行政院原子能委員會

委託研究計畫研究報告

核電廠資通安全標準及整體資產管理研究

Research on Information Security and Asset Management in Nuclear Power Plants

計畫編號：1002001INER001

受委託機關(構)：國立中正大學

計畫主持人：熊博安 教授

聯絡電話：05-2720411　ext. 33132

E-mail address：pahsiung@cs.ccu.edu.tw

核研所聯絡人員：周貽新

報告日期：　100 年　11 月　30 日

目　錄

內容

中文摘要

系統安全(safety)和電腦控制安全(security)在核能電廠儀控平台的匯合，導致相關規章的產生與採用，例如 RG5.71 是符合美國十號聯邦法規 73.54 即「數位計算機及通訊系統與網路的保護」的規定所訂定的核能規章(nuclear regulatory guide)。但是 RG5.71 中雖有說明要如何辨識與評估「重要數位資產」(critical digital assets, CDA)，卻沒有將 CDA 與核能安全之的關係定的很精準或有正規的模型化。更甚，對於重視系統安全和電腦控制安全的核能電廠，其風險評估和分析更是保障系統整體安全的重要一環，然而，以我們目前研讀之絕大多數重要的核能規章，都沒有同時考量到系統危機(hazard)和電腦儀控網路威脅(threat)之間的關係所共同引發的風險問題。因此，當我們要將這些規章應用到實際核能電廠儀控時，會有一些實行細則並沒有在規章中清楚交代。本計畫的主要目標是提出一套正規模型，除了使系統評估者可以塑模核能系統安全與電腦控制安全的關係之外，進而找出系統的安全弱點(vulnerability)、危機(hazard)與威脅(threat)與核電廠系統整體風險之關係。透過本計畫的實踐，我們建構核能儀控平台的正規模型，供日後研究與設計，亦有助於提升各主要核能安全規章中正規風險分析的完整性。更具體而言，我們將詳細討論核能電廠中重要數位資產在系統安全和電腦控制安全匯合考慮的情況下，所可能潛在的風險，以及如何透過整體分析風險的方法，整合存取控制、風險控管策略等安全控制機制，有效地提升系統安全與電腦控制安全之間的協同作用(synergy)。並且透過本計畫中所提出的相關理論與實現方法，不僅提升核能系體整體之安全，同時能提供相關研究人員很紮實的設計與驗證訓練。

Abstract

The convergence of safety and security issues in nuclear plants has led to the adoption of regulatory guides such as RG 5.71, which conforms to the title 10 of the Code of Federal Regulations (CFR) 73.54 regulations on the protection of digital computer and communication systems and network. Though it describes how critical digital assets (CDA) are identified and assessed, but the exact relationship between a CDA and nuclear *safety* is neither estimated accurately nor formally modeled. Moreover, for such safety-and-security-critical nuclear power plant systems, related risk assessment and analysis are required for ensuring the safety and security of the whole system. Nevertheless, we found that most of the published nuclear regulatory guides we surveyed do not estimate the risk incurred jointly due to both safety and security considerations. Specifically, there is a lack of a unified risk assessment method that considers the relationship between safety hazards and security threats. Thus, when such regulatory guides are applied to real nuclear plants, we are often faced with implementation details that are not covered in the guides. The main goal of this project is to propose a formal model for not only establishing the model for the safety and security of nuclear power plant systems, but also for supporting the

discovery of the relationship among the vulnerabilities, hazards, and threats of nuclear power plant systems. In this project, the nuclear instrumentation and control (I&C) systems are formally modeled for research and design. More specifically, our project not only proposes a unified risk assessment method that addresses both safety and security concerns, but also proposes effective methods to mitigate the risks and improving the synergy between safety and security by integrating some safety or security procedures or policies such as access control design, risk management, etc. The proposed theories and implementation methods not only make nuclear I&C safer and more secure, but also provide rigorous training to related personnel in developing such systems.

壹、計畫緣起與目的

現今的資訊科技與網路技術蓬勃發展，相關的系統裝置及控制軟體也日新月異。這使得核能電廠裡在儀控平台上整合新的裝置與技術的時機也越趨頻繁。另外，網路的發展帶來許多的方便與作業流程上的改善，但是也同時導致很多安全上的不確定性以及可能的外在威脅。原本系統安全(safety)和電腦控制安全(security)是兩個不同的領域，各有各的專業、技術、工具、術語、目標以及發展趨勢。但是，現在很多安全系統(safety-critical systems)例如核能電廠儀控平台，已經面臨電腦控制安全的問題，因而導致此兩個領域的匯合(convergence)。

首先我們研究了目前主要核能安全國際組織的相關規章，比較了各核能安全規範的異同，以助我們了解核能安全的訂定。以核能電廠的二個重要系統：高壓爐心注水系統(high pressure core flooder, HPCF)與反應器急停隔離功能系統(reactor trip and isolation functions, RTIF)，做其重要數位資產的辨識與量化其資產價值，以為後續風險評估所利用。

而本計畫主要目標是提出一套正規模型，除了使系統評估者可以塑模核能系統安全與電腦控制安全的關係之外，進而找出系統的安全弱點(vulnerability)、危機(hazard)與威脅(threat)與核電廠系統整體風險之關係。具體而言，我們將詳細討論核能電廠中重要數位資產在系統安全和電腦控制安全匯合考慮的情況下，所可能潛在的風險，以及如何透過整體分析風險的方法，整合存取控制、風險控管策略等安全控制機制，有效地提升系統安全與電腦控制安全之間的協同作用(synergy)。

貳、研究方法與過程

在此章節中，我們將討論主軸分為以下四個方向：核能安全相關之研究，核能電廠重要數位資產之辨識與評估，系統安全暨電腦控制安全之整合風險評估方法論，以及風險評估模型與存取控制之整合與控制流程訂定。

在第一節中，核能安全相關之研究包含了：各國際組織發表核能安全規範，設計基準威脅，安全風險評估方法，以及存取控制設計。

一、核能安全相關之研究：

(一)、各國際組織發表之相關核能安全規範

為了能夠發展出一套完整的電腦控制安全與資產管理之方法，我們首先針對目前世界各國的規範與做法進行探討，主要針對各國目前現行的法規與遵行的規範作分析與整理，並且從中探討不足或應予以加強的部分，進而提出我們的改進方式，以助加強我國目前電腦控制安全與資產管理現行法規與安全規範。

根據我們的所收集的資料，我們發現目前各國所遵循的法規或安全規範，絕大部份是遵循國際原子能總署[1]所制定的標準規範，依造實際情況做改進後，實施與遵循。除此之外，美國核能管制委員會所提出的監督指南文件(Regulatory Guides)[2]，也廣受核能產業廠商的採用。對於其他工業上的標準，則大多是依據國家標準技術研究院所致敬的標準來做建設與維護。以下我們將針對目前國際上重要核能與工業國際組織與團體作簡介。

1. 國際原子能總署(International Atomic Energy Agency, IAEA)

國際原子能總署成立於 1957 年 7 月 29 日，該組織之主要宗旨為促進和平利用核能源，並且抑制其用於任何軍事目的。國際原子能總署於各國政府之間扮演著論壇的角色，促進全球核能科學及核能技術的進步、發展與合作。

國際原子能總署鼓勵和平的應用核能技術，並且訂定了核能安全公約，提供了國際安全保障，以防止濫用核能源技術與核能原料，對於核能安全(Nuclear safety)[3]以及核能安全標準(Nuclear Security)[4]，訂定了許多標準與規範，並且監督各國的實施狀況。

由於目前大多是擁有核能發電廠的國家多已加入 IAEA 的組織當中，因此 IAEA 所提出的規範目前廣為各國遵守，因此在本計畫當中，我們首先針對 IAEA 所提出的各項系統安全(safety)和電腦控制安全(security)規範作探討，並且與其他組織所建立的規範做比較，找出其中的優缺點，最為改進的依據。

(1) IAEA Nuclear Security Guidelines

核能安全準則(Nuclear Security Guidelines)為國際原子能總署主導，與各界專家共同研討所訂定出的一系列安全準則，並且由所有會員國共同審查通過，因此內容十分完善，核能安全準則共可分為 15 份準則。

核能安全準則主要討論內容為如何預防、偵測與反應對於非法的竊取、破壞與入侵核能設施或核能原料的議題。核能安全準則之主要內容分類可分為四類，為：核能基礎安全、相關建議、實施指南與技術指導。

核能安全基礎討論的議題包含了目標、概念及原則等，並且提供基礎的安全性建議。相關建議部分則是提供了國際原子能總署會員國對於核能安全基礎的最佳作法。實施指南是進一步的提供設計上的建議、措施及相關資料。技術指導部分，提供了詳細的指導、措施，與人員培訓的方式。

以下精簡介紹此 15 份核能安全準則之重點：

A. 技術與功能規格 Technical and Functional Specifications [5]：提供會員國以及設備製造廠商，對於設計、測試、驗證以及購買輻射監控設備等之規範。

B. 核能取證支援 Nuclear Forensics Support[6]：描述取證之工具與程序，其中包含了累積數十年的非法運送、販賣等法律經驗。

C. 監控放射性物質於國際郵件營運 Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators[7]：介紹與提供放射性物質檢測技術與設備，提供給有需要之郵政營單位，此準則是與國際郵政聯盟(Universal Postal Union)共同訂定。

D. 保護核電廠免於破壞之安全 Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage [8]：提供評估安全防護核能發電廠受到攻擊的準則，並分別討論結構、系統與元件等，強調這些組件的破壞與協同防護機制。

E. 辨識放射性來源及設備 Identification of Radioactive Sources and Devices[9]：提供非專業人士或組織對於放射性物質、設備支出被鑑定方式，以及工作環境中可能接觸到的情形。

F. 禁止非法販售與運送放射性物質 Combating Illicit Trafficking in Nuclear and other Radioactive Material [10]：藉由提供專業知識，輻射性物質應該交由技術人員處理與運送，不應該遭到不法之行為干涉。

G. 核能安全文化 Nuclear Security Culture[11]：解釋核能安全的基本概念與文化，並討論到核能的電腦控制安全文

化和系統安全文化的關係，它提到電腦控制安全和系統安全在目標上相同，都是要降低和限制核能放射物質帶來的風險,而且這兩者在原則上都應該保持懷疑的態度,謹慎地做有效的雙向溝通。雖然有時候系統安全和電腦控制安全的要求不同，但它們必須共同被重視和加強，甚至必須要培養一個整合系統安全和電腦控制安全的方法，以及如何安排相關政策之方式。

H. 對於內部威脅之預防與保護措施 Preventive and Protective Measures against Insider Threats[12]：提供指導主管單位，如何預防任何來自內部的威脅、外部威脅與內外部共同勾結威脅，及其相關措施。

I. 放射性物質之運送安全 Security in the Transport of Radioactive Material[13]：提供指導放射性原料之輸送方式，避免對環境造成傷害以及其他竊盜、破壞等惡意行為的發生。

J. 開發、使用與維護設計基準威脅 Development, Use and Maintenance of the Design Basis Threat[14]：提供指導如何開發、使用和維護設計基準威脅，設計基準威脅為一個描述的屬性與特點，潛在的內部或外部威脅可能產生惡意行為，如對擅自拆除或破壞的實物保護系統的核材料。

K. 放射性來源之安全 Security of Radioactive Sources [15]：提供指導與建議採取措施，並提出整合系統安全和電腦控制安全的方法。但是只有一段概念性的描述，主旨還是在說明整合兩者是非常重要的事。根據本文件的附錄，有提到電腦控制安全的方法包括了存取控制、錄影監控等，但沒有提到系統安全的方法包括哪些。然

而，雖然它沒有進一步詳細說明在技術上如何整合系統安全與電腦控制安全的關係，但已經非常明示核能的安全必須同時考慮系統本身的設計與來自網路可能造成的威脅。此為落實對於放射來源之預防、偵查和應對惡意行為涉及，供監管設立之準則。

L. 核能安全教育學程 Educational Programme in Nuclear Security [16]：提供了理論、知識和實務，以滿足核能安全準則。提供國家擬定自己的學術方案，以滿足該國的教育在該地區的之核能安全需求。

M. 建議的核能安全於材料、實體防護與設施 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities[17]：提供指導各國及其主管機關，如何發展、加強、實施和維護對核能原料和核設施之實體保護制度。

N. 建議的核能安全於放射性原料與設施 Nuclear Security Recommendations on Radioactive Material and Associated Facilities [18]：提供指導各國及其主管機關，如何發展、加強、維護目前的安全制度與相關措施。

O. 建議的核能安全於其他放射性原料之規範控管 Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control[19]：提供指導核能原料之檢測、評估方式、警報或未經授權的行為，以及核能安全問題涉及核能原料或其他放射性物質進行監管控制。建議的行動包括確認一個可信的威脅，評估和封鎖行為的企圖和應對的核安全事件。

(2) IAEA Safety Standards

此安全標準是由國際原子能總署所訂定之基本安全原則、安全需求與安全指南，用來確保人員與環境的安全性，除了一般安全標準外，也額外對於其他議題，例如：核能發電廠、燃料循環、放射性物質處置、放射性物質之應用等相關議題，提出安全上的額外標準。而此安全標準之範圍，則分為：核能發電廠安全(Nuclear Safety, NS)、輻射性安全(Radiation Safety, RS)、運輸安全(Transport Safety, TS)、核廢料安全(Waste Safety, WS)及一般性安全(General Safety, GS)。

(3) IAEA INSAG Series

國際核安全集團(International Nuclear Safety Group，INSAG) [20]是由國際原子能總署(IAEA)的主持下所組成，主要由具有高度專業能力的專家所組成，目的是監控組織、研究單位、學術單位以及核能工業之安全與提供專業性的諮詢與指導核能安全相關的辦法、政策與原則，並且發布了一系列的文件(共 24 份)，內容包含各種安全方面的問題。在INSAG-10 [21]文件當中，提出了關於系統安全的深度防禦，主要分成五個主題：

A. 總結了主要在深度防禦的安全概念的歷史發展。
B. 就目標、策略、物理屏障和保護層面來討論深度防禦。
C. 介紹深度防禦的實施、安全的評估，並說明各種要素之間的相互關係。
D. 說明當前的深度防禦如何操作可增強核電廠的運作。
E. 提出深度防禦可以應用於核電廠系統的未來發展。

表 1 為 INSAG-10 所提出的五層深度防禦層級，主要說明各層級之目的與必要方法。

表 1. 深度防禦的層級

深度防禦層級	目的	必要方法
層級 1	防止非正常操作和故障	保守的設計和高品質的建設與運作
層級 2	運作不正常和故障檢測的控制	控制、限制和保護系統及其他監控功能
層級 3	設計基準事故的控制	安全措施和事故處理步驟的策劃
層級 4	嚴苛的機器設備控制條件，包括事故發展的預防以及減輕嚴重事故的後果	輔助性措施和事故管理
層級 5	減輕排放大量放射性物質之後所產生的放射性後果	廠外緊急反應

2. 美國核能管制委員會(The U.S. Nuclear Regulatory Commission, NRC)

為了妥善維護居民的健康，保護環境不會受到汙染，美國於 1975 年成立核能管制委員會[22]，管理核能相關之事務，主要任務為規範與監督核能反應爐的安全機制、放射性物質以及核能反應原物料、核廢料的管理，無論是在醫療或工業上都由核能管制委員會所監督。

美國核能管制委員會制定了一系列的法規指引(Regulatory Guides)，其中包含 RG 5.71[23]為美國在遭受到 911 恐怖攻擊事件後，提升國內核能發電廠之儀控安全性的需求文件，並且規範須於近期內確實完成以提升安全性。NRC 對於系統安全(safety)和電腦控制安全(security)的規範，主要分別描述在 RG 5.71 及 NRC 網站中的各項規章與指導原則(Regulations and Guidance)。概略來說，RG 5.71 是偏重電腦控制安全(security)在網路環境中的規範，而 NRC 網站中的安全規章則是偏重討論核電廠本身的系統安全(safety)。以下，針對 RG 5.71 做更詳細的介紹。

(1) NRC RG 5.71

RG 5.71 是符合美國十號聯邦法規 73.54 即「數位計算機及通訊系統與網路的保護」的規定所訂定的核能法規指引(nuclear regulatory guide)。RG 5.71 主要描述一套管制立場(regulatory position)，其中以一套防禦系統架構提升防禦策略及一套依據 NIST SP 800-53[24] “Recommended Security Controls for Federal Information Systems” NIST SP 800-82[25] “Guide to Industrial Control Systems Security” 中所規定的安全控制機制。

NIST 所訂的兩套資安標準 SP 800-53 及 SP 800-82 主要基於已熟知的網路威脅、風險及弱點，並結合相等熟知的對抗策略與保護技術。美國核能管制委員會(Nuclear Regulatory Commission, NRC)將此兩套標準中具高衝擊的電腦控制安全機制進行修剪，使其能夠更符合核能電廠裡的系統而且符合 10 CFR 73.54[26]的規範。在 RG 5.71 中，NRC 明確訂出這些為核能電廠客制化的電腦控制安全機制，並且將這些電腦控制安全機制分為三大類，包含技術類、操作類以及管理類。並且，在 RG 5.71 中特別針對如何辨識重要數位資產(critical digital assets，CDA)[27]提出一套流程。透過 CDA 辨識的流程可以發現，RG 5.71 將系統安全、電腦控制安全以及緊急之預備措施(safety, security and emergency preparedness, SSEP)功能相關之資產都當作 CDA。可以見得，RG 5.71 中雖然主要針對的是資料安全，但對於核電廠數位化後，核能安全的問題是必須從設備自身系統的設計安全、網路連結使用的通訊安全，以及緊急的預備措施都要一併考量在內。

RG 5.71 中提出了層級 0 至層級 4 的深度防禦的模型，是以電腦控制安全為考量，而且這些層級之間是有存取的方向性。除了 RG 5.71，NRC 也有一系列的安全規章文件進一

步針對網路和系統的安全分析。在 NRC 的網站中，有一項研究活動(Research Activities)，與系統安全有關的主要有三個部份：

A. 數位化的儀器和控制的安全規章，包括了：暫行人員管制指引(Interim Staff Guidance, ISG)，10 CFR Part 50[28] (主要是針對核電廠的基本設計準則，包括二份文件：10 CFR 50.55a[29]與 10 CFR Part 50 Appendix A[30])，SECY 文件(共 8 份，主要在討論數位化系統的規定、技術及測試等議題)，RG 系列文件(共 12 份，主要在討論核電廠數位化設備的系統安全，重點在軟體的設計和測試)以及六份系統安全評估報告。

B. 核反應爐的安全研究，包括了反應爐老化，反應爐原料的狀況，軟體模擬反應爐遭遇嚴重意外(熱量、反應爐冷卻水設備等)，機率危機分析，放射物保護等等。

C. 核廢料的安全研究。然而，NRC 在這些系統安全的文件中，比較偏向主題式的分析報告文件，或者是一段至二段的短篇描述，相較於 IAEA 提出的系統安全與電腦控制安全的文件來說，NRC 討論的內容比較少一些，但是 NRC 有提出一些較為明確的分析主題或事件。

3. 核能研究院(The Nuclear Energy Institute, NEI)[31]

核能研究院由核能相關事業、建築師、工程師等各界專業人士所組成，目的是為了監督與立法來監控核能相關事業的發展，並且提供協助核能相關企業做技術或業務上的相關問題，提供正確的解決方案，以推動核能產業的發展。

在 NEI 所提出的 NEI 08-09[32]以及 NEI 04-04[33]兩份文件當中，對於存取控制議題做討論，並提出技術安全控制規範(Technical Security Controls)。

我們進一步針對 NEI 08-09 文件當中所提出的各項規範做檢視，探討在其中於系統安全(safety)和電腦控制安全(security)整合時，可能隱含的系統弱點。

(1) NEI 08-09 Cyber Security Plan For Nuclear Power Reactors

在 NEI 08-09 中，提出了一套技術安全控制規範(Technical Security Controls)，在其附錄 D 當中，討論了如何減輕資訊系統的風險方式，分別由五個方面來討論，分別為存取控制、系統審計、系統溝通保護、認證機制及系統強化。

存取控制章節當中，提出了 22 種存取控制機制上的設計，並且詳細規範在各機制上的設計與安全規範。表 2 為存取控制策略系統需求一覽表，整理了對於各項機制提出說明該機制在系統中所保護或管理的功能、對象為何，並且列出建議的功能需求與設計須注意事項。

表 2. 存取控制策略系統需求一覽表

Account Management	Access Enforcement	Information Flow Enforcement
Separation Of Functions	Least Privilege	Unsuccessful Login Attempts
System Use Notification	Previous Logon Notification	Session Lock
Supervision And Review	Public Access Protocol	Automated Marking
Automated Labeling	Third Party Products And Control	Use Of External Systems
Wireless Access Restrictions	Insecure And Rogue Connections	Proprietary Protocol Visibility
“Open/Insecure” Protocol Restrictions	Permitted Actions Without Identification Or Authentication	Access Control For Portable And Mobile Devices
Network Access Control		

A. 系統審計章節中，說明了在做系統審計時，需要確實審核的規範與紀錄，並且說明審計紀錄應該如何做後續處理與使用。
B. 系統溝通保護章節，討論了系統應該注意的事項，避免系統暴露重要訊息或造成錯誤。
C. 認證機制章節說明了辨識與認證機制的設計要點，並且說明在設置密碼時，應該符合的最低安全性需求。
D. 最後提出系統強化的主要方式與流程，藉此來不斷強化資訊系統的安全性。

4. 國家標準技術研究院(National Institute of Standards and Technology, NIST)

國家標準技術研究院的主要任務為促進產業競爭力[34]，發展測量科學、標準與技術以提高經濟安全性並且改善目前的生活品質。NIST 訂定了許多工業標準，並且有一系列的安全相關文件，專門討論核能相關產業的規範。

由於目前由 NIST 所制定的各項工業標準廣為國際各國及各組織所採用，因此我們針對 NIST 800-53 文件，對於核能相關產業所制定的安全標準做探討，藉以了解目前各國現行對於該產業的作法與規範。

(1) NIST 800-53

在這份文件當中，主要提供各種資訊系統的安全相關規範，其中包含：個人與資訊系統的安全管理和監督職責、資訊系統的發展與可靠性、資訊系統的實作與操作以及資訊系統的安全評估及監控。為了滿足 FIPS 200[35], Minimum Security Requirements for Federal Information and Information Systems 的規範，在文件當中，說明了安全機制應如何套用到

系統各個元件當中，並且指出在資訊系統當中，對於資料處理、資料傳輸、資料儲存應該遵守的安全規格。

在風險管理策略上，也將整體策略做說明，並且針對流程當中每個步驟所對應的相關文件及規範做整理，風險管理策略流程如下圖 1 所示。

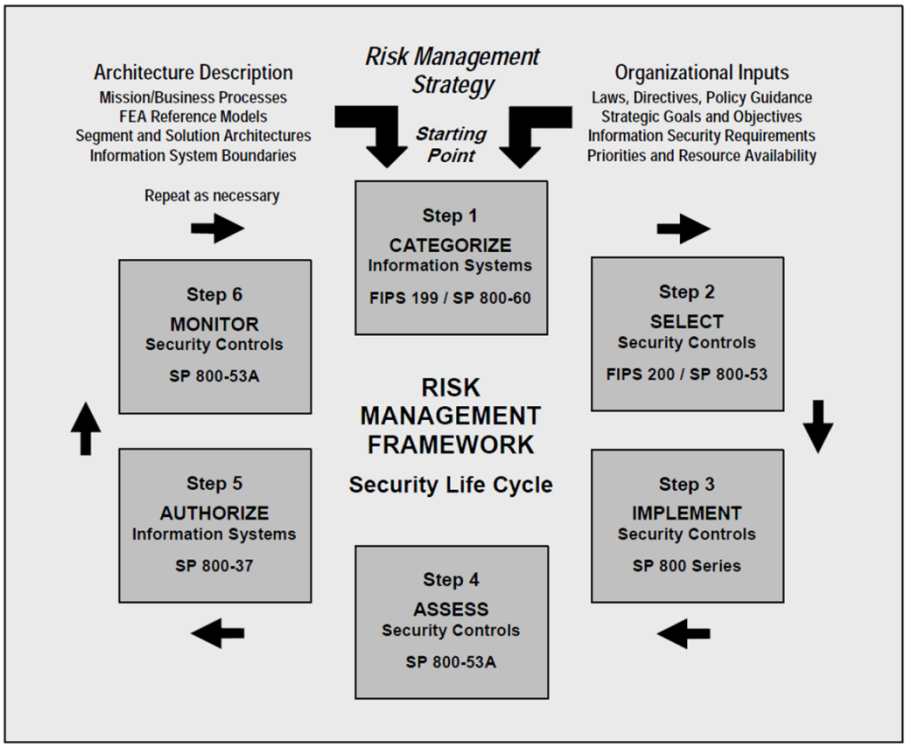


圖 1. 風險管理策略流程圖

(二)、設計基準威脅

1. 概述

(1) 定義

設計基準威脅是一種類型、結構和敵手的能力的一個概述。以下我們整理由美國核能管制委員會(NRC)及國際原子能總署(IAEA)所分別定義說明之 DBT 的異同。

A. 美國核能管制委員會(Nuclear Regulatory Commission, NRC)：

主要在防止放射性破壞行為，並防止盜竊特殊的核材料。設計基準威脅在 10 CFR 73.1(a)文件的當中清楚描述其目的及範圍。設計基準威脅的目

的為建立和實體保護制度的維護，讓特殊核材料在固定地點及運輸上都將提供更有能力的保護，以及保護核電廠中特殊核材料的使用，而核設施的持照人(licensees)負責證明他們能抵禦設計基準威脅。

B. 國際原子能總署(International Atomic Energy Agency, IAEA)：

設計基準威脅是實體保護核設施系統設計的主要考量因素之一，其基本原則為設計基準威脅的實體保護，是基於該國目前的威脅而進行評估，而該項評估是通過正式的威脅評估程序。根據國際原子能總署於 1999 年公佈的文件：INFCIRC/225/Rev.4(實體保護核材料及核設施的建議)，定義設計基準威脅是一種屬性和特性，描述一個潛在內部和(或)外部的敵手可能試圖擅自轉移核材料或破壞，對其中實體保護系統的設計和評估。從發佈的那時起，進一步發展到加強國際制度的實體保護核材料與放射性材料以及相關設施。

(2) 美國設計基準威脅規範的修訂

美國核能管制委員會：設計基準威脅規則的修訂主要做三件事情。首先，設計基準威脅規定一般的安全需求，委員會於 2003 年 4 月 29 日將類似的設計基準威脅條例施加於核電廠的運作。設計基準威脅的規則修改及加強核能管制委員會有關規定的基礎上執行這些安全指令(security orders)並取得經驗和見解。最終版的規則包含多個相關規定，例如：協調群體的攻擊，自殺性攻擊和網絡威脅。其次，委員會審議視其情形並斟酌，於 2005 年 7 月 9 日註

冊通過能源政策法案(Energy Policy Act)，當中提到了十二項開發設計基準威脅時應該考慮的規則因素。最後，設計基準威脅的規則制定過程中，提供公眾有機會參與核能管理委員會開發的安全法規。

由美國國會於 2005 年 7 月 29 日通過能源政策法案(Energy Policy Act)，該法案當中提到了十二項應該考慮的因素為：

A. 2001 年 9 月 11 日發生的事件。
B. 實體、網絡、生化和其他恐怖威脅的評估。
C. 由多個大量單獨個體所組成的協調小組和幾個內部人員攻擊潛在的設施。
D. 從受聘於該設施的人員協助處理的可能性。
E. 可能的自殺式攻擊。
F. 潛在的水基和空基威脅。
G. 具有相當規模的爆炸裝置和其他現代化武器裝備的使用。
H. 攻擊者可能具有完善的設施運作的知識。
I. 火災的可能性，尤其是火災持續時間長。
J. 協助處理用過的燃料運輸。
K. 在適當充足的規劃下，以保護公眾健康和安全以及核周圍的設施，並適當的預防對核設施的恐怖攻擊事件。
L. 從設施中盜竊或轉移核材料等的可能性。

(3) 美國核能管制委員會設計基準威脅規則的修改

修訂完之後的設計基準威脅代表了美國核能管制委員會的努力，如何修改設計基準威脅美國國家研究委員會正在開發或修訂三個附加的規則，將進一步加強核管制委員會的安全法規。 這些措施包括以下內容：

A. 10 CFR 第 52 條(Title 10, Part 52, of the Code of

Federal Regulations)法規中提到“牌照(licenses)，認證(certifications)，核電廠安全許可(approvals for Nuclear Power Plants)”，提供美國核能管制委員會新的發電反應爐框架的許可證，並將安全要求納入到他們的牌照當中。

B. 10 CFR 73.55(Title 10, Section73.55, of the Code of Federal Regulations)的“發電反應爐安全要求”，修改和更新實體保護核電反應爐運作的要求。

C. 10 CFR 73.62(Title 10, Section73.62, of the Code of Federal Regulations)的“安全評估新的核能發電反應爐的設計要求”，為新的核能發電反應爐提供了設計要求的安全評估。

2. 目標

設計基準威脅是一個全面的動機及企圖的描述，針對潛 在對手的能力而保障系統的設計與評估。這種定義允許在安全規劃的基礎上做風險管理。從歷史上來看，各國使用設計基準威脅的轉換監管制度，以實現適當的分配資源、保護核材料和核設施以防止惡意行為潛在對手，可能導致嚴重的後果，特別是放射性後果或影響的擴散，但是，設計基準威脅也可用於保護任何資產與相關的高潛在後果（例如其他放射性物質的高活性）。IAEA Nuclear Security Series No. 10 提供教導如何開發、使用及維護設計基準威脅

3. 設計基準威脅的範圍

由國際原子能總署所出版的指南“IAEA Nuclear Security Series No. 10”當中提到

(1) 描述設計基準威脅，包括設計基準威脅是什麼，為什麼叫設計基準威脅以及在什麼情況下使用設計基

準威脅，如圖 2 所示。

(2) 確認並建議各組織的角色和責任應參與制定、使用和保護設計基準威脅。

(3) 描述國家如何處理設計基準威脅的前兆來進行評估。

(4) 介紹了設計基準威脅可以如何開發，其中包括：

A. 設計基準威脅發展所需的信息。

B. 對設計基準威脅的發展進行決策。

(5) 說明設計基準威脅如何結合到一個國家的核安全制度。

(6) 解釋及探討了設計基準威脅的條件以及如何審查和進行更新。

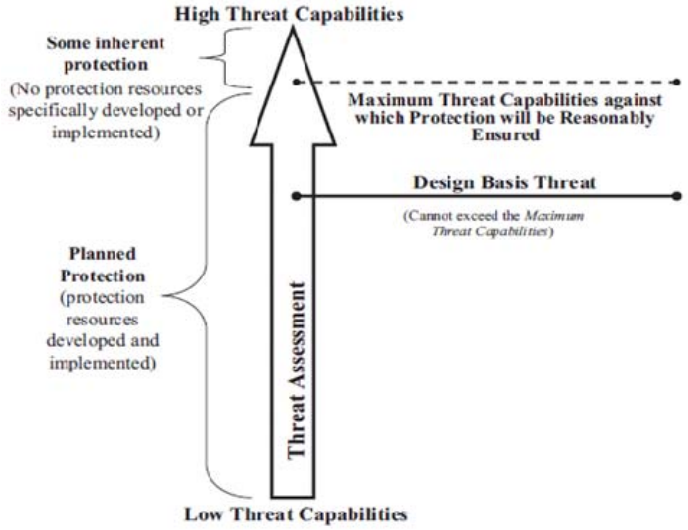


圖 2. 設計基準威脅的關係及評估

4. 防禦

核電廠是戒備森嚴的地方，有訓練有素以及武裝的警衛。他們也有層次的實體安全措施，如存取控制、水的屏障、入侵檢測以及具備戰略地位的看守塔。總而言之，這些因素構成了工廠設計基準威脅的反應。設計基準威脅從現實世界的情報信息開發，並說明敵手的能力，工廠必須要能夠防禦可能來自地面和水面攻擊的敵手。設計基準威脅的具體內容

沒有公開，可以幫助保護敏感信息，不讓恐怖分子知情。美國核能管制委員會定期檢討，必要時會增加新的設計基準威脅需求，如圖 3 所示。

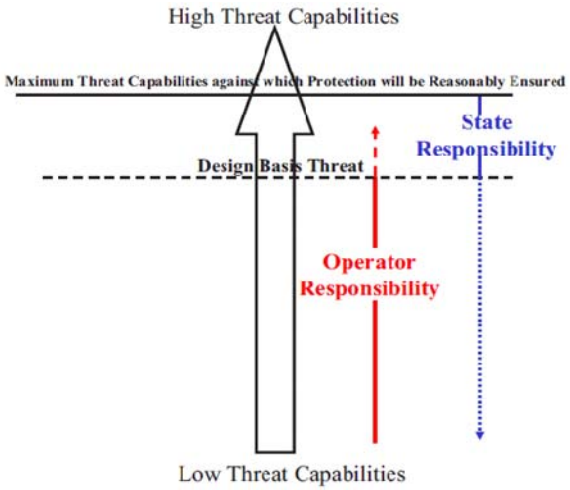


圖 3. 預防威脅的防護角色與責任

5. 實體設計保護

就前面提到的，實體保護的原則應基於該國目前的威脅評估。而這些評估的標準是通過正式的威脅評估的流程，這些威脅評估衍生出了基準威脅的設計。設計基準威脅的定義描述了該國在威脅設置上的威脅評估是完善的，以顧及其他議題（例如技術，經濟和政治議題）和進行特定系統規劃設計的要求。為了完成威脅評估到設計基準威脅之間的轉換，嚴格的分析和決策是不可或缺的。

(1) 主要議題

根據國際原子能總署於 1999 年公佈的文件：INFCIRC/225/Rev.4[36](實體保護核材料及核設施的建議)，定義了設計基準威脅，該定義包含了設計基準威脅的四個重要主題，分別是：

A. 內部和(或)外部的敵手：一個潛在的敵手有可能是任何的單獨個體或團體，被視為有意圖和(或)能力來進行惡意行為者。

B. 惡意行為導致不可收拾的後果：必要時須採取措施，以防止惡意行為，如擅自轉移或破壞材料，並防止其造成不可收拾的後果。

C. 屬性及特性：描述潛在的敵手擁有進行惡意行為能力的屬性和特性。惡意行為能力可能包括武器、炸藥、工具、運輸、業內人士和內部勾結、技能、策略和人數。這些能力幫助確定檢測、延遲、反應標準進行有效的設計和評估實體保護系統。

D. 設計與評估研究：設計基準威脅被定義在國家層級，是用於幫助建立實體保護系統的設計性能要求的一種工具。一個設計基準威脅也可以幫助操作員和國家當局評估系統的有效性，用來評估敵手的能力對系統的性能影響。

設計基準威脅概述了操作員和國家機關都有保護的責任和義務的特性。這些職責的劃分可能會根據不同國家而有所不同。利用設計基準威脅來定義要求操作員給予明確的保護功能，是國家有關當局的責任。

(2) 原則

實體保護的原則透過行政和技術措施來實現，包括實體的屏障。這些措施對核材料的使用、儲存和運輸的期間提供了實體保護，重要的是，這份文件定期審查及更新，以反映與符合日益進步的實體保護系統及核技術。

(3) 目標

實體保護有一個具體的目標，那就是防止敵手成功的完成惡意行為，從而實現敵手的目的。清晰

的描述威脅是保證以及有效的實體保護的一個重要的前提。理想的情況下，將提供實體保護系統足夠的規格設計和性能需求的信息情報，以確保這一目標實現。然而，情報往往是有限的，且威脅是動態的。 實體保護系統的設計只可以有效防止目前的威脅，若拿來對付明天的威脅可能不會有效，這也是文件必須定期審查及更新的原因之一。

實體保護的目標，分兩個角度來看，分別是國家及國際原子能機構。

國家實體保護系統的目標應該是：

A. 建立減少擅自轉移核材料和(或)破壞的條件。

B. 提供信息和技術援助，以支持國家用快速和全面的措施來查詢、尋找及恢復丟失的核材料，並盡量配合安全部門減少放射性後果。

國際原子能機構的目標：

A. 提供核材料的使用、儲存和運輸過程中及核設施一套實體保護需求的建議。此建議提供給國家主管當局考慮。 而這些建議僅提供指導，不侵犯國家主權權利。

B. 要有能力提供建議，使各國當局重視國家內的實體保護制度的需求的狀態。

為了滿足明確的具體說明威脅的需要，因此引進了設計基準威脅的概念。設計基準威脅提供實體保護系統充足的系統設計及符合的標準評估的基礎。設計基準威脅還針對需要變化的實體保護系統提供進行評估的標準。設計基準威脅可以允許實物保護系統的制定，以滿足獨特核材料或設施的特色。設計基準威脅亦可以幫助避免設施和核材料導致嚴重後

果的相關惡意行為，確保設施和核材料得到需要的保護。設計基準威脅還提供相關組織單位之間的責任分配的清楚依據。

6. 設計基準威脅的價值

設計基準威脅提供了信任的基礎，使保護系統開發是適當且有效的。設計基準威脅提供了一個基礎的系統設計和一致的標準評估以及充足的實體保護系統。設計基準威脅還針對的需要變化的實體系統提供了一個基本標準保護進行評估。設計基準威脅可以允許定製的實物保護系統，以滿足獨特的功能或設施的材料。設計基準威脅可以幫助避免過度保護被應用到設施和材料上，同時確保設施和材料得到他們需要得到保護，有關的惡意行為可能導致高的後果。在這種方式下，使用的實物保護設計基準威脅的方法可以幫助減少隨意性，否則可能存在建立的實物保護要求的材料和設施受國家管轄。最後，他們需要得到保護還提供了一個清晰的依據，有關組織之間的責任分配。

設計基準威脅本身不是一個目標，而是一種工具，是為了實現一連串的目標的工具。透過設計基準威脅在國家的管轄範圍內達到核材料和核能相關設施的實體保護的規定，只要是用於設計和評估國家的實物保護的價值皆是。要做到這一點，該方法就需要被納入控制的架構及用於：

A. 建立實體保護系統的目標和要求。

B. 確定實體保護系統的設計。

C. 建立實體保護系統的評估標準。

D. 確定保護作用，是國家的責任。

在操作的層級上，檢測的方法，措施的延誤，面對惡意行為以解決敵手的反應的設計基準威脅...等，總之，每個實體保護系統的措施均應包括以及參照設計基準威脅的發展，與評估的防備。

7. 結論：

就實體保護系統來說，盜竊及惡意破壞是其最主要的二大威脅，設計者必須假設最大威脅的可能性以作為實體保護系統的基準，也就是所謂的設計基準威脅。設計基準威脅的合適性非常重要，其功能不能太強或不足。

(三)、安全風險評估方法

由於自然、外在因素的變化，導致不利系統運作的風險日益增加。風險的變化可能會產生緊急事件與危機，因此風險評估對於保障系統安全是非常重要的一環，亦被廣泛應用。風險評估在各領域中依系統的不同，其方法也略有差異。以下將我們參考研究的各風險評估方法做一整理說明，如表 3 所示。

1. ISO 27001

ISMS (Information Security Management System)是一套有系統地分析和管理資訊安全風險的方法，由國際標準組織(International Organization for Standardization)引用，並於 2005 年宣布，代替 BS7799-2 成為資訊安全管理的國際標準，提供企業建置資訊安全管理標準規範，其目標是幫助建立和維持一個有效的信息管理系統。資訊安全標準 BS7799 分兩部份出版，BS7799-1：資訊安全管理應用程式，BS7799-2：資訊安全管理系統規範，BS7799-1 版本成為了 ISO17799 的基礎，之後改名為 ISO27002，而 BS7799-2 就成為了 ISO27001。ISO27001 的設計實現一連串的 information security controls and/ or other forms of risk treatment，並採用一個總體的管理過程(overarching management process)，以確保信息安全控制滿足企業的信息安全需求(information security needs)，但安全控制技術，如 antivirus 與防火牆通常不包含在審核的範圍內，也就是說 ISO27001 不一定意味著其餘的(remainder)組織，範圍以外的地區，有足夠的信息安全管理。雖然給出了風險管理的三個要素，但卻對各要素的量化取值沒有定義。ISO27001 評估的公式考慮了三項要素，分別為：Asset Value、Vulnerabilities 及 Threats。計算風險的公式為[38] [39]：風險值＝資產價值×弱點量化值×威脅量化值

所謂的資產價值的評價是針對 Security 的三項指標進行評鑑並加總而得，分別為：機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)。資產價值= 機密性評價+完整性評價+可用性評價。

目前，對於弱點的識別沒有統一的評價標準，依各個系統的弱點對資產損害程度而定。威脅等級評估對針對威脅出現的頻率以及強度進行評估。以下為計算安全風險分析所使用到的工具，大致上分　commercial 及 open-source 兩部份，這些 open-source 的 tools 由 OWASP (The Open Web Application Security Project)組織設計、開發、操作和維護，所有的工具、文檔都是免費的，開放給想要提高 application security 的任何人下載。這些 open-source 所考慮到的 risk analysis of security 的標準 based on ISO17799。而 commercial 的這些產品都有各自的限制性，無法取代健全的風險管理判斷或經驗。以下為 open-source 的風險管理工具的資訊整理。

表 3. Open-source 的風險管理工具的資訊整理

Tools	特點	參考標準	是否付費	License	適用對象
CRAMM	A database of over 3000 security controls referenced to relevant risks	ISO27001	Commercial		政府機構/大型或中小型企業
COBRA	系統可以自己產生適當的解決方法及建議	ISO17799	Commercial		中小企業 or commercial CIEs
RiskPAC	運用上靈活性較高及全	ISO27001	Commercial		

	面性的軟件				
RiskWatch	可以列出個別資產類別的分組清單	ISO17799/ NIST SP 800-26	Commercial		政府機構/大型或中小型企業
MARCO	助於識別及處理潛在的風險	ISO17799	Open-source	GNU GPL	企業
CORAS Risk assessment Platform	方便管理、再利用分析的結果	ISO17799	Open-source	GNU Library or LGPL	
Easy Threat Risk assessment	使用者可以很快上手使用	ISO17799	Open-source	GNU GPL	中小型企業
ARMS	管理上快速、簡單	ISO17799	Open-source	Public Domain	
Open Source Requirements Management Tool	有 traceability 的功能	ISO17799	Open-source	GNU GPL	

2. NIST

由美國國家標準局(National Institute of Standards and Technology)所制訂發布的一系列與工業相關的安全規範。NIST 所制訂的兩套標準 SP 800-53 及 SP 800-82 主要基於已熟知的網路威脅、風險及弱點，並結合相等熟知的對抗策略與保護技術。其中的 NIST SP 800-30 文件更是將風險管理相關的名詞定義做一個整理，以及對風險評估的公式計算與使用的方法做一個介紹，文件中還列出降低風險的方法流程，並且一一針對各個流程的方法做一個介紹，如圖 4 所示。

在 NIST SP 800-30 文件當中，針對各種 IT 系統，提出了一套風

險評估與管理的機制，針對各種系統弱點，同時考慮發生的可能性與發生時所造成的影響。風險管理是一套流程，藉由辨識風險、評估風險等流程，試圖採取相關措施，讓風險發生時，可以降到最低的程度，並且希望讓各公司、組織可以對於風險做完善應對。雖然在 NIST SP 800-30 文件當中對於 Security 的辯識流程及評估有清楚的描述，但是很少考慮到 Safety 的部份，而文中所提出的風險評估流程圖如下圖所示[40]：

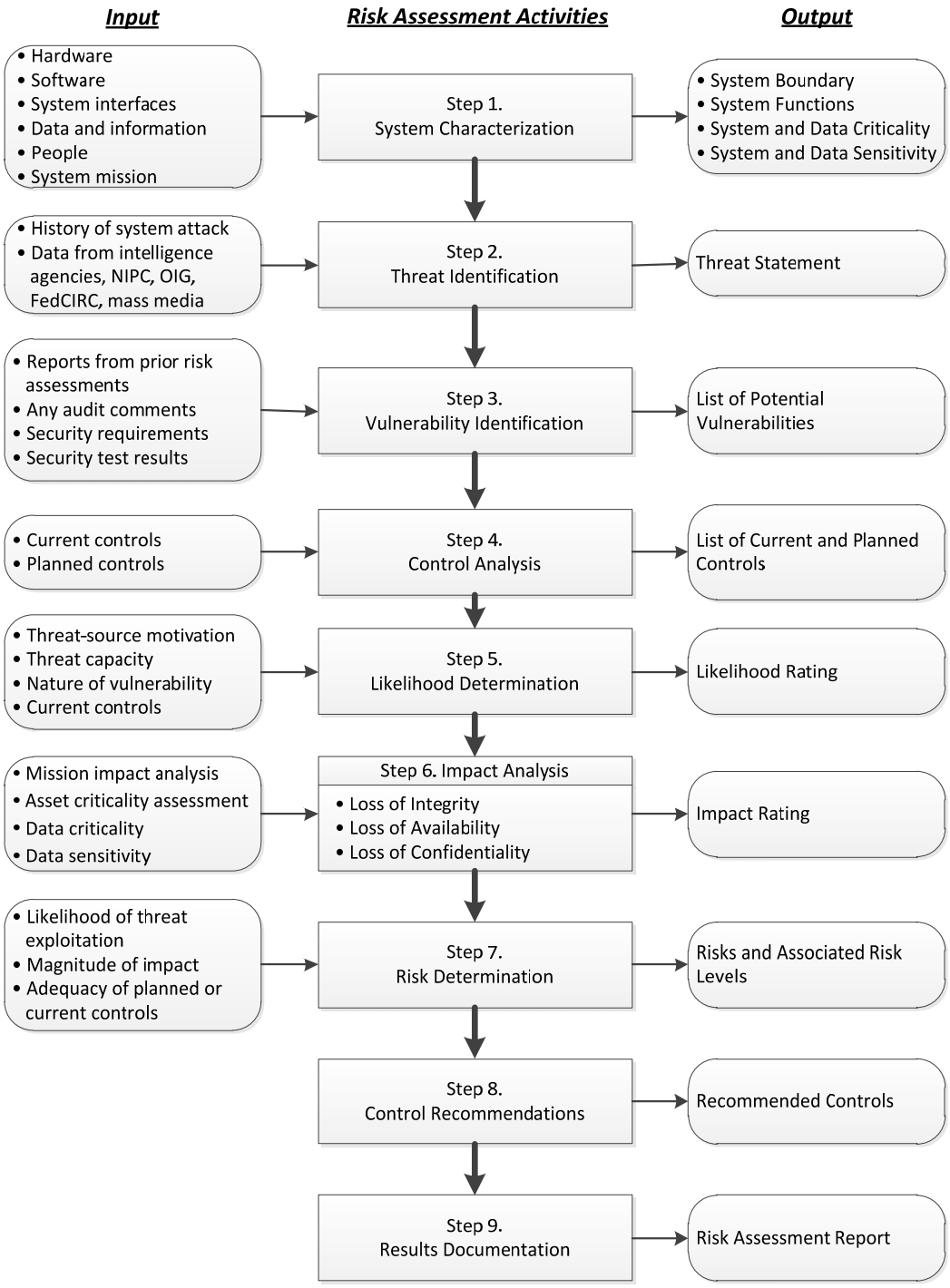


圖 4. 風險評估機制流程

Step1. System Characterization

針對所需評估的系統，做詳細的分類，例如常見的分類有：Hardware、Software、System Interface、Data and information、System mission、System and Data Criticality、System and Data Sensitivity 等，藉由將評估對象分類後，可以定義出評估對象所

影響、關聯的範圍.

Step2. Threat Identification

對於威脅評估，又可細分為兩個步驟：辨識可能的威脅來源、攻擊動機與行為，威脅的來源有三種，分別為自然威脅〈地震、龍捲風等〉，以及人為威脅〈駭客攻擊、惡意軟體等〉，與環境威脅〈停電、化學汙染等〉，另外在攻擊動機與行為方面，可能是竊取機密、惡意阻斷系統運作或者也有可能只是錯誤的操作等等

Step3. Vulnerability Identification

該步驟必須對於評估的系統，詳細的檢視，並且針對可能的各種威脅來源，列出可能的系統缺陷或系統弱點，並且製作成一份清單，以供往後在評估時使用。

Step4. Control Analysis

針對目前已經運作中或或是已經在計畫中的管制、功能等，做完整的檢視、分析，看是否會在系統中造成不當的危害，並且減少或排除各種威脅的發生的機率、可能性。

Step5. Likelihood Determination

針對威脅的動機、能力以及對於自然威脅的抵抗性和目前所擁有管制、功能之存在性與有效性，針對每一個潛在的威脅做分類，分別為高(High)、中(Medium)、低(Low)。

Step6. Impact Analysis

評估每個系統漏洞、弱點的危害等級，當一個威脅成功透過漏洞、弱點攻擊系統時，所造成的危害程度，根據系統的功能與任務，以及系統或資料的重要性、敏感性做分析，將危害分成三個等級，分別為高(High)、中(Medium)、低(Low)。

Step7. Risk Determination

藉由先前所評估的威脅發生可能性的等級權值與威脅所造成的危害程度等級權值相乘，即可得到系統的風險等級，可以組成一個風險等級矩陣(Risk-level Matrix)，如表 4[40]所示：

表 4 風險等級矩陣

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

並且在 NIST SP 800-30 文件中，定義風險等級為三級，分別為高(High：51~100)、中(Medium：11~50)、低(Low：1~10)，各等級之定義如表 5[40]：

表 5. 風險分級及相對應採取策略

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Step8. Control Recommendations

藉由風險評估流程，針對各個威脅、弱點，提出有效的應對方式，必須將危害程度降低到可以接受的範圍底下或是完全排除，並且訂定有效的計畫、政策或措施，進一步的提升系統安全性及可靠性。

Step9. Results Documentation

當完成以上風險評估流程之後，將所有資訊作完整的紀錄，製作成一份完整的評估報告，對於下一次的風險評估可以給予

參考。

3. Microsoft

我們亦參考了 Microsoft 所提出的 Threat modeling 文件[41]，此文件被應用於 Web applications，目標為幫助對最可能影響系統的威脅進行辯識及評價。要控制應用程序的安全首先先建構一個威脅模型，由於建構威脅模型是個重複的過程，在需要的時候再進行開發，並不斷的改進模型。在開發 Threat modeling process 的過程中必須了解以下幾項分析因素：

(1) Asset：資源的價值(A resource of value)。
(2) Threat：一個潛在事件，惡意或其他可能會損壞或破壞資產安全的(A potential occurrence, malicious or otherwise, that might damage or compromise your assets)。
(3) Vulnerability：系統在某些層面使威脅可能發生的弱點(A weakness in some aspect or feature of a system that makes a threat possible)。
(4) Attack：由某人或某事所做會危害 asset 的一個動作。
(5) Countermeasure：解決威脅和降低風險的防護。

該團隊亦提出一個威脅模型建構過程，如下圖 5. 威脅模型化過程所示，該流程可應用於目前正在開發和現有的應用程序，各過程的介紹如下：

Step1. Identify assets

找出系統中必須被保護的有價值的資產。

Step2. Create an architecture overview

使用簡單的圖表來記錄應用程序的結構。

Step3. Decompose the application

分解應用程序的結構，為應用程序創建安全配置文件，目的是想要利用安全配置文件來發現應用程序設計及配置中的缺陷。

Step4. Identify the threats

記住攻擊者的目標，利用對應用程序結構和潛在缺陷的了

解，找出可能影響應用程序的威脅。

Step5. Document the threats

利用通用的威脅模板來記錄每種威脅，該模板定義了一套各種威脅的核心的屬性。

Step6. Rate the threats

利用公式計算評價威脅的傷害，並且優先考慮和解決的最大風險的威脅。

公式為：Risk = Probability × Damage Potential。

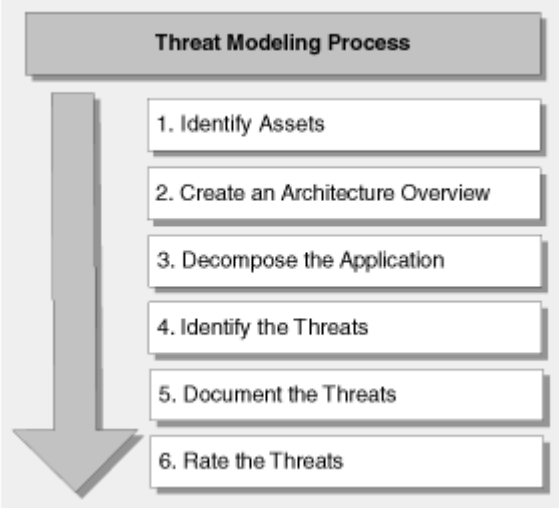


圖 5. 威脅模型化過程

威脅模型建構可以幫助管理和溝通安全風險，測試人員可以編寫測試應用程序來鑑定很容易受到威脅的分析。而且可以針對危險最大的威脅優先解決，由於實際上解決所有的威脅是不可行的，因此可以進行決策忽略掉一些威脅，因為考量到它們發生的機會很小，即使發生了，所帶來的損失很小。王平，羅濟群，黃俊傑，與王宇文所合著:「風險評估方法」

他們提出風險評估公式為[37]：

風險量化值＝發生機率×衝擊

先在系統中個別算出風險評估值，再將其加總，成為整體的風險值。優點是可以將一個複雜的系統拆解，個別分析風險評估值，

再算出整體的風險評估值。由於風險評估的評估不易，且評估的結果容易遭受質疑，因此必須要有詳細、客觀的風險分析模式與決定系統的風險值。文中提到將風險分析的方法分為定性風險分析及定量風險分析：

(1) 定性風險分析：運用已經界定出的風險評估，如資產價值、資產威脅等級、威脅發生頻率與資產脆弱等級，以及其發生的機率與威脅，決定其影響的優先等級。

Step1. 使用者依已定義好的資產價值、威脅與脆弱分級，決定相對應的風險值，其決策矩陣如表 6[37]：

表 6. 風險決策矩陣

	威脅等級	低			中			高		
	脆弱性等	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Step2. 依據威脅的程度計算其對資產價值、威脅發生可能性影響，估計風險值以此做為依據決定威脅等級，其決策矩陣如表 7[37]：

表 7. 威脅等級決策矩陣

威脅種類	衝擊(資產)價	威脅發生的可能	風險值	威脅等級
威脅A	5	2	10	2
威脅B	2	4	8	3
威脅C	3	5	15	1
威脅D	1	3	3	5
威脅F	4	1	4	4
威脅F	2	4	8	3

Step3. 使用者依據事實與估計值決定對應威脅發生頻率，對應到定義好的資產威脅等級與脆弱等級，其決策矩陣如表 8[37]，其威脅發生頻率配合定義好資產等級，依據事實與估計值決定對應風險值，其決策矩陣如表 9[37]：

表 8. 威脅發生頻率決策矩陣

威脅等級	低			中			高		
脆弱性等級	低	中	高	低	中	高	低	中	高
發生頻率	0	1	2	1	2	3	2	3	4

表 9 風險值決策矩陣

資產價值	0	1	2	3	4
發生頻率					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	5
3	4	5	6	7	7
4	5	6	7	8	8

Step4. 以定義好資產等級與威脅發生頻率，依據事實與估計值決定是否可忍受該風險，其決策矩陣如表 10[37]。

表 10. 風險忍受決策矩陣

資產價值	0	1	2	3	4
發生頻率					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

(2) 定量風險分析：以計量方式分析每一項風險對企業營運影響的程度。

舉例來說，決策者取得量化的數據後，以表 11[37]中所列的風險評估係數，依數字大小進行評估分析。因此可求得[37]：

年度損失預期值(ALE) = 單一事件損失預期值(SLE)×年度

發生率(ARO)

單一事件損失預期值(SLE) = 資產價值 × 暴露因子(EF)。

觀念	衍生的公式
暴露因子(Exposure Factor / EF)	該威脅導致特定資產損失的百分比
單一事件損失預期值 (Single Lose Expectancy / SLE)	資產價值 * 暴露因子(EF)
年度發生率 (Annualized Rate of Occurrence / ARO)	該事件每年發生的頻率
年度損失預期值 (Annualized Lose Expectancy / ALE)	單一事件損失預期值(SLE) * 年度發生率(ARO)

表 11. 風險評估係數說明

4. FEMA 風險管理文件：

由 FEMA (Federal Emergency Management Agency)所出版的一系列與建築相關的風險管理指南，尤其以其中的 FEMA 433 及 FEMA 452 都有提到風險管理。

FEMA 433 考慮到自然中可能會造成的災害，幫助 user 以科學為基礎的軟件 HAZUS-MH 來製作風險評估。

HAZUS-MH 為 FEMA 開發的一套軟件，考慮風險評估的五個基本步驟如下[42]：

Step1. Identify hazards

Step2. Profile hazards

Step3. Inventory assets

Step4. Estimate losses

Step5. Consider mitigation options

下圖 6[42]為 HAZUS-MH 的風險評估流程及輸出，圖 7[42]為減少 hazard 的流程步驟[42]。FEMA433 文件中介紹了如何做用 HAZUS-MH 軟體來計算風險評估。將計算完的數值分成三個等級，並且在圖 6 中將 hazard mitigation 的制定過程列出來。而各個步驟之間的關係則如圖 7 所示。

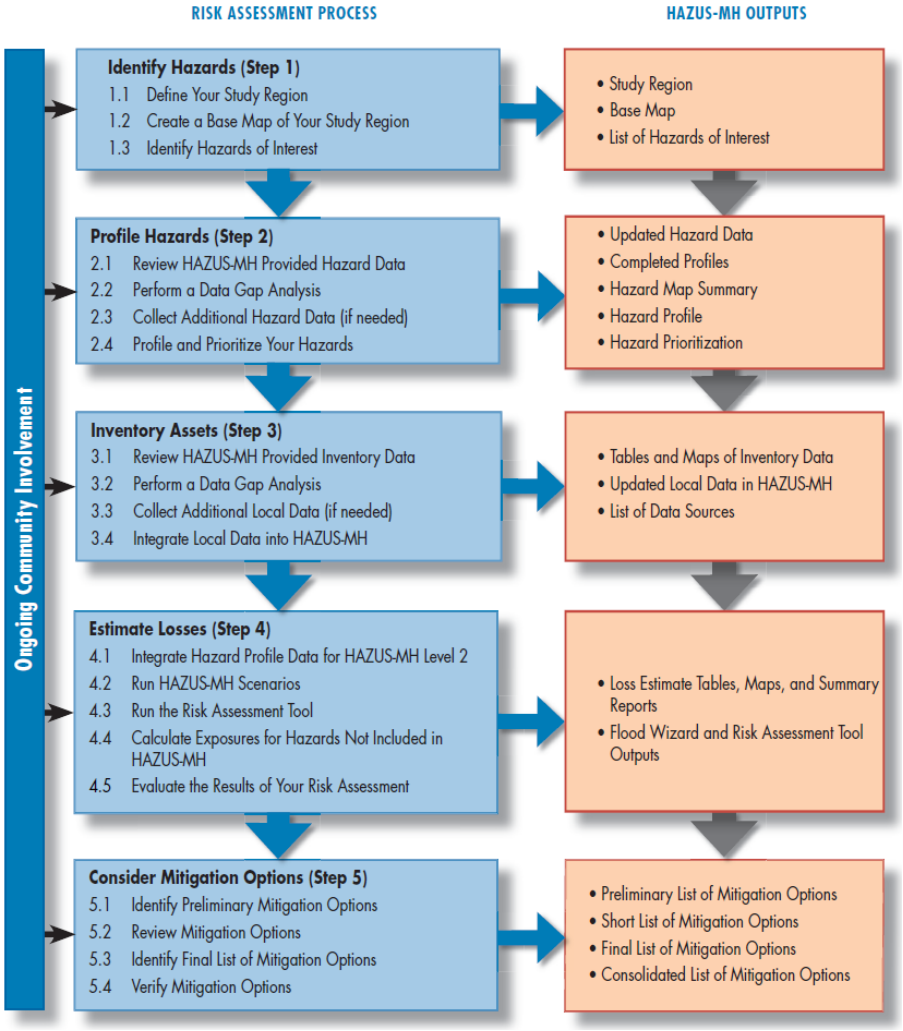


圖 6. HAZUS-MH 的風險評估流程及輸出

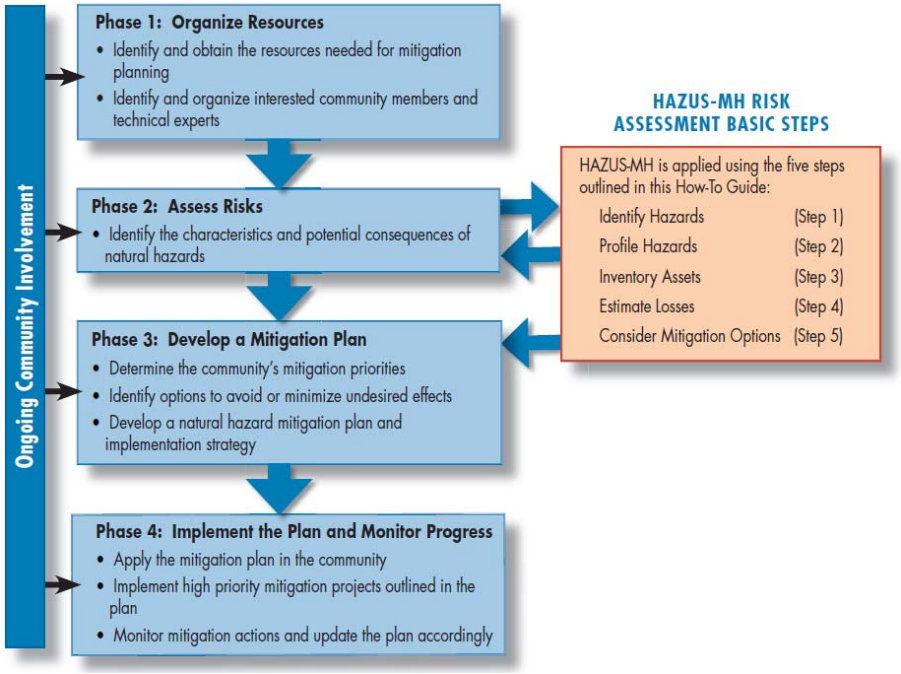


圖 7. 降低 hazards 的規畫程序

FEMA452 的文件是減少與建築及基礎相關設施相關的恐怖攻擊，因此考慮到的因素及範圍與 FEMA433 的文件有點不太一樣，各個步驟如下[43]：

Step1. Threat identification and rating

定義各個威脅及蒐集各個資訊，並決定威脅的等級。

Step2. Asset value assessment

決定 defense 的層級、定義與辯識 critical assets 及決定資產的層級。

Step3. Vulnerability assessment

利用各項依據計算出建築物的數值決定 vulnerability 的層級。

Step4. Risk assessment

利用公式 $\text{Risk} = \text{Asset Value} \times \text{Threat Rating} \times \text{Vulnerability Rating}$

計算出風險值，決定優先處理的名單。

Step5. Consider mitigation options

反覆的檢查確認 mitigation options 與成本，與 defense 的層

級。下圖 8 為各個步驟之間的關係[43]。

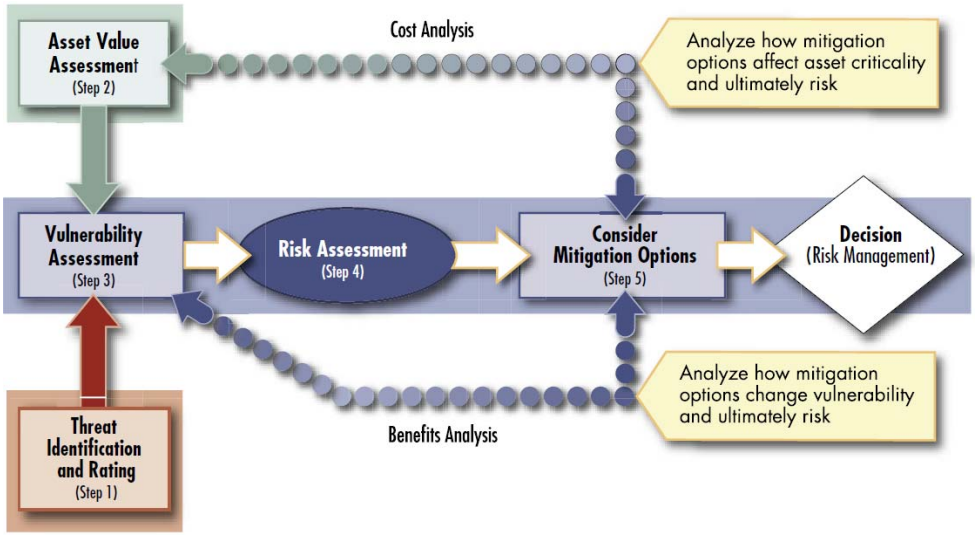


圖 8 風險評估程序模型

(四)、存取控制設計

1. 概述

在大型的系統當中，往往具備有大量各式各樣的資源，並且由各自所負責的員工來進行操作與維護，藉由分工合作的方式來完成這種系統功能，為了能夠維護系統的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，我們必須要針對每項資源做存取控制管理，只有真正需要使用到該項資源的人員，才能夠進行存取該資源，其他人員不應該任意的存取其他資源，避免對系統在成危害。除此之外，我們也可以使用存取控制來管理各種資訊，避免資訊遭到竊取或外流，例如員工的基本資料，應當只有人事主管可以完整瀏覽，其他人員不可以擅自存取其他員工的資料，以免發生帳號密碼遭到竊取的安全漏洞。

2. 存取控制模型

在目前存取控制模型當中，最常見的三種模型分別為：任意型存取控制 Discretionary Access Control

(DAC)、強制型存取控制 Mandatory Access Control (MAC)、角色基礎存取控制 Role Based Access Control (RBAC)，以下將針對這三種模型作介紹。

(1) 任意型存取控制 Discretionary Access Control (DAC)
在 DAC 存取控制模型當中，各項系統中的資源的存取控制，主要是由該資源的擁有者或管理者來制定有哪些人員可以存取該項資源，並且利用存取控制清單(Access Control List) 或存取控制矩陣(Access Control Matrix)來記錄擁有權限可以存取該項資源的人員名單。

(2) 強制型存取控制 Mandatory Access Control (MAC)
強制型存取控制模型是由系統來指定各項資源的存取權限，使用者無法任意指定或改變存取權限，由系統來記錄各項資源的存取權限於存取控制清單(Access Control List)或存取控制矩陣(Access Control Matrix)。

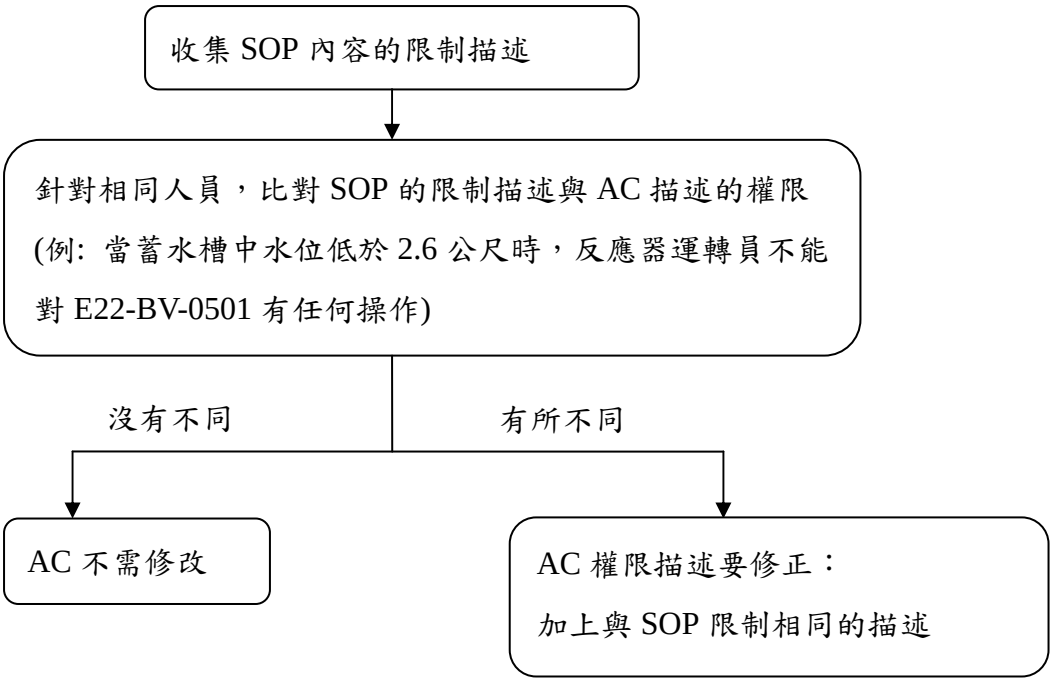
(3) 角色基礎存取控制 Role Based Access Control (RBAC)
由於在 DAC 與 MAC 模型當中，都會存在大量的存取控制清單(Access Control List) 或存取控制矩陣(Access Control Matrix)資料，每當參與系統人員有異動時，或資源的新增與移除，在管理上將會十分複雜與繁瑣，例如當我們新增了一項設備，就必須對所有員工做權限的設定，這意味著我們必須針對每一位人員的資料作新增權限的動作，當具有大量員工時，維護上將相當的耗時。因此角色基礎存取控制模型，藉由設定各種角色，並且將人員以角色來

做管理，如此一來在維護上我們只需要針對每一項角色做管理，而不必針對每份人員的資料進行操作，大幅降低操作的複雜度。

在本次的研究當中，我們發現存取控制與系統的標準作業程序(Standard Operating Procedure, SOP)有著密切的關係，彼此之間的關係將會相互影響，並且有可能造成系統發生安全性的漏洞，雖然在存取控制中的權限設定並沒有異常，並且 SOP 也沒有違法系統運作的流程，但是在兩者同時運行的情況下，將有可能造成互相干擾的情況，造成系統的安全漏洞，以下我們將舉出四種存取控制與標準作業程序發生衝突的行為，並且討論問題的解決方案。

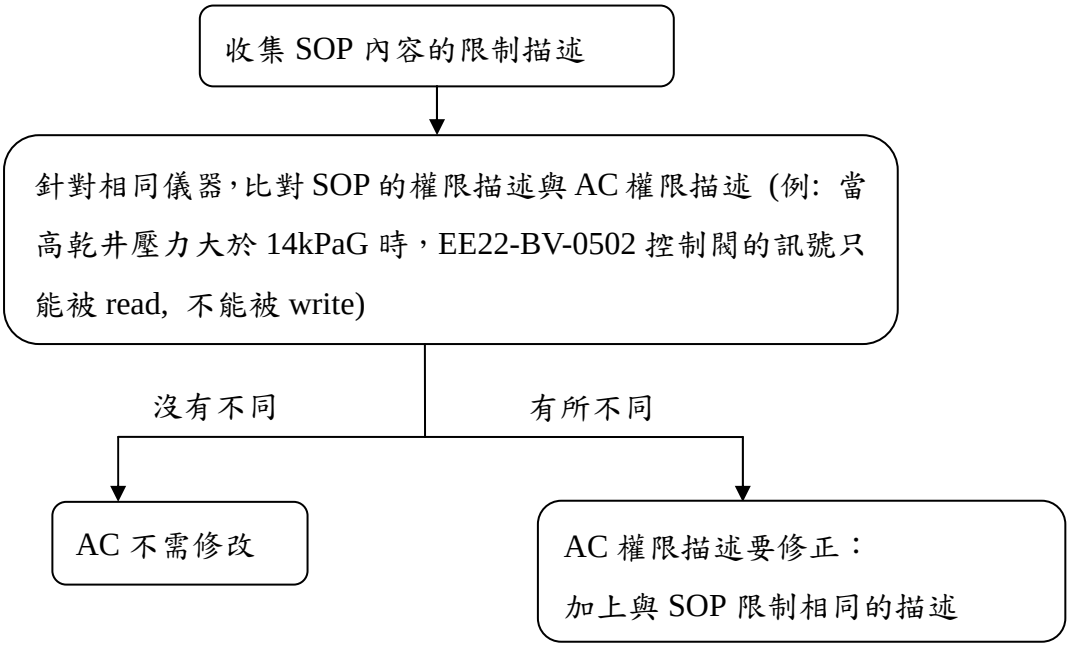
1. 存取控制設計(AC)沒有考量到 SOP 所描述的特定狀況下的權限限制。例如：在 AC 中設計反應器運轉員對 HPCF 中某控制閥 E22-BV-0501 有 open 的權限；但是在 SOP 描述中，限制了「當蓄水槽中水位低於 2.6 公尺時，反應器運轉員不能對 E22-BV-0501 有任何操作」。

發現衝突與修正存取控制之流程：



2. 不同的角色對同一儀器有相同的權限。例如：在 AC 設計裡，值班主任與反應器運轉員對 RMU 傳送來的某控制閥 EE22-BV-0502 訊號，值班主任在 VDU 上可以 read 和 write 該訊號，而反應器運轉員只能 read 該訊號。但在 SOP 中描述，限制了「當高乾井壓力大於 14kPaG 時，EE22-BV-0502 控制閥的訊號只能被 read, 不能被 write」。因此，應該讓反應器運轉員來 read EE22-BV-0502 的訊號，而不應由值班主任來執行，以免值班主任不小心 write 該訊號。

發現衝突與修正存取控制之流程：



3. 為完成 SOP 的程序，儀器的操作必須經過不同角色的權限繼承或移交才能達成。例如：在 AC 設計中只有反應器運轉員才有權限操作 open 及 close HPCF 中某控制閥 EE22-BV-0503，輔助反應器運轉員對 EE22-BV-0503 沒有任何權限。若 SOP 中描述「當蓄水槽的水位高於 7.1 公尺時，必須 close EE22-BV-0503 控制閥」。若蓄水槽的水位高於 7.1 公尺當天，恰好反應器運轉員請假，則 AC 的設計中必須正確將反應器運轉員的權限移交給輔助反應器運轉員，使得輔助反應器運轉員能在必要的時候 close EE22-BV-0503 控制閥。

發現衝突與修正存取控制之流程：

(1) 將 AC 設計中的權限轉成 SAT (Satisfiability) 問題來做正規驗證，透過驗證結果發現衝突存在：權限移交在 AC 中可以透過 COPY 這一個指令做到，將某角色(反應器運轉員)的權限 COPY 給另

一個角色(輔助反應器運轉員)。因為 COPY 將權限做了移交，就等於"輔助反應器運轉員"繼承了"反應器運轉員"的權限。當所有角色各自的權限都以 SAT formula 型態 encoding 出來時，我們可以透過 bounded model checking 的方式去驗證"輔助反應器運轉員"是否有正確繼承"反應器運轉員"的權限。如果"輔助反應器運轉員"沒有正確繼承"反應器運轉員"的權限，在我們驗證 SOP 時，就會發現 SOP 的描述，在"反應器運轉員"請假缺席時，會無法正確執行。驗證 SOP 是否能正確執行，亦可透過 model checking 做到。

(2) 修正存取控制：透過 model checking 給的反例，將反例結果反應給 AC 設計工程師，輔助工程師修正 AC，以達到正確移交權限的命令。

4. SOP 可能有「時間限制」的需要，但存取控制的設計中沒有提供時間的語意。例如：在 SOP 設計中，當 HPCS 吸水壓低於 144kPaG 超過 5 秒時，HPCF 的 pump 應該要 trip 或不啟動。在 AC 中，假設只有設定反應器運轉員有權限將 HPCF pump 啟動或關閉。如此一來，反應器運轉員對 HPCF pump 的權限，不能只照 AC 的設計來啟動或關閉，必須確定在 SOP 的條件下，尤其在有時間限制考量下，反應器運轉員必須能讓 HPCF pump 及時停止。如果只是單純驗證反應器運轉員對 HPCF pump 的權限，是無法保證可以正確執行 HPCF 的運作，但是目前 AC 的 model 沒有時間的語義。

發現衝突與修正 AC/SOP/HPCF controllers：

(1) 將 AC 設計中的權限轉成 SAT (Satisfiability) 問

題來做正規驗證，先驗證對 HPCF pump 的操作不會因為權限的設計而出錯。將 SOP 以 timed automata 來 model，透過 bounded model checker 來驗證 AC 的設計跟 SOP 的描述是否能使得 HPCF pump 系統能被正確啟動和關閉。

(2) 與其說這個 case 是 AC 和 SOP 之間的衝突，不如說這個 case 是一個非常典型而且重要的例子，明確展示出必須由 SOP 和 AC 互相補強搭配，來達到確定系統能夠正確運作。如果驗證後發現 HPCF pump 不能如 SOP 所述在條件發生時關閉，那麼就必須透過 model checking 給的反例，進一步分析錯誤是由 AC 設計錯誤所造成的，或是 HPCS 吸水壓的資訊傳送時有誤(e.g.: 計時器出錯，導致無法計時是否 PCS 吸水壓低於 144kPaG 有超過 5 秒)，或者根本是反應器運轉員沒有閉關 pump 所致…等等因素。

在核電廠裡，最大的問題經常不是外部破壞，而是內部破壞(insider sabotage)。為了防止內部破壞，一個有效的機制是二人原則(two-man rule)。在執行具潛在危險的操作(potentially hazardous operation)時或者存取危險核材(dangerous nuclear materials)時，為了防止員工單獨執行任務，核電廠會採用 two-man rule。另外，為了實行 two-man rule，經常採用的機制是職責分離(separation of duty, SOD)。SOD 主要限制兩種給定的角色(職務)不能由同一個人執行。這個限制若是事先設計時就確定，稱為靜態 SOD(static SOD, SSOD)，如果是分配角色是才確定，稱為動態 SOD (dynamic SOD, DSOD)。

二、核能電廠重要數位資產之辨識與評估

在此節中，我們將依 NRC 所述，定義何為核能電廠中的重要數位資產(Critical Digital Asset, CDA)。

(一)定義：

RG 5.71 規章中，提供一套框架(framework)可以用於辨識需要被保護的數位資產，這些資產稱為「重要數位資產」(Critical Digital Asset, CDA[8])。只要與系統安全、電腦控制安全以及緊急之預備措施(safety, security and emergency preparedness, SSEP)功能相關之資產，即為 CDA。如圖 9 所示，CDA 可以是文件、程式、資料庫等。圖 9 表示在核能系統(Nuclear System)中電腦控制安全控制(Security Control)與重要數位資產(Critical Digital Assets, CDAs)的關係圖。

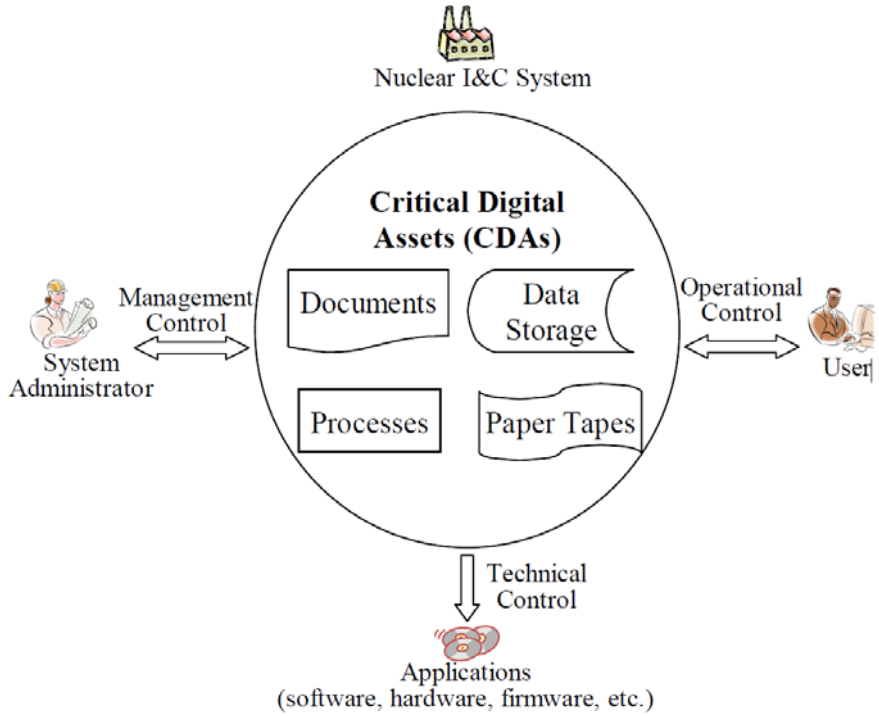


圖 9. 在核能系統中安全控制與重要數位資產

(二)辨識流程：

重要數位資產(critical digital asset, CDA)是指必須被保護不受網路異常攻擊的數位資產，它包括了：

1. 執行系統安全、電腦控制安全與緊急之預備措施的功能
2. 對於系統安全、電腦控制安全與緊急之預備措施功能或執行系統安全、電腦控制安全與緊急之預備措施功能的重要系統(critical systems)或(和)重要數位資產有不利的影響者
3. 會提供途徑使得重要系統或(和)重要數位資產違背，攻擊或降低系統安全、電腦控制安全與緊急之預備措施功能者
4. 支援重要系統或(和)重要數位資產者
5. 保護以上所述之重要系統或(和)重要數位資產免受異常攻擊者，並且包括設計基礎的威脅(design-basis threat, DBT)

圖 10 是評估是否為重要數位資產的流程[44]。這個流程結合了以上的定義，並反應了如何判斷何為重要數位資產。

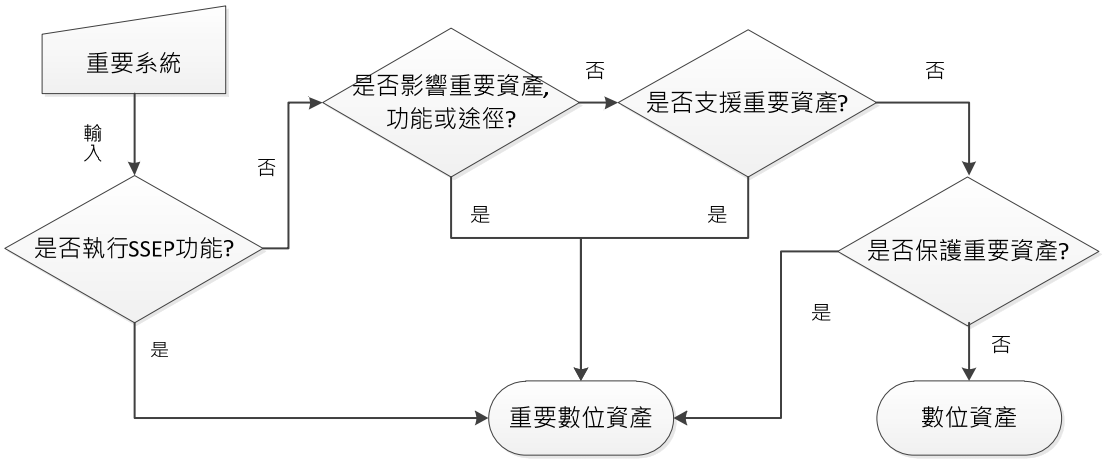


圖 10. 重要數位資產辨識流程

相較於 NRC，由於 IAEA 都是用 event 來講述核事件，對於數位

化的儀器並沒有提供明確的規範及定義，所以在 IAEA 的部份沒有找到相關 CDA 的論述或辨識方法。

我們進一步利用此 CDA 辨識流程，量化出 CDA 的價值，用以作為風險評估的參考值之一，詳細內容如下節所述。

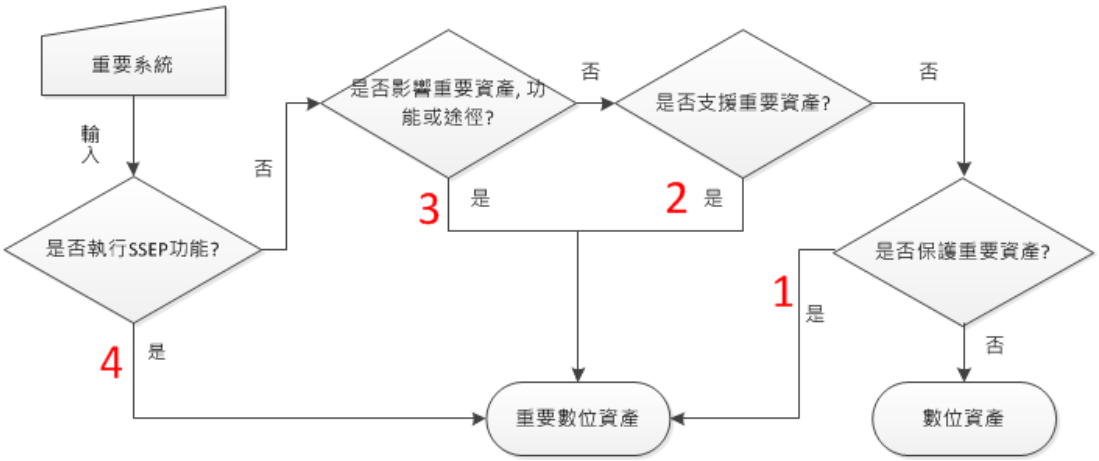


圖 11 量化重要數位資產之價值

如圖 11 所示，執行 SSEP 功能的 CDA 量化值為 4；若影響重要資產、系統功能或途徑則量化值為 3；若支持其他 CDA，則量化其價值為 2；若該元件保護其他 CDA，則量化其價值為 1。

三、系統安全暨電腦控制安全之整合風險評估方法論

在過去，系統安全與電腦控制安全，兩者之間語義上仍有差距，因此它們的風險評估方式都是分開討論的。因此，我們試圖建結系統安全與電腦控制安全的語義。據所知，我們是第一個提出整合系統安全與電腦控制安全的風險評估方法 (簡寫為 USSRAM)。此評估方法不只應用於核能電廠系統，亦可應用於其他講求電腦控制安全的系統。USSRAM 同時考量了系統安全與電腦控制安全，進而提出一套新的風險評估方法，來強調系統安全方面的風險與電腦控制安全方面的風險之關係。當系統安全與電腦控制安全之間關連性高的時候，透過我們的 USSRAM 方法分析出來的風險值也相對比該兩者關係獨立較高，顯示了此二者風險之間的相互影響力。

(一)風險評估流程

我們參考自 NIST 800-30 Risk Assessment Methodology Flowchart[45]，提出了一套新的結合同時考量系統安全與電腦控制安全的風險控制流程，如下圖 12 所示。

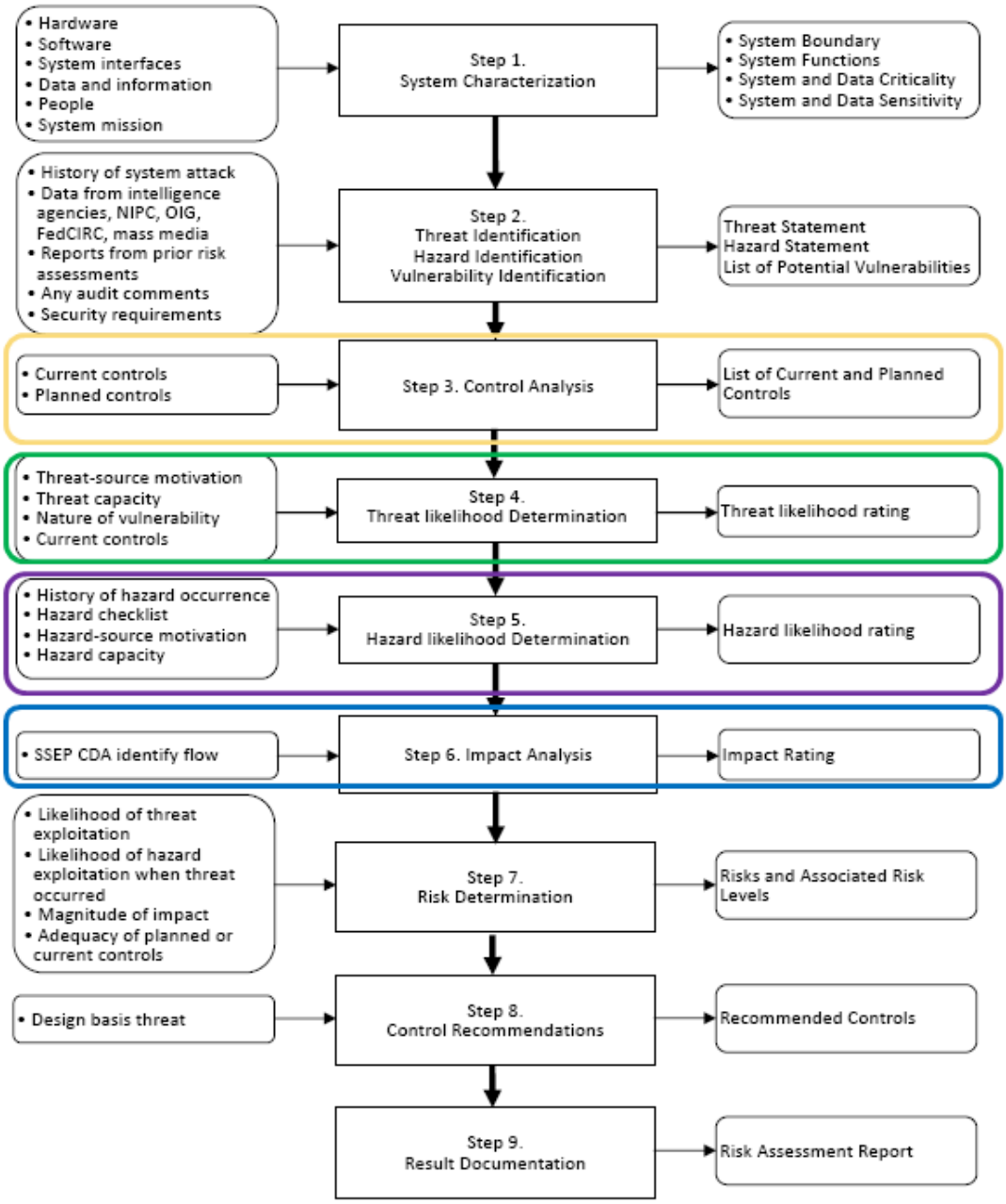


圖 12. 整合性系統安全與電腦控制安全的風險控制流程

以下針對我們提出的風險評估方法論，對步驟 3 至 6 做詳細說明。

1. Step 3：利用此控制分析，加上 security level 及 safety level 分類，所決定出該 CDA 應置於哪一層安全分層中，並得到其對應的分層數值。電腦控制安全分層(security level)[47]的依據乃依系統相關的 control 機制分類。數值

越大，代表越在外層，可能面對的風險越高，如下圖 13 所示。

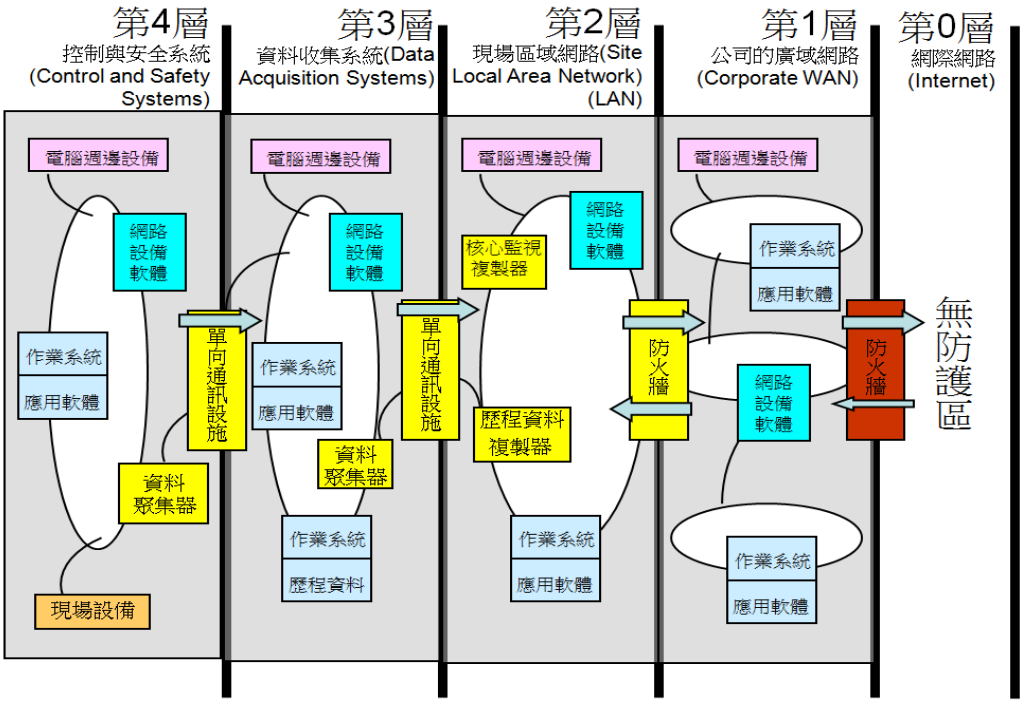


圖 13. 電腦控制安全分層

Safety Level	Objective	Essential Means
Level 0	Prevent of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 1	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 2	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 3	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 4	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

圖 14. INSAG-10 所訂之系統安全分層(Safety Control Level)

我們定義一個安全控制的參考因素 C，並定義 C 的值= Max{(5–CDA

所在之 Security Level), (5–CDA 所在之 Safety Level)}。*C* 值介於 1 到 4 之間。

2. Step 4：決定威脅(threat)發生之機率量化值，我們以 *p(t)*為記。威脅發生的機率，我們是參考自過去的歷史記錄，從記錄中去分析並認為值得成為預測未來相同威脅再發生的可能性。根據我們對同時講究系統安全及電腦控制安全的系統(safety-security critical systems) 分析得知，透過網路等方式所產生的電腦儀控風險可能會直接或間接導致系統安全的風險發生，因為對電腦控制安全可能產生的威脅，同時也可能驅使危害(hazard)的發生。

   我們將 *p(t)*值域分為四個層級：[0, 0.25), [0.25, 0.5), [0.5, 0.75), 及[0.75, 1]，分別量化為 1, 2, 3, 及 4。

3. Step 5：決定危害(hazard) 發生之機率量化值，我們以 *p(h)* 為記。與 Step 4 相似，系統危害發生的機率，我們也是參考過去的歷史資料，從中去分析並預測未來相同危害發生的可能性。並且，因為系統危害發生的機率可能是來自電腦儀控的威脅的驅使所致，所以我們可以進一步計算，在電腦控制安全的威脅發生的情況下，造成危害發生的機率有多少，這個值以條件機率 *p(h|t)*表示。

   對於講究系統安全的系統而言，危害發生的機會是微乎其微[48]，因此，我們將 *p(h)*分為四個層級：[0, 10^{-9}), [10^{-9}, 10^{-7}), [10^{-7}, 10^{-5}), 及[10^{-5}, 1][49]。而 *p(h|t)*是考量威脅發生下，危害發生的機率，重點在於了解威脅與危害之間發生的相關性。我們的風險評估方法主要就是探究這二者相關發生

時的情況下，整體風險發生的可能性，必然不致為極低才有其考量之必要。因此，我們將 *p(h|t)*值域分為四個層級：[0, 0.25], [0.25, 0.5], [0.5, 0.75], 及[0.75, 1]，分別量化為 1, 2, 3, 及 4。

4. Step 6：CDA 風險發生的衝擊影響性量化值，我們以 *I* 為記。這個部份的評估是來自於發生風險的 CDA 對電腦控制安全及系統安全的影響有多大。依據上節圖 11 所述，辨識 CDA 的流程同時也量化重要數位資產之價值，而我們合理地認為價值越高的 CDA，一旦發生風險，對整體的影響與衝擊性必然越大。因此，圖 11 同時也可用於我們量化 CDA 風險發生的衝擊影響性。*I* 值介於 1 到 4 之間。

根據以上所述，我們提出的系統安全暨電腦控制安全之整合風險評估方法論，其風險評估值為 *R(h, v, t)*，其計算公式為：*R(h, v, t) = max{min{C, I}, p(t), p(h | t)}*。其中，C 與 I 的關係量化值如下圖 15 所示：

C \ I	4	3	2	1
1	**Level 1**			
2	**Level 2**			
3	**Level 3**			
4	**Level 4**			

圖 15. *C* 和 *I* 的量化分級結果

最後，我們風險評估公式所計算出的風險值，也可以依圖 16 量化成以下四級：極度高風險(紫)，高度風險(橙)，中度風險(白)，及低度風險(藍)。

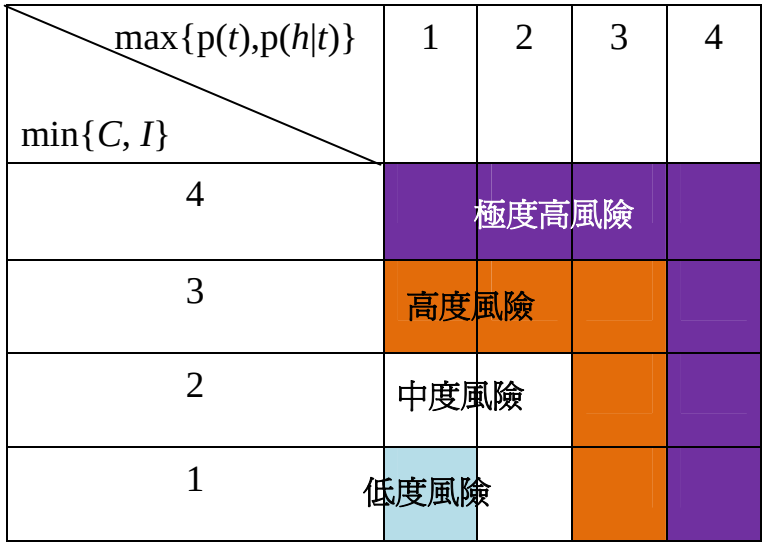


圖 16. 風險值 *R(h, v, t)分層*

對不同的風險分層，所採取的設計基準威脅策略就有所不同。例如，對於系統存在極度高風險的情況，則我們必須採取立即並嚴格的安全控制機制；對於系統存在高度風險的情況，我們可以採取嚴格的安全控制機制，但也許不必立即處理；對於系統存在中度風險的情況，我們可以採用一些監控系統來輔助監視系統是否風險危機會惡化；而對於系統在低度風險的情況，或許我們可以暫時忽略，不做任何處理。

四、風險評估模型與存取控制之整合與控制流程訂定

此節中，我們首先提出一套正規驗證存取控制設計是否安全的方法論。此方法以解 SAT 問題的角度，將存取控制的設計編碼成為 SAT 的問題，再以 SAT solver 來驗證其正確性，稱作 SAT-based security system verification (S3V) method[50]。

首先，我們先簡介此 S3V 方法：

1. 一個 framework，針對一個有限狀態的系統，驗證該系統運行時，access control design 在 security 中的正確性。
2. 正確性定義為，系統運行時，不會違反系統必須遵守的系統特性(property)。

我們使用 Protection Matrix[51]的形式，描述一個系統，在運行中欲做權限的變更時，所須遵守的規範。規範內容為權限變更前須符合的條件。圖 17 為此 S3V 方法之流程圖。

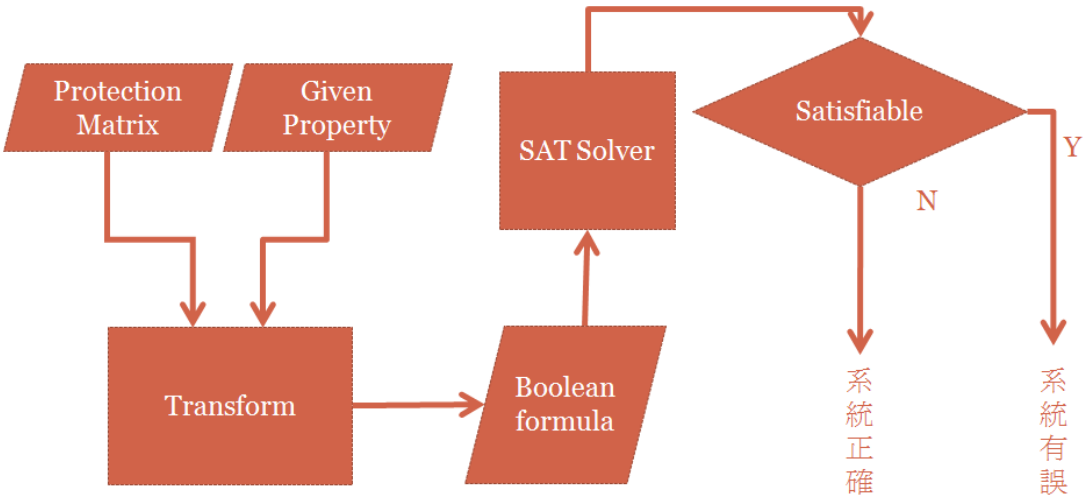


圖 17. S3V 方法之流程圖

以下我們舉例說明，如何利用我們的方法，來驗證一個 Nuclear power plant security 系統的存取控制是否為一安全設計。表 12 為 Nuclear power plant security 系統的存取控制。

表 12. Nuclear power plant security 系統的存取控制

	on	off	create	grant	take	destroy
$C_1(x,y)$	(x,x,Normal)				(y,y,Escort)	
$C_2(x,y)$	(x,x,Warning)			(y,y,Escort)		
$C_3(x,y)$	(x,x,Danger)				(y,y,Escort)	
$C_4(x,y)$	(x,x,Warning)(y,y,Escort)			(x,y,Entry)		
$C_5(x,y)$	(x,x,Warning)(y,y,Escort)				(x,y,Entry)	
$C_6(x,y)$	(x,x,Normal)			(x,x,Warning)	(x,x,Normal)	
$C_7(x,y)$	(x,x,Normal)			(x,x,Danger)	(x,x,Normal)	
$C_8(x,y)$	(x,x,Warning)			(x,x,Normal)	(x,x,Warning)	
$C_9(x,y)$	(x,x,Warning)			(x,x,Danger)	(x,x,Warning)	
$C_{10}(x,y)$	(x,x,Danger)			(x,x,Normal)	(x,x,Danger)	
$C_{11}(x,y)$	(x,x,Danger)			(x,x,Warning)	(x,x,Danger)	
$C_{12}(x,y)$	(x,x,Normal)		y			
$C_{13}(x,y)$	(x,x,Normal)					y

權限的表示與定義分述如下：

(x,x,Normal): 反應爐的狀態：正常

(x,x,Warning): 反應爐的狀態：警告

(x,x,Danger): 反應爐的狀態：危險

(y,y,Escort): 反應爐控制室的閘門的開關

(x,y,Entry): 人員是否在反應爐控制室內

以指令 1 至 11 為例，說明各指令之意義如下：

$C_1(x,y)$：反應爐狀態正常時，閘門不可通行。

$C_2(x,y)$：反應爐狀態警告時，閘門可通行。

$C_3(x,y)$：反應爐狀態危險時，閘門不可通行。

$C_4(x,y)$：反應爐狀態警告且閘門可通行時，人員進入。

$C_5(x,y)$：反應爐狀態警告且閘門可通行時，人員出來。

$C_6(x,y)$：反應爐狀態從正常變為警告。

$C_7(x,y)$：反應爐狀態從正常變為危險。

$C_8(x,y)$：反應爐狀態從警告變為正常。

$C_9(x,y)$：反應爐狀態從警告變為危險。

$C_{10}(x,y)$：反應爐狀態從危險變為正常。

$C_{11}(x,y)$：反應爐狀態從危險變為警告。

我們想驗證 NPP Security 例子的設計是否有滿足”2-man rule is safe”的特性。要滿足這樣的特性，是為了讓 NPP 的安全設計，在反應爐於危險狀態且閘門不可通行時，人員不應該在裡面。

首先，正規化描述問題：我們將驗證的問題轉換成”解 SAT 的問題”。因此，我門需要描述的問題

由以下三部份組成：

A. Init: 系統初始的狀態。

B. Commands: Protection Matrix 中描述的內容，一次執行一個。

C. Property: 系統必須遵守的系統特性。

此三部份要做 encoding 成 SAT 問題的形式。

接著將驗證問題的式子，以 SAT 形式表達為：

(Init & Commands & ! Property) = true

意即，驗證這個問題，就等同於去解轉換後的 SAT 問題。

最後，得到驗證結果為: 系統在執行五個 Command 後會違反系統特性。

A. 初始時：反應爐狀態正常，且閘門不可通行，人員不在裡面。

B. 第一步： C6(x,y) 反應爐狀態從正常轉為警告。

C. 第二步： C3(x,y) 反應爐狀態為警告時，閘門可通行。

D. 第三步： C4(x,y) 反應爐狀態警告且閘門可通行時，人員進入。

E. 第四步： C9(x,y) 反應爐狀態從警告變為危險。

F. 第五步： C3(x,y) 反應爐狀態危險時，閘門不可通行。

結果：反應爐危險請閘門不可通行時，人員在裡面。

以下圖 18 為一示意圖:

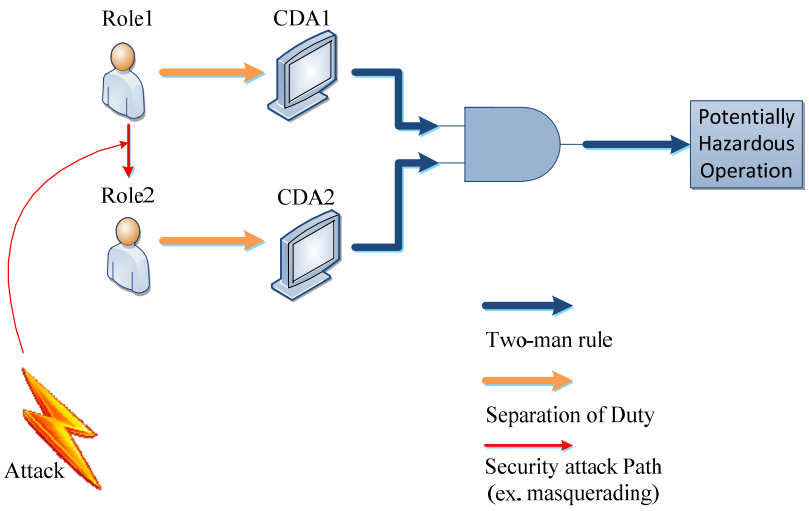


圖 18. 兩個災害同時發生的機率與電腦儀控威脅之間的關係

在核電廠中，two-man rule 是一套用於電腦控制安全監控的方法，這個方法，無論任何時候，都需要兩個經過授權的人員存在。Two-man rule 用來預防內部破壞，去禁止員工單獨在有安全上的漏洞的地點工作，以確保有潛在危險的功能無法由一位員工操作，像是觀察存取的特殊核材料。假設需存取兩個不同的 CDA 才能操作有潛在危險的功能。如圖 18 所繪，去實行 two-man rule，兩個不同的角色，Role1 和 Role2，有兩個 CDA，CDA1 和 CDA2 分別對應。不過，當使用者要成為角色時，職責分離(a separation of duty, SOD)原則必須執行，如此一來，才不會有使用者能同時有兩個角色。

在系統安全上，在隨機系統安全分析中，兩個 CDA 的同時故障通常是不可能的(罕見事件)。如果只考慮系統安全，上述的觀點是正確的。儘管如此，一旦加以考慮電腦控制安全，同時故障發生的機率也許就不是微不足道的了。以 CDA 的弱點為目標與電腦控制安全的威脅相關的攻擊，造成與 CDA 的同時故障相關的風險提高。一般的風險評估方法無法去量化，由電腦控制安全攻擊所造成的系統安全風險的增加，因為這些方法通常只有單方面的考慮電腦控制安全層面或是系統安全層面。相比之下，USSRAM 這個雙方面考慮電

腦控制安全與系統安全的方法，可以有效地評估出因為電腦控制安全攻擊所造成的系統安全風險的增加。在下章中，我們將以一例子來說明這部分。

參、主要發現與結論

在此章節中，我們將詳述各季目標之主要發現與結論。第一節針對各國際組織所提出的核能安全相關規範做比較。比較的重點在於列出各組織是否有針對系統安全(safety)，電腦控制安全(security)，設計基準威脅(DBT)，存取控制(access control)，以及深度防禦(defense in depth)等各項重點訂制定重要文件的說明。第二節以核電廠中主要的二個系統：高壓爐心注水系統(high pressure core flooder, HPCF)與反應器急停隔離功能系統(reactor trip and isolation functions, RTIF)，利用重要數位資產(CDA)辨識流程，辨識出此二大系統中各自重要的 CDAs 為何。第三節進一步針對此二大重要系統，依據我們提出的整合性風險評估方法，評估出這二個系統的風險值。最後，第四節提出整合存取控制與風險評估，進一步提出有效的安全控制流程。

一、各國際組織核之核能安全規章比較

依第二章所述之各國際組織所提出的規範，我們整理出各組織，依據系統安全(safety)，電腦控制安全(security)，設計基準威脅(DBT)，存取控制(access control)，以及深度防禦(defense in depth)各項，所訂定之文件編號。如下表 13. 核能國際組織所提之各文件彙整所示。

表 13. 核能國際組織所提之各文件彙整

	NRC	IAEA	NEI	NIST
Safety	RG 1.109 RG 1.21 RG 1.143 等	Safety Series	NEI 99-01 NEI 09-07 NEI 07-01 等	SP 800-30

Security	RG 5.71	Security Series	NEI 08-09 NEI 04-04	SP 800-30 SP 800-53 SP 800-82
DBT	10 CFR 73.1	Security Series #10	NEI 10-05 NEI 03-12 NEI 03-09	SP 800-53 SP 800-82
Access Control	10 CFR part 36 10 CFR part 20	INFCIR/225/ Rev.4	NEI 08-09 NEI 07-03A	SP 800-53
Defense in Depth	RG 5.71&安全相關法規	INSAG Series #10	NEI 08-09	SP 800-27 SP 800-39 SP 800-53

二、HPCF 與 RTIF 之重要數位資產辨識成果

(一) HPCF CDA 辨識結果

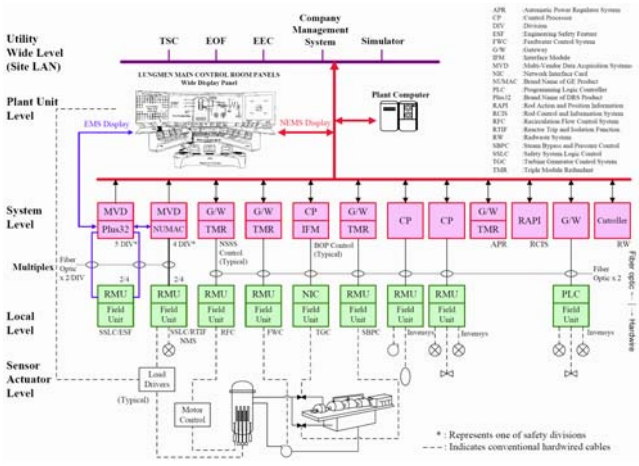


圖 19. 龍門核電廠以 ABWR 為基礎的通訊架構

HPCF 的安全功能如下：

1. 小管路斷裂後，高壓爐心灌水系統當作反應爐爐心隔離冷卻系統之後備，維持反應爐水量。

2. 在設計基準事故下，高壓爐心灌水系統跟隨其他緊急爐心冷卻系統提供冷卻水至反應爐。
3. 提供一次圍阻體隔離。
4. 維持反應爐冷卻水壓力邊界之完整性。

HPCF 系統其他功能包括在飼水喪失暫態時,高壓爐心灌水系統當作反應爐爐心隔離冷卻系統之後備，注水入反應爐，以恢復正常水位。HPCF 中有二個功能相同的迴路，HPCF 的泵會在冷凝水槽(CST)或後備水槽取水，其出口管路有最小流量，流量試驗及注水管路，管閥操作電源是由固定的電壓和頻率提供，有後備電源。運轉 HPCF 時，主要有三個模式(mode)：

1. 備用狀態模式(Standby Mode)
2. 全流量測試模式 (Full Flow Test Mode)
3. 高壓灌水模式(High Pressure Flooder Mode)

依照 CDA 辨識流程可知 HPCF 的 CDA 有: VDU、RMU、SSLC 與 Hard I/O (Sensor)

參照圖 11 (CDA 價值)，HPCF 的 CDA 中，價值量化為四的元件有：

(1). SSLC：有可控制的 trip logic，與 SSEP 的容錯功能相關。
(2). VDU:有可控制閥開關的按鈕,以執行 SSEP 功能。
(3). RMU：訊號的傳輸和控制。

HPCF 的 CDA 中價值量化為三的元件有：

(1). Hard I/O：感測資料。

(二) RTIF CDA 辨識結果

RTIF 的安全功能是為了讓反應爐保護功能(Reactor Protection System RPS)在發現異狀時，能準確又可靠地將反應爐急停。反應爐壓力過高，或水位過低，或管閥開關異常等等，都會導致 RTIF 反應爐保護系統動作。

RFIT 系統的主要元件有 5 項：

1. 感測器(Sensors)：每一控道均有自己的感測器以偵測重要之運轉參數，並將所感測到的訊號送到”數位跳脫模組”(DTM)。
2. 遠端多工訊號傳輸單元(Remote Multiplexing Unit RMU)：感測器的訊號是藉遠端多工訊號傳輸單元(RMU)或硬接線(Hardwire)傳送到 DTM。
    (1). RMU 傳送：反應爐壓力、反應爐水位、乾井壓力、控制棒驅動液壓控制單元充水集管液壓、抑壓池溫度與地震等。
    (2). Hardwire 傳送：主蒸汽隔離閥、汽機關斷閥、汽機控制閥、汽機旁通閥等。
3. 數位跳脫模組(Digital Trip Module DTM)： DTM 是屬於 SSLC(安全系統邏輯控制)之一部份。其主要功能是將感測器所送來之訊號與預設之設定值作一比較。
4. 跳脫邏輯單元(Trip logic unit TLU)：TLU 也是屬於 SSLC 之一部份。其主要功能是將由四個支控道 DTM 所送來之跳脫訊號、作一個四選二之“票

決”(Voting)，將送出跳脫訊號經由 OLU (Output Logic Unit)送到反應器保護系統。

5. 通訊介面模組(Communication Interface Module CIM)：提供低頻寬之資料傳輸。

參照圖 11 (CDA 價值)，RTIF 的 CDA 中，價值量化為 4 的元件有：

(1). RMU：工作為傳輸訊號及訊號控制器。

(2). RTIF 的 CDA 中，價值量化為 3 的元件有：

A. DTM：可以將收集來的資料與設定值做比較，防止不正常的運作。

B. TLU:將跳脫訊號送出到 RPS 的動作器。

C. Sensor：傳送資料，確保系統運作正常。

(3). CIM：提供資料的傳輸，確保系統運作正常。

三、 HPCF 與 RTIF 之風險評估

在系統安全與電腦控制安全兩個領域中，各自有一套風險評估方法，但評估系統安全上的風險時，往往不會去考慮在電腦控制安全上的問題，評估電腦控制安全上的風險時亦然。因此，我們提出一套風險評估方法，該方法不只考慮系統安全上的問題，另外還考慮電腦控制安全上的法則，最後經由系統安全與電腦控制安全之間的關聯性來連結，藉此反映出 CDA 在系統中潛在的危害大小。

在上一章節當中，提出了我們提出的理論方法與過程，在這一章節當中，參考了美國先進的壓水式反應爐(Advanced Pressurized Water Reactor, APWR)的核能發電廠(Nuclear Power Plants, NPP)，以及台灣龍門發電廠的先進的沸水式反應爐(Advanced Boiling Water Reactor, ABWR)。無論是哪種

型式的反應爐，都可以套用我們所提出的模型來做風險評估。以下舉兩個與核能發電廠相關的系統做為例子，一個是 ABWR NPP 中的高壓爐心注水系統(High Pressure Core Flooder, HPCF)的例子，另一個則是 ABWR NPP 中的反應器跳脫隔離功能(Reactor Trip and Isolation Function, RTIF)的例子。

(一)ABWR NPP 中的 HPCF

核能發電廠中有許多的冷卻系統，HPCF 是重要冷卻系統的其中之一，我們將會把焦點放在 USSRAM 如何估算 HPCF 系統裡結合電腦控制安全與系統安全的風險層級。然而，在詳細介紹細節之前，必須先描述該系統在核能發電廠的網路架構與組織，以確保 USSRAM 的每一個步驟都可以正確的被執行。

1. HPCF 系統通訊架構

HPCF 系統是核能發電廠裡重要的冷卻系統。當反應爐的溫度高於正常值時，HPCF 系統將會藉由自動或手動的方式來降低反應爐的溫度，如此可以有效地避免反應爐核心熔毀或降低意外事故的發生。在 HPCF 系統裡有兩套功能相同的迴路，每一套迴路都包含一個溢水管、一個幫浦以及三個流動控制閥。溢水管允許用來冷卻的水進入反應爐；幫浦用來驅動冷卻用的水從凝結水儲存槽(Condensate Storage Tank , CST)流向反應爐；而三個控制閥個別都有著不同的目標，例如保證冷卻水維持最小流量或控制溢水管的開關等。上述的各元件都有各自的感測器來監控各元件的運作，稱做 Hard I/O，除了上述的元件之外，其他的元件亦有 Hard I/O 來做不同的用途，例如測量溫度或收集反應爐的資訊。

(1) HPCF 系統的架構

HPCF 系統由四個主要的元件所組成：Hard I/O，遠端多工單元(Remote Multiplexing Unit, RMU)，安全系統邏輯控制(Safety System Logic and Control, SSLC)與視訊顯示單元(Visual Display Unit, VDU)，圖 HPCF 系統的資料流程。Hard I/O 元件位於接近反應爐的地方，用來偵測反應爐的溫度、閥的狀態以及偵測管線內水的流動量，而在每組監控的元件當中，包含四個做相同功能的 Hard I/O 為一組，此容錯票決機制可以確保從目標收集來的資料都可以正確無誤。RMU 為資料與控制傳輸線的機櫃，從各個 Hard I/O 設備蒐集資訊，再將這些資訊傳輸到 SSLC。SSLC 使用四選二的容錯票決機制，以確保從 Hard I/O 蒐集來的資訊在往上傳遞時的完整性，此票決機制的做法為比較四筆蒐集來的資料，然後從每組 Hard I/O 選出兩筆記錄，允許兩個訊號的偵測錯誤。票決完成後，正確的訊息就會被送到 VDU 控制器並顯示出來，將核能發電廠的各個元件的狀態提供給操作人員參考。

圖 20. HPCF 系統由下往上傳遞的資料流程

(2) 通訊架構與電腦控制安全議題

龍門核電廠的 I&C 架構如圖 19 所示，其架構分為五個層級，包括 sensor/ actuator、local、system、plant unit 和 utility-wide 層級。來自發電廠的感測器和驅動裝置的信號經由硬體會被發送到 local 層級裡的 RMU。將訊號數位化及編

碼，然後經由 system 層級的 Multiplexing System (MUX)的冗餘 fiber-optic 電纜，將訊號送到位於 plant unit 層級的主控制室(Main Control Room, MCR)。與 APWR 系統架構不同的是，ABWR 有明確的將系統安全和非系統安全的傳輸數據分開。系統安全的數據會經由 Essential Multiplexing System (EMS)傳輸，而非系統安全的數據會經由 non-EMS (NEMS)傳輸。EMS 使用週期為 20 ms 的 deterministic communication protocol。NEMS 使用頻寬為 1 Gbps 的快速 Ethernet Nodebus 架構為骨幹和一個全雙工的網路協議。

在 ABWR 式的核電廠，安全相關的系統與非安全相關的系統，都會連到主控室中的電腦；然而，它們其實是分屬不同的網路系統：EMS 及 NEMS。然而，還必須注意在重要系統安全的容錯功能系統裡的電腦控制安全攻擊，遠比傳統的網路系統更有侵略性。由於容錯系統有多個相同的數據傳輸的安全性，如偽裝需要數據傳輸的所有不同的副本攻擊路徑。例如：在核能發電廠的 I&C，有多個系統安全的 VDU 序列傳輸 A 到 D 的訊號，而攻擊因此可以偽裝成四個不同的來源訊號序列。如果不採取足夠的電腦控制安全保護，攻擊可以很容易被發現，假的數據將被丟棄。

2. 在 EMS 發生電腦儀控安全攻擊與 VDU 開/關失敗的系統安全危機

在這個例子當中，我們將焦點放在電腦控制安全方面的攻擊在 EMS 如何導致閥故障產生危險，尤其是 MBV-0001B。圖 21 說明了 HPCF 系統裡的部份故障樹(fault tree)，其中幾個原因造成閥故障的可能

性。

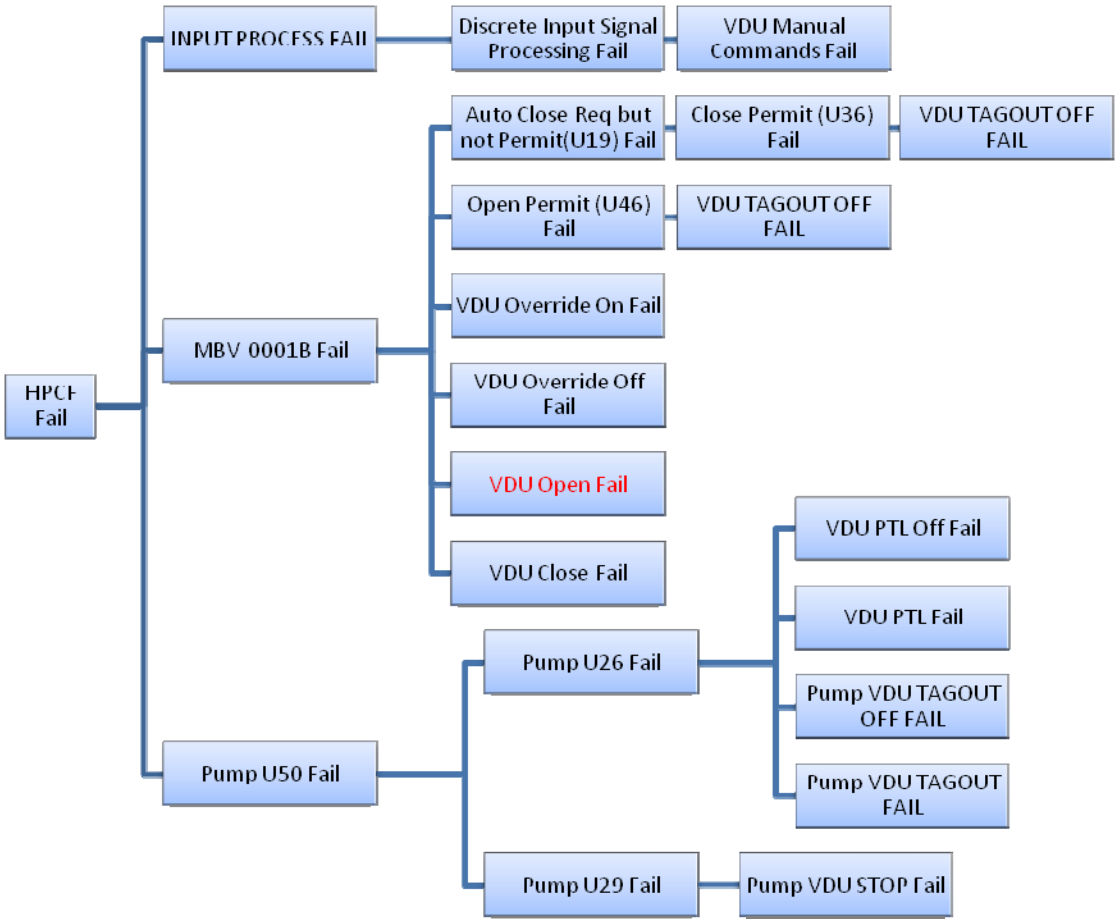


圖 21. HPCF 系統裡的部份故障樹 fault tree

我們重點是將 VDU 打開/關閉失敗的危險，有幾種不同的起始事件可能引發危險，因此，我們的目的就是展示電腦控制安全相關的攻擊如何造成這種危險。

(1) 在 EMS 上受到電腦控制安全方面的攻擊

一個與系統安全相關的 VDU 電腦可能會因為 EMS 網路上與系統安全相關的資料被截取，而使其操作受到波及。可能訊號偽裝成與系統安全相關的 VDU 控制台操作，如打開或關閉閥

門,特別是故障樹所示的MBV-0001B。由於EMS所屬的組件不會去驗證訊號發射器的真實性，ESF 序列將無法檢測到哪個是假的訊號。

(2) VDU 開啟錯誤的危險

由於一些緊急的突發事件，如反應爐異常高溫，必須打開閥門，VDU 控制台的操作員可以手動按 VDU 上相關的開關，從而打開閥門。然而,駭客可以立即發出類似的 HPCF 驅動訊號關閉閥門。實際上，這可能造成 VDU 打開錯誤失敗的危險，因為操作員會認為閥門不能打開，並可能嘗試採取更激烈的措施如關閉反應爐來伐替冷卻的動作，因此，EMS 電腦控制安全攻擊 VDU 引起打開錯誤的危險。

3. 引用 USSRAM 到 HPCF 系統

採用我們提出的 USSRAM 方法，以評估結合電腦控制安全與系統安全的風險層級到 HPCF 系統。以下將說明我們如何計算。然後將藉由我們的傳統方法所得到的結果與在 HPCF 系統裡獨立地評估電腦控制安全與和統安全的風險層級的結果做個比較。由於在這個 HPCF 的例子中使用的步驟和概念是不一定在 HPCF 系統才可運作，我們所提出的步驟與概念可以很容易地轉換成其他任何 NPP 的 CDA。此外，由於我們提出的概念不只是針對核能發電廠，還可以延伸到其他電腦控制安全與系統安全相關的重要系統，如航空電子設備、醫療設備和運輸。

Step 1. 我們將目標放在 HPCF 的重要系統安全系統，也就是連接到 EMS。

Step 2. 依照上一章節所定義描述的方式，辨識出有

哪些與 HPCF 系統相關的威脅、危險及弱點。尤其是，要辨識出偽裝成 HPCF 驅動訊號的威脅，以及像 VDU 開啟失敗的危險，在 HPCF 系統具體的辨識弱點。由於 EMS 網路架構和特定的通訊協定非常簡單，缺乏來源認證，因此容易使 HPCF 的驅動訊號被偽裝。

Step 3. 對 VDU 的電腦控制安全的控制層級與系統安全控制層級分別為 4 跟 3。因此，電腦控制安全與系統安全的控制層級 C 為 max (5－4, 5－3) = 2。

Step 4. 根據歷史記錄的資料，在 EMS 偽裝成 HPCF 的驅動訊號的這種威脅 t 的機率 p(t)算出來為 0.43，其落在第 2 區間。這是基於假冒的內容有可能在 IT 系統[56]中被發現的機率(43%)。

Step 5. 危險 h 發生與 VDU 打開/關閉失敗相關可能性機率遠小於 10^{-9}，這意味著 p(t)落在第 1 區間。然而，在威脅 t 已經發生的情況下危險 h 也發生的條件機率是非常高的，因為在威脅 t (在 EMS 偽裝 HPCF 的驅動訊號)與危險 h(VDU 的打開/關閉錯誤)有直接的相關性。因此，條件機率 P(h|t)落在第 4 區間。

Step 6. 重要數位資產 VDU 的影響值確定是 4，因為 VDU 開關可用於控制閥門、幫浦以及其他用來執行電腦控制安全、系統安全和緊急之預備措施(SSEP)功能的組件。

Step 7. 合併 HPCF 相關的重要數位資產 VDU 的電腦控制安全與系統安全的風險層級的計算公式如下。Level(C, I) = min{2, 4} = 2，level(p(t), p(h|t)) = max{2, 4} = 4，因此風險層級 *R(h, v, t)*取其最大值 max{2, 4} = 4，也因此定義這個系統為重

要的。

由於落在重要的風險層級，建議需採取對應的對策以修正有關的情況。例如在設計時就應該要防止偽裝的訊號，不是限制訊號源就是執行網路分段。

4. 獨立的風險評估

現在，讓我們比較 USSRAM 的風險評估層級與傳統的評估方法，也就是將電腦控制安全[40]和系統安全[57]風險層級分開討論。在這裡，我們需要分別的給定電腦控制安全與系統安全威脅與危險在重要數位資產 VDU 所帶來的影響。由於 VDU 主要是負責系統安全功能，因此其系統安全性的影響是非常高的。我們認為系統安全的影響值應落在第 4 區間。然而，由於 VDU 不負責電腦控制安全，我們估計電腦控制安全的影響將會相當低，我們假設其影響應落在第 2 區間。因此，我們得到以下的電腦控制安全與系統安全的控制層級。

$$R(t) = C \times p(t) \times I = 1 \times 4 \times 2 = 8$$

$$R(h) = C \times p(h) \times I = 2 \times 1 \times 4 = 8$$

因此，我們可以觀察到獨立的風險層級是相當低的。

5. 比較與結論

從以上的幾個小節當中，我們可以觀察到 USSRAM 結合電腦控制安全與系統安全所估算出來的風險層級是重要的，而按照傳統方法分開計算電腦控制安全與系統安全所得到的風險層級都很低。我們提出的 USSRAM 將建議系統設計人員應立即採取一些增強電腦控制安全與系統安全的控制機

制，以降低風險。然而，在傳統的方法裡，最高的風險評估值應該為 4 × 4 × 4 = 64。分開計算電腦控制安全與系統安全的風險評估值的話只有 8，是不可能被分類至最高風險級別的。換句話說，如果將電腦控制安全與系統安全的風險評估方法分開的話，將獲得低風險層級的 CDA，然後給予低風險層級不會有嚴格的建議對策，以增進 CDA 的電腦控制安全與系統安全。即使我們計算了個別的風險層級，我們得到 max{8, 8} = 8，這仍然是相當低的。這表示，分開計算風險值並合併到最大估計值的情況明顯低於實際相結合的風險層級。此結果表明提出的 USSRAM 方法的需要性，可以提供更準確的風險估計。

(二)ABWR NPP 中的 RTIF

RTIF 在核能發電廠裡是一個重要的系統安全功能。這裡，我們將重點放在電腦控制安全的威脅如何影響 RTIF，以及如何將 USSRAM 用於評估相關的風險，並提供適當的建議。首先，我們將描述 RTIF 的架構以及龍門發電廠基於 ABWR 的架構和數據通訊架構。

1. RTIF 系統及通訊架構

RTIF 是 SSLC 的一部份，負責反應爐的系統安全。RTIF 由四個部份組成，分別為獨立和冗餘保護的邏輯系統框架，自動跳脫和隔離功能的結果。

(1) RTIF 系統由兩部分組成，即為反應爐保護系統 (RPS) 和主蒸汽管道隔離系統閥門 (MSIVs)。RTIF 主要功能是執行 RPS，這是一

個與系統安全相關的制度和設計，提供自動或手動啟動反應爐跳脫，同時對單一故障造成的的不必要跳脫結果維持保護能力。在 RPS 系統冗餘感測器頻道之行程的決策邏輯和冗餘的四選二跳脫系統輸出跳脫邏輯。

RTIF 系統主要由感測器、RMU、數位跳脫模組(DTM)、跳脫邏輯單元(TLU)，通訊介面模組(CIM)組成。這些 RTIF 的組成元件之間的數據流程如下圖 22 所示。感測器用於收集反應爐的數位以及類比訊號的資訊，藉由硬線傳送到 RMU，然後送到 DTM 進行比較和容錯。無論有無跳脫訊號，資訊會傳送到 TLU 四選二的機制進行表決。最後，數據經由 CIM 與其他 SSLC 的元件送到 VDU 的系統安全。

圖 22. RTIF 的資料流程

2. Redundant ring 網路電腦控制安全攻擊與 watchdog 系統安全危險：在這個例子中，我們將重點放在 RTIF 的電腦控制安全如何攻擊會在 watchdog 造成系統安全的危險。圖 23 說明了 RTIF 的部份故障樹，watchdog 的系統安全危險可能是其幾個原因之一。在這個例子中，我們重點放在計時器不能重置的危險。有幾種不同的起始事件可能引發這種危險。在這裡，我們的目標是展示電腦控制安全如何攻擊這種危險的可能起始事件之一。

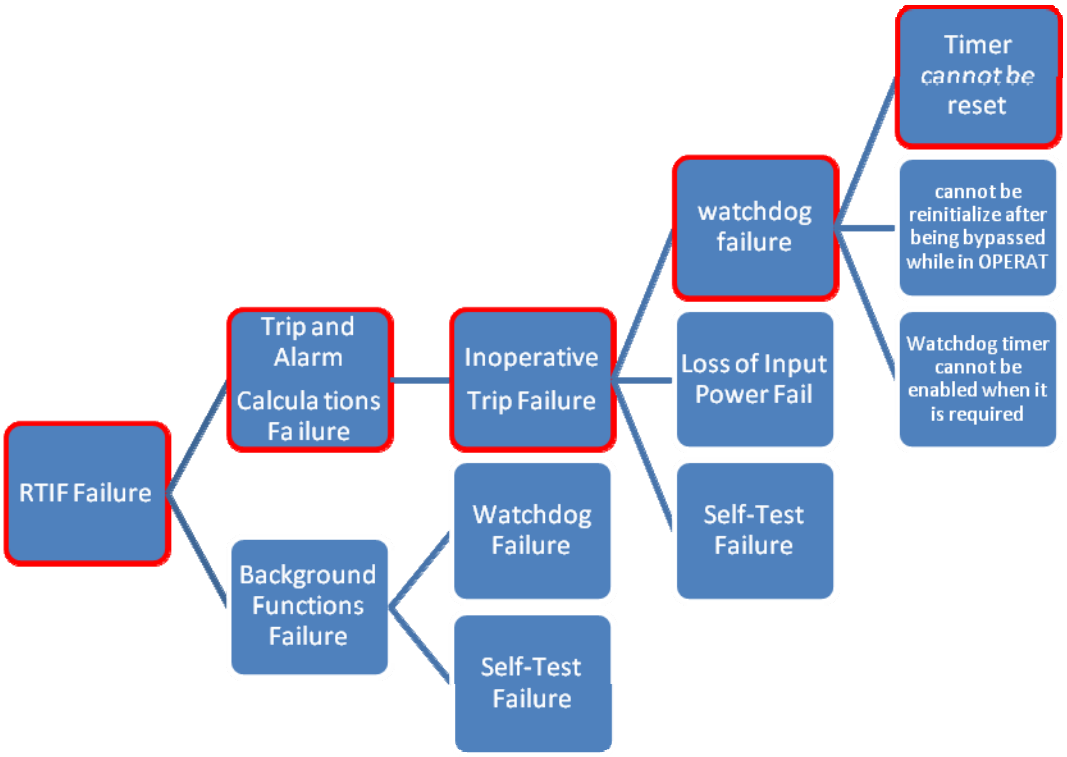


圖 23. RTIF 失效的部份故障樹

(1) 在 redundant ring 網路的電腦控制安全攻擊

ABWR 架構的不同層級裡， RTIF 的不同元件即感測器、RMU、DTM、TLU 和 CIM，實際上是由 redundant ring 網路連接，如圖 24 所示。EMS 和 NEMS 的部分是藉由與系統安全相關的網路 redundant ring 和非系統安全相關的網路 redundant ring 來實施。萬一開關故障的情況下，在 200ms 內網路重新配置完成和網路分段 (redundant network switch pair) 確保工廠持續的運作。

維護 local display unit (LDU)電腦可能會被危害在 redundant ring 發覺與系統安全相關的數

據後，它可以攻擊其元件之一，RMU 以及設置比能夠接受的時間間隔還短的 watchdog timeout。

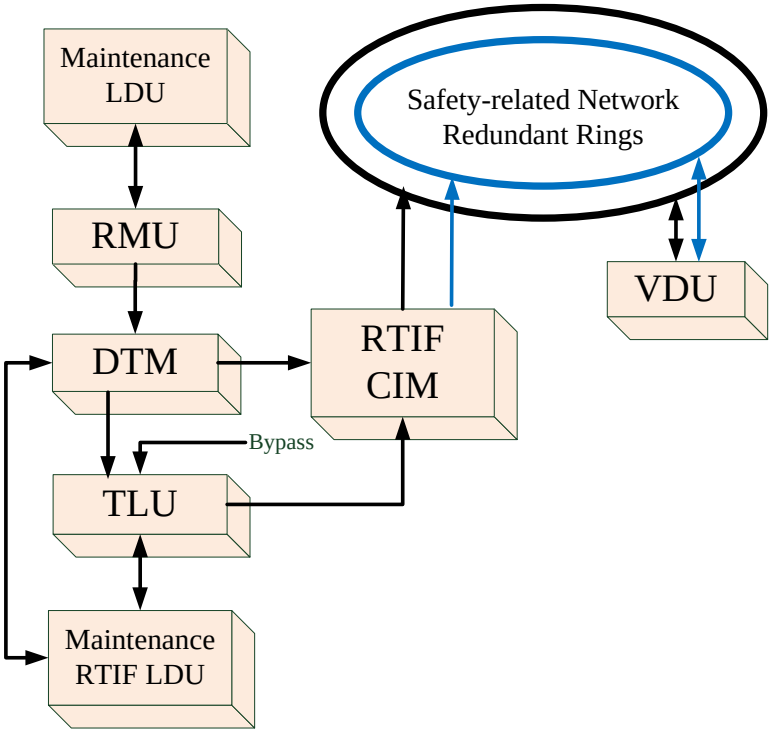


圖 24. RTIF 的通訊架構

(2) Watchdog 的系統安全危險

每個 RTIF 的組成元件，包含 RMU、DTM、TLU 及 CIM，其 watchdog 的任務為負責計算任務的時間片段、計算任務延遲時間、任務監控及抑制 watchdog 重置。一般都是採用 watchdog 重置或軟體故障期間禁用重要的系統安全系統。Watchdog times out 時 recovery procedures 會被啟動。

通常都假設 watchdog 是不能被篡改的。然而，在實際設計上重要的系統安全是沒有確保 watchdog 防止被篡改的[59][60]。

因此，在 LDU 的惡意程式，實際上可以篡

改在任何連接到 LDU 組件的 watchdog。因此，這種攻擊會導致 watchdog 無法被重置。整體結果將使 RTIF 停止正常運行。

3. 引用 USSRAM 到 RTIF 系統

由於在前面的例子中，我們已經詳細介紹了 USSRAM 如何被應用到 HPCF，在這裡我們將重點只放在應用程序的結果。

Step 1. RMU 的電腦控制安全的控制層級與系統安全的控制層級分別為 3 跟 2。因此，電腦控制安全與系統安全的控制層級 C 為 max (5－3, 5－2) = 3。

Step 2. 根據歷史記錄的資料，與 watchdog 被篡改相關的威脅 t 的機率 p(t)算出來為 0.1，其落在第 1 區間。這是在 IT 系統[56]中被發現的機率(10%)。

Step 3. 危險 h 發生與 RMU watchdog 故障的可能性機率遠小於 10^{-9}，這意味著 p(t)落在第 1 區間。然而，在威脅 t 已經發生的情況下危險 h 也發生的條件機率是非常高的，因為在威脅 t(watchdog 被篡改)與危險 h(watchdog 故障)有直接的相關性。因此，條件機率 P(h| t)落在第 4 區間。

Step 4. 重要數位資產 RMU 的影響值確定是 3，因為 RMU 是用來數位化、編碼和傳輸與系統安全相關的數據，從而影響重要的系統/功能和途徑。

Step 5. 合併 RTIF 相關的重要數位資產 RMU 的電腦控制安全與系統安全的風險層級的計算公式如下。level(C, I) = min{3, 3} = 3，level(p(t), p(h| t)) = max{1, 4} = 4，因此風險層級 *R(h, v, t)*取其最大值 max{3, 4} = 4，也因此定義這個系統為重要的。

由於落在重要的風險層級，建議需採取對應的對策以防止 watchdog 被篡改。例如 watchdog 應隱藏和複製，以確保其可用性[59]。

4. 獨立的風險評估

讓我們比較 USSRAM 的風險評估層級與傳統的評估方法，也就是將電腦控制安全[40]和系統安全[57]風險層級分開討論。在這裡，我們需要分別的給定電腦控制安全與系統安全威脅與危險在重要數位資產 RMU 所帶來的影響。由於 RMU 主要是負責系統安全的相關功能，因此其系統安全性的影響是中等。我們認為系統安全的影響值應落在第 3 區間。然而，由於 RMU 不負責電腦控制安全功能，我們估計電腦控制安全的影響將會相當低，我們假設其影響應落在第 2 區間。因此，我們得到以下的電腦控制安全與系統安全的控制層級。

$$R(t) = C \times p(t) \times I = 2 \times 1 \times 2 = 4$$

$$R(h) = C \times p(h) \times I = 3 \times 1 \times 3 = 9$$

因此，我們可以觀察到獨立的風險層級是相當低的。

5. 比較與結論

從以上的幾個小節當中，我們可以觀察到 USSRAM 結合電腦控制安全與系統安全所估算出來的風險層級是重要的，而按照傳統方法分開計算電腦控制安全與系統安全所得到的風險層級都很低。我們提出的 USSRAM 將建議系統設計人員應立即採取一些增強電腦控制安全與系統安全的控制機制，以降低風險。然而，在傳統的方法裡，最高的

風險評估值應該為 4 × 4 × 4 = 64。分開計算電腦控制安全與系統安全的風險評估值的話只有 4 跟 9，是不可能被分類至最高風險級別的。換句話說，如果將電腦控制安全與系統安全的風險評估方法分開的話，將獲得低風險層級的 CDA，然後給予低風險層級不會有嚴格的建議對策，以增進 CDA 的電腦控制安全與系統安全。這表示分開計算風險值並合併到最大估計值的情況明顯低於實際相結合的風險層級。此結果表明提出的 USSRAM 方法的需要性，可以提供更準確的風險估計。

四、整合存取控制與風險評估及有效安全控制流程

假設一個潛在的危險功能(potentially hazardous operation, PHO)只有在 two-man rule 的規範下才能操作，此時採用了兩個 CDA，分別命名為 CDA1 與 CDA2。進一步的，兩個 CDA 對應著兩個角色(Role)，Role1 對應 CDA1，Role2 對應 CDA2。給定的存取控制規範指定了 Role1 和 Role2 須遵守 separation of duty (SOD)原則。再者，假設可能有網路層面的偽裝攻擊會發生，偽裝攻擊的內容為某使用者成為 Role1 後，再去假冒 Role2。因此，SOD 原則就被違反了，這也違反了 two-man rule。

而 PHO 在這種情況下，就會被身分為 Role1 又假冒 Role2 的使用者單獨操作 。現在，讓我們去評估與使用 PHO 相關的 CDA 同時故障的風險。

假設與 CDA1 和 CDA2 兩者與危險相關的發生機率 p(h)都是 0.3。因此兩者同時故障的機率就會是 0.3 x 0.3 = 0.09，這個值明顯的比兩者各自的 p(h)來的小。進一步來看，假設偽裝威脅的發生機率 p(t)是 0.5，而且在 p(t)是 0.5 的情況下，與 CDA2 相關的危險發生的條件機率 p($h \mid t$)為 0.9，這個值明顯的比不是條

件機率的 p(*h*)大很多。這也使得兩個 CDA 同時故障的機率變為 0.3 x 0.9 = 0.27，這個值也比再個別以系統安全或電腦控制安全做評估時的 0.09 來的大。與傳統的方法做比較可以發現，USSRAM 會因為 0.27 這個比較準確的評估風險，而建議一個較有效的 DBT 措施。

在這個方法中，我們假設與同時故障相關風險的層級，在採取嚴密的 DBT 對策之前，至少為 0.1。在這個假設之下，USSRAM 因而建議存取控制規範應該對漏洞作驗證，像是因為電腦控制安全攻擊而造成 SOD 的違反。這個驗證方法建立在以 SAT 為主的電腦控制安全系統驗證(S3V)方法[50]。S3V 是一個以可滿足性為基礎的有界模型檢查方法，用來驗證一個給定的資料獨立的存取控制規範是否有滿足某個特定的通用系統安全存取時序邏輯(SATL)特性。使用 S3V，我們可以檢查某個給定的存取控制規範是否違反了一個指定使用 SATL 的 SOD 原則。而這個特性被違反的機率是可以估計的，這個機率可以當作與偽裝威脅相關的弱點存在的機率 p(*v*)。如果 p(*v*)和 p(*h* | *t*)之間有強烈關連的話，我們可以說用來檢查與強制執行 SOD 的 DBT 措施是有效的。反之，可能就需要其他的 DBT 措施來加強。

總結來說，兩個 CDA 所增加的風險會直接反映出，因為未經授權(two-man rule 被違反)的關係使得 PHO 發生的風險。因此，USSRAM 可以有效地找出這種重要風險。儘管如此，USSRAM 還是只能針對單一的 CDA 作風險評估。在上述的例子中，我們需要兩個 CDA 的風險評估。無論是 USSRAM 可以被擴充到評估兩個 CDA，或是以目前的方法去對兩個 CDA 各做一次評估，得到兩個評估後的結果，再將兩個風險以乘積的方式，當作整合後的風險。

肆、參考文獻

[1] International Atomic Energy Agency: Nuclear Safety Action Plan / www.iaea.org/

[2] NRC Regulatory Guides / http://www.nrc.gov/reading-rm/doc-collections/reg-guides/

[3] IAEA Safety series / http://www-ns.iaea.org/standards/default.asp?s=11&l=90

[4] IAEA Security series / http://www-ns.iaea.org/security/nuclear_security_series.asp

[5]IAEA Nuclear Security Series No. 1, Technical Guidance Reference Manual, Technical and Functional Specifications

[6] IAEA Nuclear Security Series No. 2, Technical Guidance Reference Manual, Pub1241, Nuclear Forensics Support

[7] IAEA Nuclear Security Series No. 3, Technical Guidance Reference Manual, Pub1242, Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators

[8] IAEA Nuclear Security Series No. 4, Technical Guidance Reference Manual, Pub1271, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage

[9] IAEA Nuclear Security Series No. 5, Technical Guidance Reference Manual, Pub1278, Identification of Radioactive Sources and Devices

[10] IAEA Nuclear Security Series No. 6, Technical Guidance Reference Manual, Pub1309, Combating Illicit Trafficking in Nuclear and other Radioactive Material

[11] IAEA Nuclear Security Series No. 7, Technical Guidance Reference Manual, Pub1347, Nuclear Security Culture

[12] IAEA Nuclear Security Series No. 8, Technical Guidance Reference Manual, Pub1359, Preventive and Protective Measures against Insider Threats

[13] IAEA Nuclear Security Series No. 9, Technical Guidance Reference Manual, Pub1348, Security in the Transport of Radioactive Material
[14] IAEA Nuclear Security Series No. 10, Technical Guidance Reference Manual, Pub1386, Development, Use and Maintenance of the Design Basis Threat
[15] IAEA Nuclear Security Series No. 11, Technical Guidance Reference Manual, Pub1387, Security of Radioactive Sources
[16] IAEA Nuclear Security Series No. 12, Technical Guidance Reference Manual, Pub1439, Educational Programme in Nuclear Security
[17] IAEA Nuclear Security Series No. 13, Technical Guidance Reference Manual, Pub1481, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities
[18] IAEA Nuclear Security Series No. 14, Technical Guidance Reference Manual, Pub1487, Nuclear Security Recommendations on Radioactive Material and Associated Facilities
[19] IAEA Nuclear Security Series No. 15, Technical Guidance Reference Manual, Pub1488, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control
[20] International Nuclear Safety Group (INSAG) / http://www-ns.iaea.org/committees/insag.asp
[21] INSAG-10, Defense in Depth in Nuclear safety, Pub1013e, Chapter 2 . THE APPROACH TO DEFENCE IN DEPTH
[22] The Nuclear Regulatory Commission(NRC) / www.nrc.gov/
[23] U.S. NUCLEAR REGULATORY COMMISSION January 2010 REGULATORY GUIDE 5.71 CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES
[24] NIST SP 800-53 Rev. 3 Aug 2009 Recommended Security

Controls for Federal Information Systems and Organizations
[25] NIST SP 800-82 Jun. 2011 Guide to Industrial Control Systems (ICS) Security
[26] NRC, 10 CFR 73.54 Protection of digital computer and communication systems and networks.
[27] U.S. NUCLEAR REGULATORY COMMISSION January 2010 REGULATORY GUIDE 5.71 CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES, A.2 CYBER SECURITY PLAN
[28] NRC, 10 CFR PART 50--DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES
[29] NRC, 10 CFR 50.55a Codes and standards.
[30] NRC, 10CFR Appendix A to Part 50 General Design Criteria for Nuclear Power Plants
[31] Nuclear Energy Institute / www.nei.org
[32] Nuclear Energy Institute , NEI 08-09 rev.6, Cyber security plan for nuclear power reactors
[33] Nuclear Energy Institute , NEI 04-04 rev.1, cyber security program for power reactors
[34] National Institute of Standards and Technology / www.nist.gov
[35] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION , FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems
[36] IAEA INFCIRC/225/Rev.4, THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES
[37]王平, 羅濟群, 黃俊傑 and 王宇文,“風險評估方法”.
[38] BS ISO/IEC 27001 Stand Alone, ” http://17799.standardsdirect.org/index.htm”, Last viewed: August 2011.
[39] ISO27001 security home, “http://www.iso27001security.com/”, August 2011.

[40] National Institute of Standards and Technology, NIST SP 800-30, “Risk Management Guide for Information Technology Systems”, Gaithersburg, MD, July 2002.

[41] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan and Microsoft Corporation, Microsoft patterns & practices, Improving Web Application Security: Threats and Countermeasures, “http://msdn.microsoft.com/en-us/library/ff648644.aspx”, June 2003.

[42] FEMA433, “Using HAZUS-MH for Risk Assessment How-To Guide”, August 2004.

[43] FEMA452, “Risk Assessment”, January 2005.

[44] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.

[45] National Institute of Standards and Technology, NIST SP 800-30, “Risk Management Guide for Information Technology Systems,” Gaithersburg, MD, July 2002.

[46] International Nuclear Safety Advisory Group INSAG-10, *Defence-in-Depth in Nuclear Safety*, Vienna 1996.

[47] “Safety Risk Management Guidance for System Acquisitions,” Version 1.5, U.S. Department of Transportation, Federal Aviation Administration, Air Traffic Organization, Office of Safety, December, 2008.

[48] J. H. Ahrens and U. Dieter, “Computer Methods for Sampling from Gamma, Beta, Poisson and Binomial Distributions,” *Computing*, Vol. 12, No. 3, pp. 223-246, 1974.

[49] United States Nuclear Regulatory Commission, *Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update*, NUREG/CR-6992, October 2009.

[50] Y.R. Chen, J.L. Yao, C.H. Lin, S.W. Lin, C.H. Huang, Y.P. Hu, P.A.

Hsiung, S.J. Chen, and I.H. Chou. SAT-based Verification of Data-Independent Access Control Security Systems *International Conference on Security and Management* (SAM), Vol. 1, pp. 126-131, 2011.

[51] E. Kleiner and T. Newcomb. On the decidability of the safety problem for access control policies. In Proceedings of the Sixth International Workshop on Automated Verification of Critical Systems, pages 91– 103. Elsevier Science Publishers, September 2006

[52] V. C. Hu, D. F. Ferraiolo D. R. Kuhn, “Assessment of Access Control Systems”, National Institute of Standards and Technology (NIST) Interagency Report 7316, September 2006.

[53] INTERNATIONAL ATOMIC ENERGY AGENCY Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[54]Nuclear Weapon Accident Response Procedures (NARP), Chapter 15 WEAPON RECOVERY OPERATIONS

[55]Mitsubishi Heavy Industries, Ltd., *US-APWR Design Description*, October 2006.

[56] WhiteHat Security, Inc., WhiteHat Website Security Statistic Report, 11th Edition, Measuring Website Security: Windows of Exposure, 2011.

[57] P. Kafka, “Probabilistic Risk Assessment for Nuclear Power Plants,” *Handbook of Performability Engineering*, pp. 1179-1192, 2008.

[58] C.-F. Chuang and H.P. Chou, “Investigation of Data Communication Systems in Lungmen Nuclear Power Plant Project,” *IEEE Transactions on Nuclear Science*, Vol. 53, No. 3, pp. 1443-1449, June 2006.

[59] I. Exman and S. Reznitsky, “To be and not to be at the same time:

Hidden Watchdog Timers," in *Proceedings of the 26th IEEE Convention of Electrical and Electronics Engineers in Israel*, pp. 897-900, November 2010.

[60] P. Sousa, N. F. Neves, P. Verissimo, "Hidden problems of asynchronous proactive recovery," in *Proceedings of the 3rd Workshop on Hot Topics in System Dependability*, 2007.