社會程序）來支援整體的安全政策。當存在有相互衝突的目標時，引用兩種管理的方法能確保權衡能夠得當：（1）建立嚴謹並且詳細的規範，但是此法會犧牲彈性；（2）讓員工去做決策，但是此法會增加判斷錯誤的機會。折衷的辦法就是讓員工作決策，但是設立遵循組織安全政策的誘因，而且讓員工感覺當他們做偏向安全的決策時，管理階層會支持他們。

2.界定權責

- 管理階層必須很清楚地界定在組之內安全的職務（responsibility）、責任（accountability）、和權力（authority）。權力乃指命令和決定行動的權利；而責任意涵著對行動結果的評估。此三者必須一併存在；如果人們被賦予安全的職務但不用對結果負責的話，他們會將他們的努力轉放在他們正被評估的目標上。同樣的，如果人們被賦予職務而且需對結果負責，則他們必須給予權力來做事以能成功，同時組織應建立一套方法來測量績效。

3.建立溝通管道

- 需要建立一套管道以傳播並回饋資訊。這些管道包括比較真正的績效與想要的績效的方法以及確保所需的行動被執行。
- 雖然大多安全計畫提供集中化的危險監督與查核系統，但是資訊必須到達需要資訊的人手中。這種溝通需要在組織中各個層級上有重複的管道以及互相檢查。

4.設置系統安全機構

安全機構在組織中必須是高層級而且獨立的角色。它的職責包括：

- 參與安全政策的設置與實施
- 記錄並追蹤所有的危險與它們的解決方案
- 教育與推廣
- 採納與發展準則
- 參與並執行危險分析以及其他系統安全程序
- 進行趨勢分析並修訂安全文件
- 計畫並監督安全議題的測試與運作
- 參與計畫的審查與重要基點會議（milestones meetings）
- 與其他安全機構的聯繫
- 事故調查與分析

II安全文件（Documentation）

在系統安全中有三種文件：規畫文件、資訊系統、和報告。

1.計畫書（Program Plans）

» 系統安全計畫書（system safety program plan）描述系統安全的目標與如何達到目標的方法。它提供管制單位與管理單位一個用以評估進度與順從安全規範的底線。

2. 安全資訊系統

- 系統安全資訊系統包括：更新的系統安全計畫書；所有活動的狀況；危險分析的結果；所有已知的危險的追蹤與狀況；事件與事故以及其改善措施；趨勢分析資料；等等。

- 安全資訊系統並且可用於描述、診斷、評估、與改進。因此，它提供資訊可以（1）偵測趨勢與偏差已預知事故的發生；（2）評估安全控制措施與規範的效能；（3）比較模型、風險評估的結果與真實行為之差距；（4）確認與控制危險並改進設計與規範。

- 資訊可由公司與業界來收集。業界分享的資訊可加入有關危險的知識以及有效與無效的控制方法。在公司內，資訊系統可提供分析過程的回饋以及外加之控制或更改之需求。

- 一個有效的資訊系統必須不僅含括事故，還要包括意外事件。檢驗與瞭解這些事件可以警惕我們可能事故的發生並且告訴我們有哪些情境需要控制。例如民航界要求報告每一事件。

- 所有資訊必須及時收集、必須正確、必須用有用的格式傳播給適當的人。

2.1 資訊的收集

- 所收集的資訊有下列幾種：績效（performance）與運作（operational）資料；事故與事件調查；研究與評估的結果；技術資訊例如規範、手冊、和和專業文獻。

- 資訊收集的方法可能影響資料的精確度。在收集資料時可能有兩個問題產生：（1）資料被有系統地過濾或壓抑；（2）資料不可靠。資料通常從事故與事件報告得到。這些報告大多只確認出在時間上接近所發生的事（proximal event）而鮮少有早期或因果關係的因素如管理的問題或組織上的缺失。還有，運轉員的報告常過濾而針對技術上的問題；管理階層的報告通常指向運轉員的疏失為事故與事件之主因。一般安全檢查也傾向只確認出少數幾個情境類別。而事故報告通常在發生後由困惑的目擊者收集，因此很難重建事件的經過。

❑改進資料收集的完備性與可靠度可用下列方法：查核表、給予資料收集者特別的訓練、將結果回饋給資料收集者、以及固定的程序。

- 重要事件報告技術（critical incident technique）可用以從有經驗的人員對於事件或事故的回憶中收集有關危險、事件、和不安全情境與施行方法的資訊。
- 模型事故分析表格（model accident analysis forms）可以將多重因素與事件包含進去。這些表格可能要求先前的警告與避免的因素以防範事故再度發生，因此它們可產生實用的建議。
- 自動化監督系統（automated monitoring systems）（如黑盒子）可以增進資料收集的正確性與完整性。儀器可提供重要參數的偏差值與趨勢，以及警報。

–2.2資訊的分析

– 必須將大量的資料濃縮成有用的資訊，不至於被誤導。

–2.3資訊的傳播

– 傳統上，資訊以查核表、規範、實施法則（codes of practice）來傳播。資訊呈現的方式應該與使用者的認知型態與模型相符合，並且與和安全相關的決策環境（如CAD，規畫、時間表、與資源分配系統）整合在一起。

3.安全報告（Safety Reports）

－安全報告有：危險報告表、設計文件、危險分析報告、和安全評估報告。

●危險報告表：

» 內含潛在問題的敘述與目前對它做了什麼。這些報告整合成危險記錄表以為危險稽查與追蹤系統。表格包括：危險的描述與分類，應對行動的歷史，行動的確認（verification），還有相關的系統或次系統，運轉的階段，原因和可能的後果，改善或防範的措施。

●設計文件：

－描述安全相關的設計決策的理念以及由於安全因素所加入的設計特性。這些資訊在安全審查（safety reviews）與維護（maintenance）時非常重要。它也可用於撰寫運轉與維護程序、安全手冊、與訓練手冊。

●危險分析報告：

－報告所使用的分析程序與結果。通常彙整成安全評估報告。

●最終安全評估報告：

» 用於（1）決定是否符合安全要求；（2）提供系統使用者與運轉員詳盡的系統危險、危險的次系統和運轉的描述。包括：

- 系統與次系統以及運轉特徵的描述
- 每一個危險的記錄-包括潛在的原因、所施行的控制、確認活動的結果、偏離要求（deviations from requirements）或免於要求（waivers from requirements）。
- 風險評估
- 危險分析與確認活動的摘要-使用的方法、資料的來源、分析的假說以及它們對結果的潛在影響
- 安全相關的設計與運作的極限
- 危險物品
- 偶發事件與緊急程序
- 事件與事故的記錄

第三單元

危險分析

1.危險分析歷程

–因危險分析目的的不同，所採用的分析歷程會有所不同。

».危險分析的目標

（1）開發：檢驗新系統以確認並評估潛在危險，消除與控制它們

（2）運轉管理：檢驗新系統以確認和評估危險以便提昇安全水準、制訂安全管理政策、訓練人員、並且提昇運轉效率與安全的動機

（3）檢定：檢驗一規畫中或現存的系統以證明其安全水準可為管制機構或大眾所接受

此三個作業又可細分為下列的次作業：

■開發與運轉管理

➢確認出單一或合併可發生事故的危險

➢證明特定的危險不存在並且不需要保護器具

➢決定系統危險可能造成的損害效應

➢評估與危險相關之因果因素：（a）決定危險可能會如何產生、危險的本質、和可能的後果；（b）檢驗因果因素間之關係

- 確認安全設計的標準、安全設備、或程序。這些可用以消除、降低和控制所確認出來的危險
- 尋找避免或消除特定危險的方法
- 決定控制那些無法消除的危險的方法而且如何將這些控制納入設計中
- 評估危險控制的合適性
- 評估品質保證的資訊-品質的類別、所需的接受測試與檢驗（acceptance tests and inspections）和需要特別關心的項目
- 評估規畫的更改
- 調查事故與事件報告。決定它們是否有效度，如果有，決定它們的原因。

■檢定

- 證實設計達到安全水準
- 評估那些無法消除或避免的危險對社會的威脅

2.一個有效的危險分析歷程之特性

危險分析的歷程是持續的、反覆的。危險確認與分析從計畫概念的階段就開始解持續到系統除役。

3.歷程的步驟

（1）目的的界定
（2）界定範疇
（3）界定並描述系統、系統界限、和用以分析的資訊
（4）確認危險
（5）收集資料
（6）依據潛在的效應和可能性將危險分次序
（7）確認因果因子
（8）確認出預防或改善措施以及一般設計的標準與控制方法

（9）評估預防或改善措施
（10）確認所施行的控制方法是正確和有效
（11）將所選的、未解決的危險量化-依發生的概率、經濟的影響、潛在的損失、和預防或改善措施的費用
（12）將剩下的風險量化
（13）運轉經驗的回饋與評估

危險分析可分為三個基本功能：（1）確認危險，（2）確認並評估危險之因果因素，（3）評估風險。

4.危險的確認

危險的確認起始於計畫概念形成的階段，可是危險的清單在整個生命週期中持續地更改。

在計畫的最早期所進行的危險確認稱為「初期危險分析Preliminary Hazard Analysis（PHA）」，它包括：

(1)決定在系統運作期間可能有何危險存在，它們相對的量如何

(2)發展系統設計的準則、規格、和標準

(3)發動控制某個危險的行動

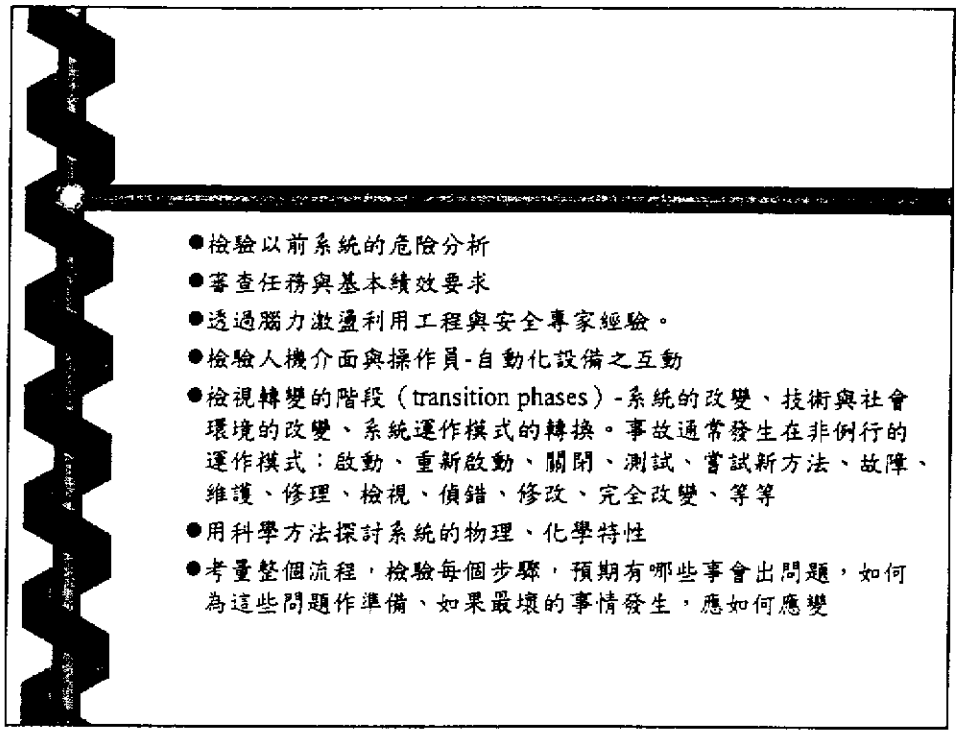
(4)確認行動以及風險承擔（risk acceptance）的管理與技術的責任並確保對危險實施有效的控制

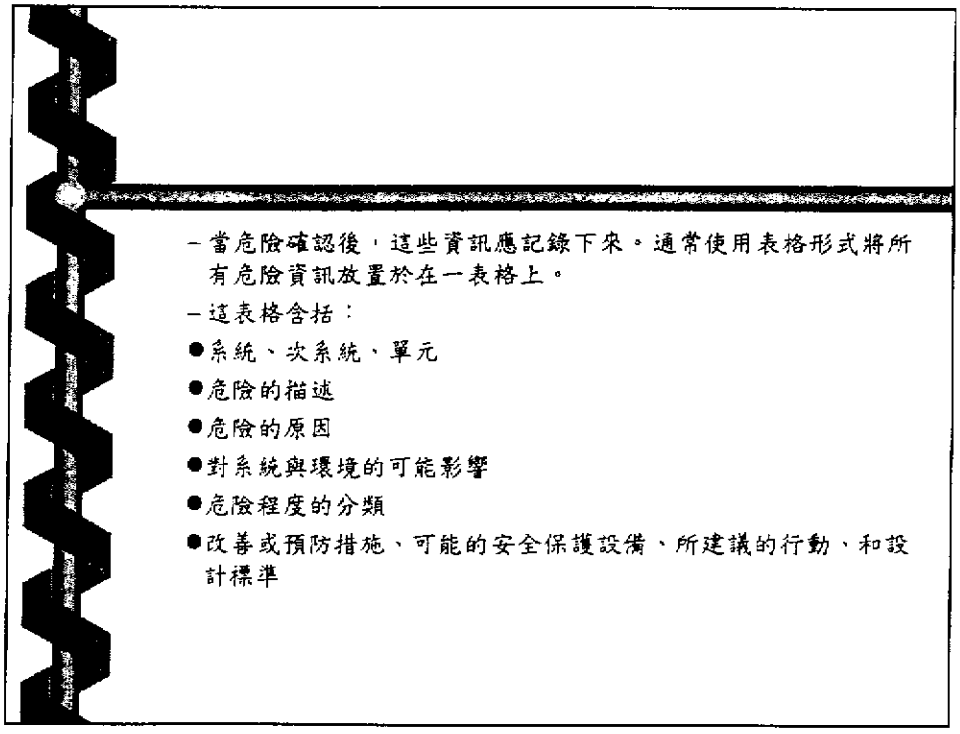
(5)決定安全問題的規模和複雜度（需要多少管理和工程注意力以降低並控制危險）

- 危險確認程序的產出物用以發展系統安全要求、準備績效與設計規格、規畫測試、準備運轉指示、以及管理的規畫。結果可當作日後分析的架構以及確保實施安全作業的管理與技術責任。

- 大多數危險確認的程序包括較低結構化的程序：

- 審查相關的歷史安全經驗、所獲取之教訓、問題報告、事故與事件檔案
- 用已發表的危險系列（hazard lists）與查核表（checklists），探討施行標準與細則。
- 檢驗基本能源來源、能源流程、和高能量項目以及控制的方法
- 考慮危險材料，例如，燃料、發射火藥、雷射、爆炸物、毒物、和壓力系統
- 檢視潛在介面問題，例如，材料不協調、誤觸的可能性、污染、惡劣的環境情節


●檢驗以前系統的危險分析
●審查任務與基本績效要求
●透過腦力激盪利用工程與安全專家經驗。
●檢驗人機介面與操作員-自動化設備之互動
●檢視轉變的階段（transition phases）-系統的改變、技術與社會環境的改變、系統運作模式的轉換。事故通常發生在非例行的運作模式：啟動、重新啟動、關閉、測試、嘗試新方法、故障、維護、修理、檢視、偵錯、修改、完全改變、等等
●用科學方法探討系統的物理、化學特性
●考量整個流程，檢驗每個步驟，預期有哪些事會出問題，如何為這些問題作準備、如果最壞的事情發生，應如何應變


－當危險確認後，這些資訊應記錄下來。通常使用表格形式將所有危險資訊放置於在一表格上。
－這表格含括：
●系統、次系統、單元
●危險的描述
●危險的原因
●對系統與環境的可能影響
●危險程度的分類
●改善或預防措施、可能的安全保護設備、所建議的行動、和設計標準

- 當危險發生時的運轉階段
- 負責確保安全保護設備的組織
- 確認有效控制危險的方法（測試、證明、分析、檢視）
- 其他所建議與需要的行動
- 危險解決過程的狀況與附註

– 危險程度（**hazard level**）

- 危險類別或程度是以可能性和嚴重性來定義並用矩陣的格式來界定以輔助訂定先後順序。由於分析的深度端賴於危險的嚴重性，因此最壞的後果必須及早決定。對危險的敏感度的評估應考慮到暴露的時間與廣度，而且預警的時間也很重要。
- 危險嚴重性的界定因業別而不同：

- MIL-STD-882B
  - Category I：災難；可導致死亡或系統失去
  - Category II：緊要的；可造成重傷、嚴重職業病、或主要的系統損害
  - Category III：邊緣的；可造成次要傷害、次要職業病、或次要系統損害
- NASA
  - Category I：損失生命或車輛
  - Category II：任務失敗
  - Category III：其他

5.危險因果分析

當危險確認之後，必須確定每一危險情境之因果關係。危險原因的資訊可作為制訂安全要求與設計限制之參考。

因果分析可分為系統與次系統：

（1）系統危險分析-將系統視為整體，確認系統如何運作，系統組件間之介面和人機介面如何造成危險。將系統運作分段成一序列的事件與動作。

（2）次系統危險分析-

●檢視每個個別次系統並決定它們的運轉或故障模式對系統危險的影響。這種分析確認出組件故障模式、人們重要的輸入錯誤、與績效、運轉下降、功能故障、非期待的功能、和誤啟動的功能相關之次系統運轉或故障模式。

●報告格式：

◆每一危險之描述

➪系統模式

➪次系統的模式

➪危險的描述

➪危險的影響

➪每一危險的可能性

■每一危險之原因事件

■危險間之互動

■如果有進行量化分析，則應包括：

⇨事件發生速率

⇨事件修理速率

⇨系統時間的限制

■對系統安全之影響評估

■系統危險控制方法之建議

（3）運轉危險分析-此分析在設計完成後才進行。運轉分析檢視運轉員若遵循或不遵循運轉程序，他們可能造成系統危險的所有可能途徑。在分析過程中，運轉程序被分解成階段或作業，進而對於每一階段和作業，分析其動作之順序可能造成的危險。

6.風險評估（risk assessment）與接受（acceptance）分析

●在系統設計開發完成後，整個系統需要評估以確定所剩餘之風險與系統是否可被接受使用。

●接受分析不僅含括危險與事故機率與後果的估計，而且對於每一危險應記錄其潛在的原因、所實施的控制與危險的追蹤、以及確認的結果。接受分析尚含括風險機率評估（probabilistic risk assessment）。此評估分析事故發生的概率與嚴重性以及危險程度。但是風險機率評估的精確度因目前故障和人為疏失數據的不精確度而有所爭議。

II危險分析模型與技術

A.查核表（Checklists）

- 查核表是用以傳承經驗的方法，它可提供回饋給工程過程。查核表是用於已經非常瞭解的系統的設計。這些系統的標準設計特徵（design features）和知識已隨時間經過而日漸成熟。
- 查核表可以引導思考。基本的查核表只是一系列危險或特定設計特徵。其他也可用開放式的問題來刺激思考與詢問。例如，問說「系統會如何保護倖免於EMI」
- 適用階段-可適用於整個生命週期。在危險確認的階段，它可提供有關危險或高風險情境的資訊，幫忙確保危險不至於被忽視。在設計階段，它們確保符合施行的細則與標準。設計的查核表通常用一系列「如果怎樣-會怎樣」的問題。在運轉的階段，查核表可用於定期稽核或確保程序中每一步驟沒被遺忘。從危險分析所獲取的資訊應該用於設計運轉查核表。

- 缺點-

■ 查核表可能讓使用者過度依賴它們而忽略了不含括在表上的項目。另外，查核表可能包含太多的問題而變得很難用或者使用者誤以為所有的問題都已經考慮過。查核表常誘過度的自信；誤以為如果每一項目都符合則系統應該是安全的。再者，查核表無法顯示出危險之相對重要性或不同保護措施之相對有效性C

■ 查核表常未考慮到特定情況是否適用。

B.故障樹分析（Fault Tree Analysis）

- 用於分析危險的原因。故障樹之最上層的事件（top event）必須用其他方法確認出來。FTA用Boolean logic來描述會造成危險事件之個別事件之組合。每一層次列出會造成上一層次問題之基本事件。中間事件（intermediate events）乃「假事件」（pseudo-event），也就是真正事件的抽象化；它是基本或主要事件的組合。如果需要量化（假如所有的基本事件之個別概率是已知的話），top event 的概率也就可以算得出來。
- FTA包括四個步驟：（1）系統界定，（2）故障樹的建構，（3）質化分析，（4）量化分析。

(1)系統界定：必須確定最上層的事件、最初的情境（initial conditions）、現存事件（existing events）、和不容許事件。分析師使用系統功能圖（system functional diagrams）、流程圖（flow diagrams）、邏輯圖（logic diagrams）來分析與界定系統界限。對那些可能有幾個狀態的組件，分析師必須決定分析那個會發生最上層事件的系統狀態。

(2)故障樹的建構：分析師首先假設一特定系統之狀態以及最上一層事件，而後寫下最上一層之原因事件以及用邏輯符號（AND和OR gates）來描述原因事件之間的關係。

AND

OR

NOT- either no X flow or no Y flow

(3)質化分析：目的在於將故障樹削減到一個表達足以造成最上層事件之基本事件的組合，也就是僅將最上層事件與主要事件的關係描述出來。此稱cut set。質化分析的目的就是尋找最少的cut sets，這cut set 代表會造成最上層事件的一些基本事件而且數目不能減少。Cut set定義為如果cut set內之一事件不發生的話，最上一層事件就不會發生。最少的cut sets可以提供資訊以確認出系統的弱點。例如，確定每一事件的重要性及其排序。

(4)量化分析：用最少的cut sets由基本事件發生的概率來計算最上層事件之概率。如果所有cut sets在統計上是獨立的，也就是說，同一事件不出現在兩個或以上的cut sets時，最上層事件之概率是所有cut set概率之總和。

●FTA需要在系統設計完成後，對其所有運轉模式行為有透徹的瞭解時，最有效用。FTA也可應用到以完成或現有的系統以證明此系統是安全的。

●用處：

■圖形的格式可以將事件的關係顯示出來並且幫忙瞭解系統、偵測問題。

■可幫忙分析師確認會導致危險的情節並可建議消除或控制危險的可能性。

■對於某個特定的事件，知道最少的cut set 可以讓分析師對系統的潛在弱點有所瞭解。

C.管理疏忽與風險樹分析（Management Oversight and Risk Tree Analysis）

- 基本上，MORT是一個標準的故障樹再加上管理功能、人們行為、和環境因素的分析。旨在確認出因規畫不善、操作檢查不妥、或組織內資訊交換有限而創造危險或使危險無法早期發現的問題、缺陷、和失察。
- 此方法使用1,500件基本事件或因素的檢查表以幫助發現安全問題。

D.事件樹分析（Event Tree Analysis）

- 事件樹分析是利用決策樹技術，將問題分為較小的部份。它利用往前尋找（forward search）的方法確定最初事件（例如，管線破裂）之後發生的所有系列事件以確認出各種可能之後果。這種最初事件可能是系統組件的故障或其他的外在事件。
- 事件樹由左到右，每個分支對應到兩個方案：（1）防護系統的成功（上支），（2）防護系統的失敗（下支）。等到事件樹畫好之後，可以選擇每一個接續的標題下之分支來追蹤所有的途徑（path）（每一途徑對應至一個事故的序列）。
- 一個途徑的整體概率乃是各個分支概率相乘之結果，而事故之整體風險是所有導致事故之途徑的概率的組合。
- 此分析方法適用於當大多的設計以完成後，因此它用於評估現有設計。

E.原因-後果分析（Cause-Consequence Analysis）

●原因-後果分析由一個緊急事件（critical event）開始，決定此事件之原因和後果。原因-後果圖顯示出時間上的依賴性與事件間之因果關係。

●分析的程序起始於選擇一個緊要事件，而後尋找構成這個事件之因素，再確認出此事件延續之潛在影響。最後，這些因素的關係用圖形來描述。

●好幾個「原因表」可連接至一個「後果表」。「原因表」描述會導致緊要事件之不同的前置事件順序以及這些順序會發生的情境。

●符號：

■gate-描述原因事件間之關係；

■vertices-描述後果間之關係。

F.危險和操作性分析（Hazards and Operability Analysis）

●此技術不僅著重在安全，而且也在有效率的運作。它是基於事故之系統模型，假設事故是因偏離了設計或運轉的原意而發生的。因此，它確認出所有可能偏離設計所期待之運作以及和這些偏離有關之危險。

●利用新系統的描述，分析團隊（由不同系統方面之專家組成）會考慮：

■系統設計的原意

■偏離原意的潛在點

■偏離之原因

■偏離之後果

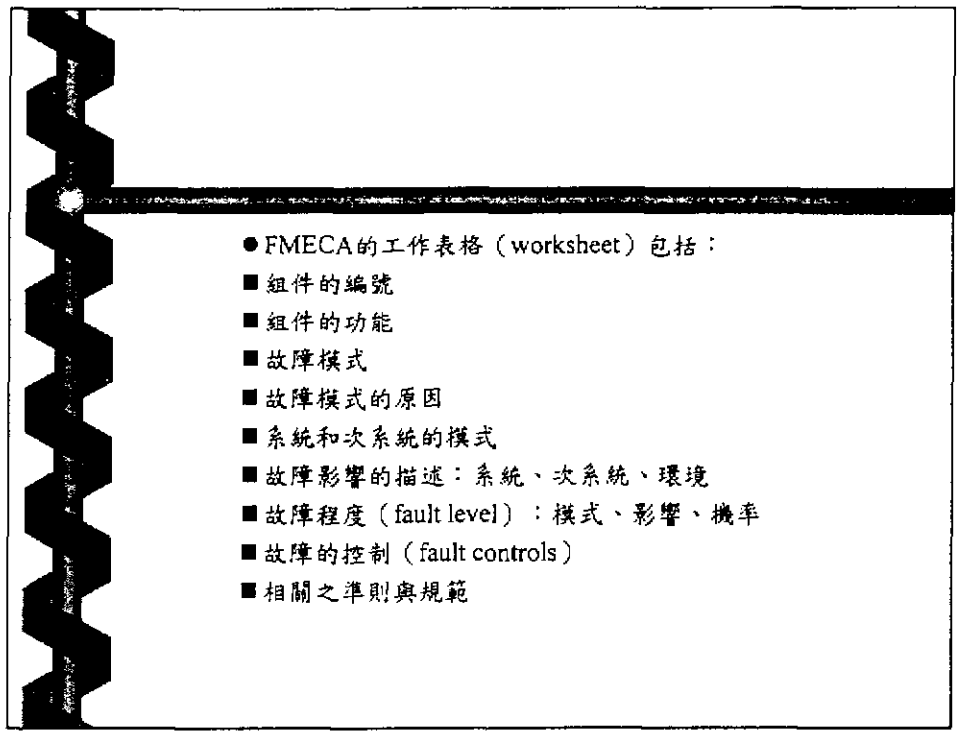
G.故障模式與效果分析（Failure Modes and Effects Analysis）

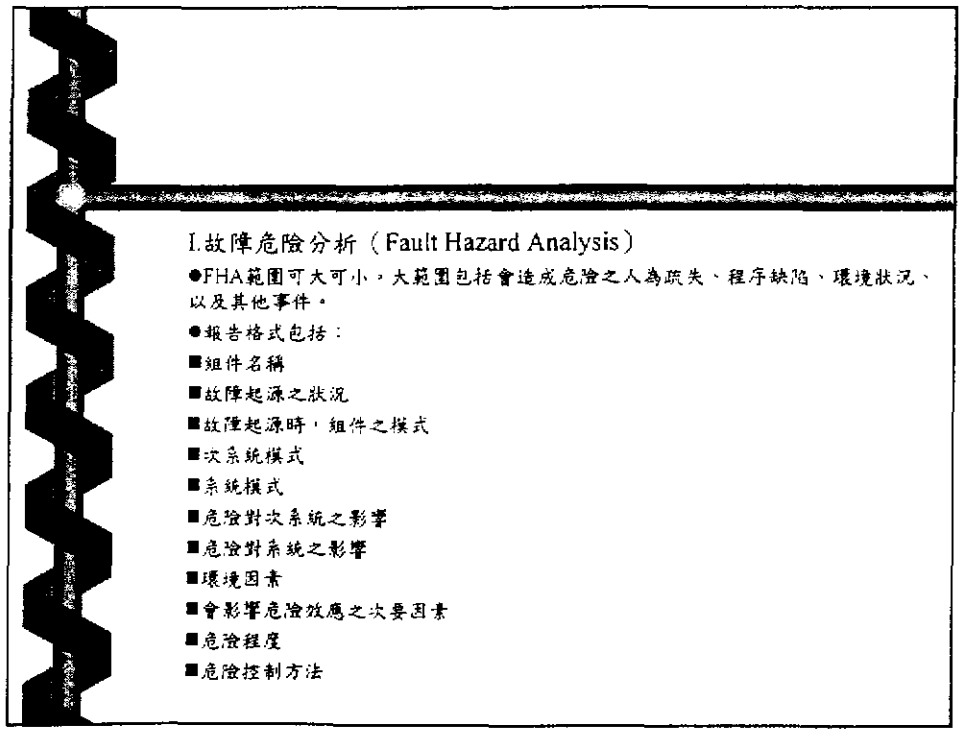
●分析首先將所有組件確認出來並將之表列，而後考慮其所有之運轉模式可能之故障模式。對於每一故障模式，確認出對其他所有之系統組件的影響以及對整個系統之影響。然後，計算每一故障模式結果之嚴重性以及概率。

●分析的結果用表格方式依序分列來記錄：組件、故障概率、故障模式、每一模式有%故障、和影響（緊要和非緊要）。

H.故障模式、效果、和緊要性分析（Failure Modes, Effect, and Criticality Analysis）

- FMECA是FMEA再加上緊要性分析。因此多了兩個步驟：（1）控制的方法，（2）控制程序會產生之改變。
- 緊要性的排序是以概率或頻率來表達。也可以用1到10來表示產生問題的主要項目。另外，提供需要採取之預防與改善方法以及保護設備。


●FMECA的工作表格（worksheet）包括：
■組件的編號
■組件的功能
■故障模式
■故障模式的原因
■系統和次系統的模式
■故障影響的描述：系統、次系統、環境
■故障程度（fault level）：模式、影響、機率
■故障的控制（fault controls）
■相關之準則與規範


I.故障危險分析（Fault Hazard Analysis）
●FHA範圍可大可小，大範圍包括會造成危險之人為疏失、程序缺陷、環境狀況、以及其他事件。
●報告格式包括：
■組件名稱
■故障起源之狀況
■故障起源時，組件之模式
■次系統模式
■系統模式
■危險對次系統之影響
■危險對系統之影響
■環境因素
■會影響危險效應之次要因素
■危險程度
■危險控制方法

第四單元

人員作業疏失本質與基本觀念

❁人為疏失的本質

● 人為疏失的定義：

－人為疏失的表徵

- ■未能達到預期的系統目標或標準的作業結果
- ■偏離作業者所預期的
- ■通常會帶來負面的後果

●一般對於人為疏失的看法

2. 凡是人都會犯錯

» 人犯錯是無法避免的，無法防患於未然，因此：
(1)由機器來取代人的作業—自動化
(2)若機器無法取代人的作業，就交由上帝

-2. 人為疏失乃因人謀不臧，管理不善所引起的。

■人謀不臧乃由於人員素質不良、動機不善、過度自信、精神渙散、不小心或投機取巧

■管理不善乃由於紀律鬆懈，監督不週。

-因此，加強監督管理與訓練，處罰當事者成為矯治人為疏失的主要補救措施。

事實上，由事故分析發現：

- 1.大多數的事故是由一連串小疏失衍生而成。
  - —錯誤鍊(Error Chain)

2.大多數的疏失是當事者觸發系統的潛在問題而產生的。

這些系統的潛在問題乃是系統元素間(亦即，人員、硬體、軟體、作業)以及它們與環境的不協調

疏失V.S.違規

●疏失：

◇執行上的失敗

◇規畫上的失敗

－→大多是無意的

－→由資訊的問題引起（例如，遺忘、不注意、知識不完整），可由改善工作場所中所需資訊的品質與傳遞來降低疏失。

● 違規：

✈偏離安全作業程序、標準、或規則。

✈這種偏離大多是蓄意的。

✈通常有動機的問題（例如，士氣低、監督差、不關心、賞罰不明），因此解決的方式需要動機的激勵與組織的改造。

● 疏失與正確行為是一體兩面

● Constant Error vs. Variable Error

－人為疏失的類型

1.Swain and Guttman

（1）Omission (忽略)

－-整個作業或作業中的步驟

（2）Commission (做錯)

» -選擇錯誤、順序錯誤、時機錯誤、

» 動作量或質上的錯誤

– 2.Norman

– 人的行為歷程是：

– 意向→動作→評估結果

– 人為疏失的類型有：

- Mistakes(錯誤)
- 疏忽(Slips)和遺忘(Lapses)

3.Rouse

– 監控作業歷程：

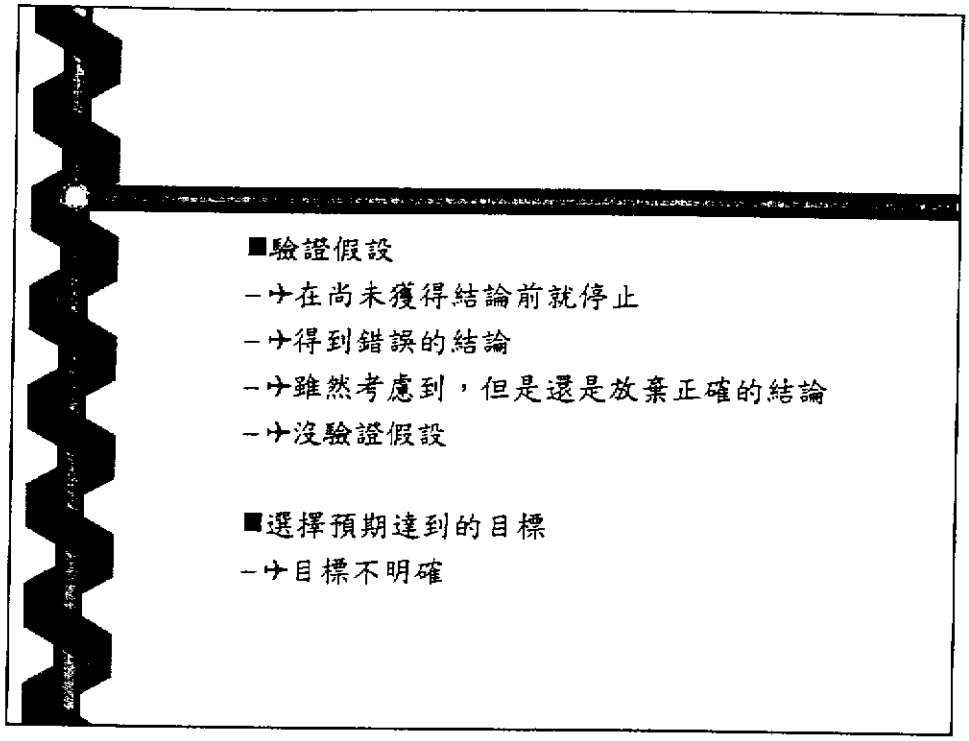
- 觀察系統狀態
- 選擇造成目前狀態原因的假設
- 驗證假設
- 選擇預期達到的目標
- 選擇因應作業程序
- 執行作業程序

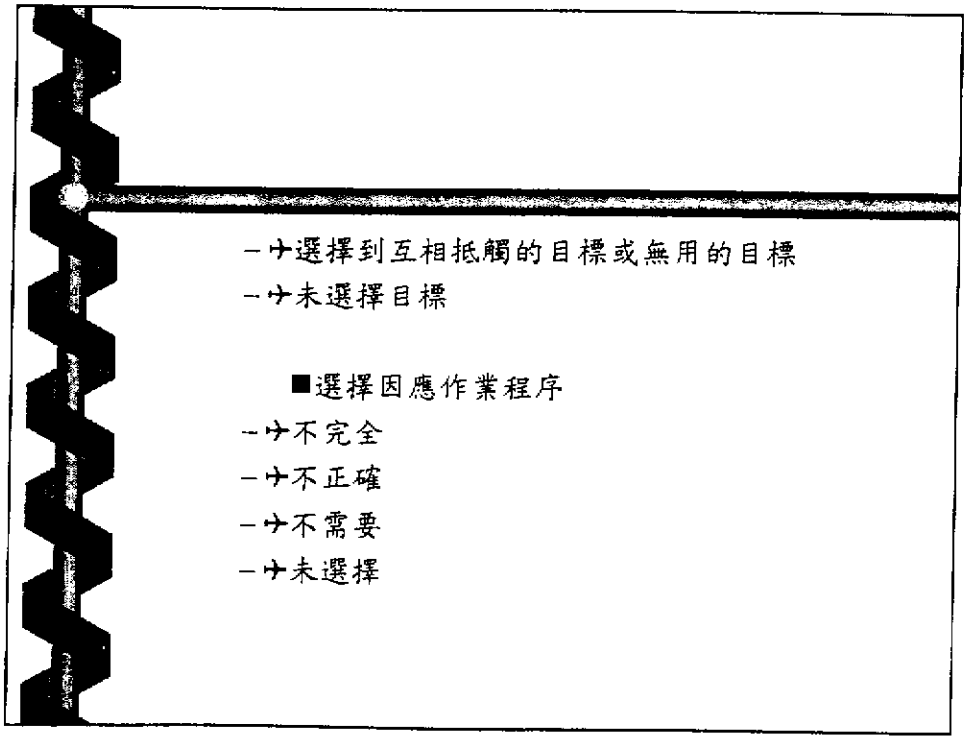
■觀察系統狀態

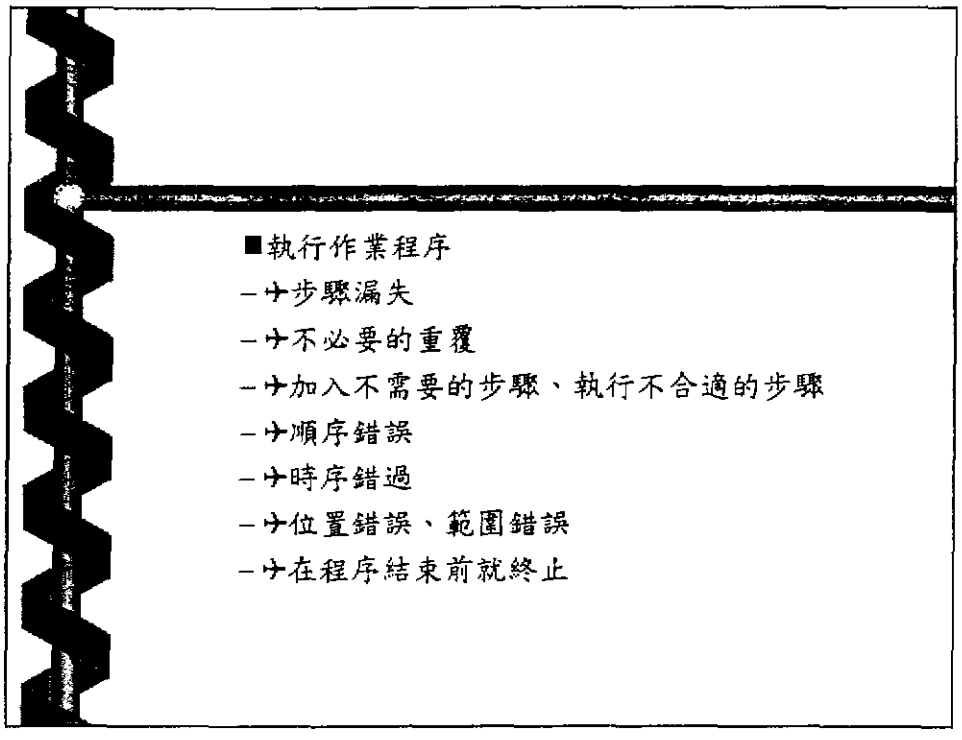
- 讀取資訊時未適當的覆檢
- 資訊解釋錯誤
- 沒有觀察足夠的變數
- 觀察不合適的狀態變數
- 沒有觀察任何變數

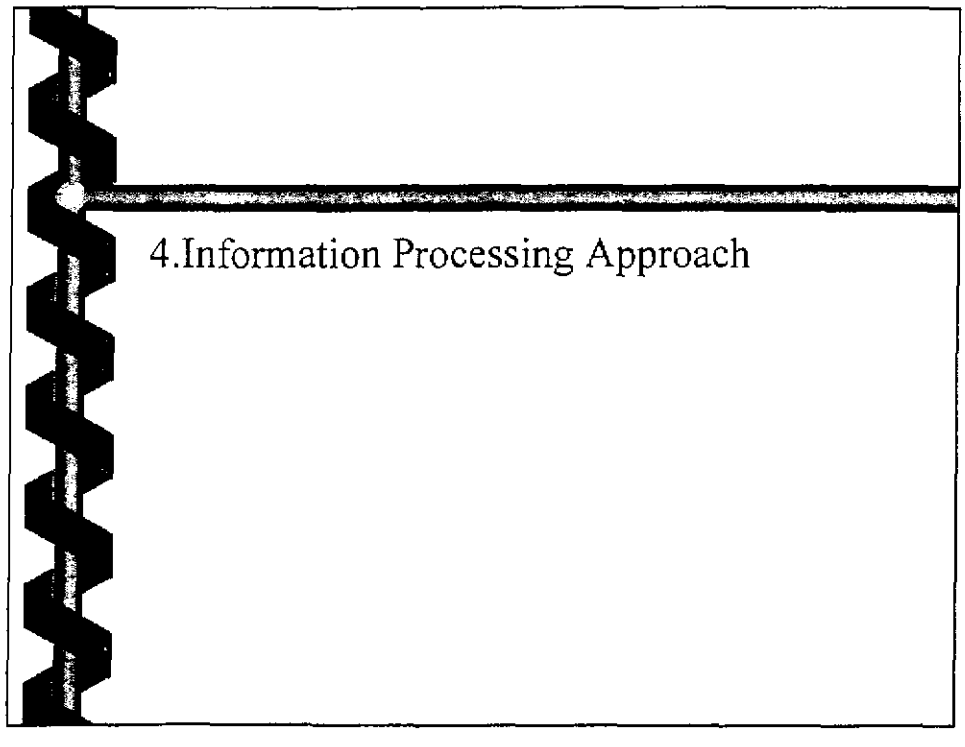
■選擇造成目前狀態原因的假設

- 假設並不能造成如此的狀態
- 應優先考慮最可能的原因
- 考慮的出發點費力過高
- 考量的假設與目前所觀察到的變數在功能上無關


■驗證假設
－→在尚未獲得結論前就停止
－→得到錯誤的結論
－→雖然考慮到，但是還是放棄正確的結論
－→沒驗證假設
■選擇預期達到的目標
－→目標不明確


－→選擇到互相抵觸的目標或無用的目標
－→未選擇目標
■選擇因應作業程序
－→不完全
－→不正確
－→不需要
－→未選擇


■執行作業程序
－→步驟漏失
－→不必要的重覆
－→加入不需要的步驟、執行不合適的步驟
－→順序錯誤
－→時序錯過
－→位置錯誤、範圍錯誤
－→在程序結束前就終止


4.Information Processing Approach

5.Rasmussen的作業行為層次

依作業的純熟度與情境的熟悉度分為：

- 技能基礎(Skill-based)
- 規則基礎(Rule-based)
- 知識基礎(Knowledge-based)

技能基礎(Skill-based)

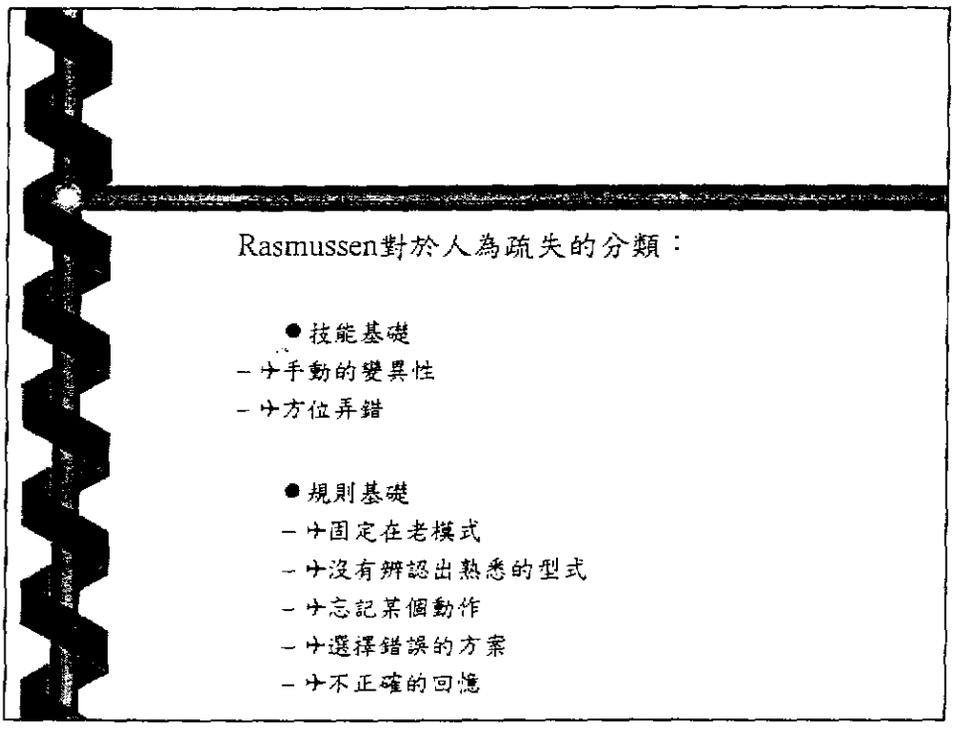
通常用無意識的方式來執行例行且高度熟悉的作業，僅偶而有意識地檢查其進度而已

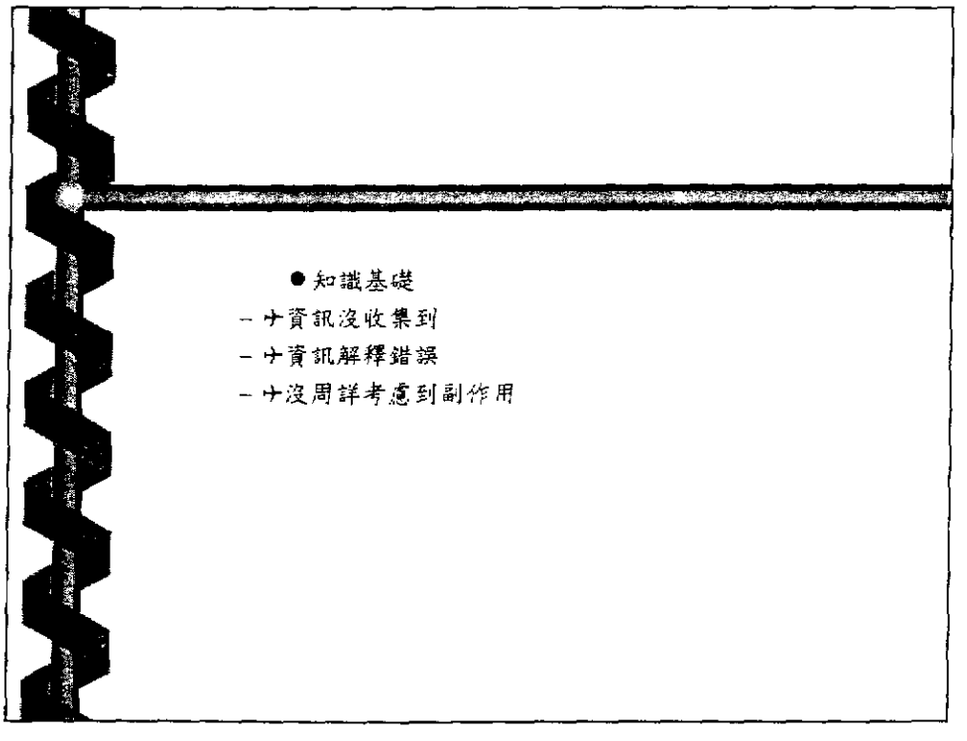
規則基礎(Rule-based)

- 遇到以前碰過的問題，而且已有解決方案
- 引用先前儲存的法則：
  如果（這個狀況）則（進行這些動作）
- 無意識地作pattern-matching
  Sign↔Symptoms
- 用意識思考來檢查此解決方案是否合適

知識基礎(Knowledge-based)

- 遇到不熟悉的狀況，無法用已知的方法來解決，必須訴諸於緩慢、費神、容易出錯的思考以找出適當的解決方案。


Rasmussen對於人為疏失的分類：
● 技能基礎
– 十手動的變異性
– 十方位弄錯
● 規則基礎
– 十固定在老模式
– 十沒有辨認出熟悉的型式
– 十忘記某個動作
– 十選擇錯誤的方案
– 十不正確的回憶

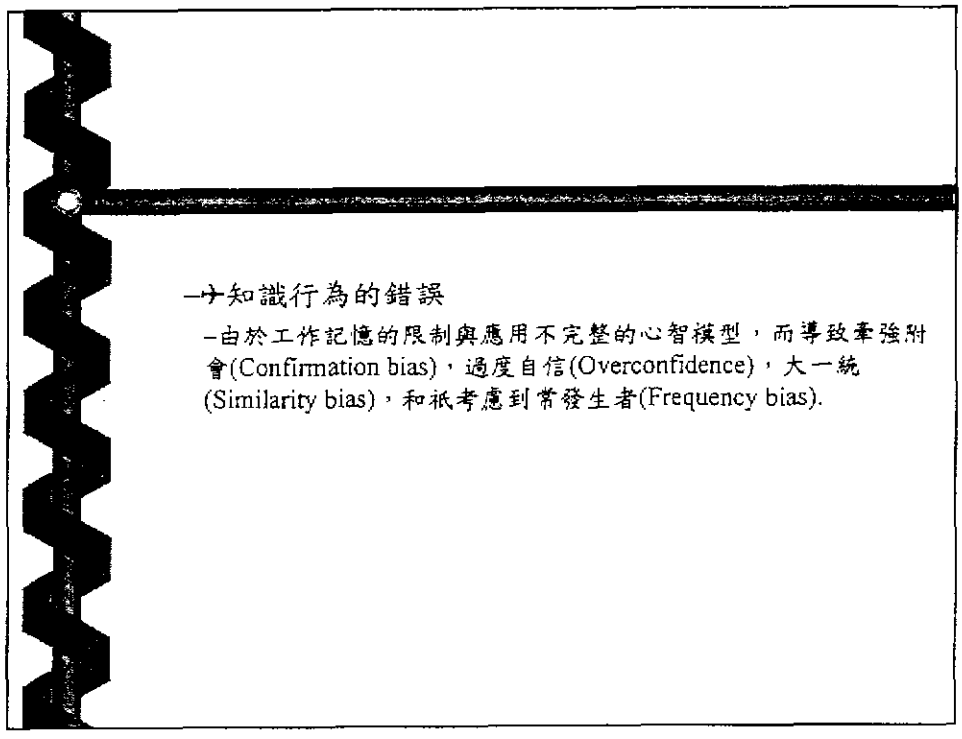

● 知識基礎
– 十資訊沒收集到
– 十資訊解釋錯誤
– 十沒周詳考慮到副作用

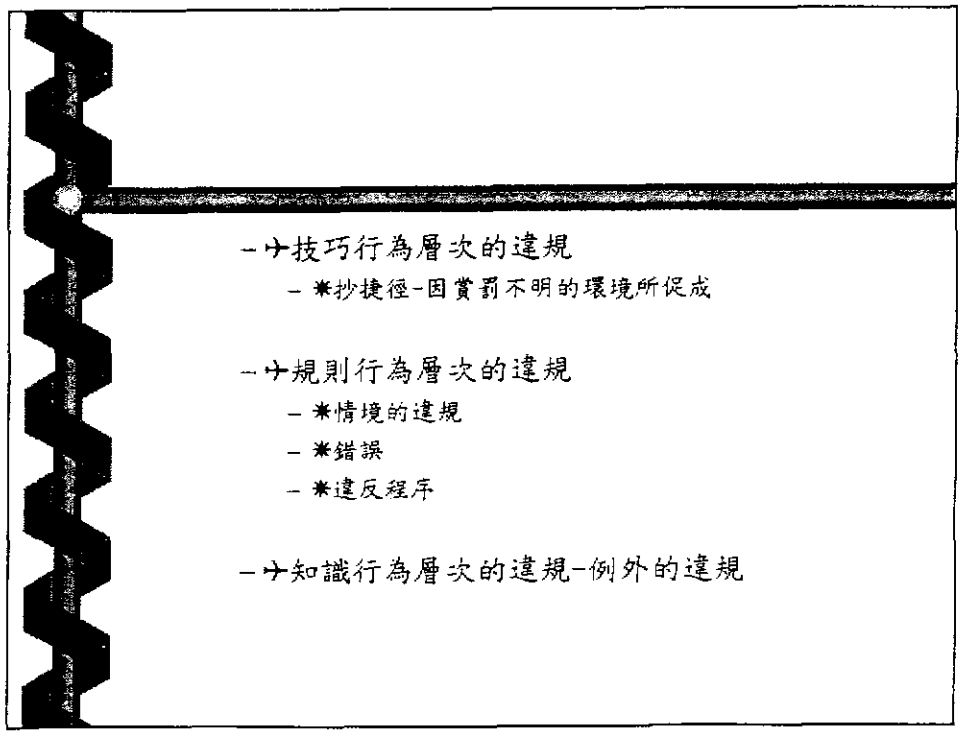
6.Reason的Generic Error-Modeling System

- Active Failures vs. Latent Failures
  - 1.從發生失敗到顯現出後果的時間
  - Active failure-立即直接影響
  - Latent failure-蟄伏一段期間
  - 2.造成失敗的人
  - Active failure-與系統直接接觸的人
- Latent failure-管理階層

Active Failures

- ✈技巧行為的疏忽(或遺忘)
  - ✱注意力疏忽(Attention slips)
  - ✱記憶遺忘
  - ✱知覺錯誤
- ✈規則行為的錯誤
  - ✱錯用了好的規則
  - ✱應用了壞的規則


–知識行為的錯誤
–由於工作記憶的限制與應用不完整的心智模型，而導致牽強附會(Confirmation bias)，過度自信(Overconfidence)，大一統(Similarity bias)，和祇考慮到常發生者(Frequency bias).


–技巧行為層次的違規
– *抄捷徑-因賞罰不明的環境所促成
–規則行為層次的違規
– *情境的違規
– *錯誤
– *違反程序
–知識行為層次的違規-例外的違規

人為疏失發生的機制

- Accident-Proneness Theory
- Job Demand V.S. Worker Capability theory
- Rasmussen的不協和論
- Reason的病原論

第五單元

促成人為疏失的因素

疏失發生的情境：當作業的要求超過個人的能力或工作的情境使得人類的特性問題加劇

- 疏失的近因
  - 作業的要求（Task Demands）
  - 工作的環境（Work Environment）
  - 個人的能力（Individual Capabilities）
  - 人類的特性（Human Nature）
- 疏失的遠因
  - 組織的弱點（Organizational weaknesses）-制度、程序、溝通、文化

第六單元

人為疏失的防治

I.疏失的偵測

技能基礎的錯誤

⊙自我監督或依賴回饋資訊來作控制

用知覺分析和回饋檢查來偵測疏失。疏忽和遺忘比錯誤可能偵測得到，但是有些疏失（如遺漏步驟）就很難偵測

⊙他人發現

-此法對於診斷錯誤與作業人員在壓力之下特別有效

⊙ 系統對疏失的反應

- 十牽制：避免使用者表達不能實現的意圖
- 十警告
- 十不作任何事：對不合理的輸入不反應
- 十自我更正：就照我的意思作
- 十讓我們談一下
- 十教教我：系統要求使用者教它

- 利用forcing function
  - 所謂「forcing function」就是除非疏失已被更正，否則會避免動作能夠持續進行的設計。它是用以避免某些技能基礎疏失發生的標準作法。例如，螺絲只能符合一邊，如此螺絲才不會裝錯。當疏失的後果會嚴重的話，就有理由去設置forcing function。

--規則基礎的錯誤

■誤用好的規則

■應用壞的規則

➢定期有系統地審查程序書-

» 但是如果一個複雜系統擁有非常多的法則與程序且這些程序時常更改的話，此法工作量浩大。因此必須先確定問題的嚴重程度，以決定是否需要審查法則與程序。

II.減少個人疏失

■疏忽與遺忘

➢改善設計-

» 增加控制器的分辨性；避免多重控制模式；改善控制器的安排；改善設計使得疏失可以立即更正；將一些不適合人員的作業自動化

➢訓練-

» 改善作業的經驗；練習以維持純熟度

➢工作設計與作業方法-

» 將人工作業簡單化與標準化；如果遭到分心或干擾，在恢復作業前應重新檢驗前兩三步驟；

➢監督與管理-

»改善規畫以避免分心或干擾；透過妥善安排工作時程以消除不必要之時間壓力；加強監督或由同伴檢查重要之步驟；輪換工作；推廣互相檢查和挑戰的價值觀

■減少規則基礎錯誤

➢訓練-

– 中加強訓練直至熟練到技術基礎；增進程序知識；練、習使用多重、不同的跡象；練習將意向說出來；練習在不同程序間作轉換；特定的重要安全作業專業化

➢設計-

– 中資訊重複，清楚的標示，顏色加碼；增加forcing function

➢程序書-

» 中清楚地描述程序中重要的決策點；簡化程序並避免程序間的不一致性；消除程序書上的錯誤

➢工作方法-

– 中避免不智的使用經驗法則

■減少知識基礎錯誤

➢訓練-

– 中加強問題解決方法的練習；危險察覺（hazard awareness）課程；團隊作業與溝通練習；發展平行思考能力；發展正確的心智模型

➢設計-

– 中提供不同層次的資訊

➢監督與工作計畫的檢查

➢工作方法-

– 中應用系統與組件的知識和物理的基本原則於不熟悉的問題情境

■減少違規

➢動機

➢風險評估，風險知覺與益處間之平衡

➢監督，團體行為的常模，管理階層的承諾

-工作場所降低人為疏失的方法

1.狀況察覺：維持警覺性以期待可能會觸發疏失的情境和有瑕疵的防禦設施。所用的行為包括：

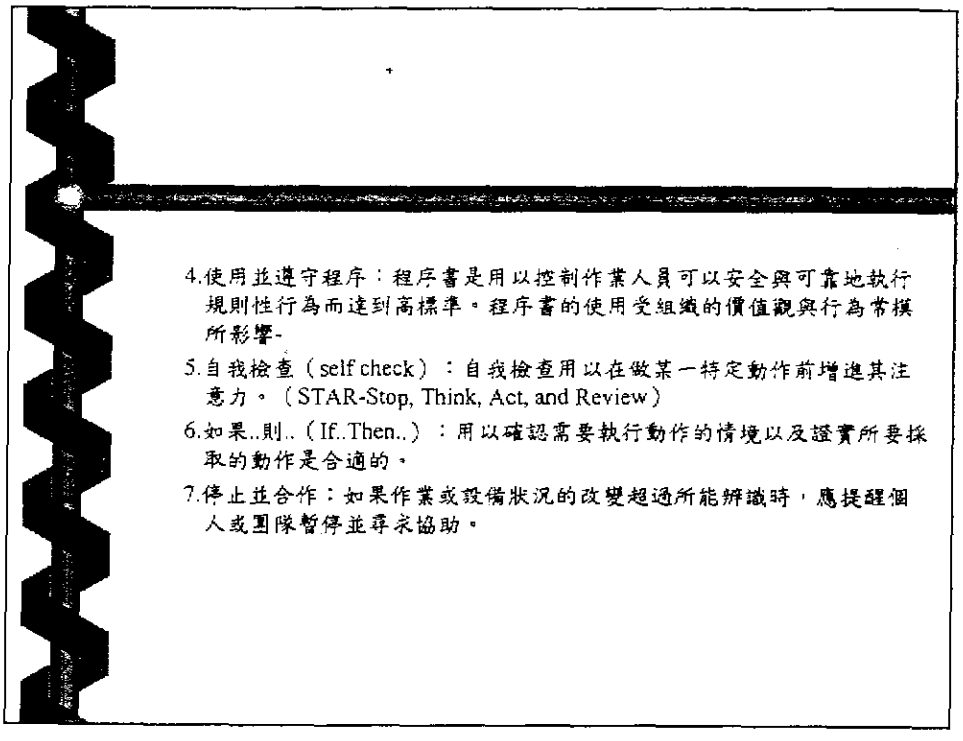
»+監督（monitor）-經常掃描所進行的作業、環境、自己和同伴的狀況以辨認出不良的情境

»+解釋-期待可能會觸發疏失的情境和有瑕疵的防禦並決定如何改變工作的情境與應變措施

»+干預-執行所需要之改變以避免觸發疏失的情境和有瑕疵的防禦

2.溝通三部曲：發訊息者發出訊息，接收者確認收到訊息，發訊息者確認接收者所收到訊息是正確的。

3.暫停（time out）：暫停可讓工作同伴獲取有關工作情境更準確的資訊。它包括將工作暫停以討論工作特定的情境，這樣做，可以讓工作人員依據真正的資料對於工作、環境、與個別狀況有共通的瞭解。

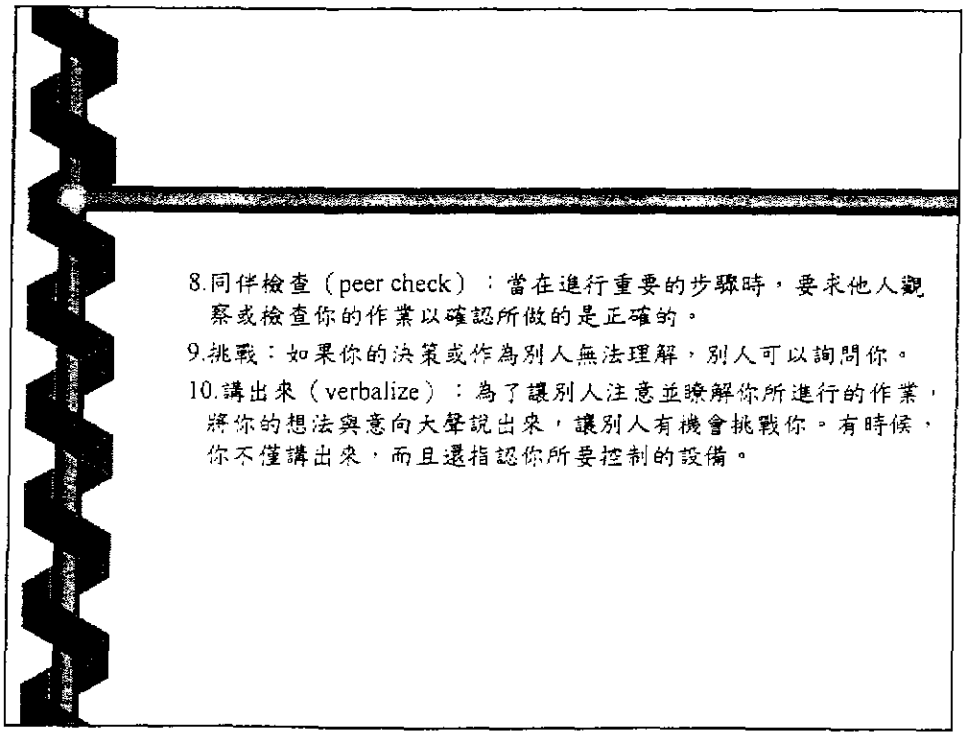


4.使用並遵守程序：程序書是用以控制作業人員可以安全與可靠地執行規則性行為而達到高標準。程序書的使用受組織的價值觀與行為常模所影響-

5.自我檢查（self check）：自我檢查用以在做某一特定動作前增進其注意力。（STAR-Stop, Think, Act, and Review）

6.如果..則..（If..Then..）：用以確認需要執行動作的情境以及證實所要採取的動作是合適的。

7.停止並合作：如果作業或設備狀況的改變超過所能辨識時，應提醒個人或團隊暫停並尋求協助。



8.同伴檢查（peer check）：當在進行重要的步驟時，要求他人觀察或檢查你的作業以確認所做的是正確的。

9.挑戰：如果你的決策或作為別人無法理解，別人可以詢問你。

10.講出來（verbalize）：為了讓別人注意並瞭解你所進行的作業，將你的想法與意向大聲說出來，讓別人有機會挑戰你。有時候，你不僅講出來，而且還指認你所要控制的設備。

－組織內確認與控制疏失的方法

1.建立「持續改善」的文化：不滿於現狀。持續確認出組織內潛在的弱點。

2.設置一個事件報告系統，匯集固定期間內所有的事件，對事件進行肇因分析

»❑運轉經驗研討會：利用內部與業界運轉的經驗和教訓，讓組織能夠改善。這個研討不僅討論事件發生的經過，並討論可能發生疏失的情境及其原因。用於確認疏失的原因和相關的組織弱點。研討著重於如何防治此事件的發生。

3.召集組織內所有層級的人員參與進行問題解決的活動，著重安全文化的提昇-建立共同的願景與目標，推動有效的溝通

－❑人員績效會議：定期討論有關人員作業績效議題，由經理、監督者、工作人員參加，並且推廣開放的溝通和合作。對話的議題可包括：（1）工作後的檢討，

»（2）不合理的作業要求與標準，

»（3）所受的訓練不足以增進個人能力，

»（4）工作環境、行為常模、流程的瑕疵、防禦的瑕疵，

»（5）會逾越人們極限的工作情境

－❑報告卡（Report cards）：讓工作人員將工作場合中一些不良的狀況（如：標示品質、燈光、噪音、程序書不當）報告上級。

4.自我評估：找尋優勢與改善之空間。

5.訓練：訓練線上工作人員、領班、經理能夠認識會發生疏失的狀況、如何消除或降低疏失。訓練的技術包括利用模擬機經歷這些情境與有瑕疵的防禦，或利用on-the-job training讓他們有機會去偵測並改善這些潛在狀況。

6.管理階層持續監督與控制所產生的改變，因此組織對安全議題會發展出正面效應。管理階層對於安全的承諾會透過決策的過程而發酵。

7.Benchmarking：與其他業者相比較，確認出好的作法，發覺出創新的思考或方法。有效的benchmarking方法包括：

- 在作benchmarking前應充分瞭解所要比較的過程
- 決定benchmark的測量方法
- 選擇要benchmark的對象，收集與分析資料
- 確認出間距與好的作法
- 將結果報告主要的成員
- 評估並施行改善

8.文化調查：問卷著重於組織成功的要素或重要的行為。調查在這些方面的表現以及該改進的地方。

設置安全作業改善計畫的步驟：

（1）創置事件與事故之人因資料庫

（2）定期重估作業人員的績效

（3）改善資訊顯示以提供清楚的跡象

（4）在團隊作業時，知覺到互動過程中增加風險的因素（如，傾向風險、團隊思考偏差）

第七單元

安全管理

I.安全管理系統

– 所謂「安全管理系統」就是組織透過管理過程來控制風險。

– 三種建立安全管理系統的方法：

- 系統方法
- 著重於安全文化與態度
- 安全稽查-是一種實施方法

– 這三種方法將人與風險管理面結合在一起，強調：

- 管理階層承諾的重要性
- 設定清楚的安全目標
- 妥當地溝通所需要的資訊

–系統方法

– 系統含括：

- 結構的元素-主要崗位、報告的關係、委員會與其他團體、安全文件。
- 過程-動作、問題解決、資訊的提供與溝通
- 連結點-回饋迴路
- 外在影響-政府、立法機關、經濟、科技、改變的速度、與公眾意見
- 次系統-控制（決策、政策、策略規畫），監督，執行（運轉、維護），溝通

- 因此，安全管理有以下六個元素：政策、組織、規畫與執行、測量績效、審查績效、與稽查。這些元素由員工的參與、持續的改善、資源的提供、與風險控制等過程來支援。元素間靠回饋迴路來連結。

- 一個有效的安全管理系統需要有功能面（包括管理控制、監督、執行、與溝通）與人性面（領導力、政治與安全文化等次系統）。

II.安全管理績效的測量-安全稽查

-至少有六種安全稽查：

1.對特定的議題（如人為因素、危險物質、或環境）稽查

2.工廠技術稽查（plant technical audit）-深度審查所有工廠和技術人員所執行的過程

3.定點技術稽查（site technical audit）-定期檢驗所有特定的工作

4.確認稽查（compliance audit or verification audit）-用於檢驗這個組織是否符合安全的要求

5.有效性稽查（validation audit）-著重於檢驗是否採納了正確的次系統和組件，是否進行正確的監督，是否設置了合適的次系統

6.管理安全稽查（management safety audit）-每年進行一次，包含一般安全議題

安全稽查之原則

- 採取正面態度，而非一心想找錯誤
- 確認出偏離準則點
- 促進對造成偏離的事件分析
- 強調好的實施方法
- 要有專業態度、公正、與客觀
- 將稽查整合入安全與風險管理系統
- 盡量客觀、準確地評估一個管理功能
- 提供一個風險狀態的測量方法
- 指認出重要區域的優缺點
- 提供一個清楚改善的準則
- 成為一個監督改善的方法

發展安全稽查的階段：

1.訪問與熟悉所要稽查的場地
2.設計問卷
3.稽查安全的前提基準與活動
4.確認回答與稽查的分數
5.分析結果
6.確定問題點
7.準備並遞交報告
8.執行建議事項
9.監督改善過程

其他技術：

●行為抽樣（Behavior Sampling）

»適用於評估例行的低風險、高可能性的作業。它用以確定在工作場所之不安全行為。需要在隨意的時機對行為作一連串的觀察。需要至少一個觀察員進行觀察。觀察員要熟悉所要觀察的行為。工作人員在觀察時不改變其行為。每次觀察要區分出安全與不安全行為。抽樣的樣本需要至少600次。計算出不安全行為的百分比。

●工作場所的檢視（Workplace Inspections）

– 用於評估不安全行為的程度與結果。檢視範圍不僅包括工作場所，還包括：工作方法、工作環境、與員工的設施。檢視需要相當的知識與技能，不可盲目的仰賴查核表。

» 檢視的類型有：

- 正式的檢視-每年一次，最詳細；用於確認所有的安全狀態
- 重複檢視-用於監督在偵測出特定危險後的改進成效
- 找出危險-每日調查以評估工作場所風險
- 對特定事件的檢視-用於收集特定事件的資訊

執行原則：

- 必須作觀察，不僅是看而已
- 深入檢驗每個細節
- 花時間慢慢檢視
- 要有耐心與小心
- 問兩個主要問題：什麼出了錯、為何出錯
- 問「如果這些事發生，會導致什麼後果？」

III.風險管理

1.建立安全態度
2.進行保守決策

第八單元

作業安全行為稽查系統

I.作業行為模式

計畫->執行->評估->修正

II. 作業行為認知歷程

知覺->思考/決策->動作->回饋

III. 安全行為作法

- 維持狀況察覺
- 有效溝通與討論
- 使用與遵循程序書
- 自我查證
- 同僚互檢
- 驗證與模擬作業法則
- 說出思考與動作過程，讓同僚知道

IV. 作業分析

- 將作業分解至行為單元步驟
- 審查進行此步驟所需之資訊與控制需求、作業的要求（速度、精確度、負荷等等）、知識與技能需求，以確認出訓練、人機介面設計、作業設計之合理性。
- 檢視作業情境，以確認出影響作業的情境因素

V. 安全行為稽查系統

依包商作業階段，分下列幾個單元：

- 包商報到
- 作業前計畫
- 作業執行
- 作業完成
- 作業後評估
- 改善提案與安全資訊的管理

A.包商作業人員報到

1.是否具備作業相關知識與技能？
2.是否瞭解工作內容？
3.是否瞭解相關之安全規定與準則？
4.此作業與非核電廠相同之作業是否有差異點？
這些差異點何在？對安全有何影響？

B.作業前之規畫

1.作業計畫是否可行？
- ■作業時間是否有足夠？
- ■人力是否符合作業需求？
- ■分工作業負荷是否合理？

2.本作業是否會影響機組安全與工安？若會，計畫有評估其風險並演練過？

3.本作業與其他作業、其他部門、或系統設備有無關聯？

- ■若有關聯，在進行何步驟前需要與其他人員與部門作溝通、協調？
- ■溝通、協調需要用何種方式？
- ■如何確認溝通、協調對方已獲得訊息且完成相關應對作業？

4.本作業有那些設備管路禁止操作、攀登、踐踏或掛掉？

5.本作業需要那些工具設備？

- ■這些工具是否備妥？是否符合安全規範？
- ■工具應如何正確使用？

6.作業前之簡報是否進行？每位作業人員是否瞭解其任務要求、作業內容、每一步驟的細部動作與關鍵安全步驟、以及安全規定？

- ■在進行每一步驟時需要那些資訊？這些資訊如何獲取？
- ■在進行每一步驟時需要操作那些控制器或工具？如何進行操作？如何確認操作動作的完成？
- ■關鍵安全作業步驟是否瞭解？是否模擬演練並標明於程序書上？

7.作業過程中有那些停留查證點？是否在施工前有通知品管人員查證？

8.本作業之作業環境與作業本身是否容易引起人為疏失？

- ■這些疏失在進行那些步驟時會發生？（應將這些作業點標明為檢查點）
- ■那些疏失會牽涉那些潛在危害（hazards）？

9.那些動作和情況會觸發這些危害的發生？

10.這些危害的發生應如何辨識、偵測與控制？

- ■發生時，應如何及時將狀況向廠方報告？向誰報告？

11.危害相關之防護器具是否攜帶並知道如何使用？

12.危害發生應如何應變？

- ■應變時，應如何及時將狀況報告？向誰報告？
- ■應變程序書是否熟悉並且攜帶？應變程序是否演練過？
- ■是否知道如何將危害侷限於局部？
- ■是否知道緊急疏散程序與路線？

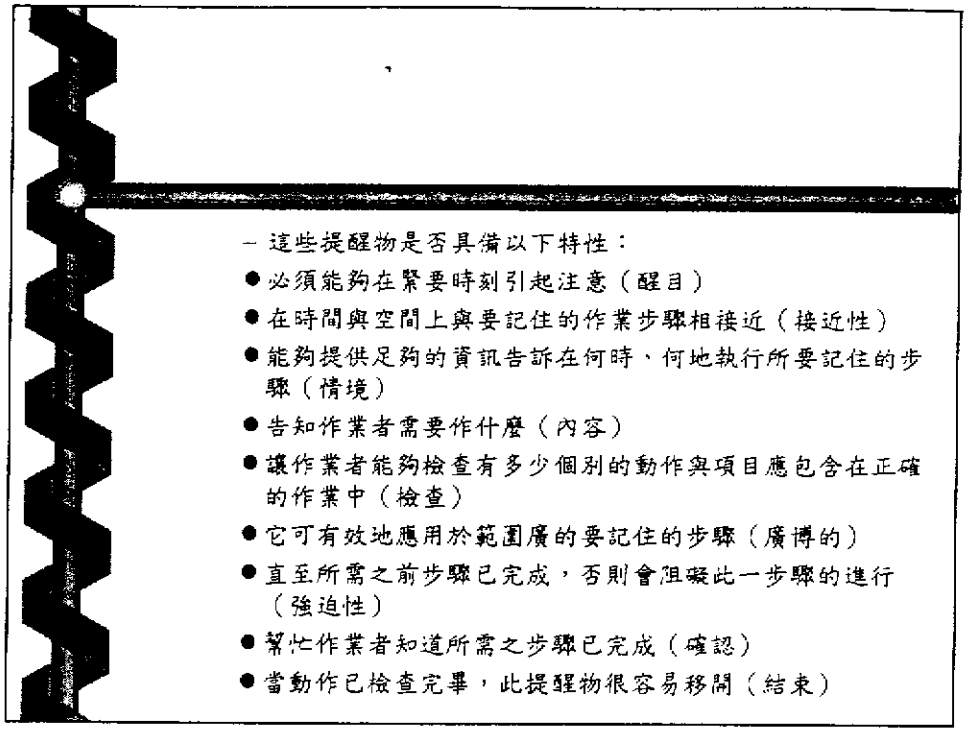
C.作業進行階段

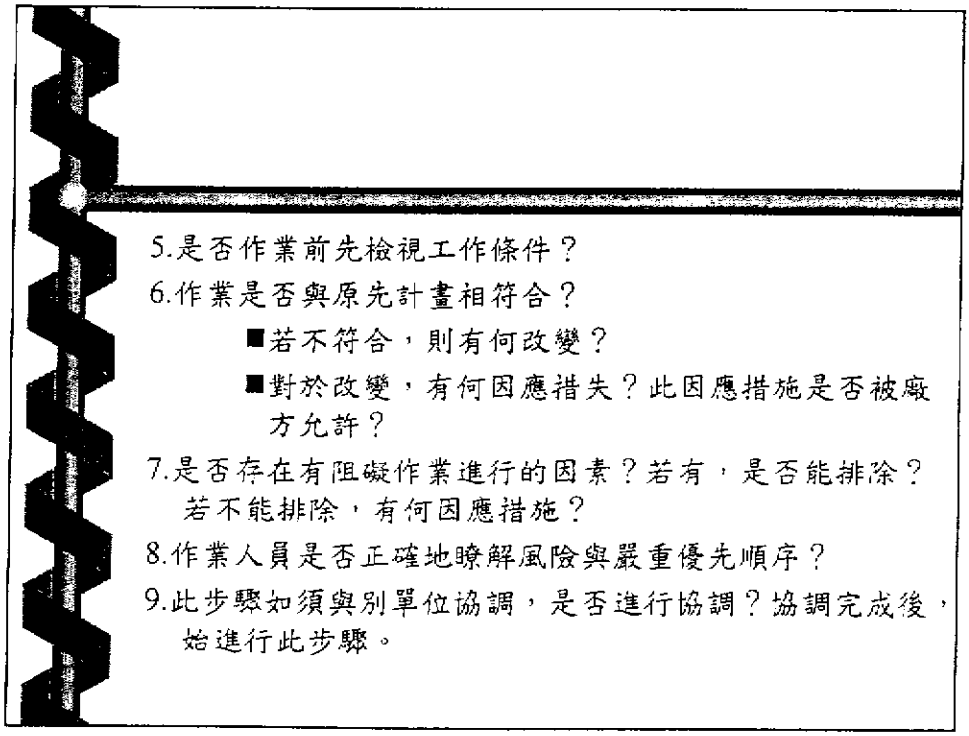
1.是否有掛卡？

2.是否攜帶程序書與相關文件和圖面？

3.合適的工具與輔助器材是否具備？會使用？

4.是否攜帶輔助工具與防護器具？防護器具是否配戴完整？是否有作業的提醒物（reminder）？


– 這些提醒物是否具備以下特性：
● 必須能夠在緊要時刻引起注意（醒目）
● 在時間與空間上與要記住的作業步驟相接近（接近性）
● 能夠提供足夠的資訊告訴在何時、何地執行所要記住的步驟（情境）
● 告知作業者需要作什麼（內容）
● 讓作業者能夠檢查有多少個別的動作與項目應包含在正確的作業中（檢查）
● 它可有效地應用於範圍廣的要記住的步驟（廣博的）
● 直至所需之前步驟已完成，否則會阻礙此一步驟的進行（強迫性）
● 幫忙作業者知道所需之步驟已完成（確認）
● 當動作已檢查完畢，此提醒物很容易移開（結束）


5.是否作業前先檢視工作條件？
6.作業是否與原先計畫相符合？
■若不符合，則有何改變？
■對於改變，有何因應措失？此因應措施是否被廠方允許？
7.是否存在有阻礙作業進行的因素？若有，是否能排除？若不能排除，有何因應措施？
8.作業人員是否正確地瞭解風險與嚴重優先順序？
9.此步驟如須與別單位協調，是否進行協調？協調完成後，始進行此步驟。

10.進行每一步驟前，是否有足夠的資訊以完成作業？

11. 進行每一步驟前，是否核對所要作業的設施是正確的？

12. 進行步驟時，是否擷取到所需的資訊？

■這些資訊顯示出設備的狀態為何？

13. 如對此步驟有所疑慮或對狀況不甚了解，是否停止作業並請求他人支援與協助？

14.進行的步驟動作結果是否合乎作業要求？

15.關鍵動作完成後，是否有請同伴或廠方品管人員檢查？

16.動作完成後，系統狀態是否與預期相符合？

■如非與預期相符合，發生了什麼問題？

■這問題若持續下去，會對系統安全產生什麼後果？

■應如何處置（應用那些法則）以解決此問題？

■這些法則有無副作用而對系統安全產生影響？

17.此步驟如屬檢驗點，是否停止並立即請求廠方品管人員檢查？

D.作業結束

1.是否有觀察比較、核對、確認作業如預期結果？
2.復原作業前是否先知會相關單位？
3.是否將原設備復原並清除作業現場？
4.是否執行重置作業，並確認所有相關組件介面恢復正常？
5.是否進行系統檢測，以確認系統恢復正常？
6.是否將檢查點彙整驗收？

E.作業檢討

1.在作業中有何意料之外的事發生？
2.在進行那些步驟時容易發生疏失？監工是否知道這些狀況？
3.有那些情境容易造成這些疏失？
4.訓練是否涵蓋所需之知識與技能？
5.程序書是否正確、能用、易懂？
6.作業的計畫是否合理？時間是否足夠？

7.工作場所的資源與資訊是否足夠？

8.工作流程是否有效率？

9.有那些經驗可以承傳？這些經驗是否有正式記載於文件中？

10.監工是否提供所需的支援與指導？

G.作業改善

1.改善的提案是否考慮到有效性、顯著性、持續性、難易度、經濟性、及時性？

2.各提案的評估是否就有效性、顯著性、持續性、難易度、經濟性、及時性等項有指標得以綜合量化評價？

3.提案的決策是否以安全為優先考量？

4.改善案的效果是否持續地追蹤？