國立交通大學

資訊管理研究所

National Chiao-Tung University

Institution of Information Management

一個針對衛星通訊的彈性存取控制演算法

A Dynamic Access Control Algorithm for Satellite Communications

研 究 生： 張 中 寰

指導教授： 羅 濟 群 博士

一個針對衛星通訊的彈性存取演算法

An Dynamic Access Control Algorithm for Satellite Communications

研究生：張中寰　　Student: Chung-Huan Chang

指導教授：羅濟群　　Advisor: Chi-Chun Lo

國立交通大學

資訊管理研究所

碩士論文

A Thesis

Submitted to Institute of Information Management

College of Management

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Business Administration

in

Information Management

June 2006

Hsinchu, Taiwan, the Republic of China

中華民國　　九十五 年　六 月

一個針對衛星通訊的彈性存取演算法

研究生：張中寰　　指導教授：羅濟群 博士

國立交通大學

資訊管理研究所

摘要

隨著無線網路與行動通訊的出現，使得在此架構下的應用需求不斷增加。尤其在國際電信聯盟所制定的 IMT-2000 規範完成後，提供陸上與衛星兩種傳輸媒介，更使得 IMT-2000 無論在便利性與傳輸速度的考量上都具備優勢。在無線網路其中以衛星通訊的使用，最具潛力及發展性。然而，由於訊號在空氣中傳播，資料安全性與保密性也受到考驗。因此，資訊安全機制之研究，將是未來無線網路中重要且急需解決的問題。而在本論文中，我們將探討衛星通訊環境中存取控制機制，有效率的存取控制機制可使得通過授權的使用者存取所被授予權限範圍內的資料，如此，可以防止非法或是雖經授權但無相關權限存取的合法使用者存取資源。在本論文中我們透過實作證明我們的演算法能有效的指派使用者所需權限，使系統不但能保證各項資源的安全性，亦能兼顧本身之彈性。

關鍵字：衛星通訊，存取控制，風險管理

An Dynamic Access Control Algorithm for Satellite Communications

Student: Chung-Huan Chang Advisor: Dr. Chi-Chun Lo

National Chiao Tung University

Institute of Information Management

Abstract

Due to the growth of the wireless technologies, the application requirements constantly increase under the wireless network architecture. The IMT2000, issued by ITU, provides territory and satellite transmission media for mobile communications and, thus, it stands an advantageous position in terms of convenience and speed. It has more potentiality and development. However, data security and confidentiality are threatened due to data transmission on the air. Hence, the study of secure schemes is an important issue in the wireless network environment.

Access control is one of the most important parts of satellite communication, and it enforces users that are restricted to access authorized activities according to the authorization plan. Consequently, illegal users or legal users with illegal access right can be prevented to ensure the security of the system. In our research, we have implemented our algorithm and proved that it protects every resource in the system effectively, and it makes the system more flexible, too.

Keywords: satellite communication, access control, risk management

誌謝

碩士生涯時間過得飛快，轉眼即將畢業，而畢業論文能夠得以如期完成，不得不感謝身旁的人給我許多幫助、建議、協助、與鼓勵。我首先要感謝我的指導教授羅濟群老師，在羅老師自由研究的學風下，讓我在撰寫本論文時不會備受壓力；但在跟羅老師討論時，老師卻能準確地挑出自己研究上的缺失，並給予相當大的幫助，我也從中學到許多做學問的方法及態度。其次我要感謝博士班的黃俊傑學長與程鼎元學長，前者不斷督促指導我的論文，使我的論文更加完善與充實；而後者則是當我碰到瓶頸的時候，給了我許多協助及資訊，幫助我解決眾多論文相關的疑問。第三要感謝的當然是網路研究室們的同學與學弟們，雖然我們沒有女同學可以增添色彩，不過我們的友誼卻是最大的寶藏。元琮、文典與尚衛，我不會忘記我們共同修課跟寫作業的時光；友義、堯欽與仁豪，我相信我們四個苦中作樂的技術應該是無人能出其右；最後是智超，這兩年麻煩你不少事情，你的慷慨大方我會一輩子銘記在心；而勇璋、平祺、彥劭、士宏與展翊這五位學弟們也總是在我壓力大時陪我一同聊天解憂，辛苦你們了。最後我要感謝我的家人，在寫論文的這段時間包容與支持我，區區幾行話實在無法表現我對你們的感謝與愛情。

屈指一算，待在交大的求學生涯也六年了。回顧這中間日子酸甜苦辣都有，但最大的收穫就是在此認識了許多優秀的老師、學長姐、同學、及學弟妹。不論相處時間的長短，每個人對我的影響都佔有一席之地。能夠在交大資管所求學，相信是我這輩子最美好的回憶之一，我可以在這段時間與這麼多的好同學、好夥伴、好朋友相知相惜，是我研究生涯中最引以為傲的地方，因為有你們的陪伴，我的人生經歷過一段最幸福的時光。

圖目錄

表目錄

壹、 緒論

一、 研究背景與動機

隨著資訊科技的進步及基礎平台建構，使得各式符合人類需求的應用系統可在此平台上傳遞資訊。尤其無線網路與行動通訊的出現，使得以位置為基底的服務(Location Based Service, LBS)成為可行。而第三代的行動通訊，它因結合了語音與數據的通訊平台，且在 ITU 組織所制定的 IMT-2000 (International Mobile Telecommunications 2000)的規範中，要求在移動狀態需維持 384Kbps 及靜止狀態下能維持 2Mbps，未來的第二階段(phase 2)希望能達到 20Mbps，故它可以同時提供全球普及無縫漫遊、高效率、服務品質、頻譜效率與低成本之行動多媒體傳輸服務。

3G IMT-2000 因藉由衛星通訊，故可涵蓋的範圍非常廣泛，且具有以位置為基底的特性，具有機動性，且由於衛星通訊具有無線傳遞與高延遲的特性，故資訊安全的問題顯得更為重要。故在此環境中資訊安全政策中的彈性存取控制模式更顯得重要，因為能適當給予使用者所需之權限且不會有權限過大造成資訊安全上的疑慮或權限過小造成使用者之不便。

由於現今的科技發展速度之快已是今非昔比，未來衛星通訊網路的應用範圍與使用的普遍度將會逐漸提升，但是現今用於衛星通訊的安全機制，大部分採用私人虛擬網路(Virtual Private Network, VPN)維護資訊安全，然而 VPN 會影響衛星通訊的效率，因此，替衛星通訊找出一個合理授權且具備效率與彈性之存取控制模式則成為本論文之主要動機。

二、 研究目的

資訊安全的規劃，可從管理面跟技術面層面作說明。就管理面而言，組織必須了解自身的資訊安全需求，並且進行風險評估。因此，需要有一套方法學來協助單位完成資訊安全需求規劃，並做風險分析。只有通過風險評估，組織可以確定風險和安全漏洞對資產的威脅，並估計風險發生的可能性以及潛在的影響。現有的 ISO / IEC 17799 資訊技術──資訊安全管理的實施要則，可以實現組織對安全性需求的規範，但未對風險評估部分做說明；另一個由美國商業部所屬國家技術與標準局(National Institute of Standards and Technology , NIST)所建議的風險管理(risk management)中如何進行風險分析(risk analysis)方法論，它可以彌補風險評估的不足。因此在本文中，將針對此兩項做一概略描述。

就技術層面而言，就必須針對相對的通訊平台，提供不同的資訊安全解決方案，以滿足認證要求、存取控制、完整性、資料傳輸的私密性等等的資訊安全要求。故在本論文中，除了要具備原本存取控制的安全性需求，還要於機制設計過程中，需同時滿足效率及動態存取的要求。針對存取控制而言，其模型的目的首重對於系統以及環境下的安全程度，其次重視整個模型在設定跟維護上的管理合理性與彈性，本計畫之目的是希望提出一個能符合衛星通訊下的環境、同時具備高度安全性與管理彈性之存取控制機制，在未來發展衛星通訊時能兼顧高度資訊安全跟系統容易維護兩項優點。

三、 章節規劃

本論文主要之目的在於，研究應用在衛星通訊上之安全且彈性的存取控制模式；第二章則是文獻探討，回顧截至目前為止發展的各類型存取控制模式並列出其優缺點，以及從常用之風險分析模式做一探討；第三章說明本篇論文所採

用的改良方法與系統架構；第四章介紹系統實作的模型；第五章則是針對本系統討論未來可研究的方向。

貳、 文獻探討

一、 衛星通訊環境

隨著網際網路發展日漸蓬勃，通訊的範圍與效率越顯其重要性。不論是使用衛星網路將各地網際網路的骨幹線路(Internet Backbone)加以連結、或是直播存取的網路服務都是目前炙手可熱的研究方向。整體而言衛星的通訊特點如下：

(一) 衛星距離遠，故通訊涵蓋範圍大。

(二) 擴充容易，無纜線架設等問題。

(三) 傳輸價格決定因素並非距離，而是頻寬、頻道數與傳輸速率合理收費。

(四) 地面設施少，因此即使發生任何災害也能迅速回復通訊。

(五) 由於衛星通訊屬於廣播式傳輸，可應用於多點傳輸的服務上。

目前衛星的種類分為同步衛星(geostationary satellite, GSO)、中軌衛星(MEO)與低軌衛星(LEO)，前者的訊號涵蓋範圍地球的三分之一，因此只需三顆同步衛星即可完成全球通訊，也能藉由三顆衛星替使用者定位，但是缺點是運行軌道距離地面過遠，訊號延遲會比後面兩者嚴重，通常延遲為 250-280ms；而後兩者相比 GSO 的衛星，體積與重量均較前者來得小，而且延遲時間也因為軌道離地面較近延遲較短。

本論文作為主要探討對象的同步衛星，目前最常採用的傳輸方式是 bent-pipe 方式傳輸，亦即衛星僅作為地面兩個溝通點的重複器

(repeater)，將兩地的訊號轉傳(relay)之用，並無並行處理(onboard processing；OBP)的能力。至於通訊協定則沿用一般網路使用的 TCP/IP 或者 UDP/IP 通訊協定。然而衛星通訊協定採用 TCP/IP 時將會遭遇到動態拓樸及較長的封包來回時間(Round Trip Time, RTT)的問題，造成延遲時間過長與效率不彰一直是令人詬病的問題。為了解決延遲時間過長的問題，大部分的衛星通訊業者與應用程式的開發者會採用效能強化代理伺服器(Performance Enhancing Proxies, PEP)用來加速 TCP/IP 的衛星網路，下圖 1 為採用 PEP 的衛星通訊示意圖：

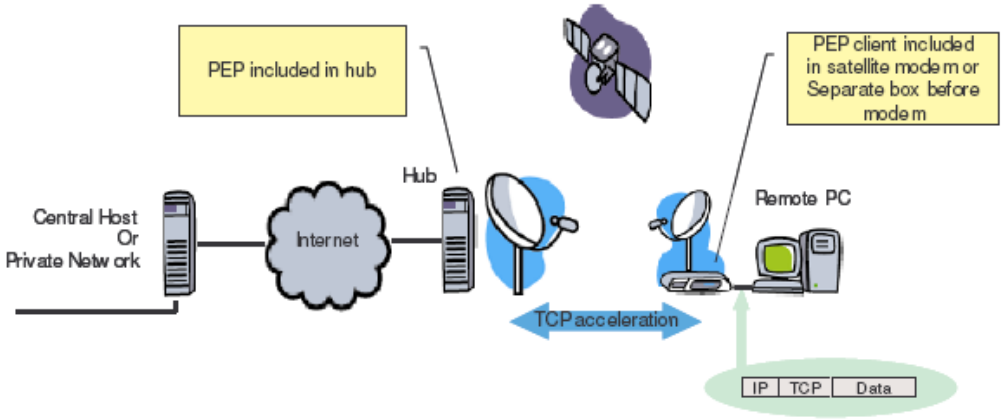


圖 1：採用 PEP 的衛星通訊示意圖

在衛星通訊中，由於傳播的範圍過廣，因此通常會採用私人虛擬網路(Virtual Private Network, VPN)進行加密傳輸，避免重要資訊遭人竊取，但是也因此增加了整體網路的傳輸負擔，特別是衛星與基地台之間的通訊，由於 VPN 的加密導致原本衛星使用的 TCP acceleration 變得無法使用，如下圖 2 所示：

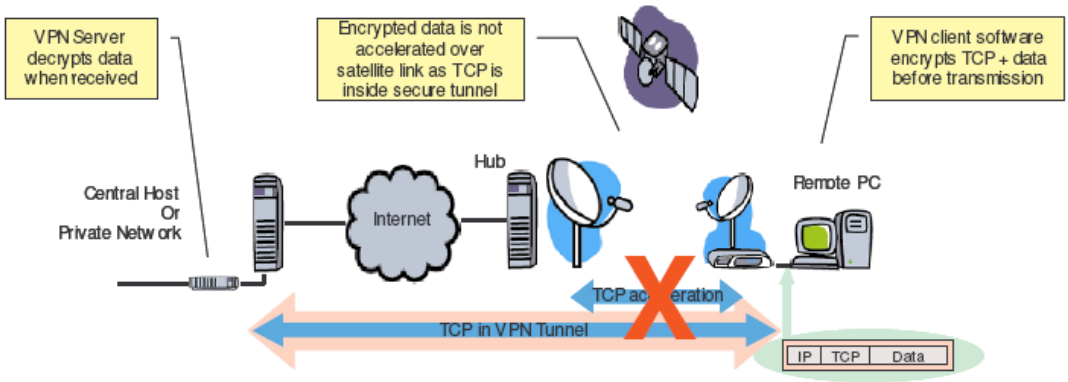


圖 2：使用 VPN 後導致 TCP acceleration 無法運作

二、 風險評估法則

所謂風險管理(risk management)指的是可以接受的成本，確認、控制、排除可能影響資訊系統的安全風險或將其帶來的危害最小化的過程。於風險管理上，主要包括風險評鑑(risk assessment)、風險處理(risk treatment)、風險承受(risk acceptance)及風險溝通(risk communication)等四項。

所謂風險評鑑指的是評估資訊安全漏洞對資訊處理設備帶來的威脅和影響及其發生的可能性。風險評鑑主要又包含：風險分析(risk analysis)及風險評估(risk evaluation)。其中風險分析，指的是以有系統的方式利用資訊，以識別來源並估計風險的行為，它包括風險的識別(risk identification)及風險估計(risk estimation)；換句話說，藉由風險識別及評估風險所帶來的衝擊等程序，以提出如何降低風險的建議方案。而風險分析是風險管理的基礎，它主要探討資產(Asset)、弱點(Vulnerability)與威脅(Threat)三要素間的關係。所謂的資產，即是對組織有價值的任何事物；所謂的弱點，即是一項或一組資產能夠被威脅利用的脆弱處。而所謂的威脅，即是一個意外事件可能導致系統或組織的損害的潛在原因。而三要素與風險分析間的相依圖，如下圖 3。

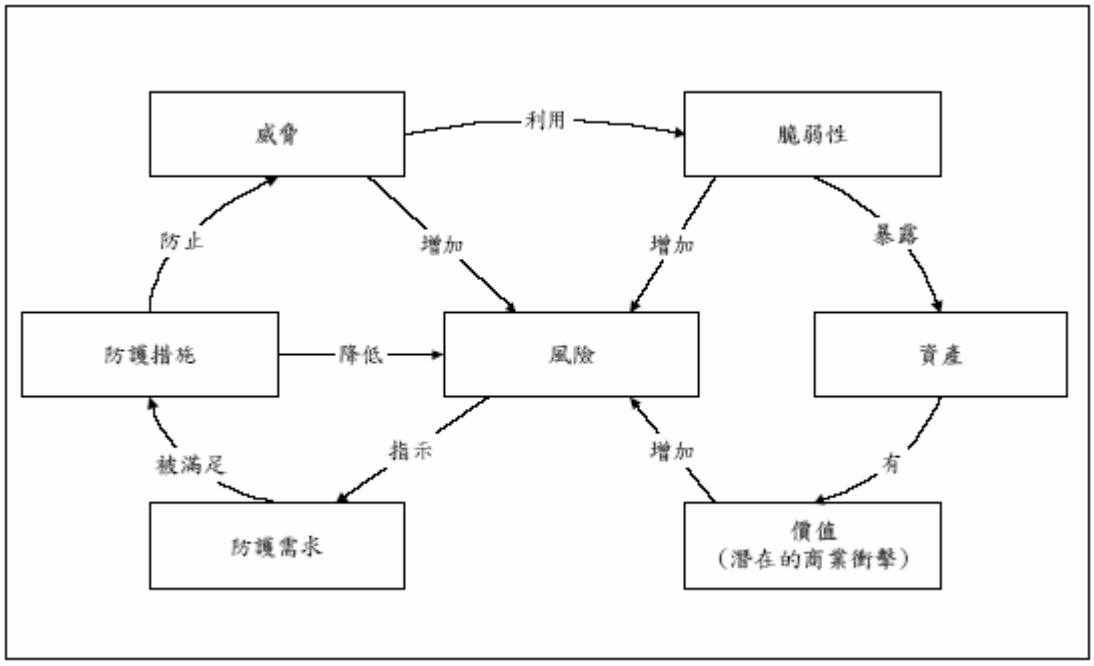


圖 3：風險分析中各要素的關聯

由於風險分析是風險管理架構的基礎，因此，本論文將先介紹幾種現有的風險分析模式，現有的風險分析法包括：

(一) HazOp

HazOp 是 Hazard and Operability 的縮寫，中文是危害及可操作性分析。如同 What-If 分析，是一種強調腦力激盪，集眾智產生新認識、新觀念的分析方法。不同於 What-If 的是 HazOp 跨越 What-If 分析結構鬆散的門檻，藉著引導詞(Guide word)與製程參數的結合，進一步探索系統設計與操作程序內潛藏的缺陷。因為是集體創造，HazOp 必需集合各種不同經驗、知識，和專業訓練的人在小組會議中相互研討設計及操作上的問題。這些問題通常是與設計的預期目標生歧異之情事。分析小組設法找出偏差或偏離(deviation)的原因，以及其可能造成的後果。藉由危害後果評估，可進一步實施量化風險分析。但量化風險分析不是 HazOp 小組的工作。HazOp 僅是定性地搜尋危害來源而已，並建議改善對策。

(二) 失誤樹分析

失誤樹分析((Fault Tree Analysis, FTA)，於 1961 年 H.A. Watson、A.B. Mearns(1965)研究出一種邏輯圖形的方法，以追溯系統中所有可能導致不幸結果的失誤原因群，由於分析出來的形狀如樹，因此稱失誤樹。失誤樹分析的概念是藉由目前產生之錯誤紀錄，逆向推導可能造成該錯誤發生的原因。

我們以下圖 4 當作舉例說明失誤樹分析是如何進行的：當一項產品或流程產生意料之外的錯誤時，我們將以這個錯誤為最初事件(Top event)，或稱作根(Root)，然後逐一將可能造成該錯誤的影響原因或事件加入至最初事件之底下，接著檢討各項影響原因或事件之發生機率而後加以標示。

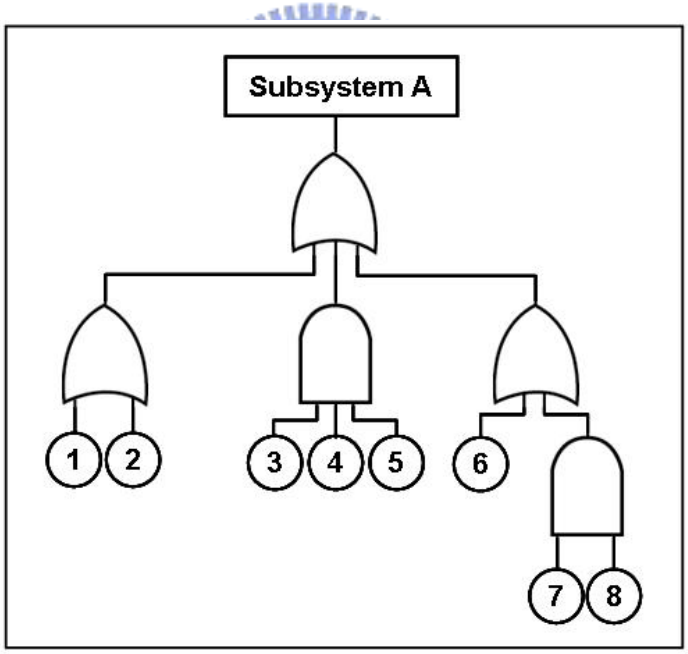


圖 4：失誤樹分析之範例圖

失誤樹分析既可用以探究意外事故發生的原因，並就每一促成因素生的機率，瞭解各失敗結果的相互因果關係，故有些安全工程師常使用它來做為意外事故防止的分析工具，或在事故生發生後的調查方法。

(三) FMECA

FMECA 是(1) FMEA (Failure Modes and Effects Analysis, 故障型式及其影響分析);(2)CA(Criticality Analysis, 嚴重度分析)兩種分析技術的總稱。與失誤樹分析一樣，故障型式影響及嚴重度分析(Failure Modes, Effects and Criticality Analysis, 簡稱FMECA)也是目前工業界的設計工程師與可靠度(Reliability)工程師常採用的方法。藉由 FMECA 以預測複雜的產品的可靠度，預估一件產品的零件在某特定的時間及情況下，如何失去其功能，故障的次數是多少，故障之後對其他零件或對整個系統會產生怎樣的影響等。

在一般標準情況下，故障型式影響及嚴重度分析共有三個指標需要預先定義與量測：

- 嚴重性(Severity, S)
- 發生機率(probability of Occurence, O)
- 偵測機率(probability of Detection, D)

每個指標的數字從程度最低 1 到程度最高 10 排序，最後 FMECA 根據這三個指標可經由下列公式計算出風險優先值(Risk Priority Number, RPN)：

$$RPN = S \times O \times D$$

下面三張表各別列出三項指標的標準。

表 1：嚴重性標準表

Rating/Rank	Effect
1	None
2	Very Minor

3	Minor
4	Very Low
5	Low
6	Moderate
7	High
8	Very High
9	Hazardous with Warning
10	Hazardous without Warning

表 2：失誤發生機率標準表

Rating/Rank	Effect
1,2	Remote: Failure is unlikely
3,4	Low: Relatively few failures
5,6	Moderate: Occasional failures
7,8	High: Frequently failures
9,10	Very High: Persistent failures

表 3：失誤偵測機率標準表

Rating/Rank	Effect
1	Almost Certain
2	Very High

3	High
4	Moderately High
5	Moderate
6	Low
7	Very Low
8	Remote
9	Very Remote
10	Absolute Uncertainty

失誤樹分析與故障型式影響及嚴重度分析此兩種方法均為業界中常用且都是依靠錯誤藉以察覺潛在的風險，但是兩者的觀念剛好相反。失誤樹分析的作法是找出已知的錯誤，檢討可能造成該錯誤發生的所有影響因素；而 FMECA 則是在事前檢查所有的元件跟流程，探討哪部分的環節可能存在潛在的風險因子。因此，如能將 FMECA 與失誤樹分析合併使用，必更能瞭解整個作業系統的危害，進而防範事故生。

(四) CORAS

諮詢式物件導向風險分析法(Consultative Objective Risk Analysis System, CORAS 是一個安全評論系統，用模型為基礎的風險評估發展出來的架構。其目的為了改善安全評論系統的方法論和電腦化為目標，使其能做出更精確、不含糊而且有效的風險評估。其架構如下圖 5：

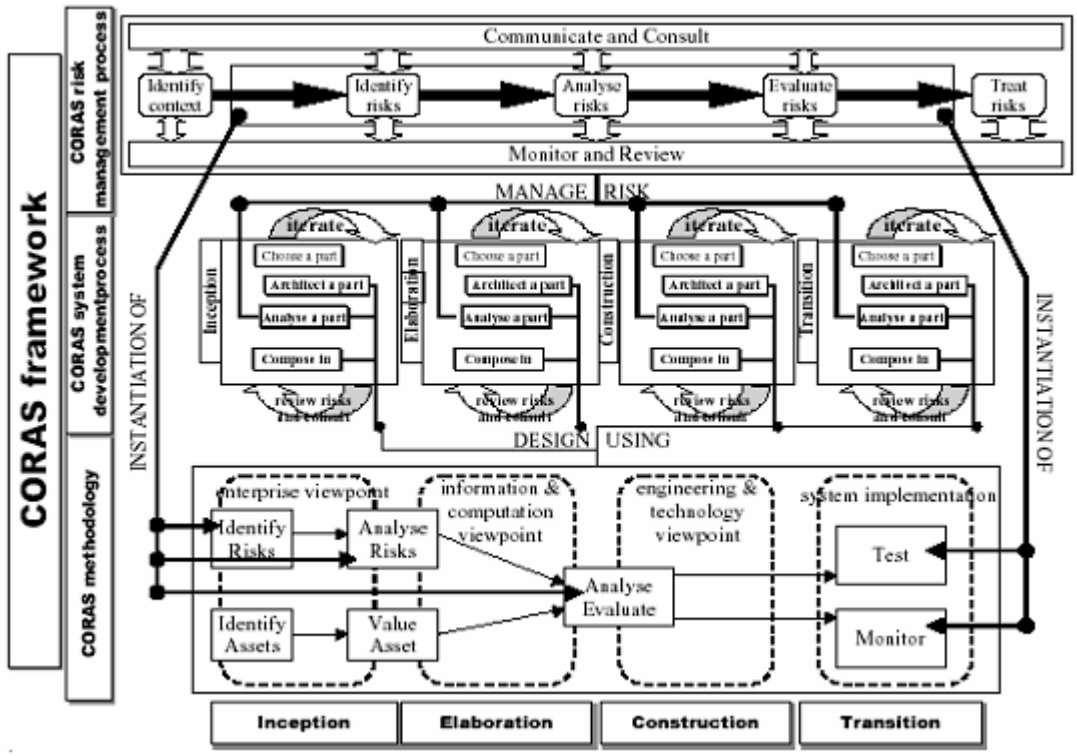


圖 5：CORAS 架構圖

在一個 Web-based 的系統中，如何使其可以穩定的運作，往往是為每個系統設計者在剛開始都會碰到的問題，而這類型的問題在牽涉到資訊安全時又特別重要、不容忽略。在通常狀況下我們可以把 Web-based 資訊系統所有的操作情況分為三種領域：

- 標準領域(Standard Domain, SD)－在系統之中能正確依照程序完成要求的所有操作情形之集合，我們稱之為標準領域。

- 錯誤領域(Failure Domain, FD)－在系統之中正確依照程序、系統卻達成與要求結果互相矛盾的所有操作情形之集合，稱為錯誤領域。

- 意外領域(Unanticipated Domain, UD)－則是指在系統之中所有不能明確詳述的操作情形之集合。

我們可以用下圖 6 說明這三個領域在系統中的分佈狀況：

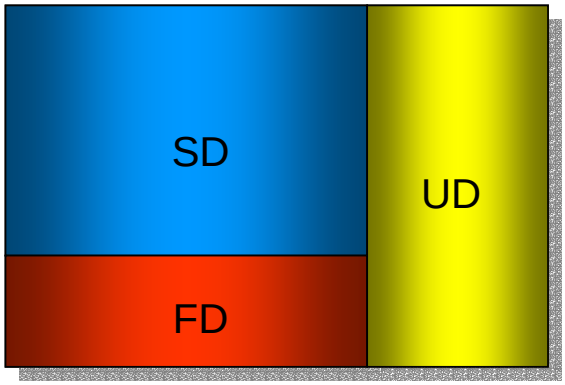


圖 6：SD、FD 以及 UD 三者於系統分佈之概念圖

一個系統的可靠度跟其錯誤領域相關，當錯誤領域所含有的元素越少時，則其可靠度就會增加；而系統的穩定性則跟意外領域有關，當意外事件越少發生，就代表系統的穩定性越強。由於權限指派錯誤而產生的問題通常屬於 UD，權限指派至錯誤的主體上即為一例，故在合理的權限指派至主體上之前，應該針對各個權限及主體的相關性進行風險分析評估，才能確保所有的權限與主體皆能無誤的正常使用以及接受系統控管。

三、 存取控制機制

本段主要是探討存取控制之安全性與重要性，為了使存取控制模式中同時具備安全與彈性，我們選擇 RBAC 作為整個模式的主要核心，故在此將已知的存取控制模式列出，並且與 RBAC 做各種比較與分析。

就存取控制而言，其目的在於確認所有直接存取資源必須為經過認證的，且經由管理存取動作的控制。有效的存取控制必須具備下列兩項前提：(1)使用者身份辨識，以確保該系統的確是被合法的使用者所使用，且杜絕非法使用者在該系統上作任何活動。(2)未經授權的使用者不可更改存取權限，否則使用者將能無限制的擴大其存取權限，違反管理的意義。目前常用的存取控制機制包括：存取控制矩陣(Access Control Matrix , ACM)、存取控制串列(Access Control Lists , ACLs)、能力串列(Capability Lists , CLs)及以角色為主存取控制(Role Based

Access Control，RBAC)。其中又以 RBAC 應用較廣，由 Sandhu 等人於 1996 年提出，它藉由角色指派來分開主受體，使得主體獲得授權以及受體可接受的存取限制這兩項動作透過角色來完成。其架構如下圖 7。

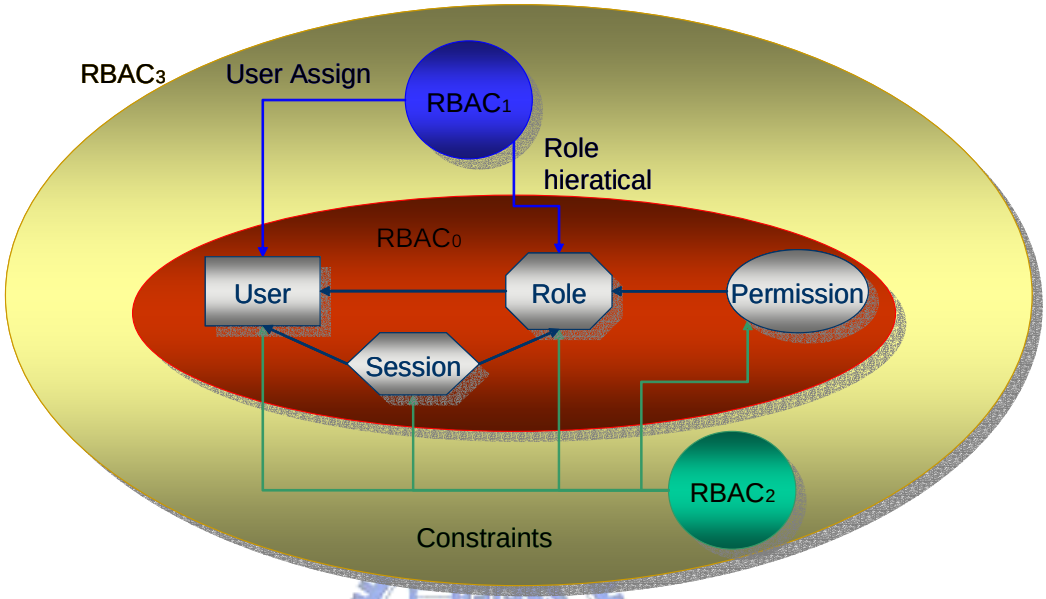


圖 7：RBAC 存取控制模式

下表 4 整理出以上各個存取控制機制的主要特色與優缺點：

表 4：各個存取控制機制的主要特色與優缺點

	存取控制矩陣	存取控制串列	能力串列	RBAC
說明	二維矩陣	資源導向	使用者導向	角色為主
	主物權力對照	以行形式儲存	以列形式儲存	主體透過角色取得權限
		每一物件對應到一串列主體，記錄主體的	每一物件對應到一串列受體，記錄特定使	

		資訊存取權限	用者的存取權限	
	指令式	指令式	指令式	語意式
優點	簡單	物件權限管理較容易	使用者權限管理較容易	簡化有效管理 提供權限細部描述 職務分工 權限繼承
缺點	量少—浪費空間 量多—不易管理	主體異動頻繁造成系統負擔 找主體較浪費時間	更動物件的權限時耗時	需以兩個資料庫維護主體與角色、角色與受體間的權限關係
主要及維護對象	人、物件	物件	人	角色
維護成本	高	高	高	低
繼承	無	無	無	有

然而若只是將 RBAC 直接導入衛星通訊環境，它無法滿足涵蓋大範圍且有行動通訊用戶的要求。因此，我們加入 GEO-RBAC 的觀念。

GEO-RBAC 主要是基於 RBAC 所延伸而出的機制，而 GEO-RBAC 遵循原本 RBAC 的模式並在角色與受體的部份加入了位置的概念，分別成為空間角色(Spatial role)跟空間感知受體(Spatially aware object)，接著再改進原本 RBAC 於空間資訊上的不足之處，使得 GEO-RABC 滿足了空間資訊安全的需要，下圖 8 說明 GEO-RABC 的核心概念跟模組。

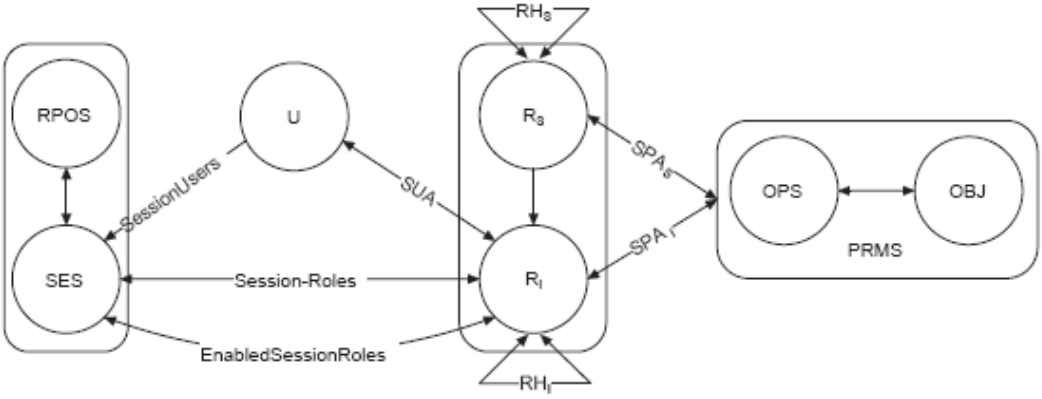


圖 8：GEO-RABC 的核心概念跟模組

GEO-RBAC 是從 RBAC 中延伸過來、專門處理有關位置資訊的存取控制模型，不但兼具原本 RBAC 在存取控制模型上的優點，而且對於位置資訊也同樣具備著相當的彈性，不論是實際位置(如經緯度)或者邏輯位置(如台灣新竹市)，都能根據該資訊決定合適的角色與相對應的權限。

為了使 GEO-RBAC 更加安全且不失彈性，我們認為單靠原本 GEO-RBAC 的模型很難達成目標，因此我們在這邊又引入彈性存取控制模型中所提到的限制式。在傳統的存取控制模型中，因為安全與容易使用這兩個因素往往是互相衝突的。要使存取控制模型更安全，一般而言有兩種方式，一種是將存取控制模型加強限制，這樣通常會導致模型被特殊化，只能適用於某些小部份的情形，並不符合我們的需要；故我們決定採用第二種方式－加入限制式，作為本計畫的一部分。加入限制式最大的困難就在於制定限制式本身就是一項極為複雜且繁重的工作，為了簡化這部份，我們採用了 Practical Safety in Flexible Access Control Models

該篇文章中的建議，儘可能簡化限制式的比較項目以及比較的種類，以減輕在制定限制式時將會遭遇到的繁重工作。首先我們先定義所有的限制式均為一個二元式，其次我們將限制式分為三個步驟：設定變數、選擇輸入項目以及比較輸入項目，如此一來我們只需數個設定動作即可進行一次限制式的比較。至於如何制定安全政策，基本上是根據權責分離與利益衝突這兩項因素作為探討基準，下面列著常見的衝突：

- 使用者衝突 User conflicts
- 權限衝突 Privilege:privilege conflicts
- 靜態使用者角色衝突 Static user:role conflicts
- 靜態權責分離 Static separation of duty
- 簡單動態權責分離 Simple dynamic separation of duty
- 連線相依的權責分離 Session-dependent separation of duty
- 受體導向的權責分離 Object-based separation of duty
- 操作權責分離 Operational separation of duty
- 順序相關的歷史限制式 Order-dependent history constraints
- 順序獨立的歷史限制式 Order-independent history constraints

限制式幫助我們增加存取控制模式的安全性與彈性，我們可以利用限制式控制 GEO-SAT-RBAC 例外狀況，除了能加強原本系統之安全度，也提供未來在管理上面多出許多彈性。

參、 適用於衛星通訊環境的彈性存取控制演算法

本章節將探討應用於同步衛星通訊環境下存取控制機制，針對同步衛星廣域傳播的特性跟使用者所處區域的地理資訊，我們設計一個以位置為基底、一開始不需使用 VPN 的 RBAC 演算法(GEO-SAT-RBAC)，並將憑證鏈(Certificate-Chain, CC)以及風險管理的觀念引進，增強存取控制的安全性，使得我們所提出的存取控制演算法於衛星通訊上的應用更加適用與富有彈性。

一、 合理指派權限

首先，我們使用 FMECA 將系統相關操作權限加以分析評估，根據其影響結果決定該權限的安全等級跟具備使用能力的相關主體。接著將針對 GEO-SAT-RBAC 中存在的各個使用者與其所具備角色的關聯性做一完整性的檢討，以確保系統本身讓所有相關權限、主體及使用者皆能在系統監控下正常運作，才能保證系統獲得最高的安全性與穩定度。

二、 存取控制機制

其次，就存取控制而言，本研究主要目的在於提出一個適用於衛星通訊環境下、對資源有效控管的存取控制架構，而這樣的架構必須能達成下列的目的：具備目前已知的存取控制模式以上的控管能力；考量衛星通訊環境下可能比一般環境更易受到攻擊，因此，加上所在位置的安全等級作為安全性控管的參考依據，稱為 GEO-SAT-RBAC (Geographical Satellite RBAC, GSR)；另外為了使這樣的存取控制架構除了具備嚴密控管的能力之外，還需要能兼顧彈性以備不時之需，因此加入條件式作為彈性控管之標準。以下我們將說明本研究所提出的存取控制架構之核心概念、設計方法與應用情境來闡述整個架構的運作方式。

GEO-RBAC 這個觀念是由 Bertino 等人於 2005 年所提出[1]，我們將此觀念導引至衛星通訊的存取控制機制的部份架構，藉由此想法說明如何訂定合適的角色供衛星通訊使用。原始的 GEO-RBAC 存取控制模式最大的問題在於當使用者申請角色時缺乏彈性與可能給予過多的權限。所謂缺乏彈性是指在相同角色(Role)下，不能同時存在不同的角色綱要(Role Schema)，也就是相同角色下所獲得的權限均一致，沒辦法依據使用者的位置不同而做出不同的彈性處置；同時因為只要申請相同的角色，即使地點不同也無法做出相對應的限制措施如減少該角色之權限。在 GSR 中，我們提出了一個方式針對 GEO-RBAC 缺乏彈性該缺點作改進，能夠配合使用者在申請角色實體時做出相對應並且適當的措施，以達到系統安全與存取控管之目的。

因此，GEO-SAT-RBAC 負責制定各個角色以及其所對應的資源權限，包括使用者在申請角色實體時的必須一併記錄該使用者目前的位置資訊，以及該角色所屬的安全層級。如此一來，一方面是作為指派角色的依據，另一方面則是用來計算當有使用者扮演著某種角色時，必須根據其位置和能力來計算安全層級，之後才會讓該使用者存取屬於該角色且符合安全層級中的資源。而在位置的考量上，為滿足衛星的特性，我們用地面接收站作為固定的使用者使用，以及該使用者現在所在的 NCC 作為存取控制機制使用。最後，考量到實際應用層面，我們針對例外的部份加入了安全性政策機制，以滿足在實際使用中偶發的例外狀況，下圖 9 即為本論文之流程圖，圖中的 NCC 為衛星通訊網路中的網路控制中心(Network Control Center)，存有使用者本身資訊及權限列表。

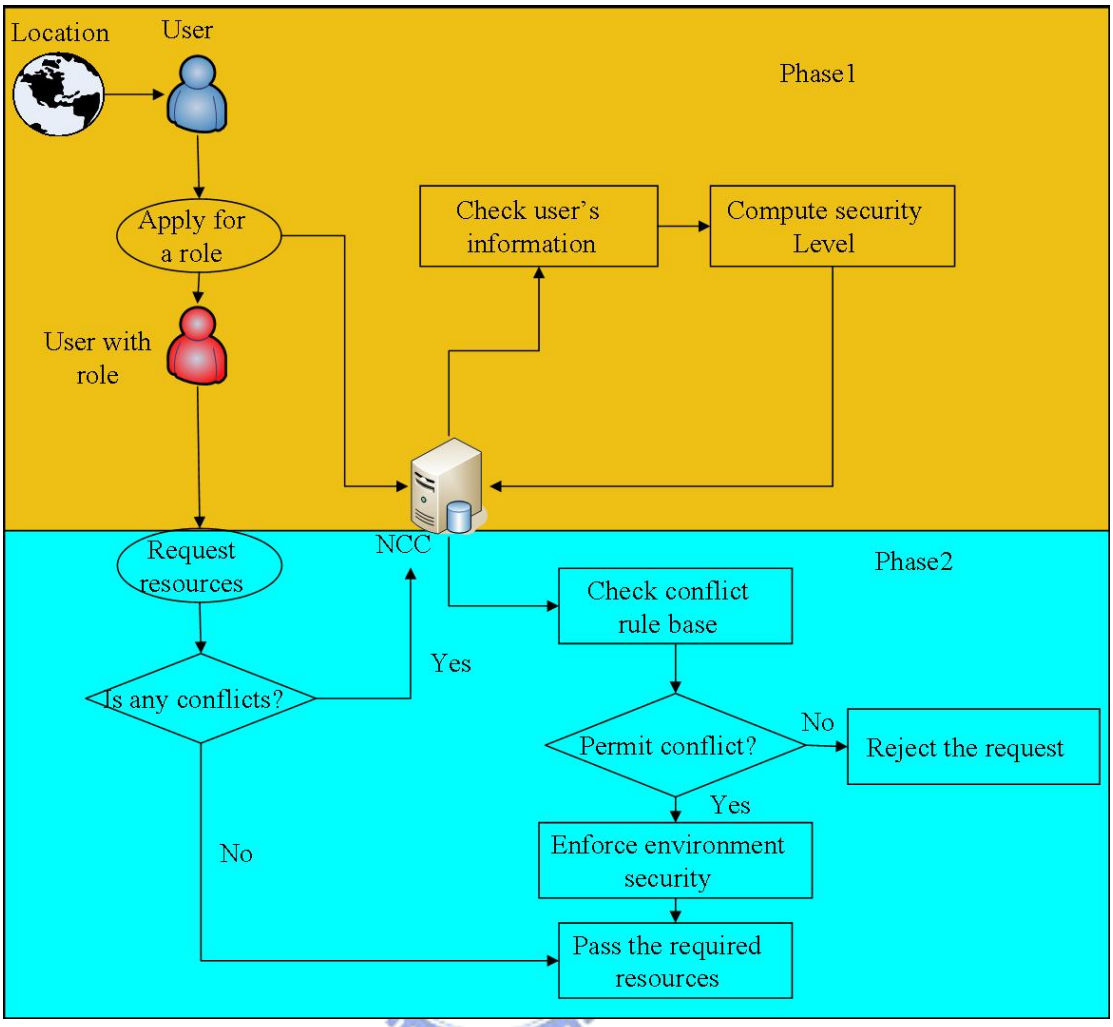


圖 9：GEO-SAT-RBAC 結合憑證鏈的存取控制演算法

我們在評估 GEO-SAT-RBAC 中的安全性時，看到 GEO-RBAC 雖然有針對使用者的空間資訊決定是否允許使用者申請特定角色，我們認為這部份仍然有可能出現缺失或漏洞，因此我們加入憑證鏈(Certificate Chain)的概念，藉由使用者本身的位置資訊跟轉送使用的接收站資訊，例如頻段，再根據預先定義於系統中的各區域信賴度加以計算評估，最後決定該使用者能夠存取的安全等級之物件。如此，可以防止任何合法使用者在非安全區域存取同等於原註冊區域的安全層級資訊，以增加整個系統的安全性。

(一) 憑證鏈(Certificate Chain)

首先我們介紹憑證鏈的概念，藉由此特性我們可以算出使用者所在位置的安全等級。當使用者透過衛星通訊網路申請網路時，勢必經過數個接收站跟衛星轉傳後才能回到使用者原註冊位置，使用者不但需要經過認證以確保是本人申請角色實體，我們也要確保該使用者所使用的路徑是足夠安全的，若不是安全的，就必須將原本屬於該角色的部分重要權限拿掉，以避免在傳遞過程中不小心被他人竊取機密資料。那麼我們如何判定一條路徑是足夠安全的？故我們將引進憑證鏈的觀念。而憑證鏈的概念可用下圖 10 來說明：

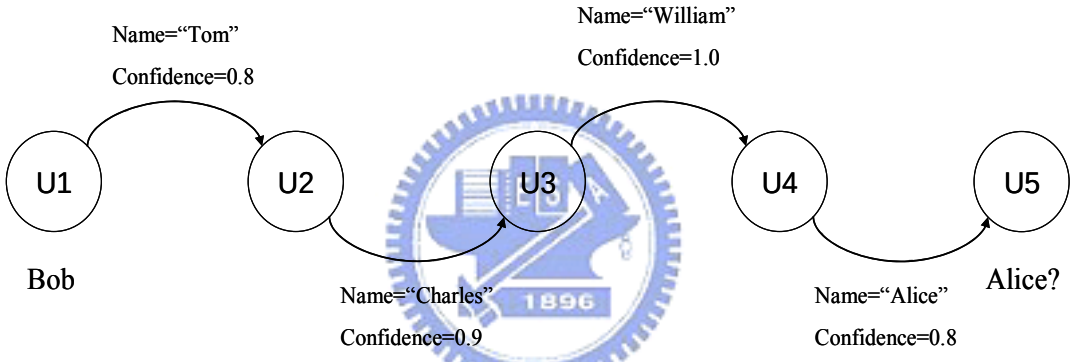


圖 10：憑證鏈的概念

假設 U1(Bob)要將某些資訊傳給 U5(Alice)時存在這樣一條路徑，那麼 Bob 將資訊傳到 Alice 手上時可以信賴這條路徑的程度就是這條路徑(憑證鏈)的信賴度。憑證鏈的信賴度應要大於我們在這條憑證鏈上能傳送資料的機密度，我們才能相信這條傳送路徑在傳送這些機密資料時被竊取的機率會低過其他路徑。而在本計畫中由於衛星傳送之特性，我們可將每個衛星轉傳所使用的接收站當作上圖中的 U2~U4，設定每個接收站都具有各自的信賴度，而當我們使用衛星網路時會根據使用者與傳送的路徑決定該條路徑的信賴度，接著對照信賴度與安全層級，決定該路徑上能傳送的機密資料有哪些。

在本研究中，我們定義 GSR 的憑證鏈，指的是地面接收站彼此會建立一個

相互信賴關係，而之間的信賴度是以百分比來定義，百分比越高代表相互信賴程度越高，百分比越低表示相互信賴程度越低。當整條鏈路經由計算後發現百分比過低，代表整個通信鏈路極不安全，此時使用者所具有的存取權限不應與在原註冊位置所具有的存取權限一樣，應該要更低以滿足安全性政策的定義。因此，故使用者可以透過此定義方式，產生更有彈性的 GSR。下面兩張示意圖，圖 11 及圖 12，分別說明 Stationary User 跟 Mobile User 在建立憑證鏈的示意圖，其中紅色的地面接收站代表使用者連回原註冊地點所使用的地面接收站：

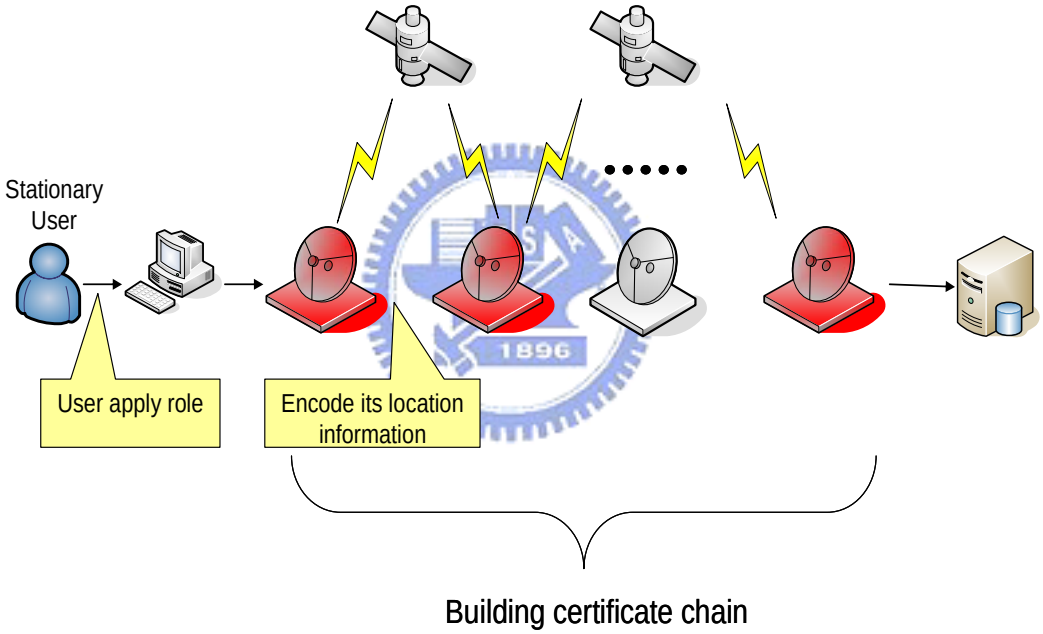


圖 11：Stationary 使用者的憑證鏈

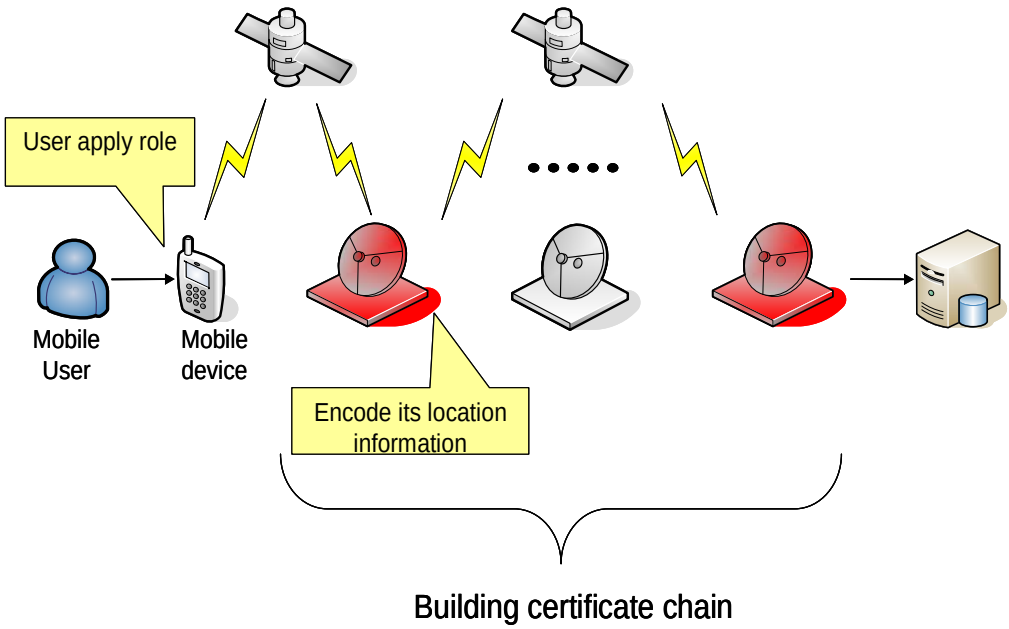


圖 12：Mobile 使用者的憑證鏈

定義憑證鏈上各個地面接收站的信賴度，我們認為可以採用目前已經提出的一些風險管理分析模式針對各個地面接收站作資訊風險評估報告，再根據它們的風險值決定它們在憑證鏈上的信賴度。風險值越高者代表該地面接收站越容易洩露機密資訊，因此我們可以將該信賴度調低；反之風險值越低代表機密資料越不容易洩露，該接收站也越可靠，故信賴度將會設定很高。下為 GEO-SAT-RBAC 結合憑證鏈方式的存取控制機制。所謂憑證鏈，指的是地面接收站彼此會建立一個相互信賴關係，而之間的信賴度是以百分比來定義，百分比越高代表相互信賴程度越高，百分比越低表示相互信賴程度越低。當整條鏈路經由計算後發現百分比過低，代表整個通信鏈路極不安全，此時使用者所具有的存取權限不應與在原註冊位置所具有的存取權限一樣，應該要更低，以滿足安全性政策的定義。因此，故使用者可以透過此定義方式，產生更有彈性的 GEO-SAT-RBAC 機制。

(二) GEO-SAT-RBAC, GSR

接著，在本研究中我們將 GSR 分成兩部份，包括：Phase1－使用者申請角

色實體和 Phase2－使用者存取資源。Phase1 使用者申請角色實體是當使用者建立連線時，我們可以根據他的帳號以及他所申請的角色、位置建立安全層級，對其要求的角色判斷使用者是否可以申請該角色，並且修改原本角色的權限，使其符合安全層級的標準，保證系統安全性；Phase2 使用者存取資源則是當使用者提出存取某些資源的要求時，我們根據之前建立的安全層級評斷這樣的要求是否允許，若允許則直接完成該次要求。另外為了突顯 GSR 比 GEO-RBAC 所具備的彈性，我們準備例外機制以滿足不被允許的要求，如此一來跟原本 GEO-RBAC 存取控制模型相較起來，GSR 在一般狀況下顯得更嚴格卻能在小地方不失彈性。

整個系統架構所組成的元件如下：

- 角色系統資料庫(Role Database)－本系統主要資料庫，存放使用者帳號，供申請之角色、和各角色之權限。使用者必須在一開始先透過衛星網路連線到此資料庫通過帳號認證以及申請進入系統之角色。

- 區域安全層級資料庫(Security Level Database)－記載著各區域所涵蓋之範圍、區域安全之等級、各衛星與接收站之信賴度。當使用者登入系統後須立刻比對該使用者所傳遞的位置參數跟計算所通過接收站憑證鏈之信賴度，根據信賴度及使用者之角色決定需要取消哪些存取權限，以保障系統安全。

- 衝突規則資料庫(Conflict Rules Database)－記載各種存取控制之規則，如使用者帳號與申請角色實體之衝突、角色降低權限後造成原本可使用資源無法使用之衝突、以及角色申請暫時恢復原本權限的請求等。

- 衛星接收站跟使用者通訊設備－使用者直(間)接與衛星通訊時必須傳遞自身位置之資訊，而接收站在轉送訊號時也必須將自己的識別碼或頻段傳回給角色系統資料庫所在之系統，以判斷使用者是處在何種安全層

級環境之下，以及需要調降至何種安全層級。

- 轉傳衛星－由於本計畫預計使用之衛星為 GEO 衛星，且目前衛星上鮮少具有處理能力，故我們假設衛星只有提供轉傳功能。

Phase1－使用者登入與申請角色實體(Role Instance)

Phase1 演算法如下所述：

1. 使用者透過衛星網路登入系統，傳遞自己本身之帳號、申請角色與位置三個參數申請角色實體。

2. 檢查使用者帳號與其申請之角色是否存在於角色系統資料庫之中，若使用者帳號與角色皆合法則將角色指派給使用者。

3. 檢查使用者本身跟中間轉傳之地面接收站的位置參數，比對區域安全資料庫內預先定義之區域安全層級後建立憑證鏈，計算該使用者的信賴度以決定該角色的安全層級。

4. 根據使用者的角色和角色所在地安全層級決定是否需要調降該使用者的權限，且將調整過後的角色實體回傳給使用者。

Phase1 的演算法可用下圖 13 表示：

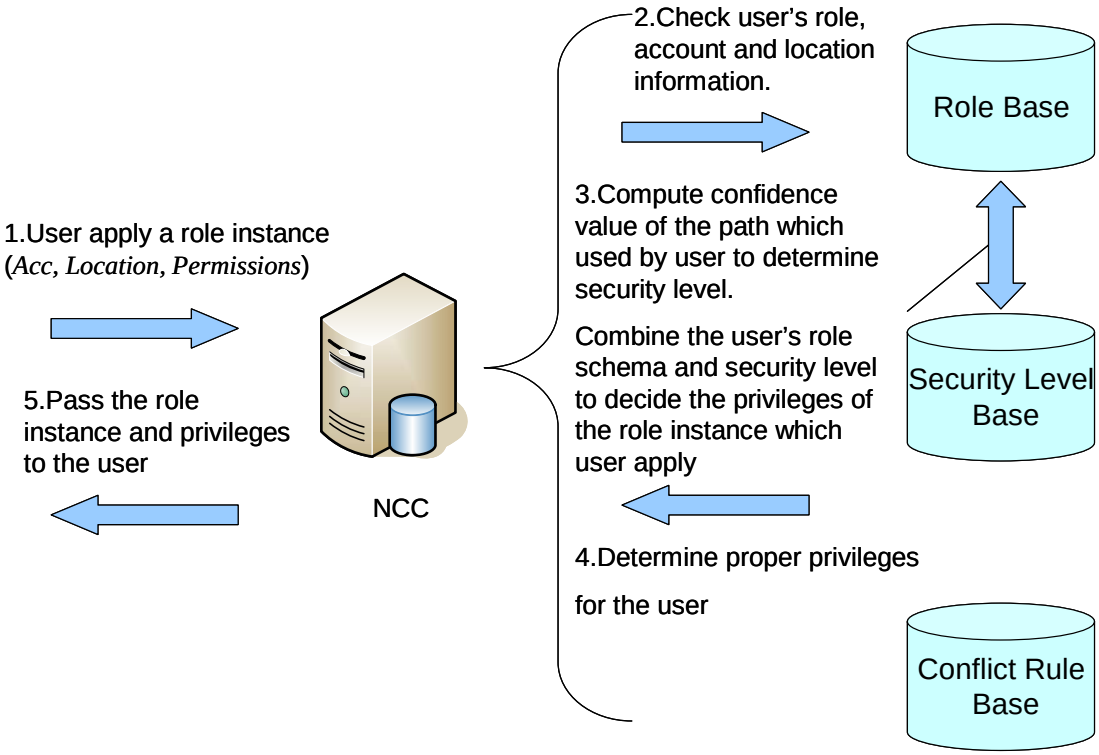


圖 13：Phase1 演算法

(1)使用者申請角色實體時需將自己的帳號、位置資訊與所要的權限(Account, Location, Permissions)傳遞到 NCC，作為 NCC 計算使用者申請角色實體與權限的安全層級之參數。

(2)NCC 檢查使用者的帳號與位置，並根據角色系統資料庫的規則決定使用者的帳號與位置是否可以申請該角色、並且將該角色所含的權限列出。

(3)依照之前使用者所傳遞的位置資訊查出使用者經過的接收站，接著查詢各個接收站在安全層級資料庫中預先定義的信賴度後計算整條鏈路的信賴度，再根據資料庫預先定義的安全層級表決定使用者角色的安全層級。

(4)使用者角色的權限會依據安全層級跟使用者所要求的權限，減少不相符的權限，確保重要資訊不會因此外洩。

(5)將適當的權限分配在角色上，再將角色實體(Role Instance)回傳給使用者。

Phase2－使用者存取資源 (User Accesses Resources)

Phase2 演算法如下所述：

1. 使用者要求存取資源

2. 檢查該使用者提出之要求是否符合預先定義各項權限的安全層級，若是則略過 3.、4.、5.。

3. 檢查衝突規則資料庫是否存在該例外，若是則進入 5.，否則進入 4.。

4. 拒絕使用者的要求，重新回到 1.

5. 系統要求使用者提高安全層級.

6. 允許使用者存取資源

在使用者獲得角色後，使用者可以檢視自己的角色與可使用的權限，使用者可以正常要求與合乎規則操作資源，但是我們很難預測使用者，特別是可以申請高等權限角色的使用者，很有機會要求某些高過他目前安全層級的資源，基於安全考量下一開始我們是拒絕將這樣的權限分派給他申請的角色，但是我們無法確保使用者是否有特殊狀況像是臨時或者有緊急情形發生，因此我們在這邊增加了彈性措施以滿足這樣的臨時需求，衝突規則資料庫也因此應運而生。衝突規則資料庫中放置許多衝突規則，當有使用者提出衝突狀況的要求時，我們可以根據這些預先設想的情況而寫下的衝突規則來決定是否允許這樣的例外發生。下圖 14 說明 Phase2 使用者存取資源以及例外狀況之處理：

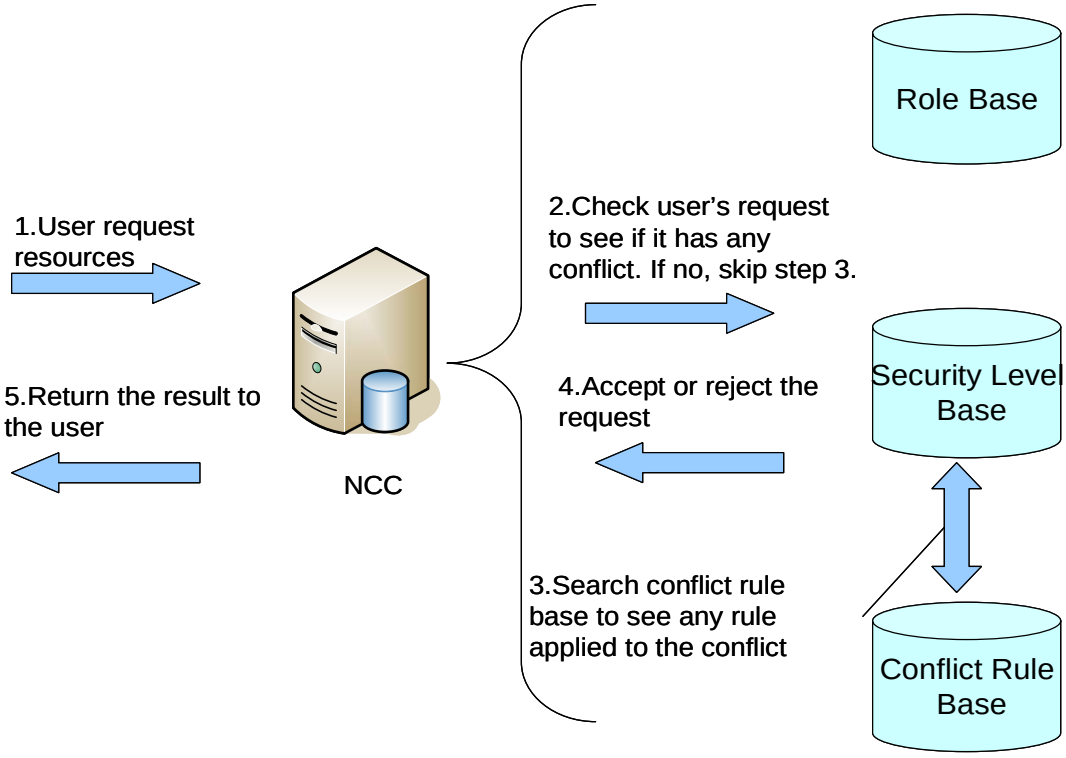


圖 14：Phase2 演算法

(1)使用者提出要求存取某些資源。

(2)檢查使用者的要求是否存在衝突(即根據他的角色以及安全層級關係，造成他無法使用這些權限)，若沒有衝突可以直接省略步驟 3.，亦即表示這是一個合法的要求不需要進入到例外步驟處理。

(3)例外處理的步驟，當使用者的要求進入這步代表使用者的要求發生衝突，此時檢查衝突規則資料庫裡中是否存在這樣的衝突規則，若無則直接拒絕使用者的要求；如果有的話就要求使用者加強他的環境安全性，例如使用 VPN 等加密技術保證資訊外洩的機率降到一定程度以下，也就是提高使用者的信賴度。

(4)NCC 將結果(接受、拒絕跟增加信賴度)計算出來。

(5)將結果傳回給使用者。

另本研究為說明上述方法之可行性，故在此將完整模式的定義以下述斷落詳述，並於附錄 A 附上虛擬碼(Pseudo Code)：

定義：

假設 *USERS, ROLES, PRMS, SESSIONS, and LOC* 分別為 users, roles, permissions, sessions and locations 的有限集合。

Definition.1－位置(Location)

Set of Location $L = \{l_1, l_2, l_3, ..., l_k\}$ from LOC where $LOC = \bigcup_{i=1}^{k} l_i$ and $l_i \cap l_j = \varnothing$ if $i \neq j$. 每個區域具有一個以上的接收站，如圖 15。

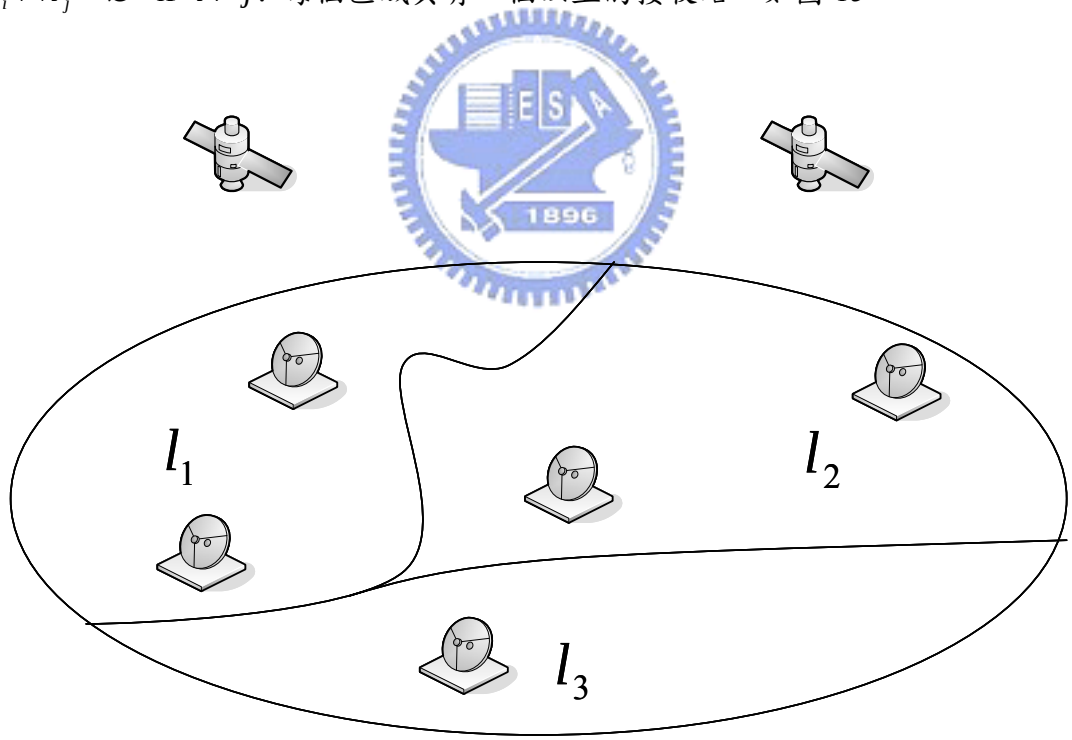


圖 15：地理位置定義

Definition.2－角色(Role)

我們將角色用成對(pair)的方式定義，其中 R 是角色名稱，而 L 是由

$\{l_1, l_2, l_3, ..., l_k\}$組成的位置集合。我們先定義角色概要(Role Schema, *RS*)及其權限，當使用者申請角色實體時根據角色概要指派一個角色實體(Role Instance, *RI*)，其中 *RI* 的權限會參考原本 *RS* 的權限與使用者的位置l_u。我們用圖 16 作為說明，在l_1中能啟用的權限有p_1與p_2，同理在l_2能啟用的權限則有p_1、p_2以及p_4；而l_3較不能信任，只能啟用權限p_1：

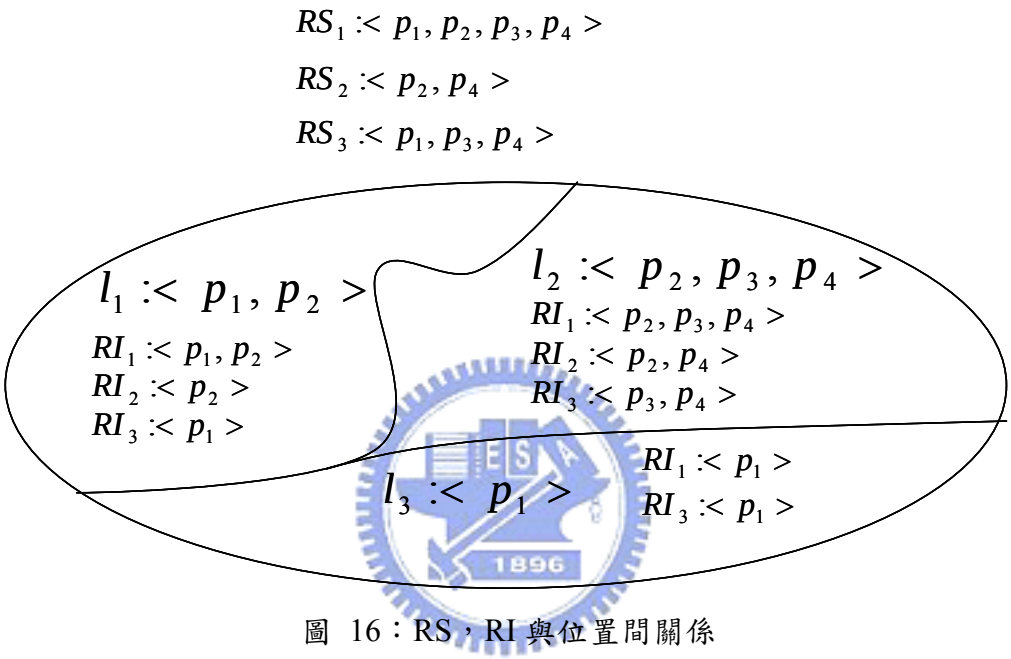


圖 16：RS，RI 與位置間關係

Definition.3－使用者指派(User Assignment)

使用者指派用*UA*表示，指將存在於 *ROLES* 中某個角色指派給存在於 *USERS* 中的特定使用者。我們用下列方程式表示使用者指派、*USERS* 跟 *ROLES* 三者間的關係以及使用者申請角色實體的條件式：

$$UA \subseteq USERS \times ROLES$$

$$UserApplyRole_u(r) = \{u \in USERS \mid (u, r) \in UA\}$$

Definition.4－權限指派(Permission Assignment)

我們用 *PA* 代表權限指派，也就是將權限依據位置將權限分派到角色上，我們用下列方程式表示權限指派與 *PRMS*、*ROLES*、跟 *LOC* 三者的關係以及權限指派给角色的條件式：

$$PA \subseteq PRMS \times ROLES \times LOC$$

$$PRMSAss_p(r,l) = \{p \in PRMS \mid (p,r,l) \in PA\}$$

Definiton.5－信賴度(Confidence Value)

我們可以預先針對每塊區域甚至是同個區域中不同接收站定義其信賴度(Confidence Value, *CV*)，信賴度的高低由風險分析模式計算出該區域的風險權重 *Risk(l)*，以百分比表示，再依下列公式計算出信賴度：

$$CV(l) = 1 - Risk(l)$$

其中 *Risk*(*l*) 即為區域 *l* 的風險值，我們考量到要減輕系統的在即時運算的負擔、權限在指派於角色上的變動頻率和一旦權限分派錯誤可能造成的後果跟損失，我們建議採用故障形式及其影響與重要性分析(FMECA)將每項權限失誤的機率、以及一旦產生失誤結果時所可能造成的危害結果預先詳細定義與列出，再根據這兩者的狀況，依照權重調整其風險值。

當使用者傳遞資訊的路徑需要經過兩個以上的區域時，其信賴度為各別信賴度的之乘積，公式如下：

$$CV(l_1, l_2, ..., l_k) = (1 - Risk(l_1)) \times (1 - Risk(l_2)) \times ... \times (1 - Risk(l_k))$$

Definition.6－安全層級(Security Level)

考量各種外在因素(如政治、外交等)，我們可能將衛星所涵蓋之範圍切割成許多區塊，若針對每塊區塊的信賴度定義各個角色在該區域所擁有的權限則過於繁瑣且複雜，因此我們將信賴度按照故障形式及其影響與重要性分析加以劃分成數個層級稱為安全層級。在安全層級的劃分上我們也應用故障形式及其影響與重要性分析的影響階級，我們用下列公式表示：

$$CV(l) \rightarrow SecurityLV(l)$$

而區域中所能啟用的權限必須要符合該權限所要求的安全層級，其中權限 p 的安全等級取決於故障形式及其影響與重要性分析計算得來的該權限之影響階級(Rank)：

$$PRMSEnable\ (p,l) = \{p \in PRMS \mid l \in LOC \mid SecurityLV\ (l) \geq SecurityLV\ (p)\}$$

Definition.7－衝突(Conflict)

為了增加 GSR 的彈性，我們允許使用者要求原本屬於該角色、卻因為安全層級機制而拿掉的權力，我們稱這樣的情形為衝突(Conflict, *CFT*)，我們用下列方程式表示：

$$CFT(p,l) = \{p \in PRMS \mid l \in LOC \mid SecurityLV(l) < SecurityLV(p)\}$$

假設 *CFTRULES* 為衝突規則之集合，當發生權限衝突時，若 $CFT(p,l) \in CFTRULES$ 就進入例外處理機制；否則拒絕該衝突要求。

我們將前述七個定義中重要的符號與其意義整理於下表 5 ：

表 5：GSR 的注釋與其意義

符號	意義
LOC	所有位置之集合
l	*LOC* 之元素
ROLES	所有角色之集合
r	*ROLES* 之元素
UA	使用者指派角色
PA	角色指派權限
CV	信賴度
SecurityLV	權限或區域之安全層級
CFT	權限安全層級與區域安全層級衝突

完整的演算法如下所述：

Step1.檢查使用者帳號、密碼，若合法則允許使用者登入系統；否則拒絕使用者登入。

Step2.使用者申請角色。

Step3.檢查使用者的帳號是否可以申請該角色，若否回到 Step2 讓使用者重新提出角色申請。

Step4.檢查角色的每一項權限之安全層級是否超過目前使用者所在位置的安全層級，若是則取消該權限。

Step5.將調整過後的角色實體指派給使用者。

Step6.使用者要求存取資源時檢查使用者所在位置的安全層級，若使用者所在位置的安全層級在權限安全層級之上時，略過 Step7、Step8 跟 Step9。

Step7.使用者提出的要求產生衝突，檢查是否允許該衝突存在，若是則略過 Step8。

Step8.拒絕該項要求

Step9.要求使用者提升安全層級

Step10.允許使用者要求

肆、系統設計與模擬

一、系統測試平台

為了增加本論文的發展性，因此我們用一般常見的網頁伺服器(Web Server)做為示範平台。

平台：

作業系統－WindowsXP

Web Server－Internet Information Service (IIS) 5.1

Web Page－ASP .NET with C# .NET

Database－MSSQL 2000

.NET Framework 以角色為基礎的安全性控管允許 Web 應用程式開發人員自訂 Web 應用程式的使用者身份、驗證方法以及角色定義方法，如下圖 17 所示：

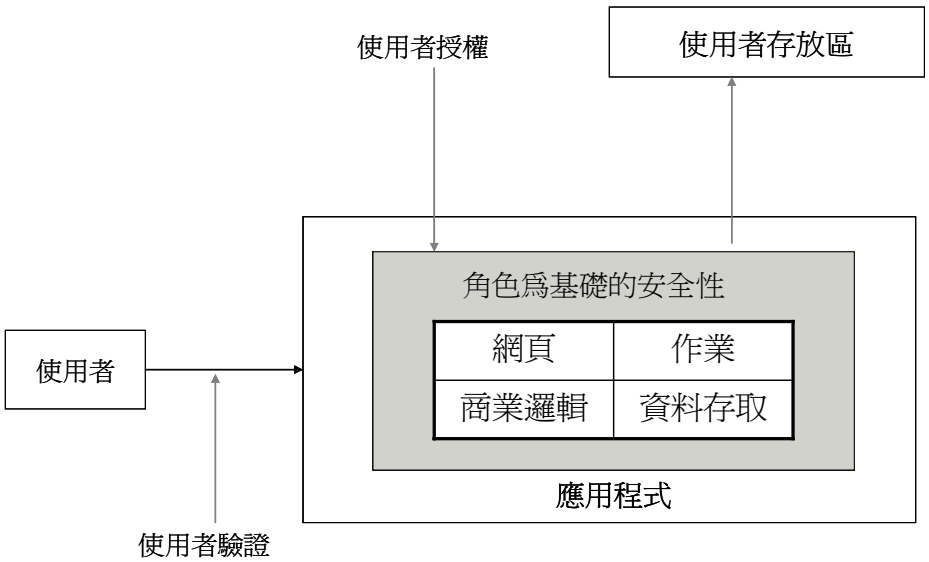


圖 17：Microsoft NET Framework Web 應用程式概念圖

首先我們將 GSR 相關的元件依照 FMECA 方法檢視整個系統、子系統、模

組與其元件，分析的流程圖如下圖 18：

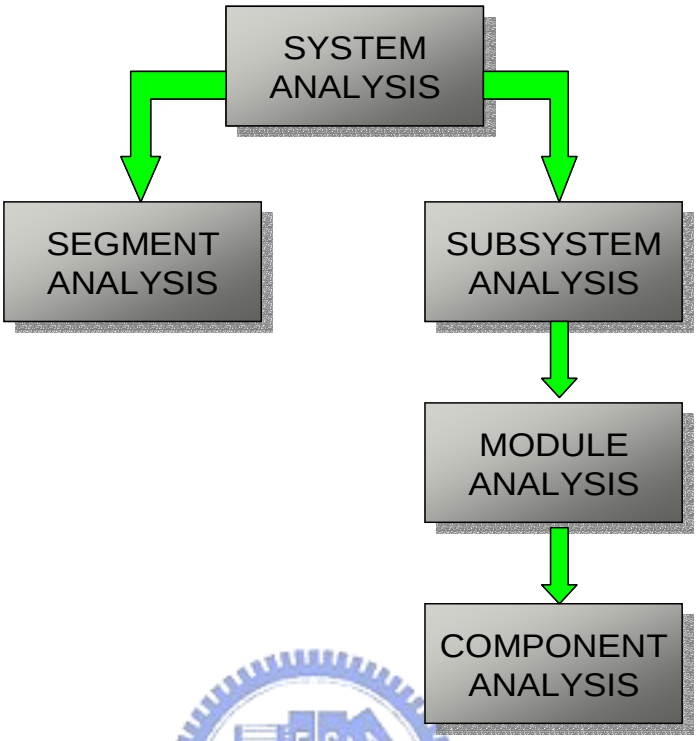


圖 18：實作 GSR 系統之 FMECA 前置分析流程圖

接著將 GSR 按照基本模型實作與修改而成，完整架構圖如下圖 19，其中以紅色框線標示的部份即為我們新增或修改的部份：

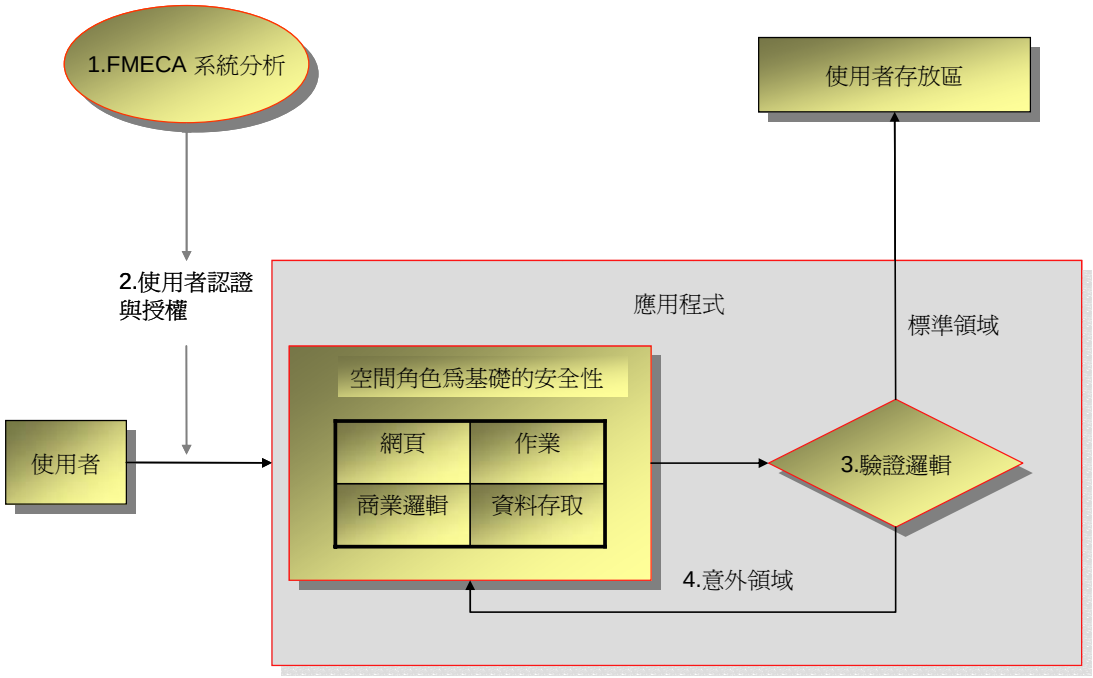


圖 19：實作系統架構圖

二、系統運作流程

(一) 前置作業階段

一開始我們 FMECA 檢查整個系統所包括的項目如登入系統的使用者、角色、資料庫以及各項受體的操作權限，確保系統運作的結果皆能落入正常領域之中。

(二) 使用者登入階段

當使用者輸入其帳號密碼時，我們會先從資料庫中尋找該帳號，比對使用者密碼確認無誤後再要求使用者給予目前的位置資訊，然後發給使用者一空間角色實體，裡面包含使用者身份、位置、角色、信賴度以及安全層級。

(三) 使用者根據獲得之權限進行操作

依照前述之範例，如果使用者在通訊過程中並沒有任何轉傳，那麼系統將會根據目前使用者所獲得的空間角色實體中的角色搜尋資料庫指派適當的權限給使用者，讓他可以按照自己所獲得的權限進行操作；但是當通訊過程中間若有經過其他基地台轉送時，將會引入憑證鏈，重新計算使用者的信賴度與安全等級，而所獲得的相關權限也將受到限制，導致某些權限可能無法執行。

(四) 使用者提高安全度

當使用者必須使用到被取消掉的權限時，使用者必須額外提出申請交給驗證邏輯檢驗以提高安全性。我們的作法是讓使用者提出 VPN 的申請，由系統提出挑戰讓使用者回應，若通過的話則系統與使用者重新建立 Tunnel，並且將原本取消的權限開放。

三、系統實作範例

傳統上憑證鏈之信賴度區間介在-1(完全不可信賴)到 1(完全信賴)之間，每經過一個 node 後會乘以信賴參數後調整原本之信賴度，但在本計劃中，對於非可信賴之個體都不應接觸到非其所屬之權限或物件；另外為了簡化系統複雜度、加強可用性的情況下，我們將憑證鏈之信賴度區間設定成 0(完全不信賴)到 1(完全可信賴)。在 Deutsch 的假說中提到，若任一個體對於某件事情屬於有益(Va+)或有害(Va-)之集合裡，其信賴之抉擇會出現在「已知 Va-所造成的影響大於 Va+，要使得 (Va+) * 有益之主觀機率值 ＞ (Va-) * 有害之主觀機率值 ＋ 安全層級」,其中主觀機率值與安全層級都會因每個人的情況而不同。因此本方法中角色的安全層級以及憑證鏈的信賴度在做計算時會跟系統預先定義在資料庫中的使用者起始信賴度、各區域的劃分跟區域的安全層級依據 FMECA 評估方法有關，另系統管理者們也可以根

據本身需求決定設定這些起始值。本論文中所提到之憑證鏈計算所使用到的使用者起始信賴度、各區域的劃分還有區域的安全層級僅作為範例之參考。

我們沿用第三章中的圖 15 與圖 16 的情形作為範例，分別定義出三個位置 Location1(l_1)、Location2(l_2)跟 Location3(l_3)，角色概要也分別有三個－Role Schem1(RS_1)、Role Scheme2(RS_2)與 Role Scheme3(RS_3)供使用者申請角色用。其中 RS_1 具有四項權限$< p_1, p_2, p_3, p_4 >$，RS_2 只具有$< p_2, p_4 >$兩種權限，而 RS_3 具有$< p_1, p_3, p_4 >$三種權限，RI_1, RI_2, RI_3 則是分別為對應至 RS_1, RS_2, RS_3 的角色實體。

最後在本論文中來說我們為了方便計算，我們將原本 FMECA 十層的危害程度簡化並對應到為三層的安全層級，並且平均地劃分該三層信賴度。下圖 20 說明我們如何把原本的十個階級對應到簡化後的三個層級：

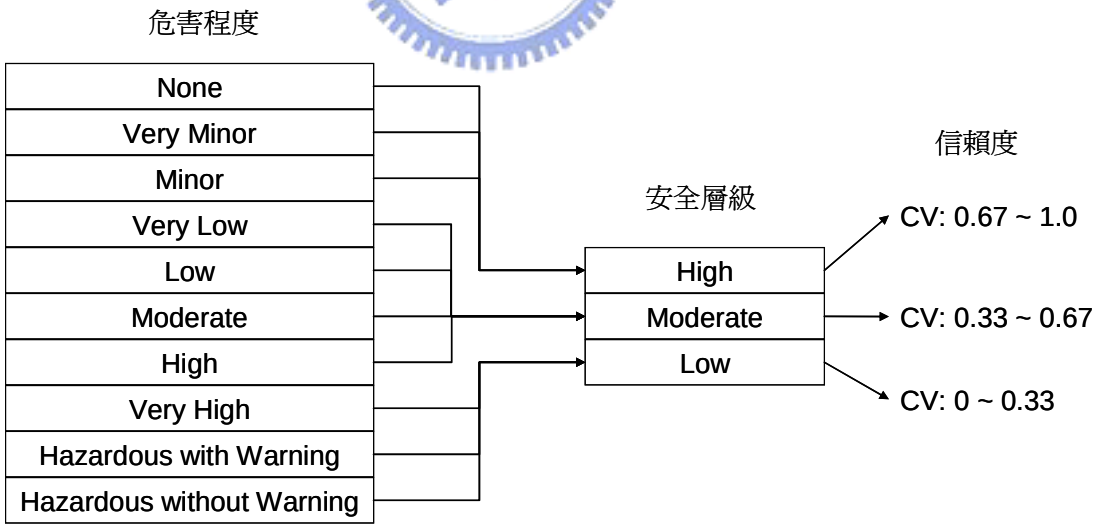
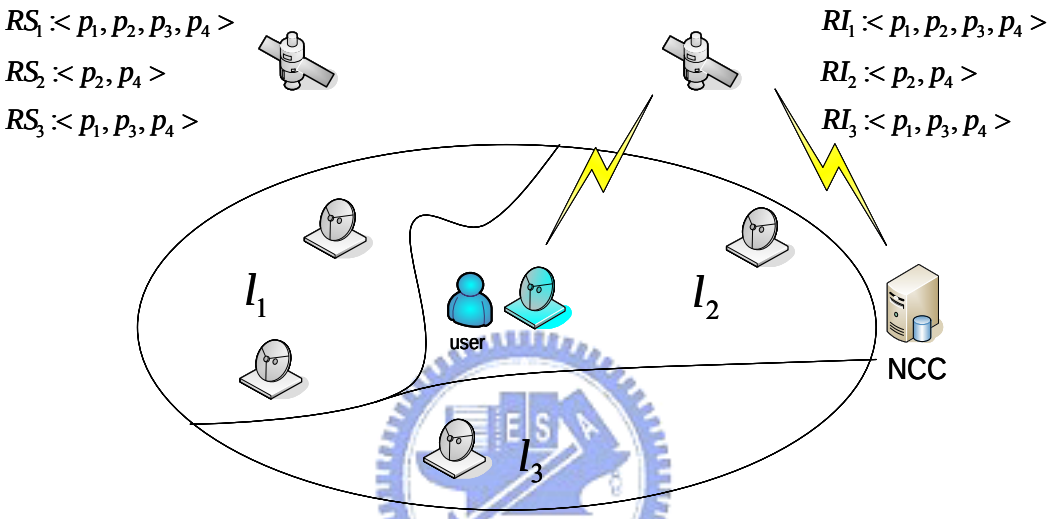


圖 20：FMECA 十個階級對應成三個安全層級及其信賴度區間

下面我們將用兩個不同的範例解說我們實作的系統如何運作，以保證使用者能在系統控管下正常存取資源，防範其他較：

(1)Case 1－使用者不需經過轉傳即可到達 NCC

圖 21 表示使用者處於l_2，不需要經過任何轉傳即可連回自己的 NCC 存取資源。在此案例中使用者的信賴度是$CV(l_2)=0.95 \Rightarrow SecurityLV(l_2)=High$，而$High \geq High > Moderate > Low$，依照我們的演算法無論使用者獲得何種角色實體皆可獲得原本角色概要之完整權限。



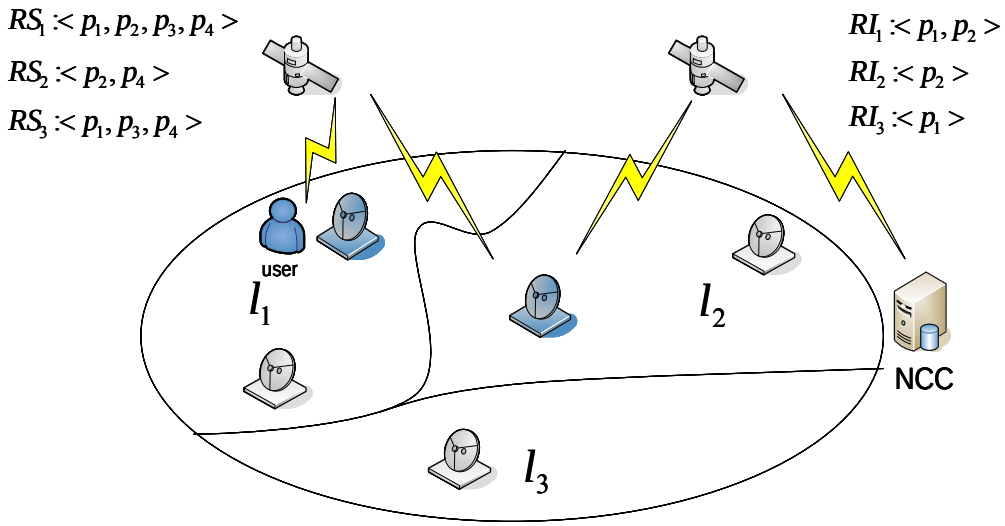
$SecurityLV(p_1)=Low$
$SecurityLV(p_2)=Moderate$
$SecurityLV(p_3)=High$
$SecurityLV(p_4)=High$

$l_1 : CV(l_1)=0.7, SecurityLV(l_1)=Moderate$
$l_2 : CV(l_2)=0.95, SecurityLV(l_2)=High$
$l_3 : CV(l_3)=0.4, SecurityLV(l_3)=Low$

圖 21：使用者不需轉傳即可到達 NCC

(2)Case 2－使用者需要經過一次轉傳才能到達 NCC

圖 22 說明當使用者處於l_1時，必須透過l_2的接收站轉傳才能順利讓使用者存取到遠在l_2的 NCC。而在此案例中使用者安全層級因為轉傳而被降低成$CV(l_1,l_2)=CV(l_1)\times CV(l_2)=0.7\times 0.95=0.665 \Rightarrow SecurityLV(l_1,l_2)=Moderate$，而$Moderate > Low$，使用者在分別申請$RS_1, RS_2, RS_3$超過安全層級 C 以上的權限如p_3, p_4將會被取消。



$SecurityLV(p_1) = Low$
$SecurityLV(p_2) = Moderate$
$SecurityLV(p_3) = High$
$SecurityLV(p_4) = High$

$l_1 : CV(l_1) = 0.7, SecurityLV(l_1) = Moderate$
$l_2 : CV(l_2) = 0.95, SecurityLV(l_2) = High$
$l_3 : CV(l_3) = 0.4, SecurityLV(l_3) = Low$

圖 22：使用者需要經過接收站轉傳一次才能到達 NCC

在本論文實作的系統中，提高使用者安全層級的作法是由使用者與 NCC 建立虛擬私人網路(Virtual Private Network, VPN)，如此一來即使經過轉傳，也不會增加任何被竊聽之風險，故可以將憑證鏈上所經過的全部區域之信賴度都設定成 1，亦即使用者可以不受轉傳的影響，獲得原本被系統取消之權限。但是一旦建立 VPN 後，就如第二章所述 PEP 功能無法使用，因此 PEP 的加速功能將喪失，而衛星通訊將會由於 VPN 的關係，延遲時間將會變得更長。

伍、結論與未來研究方向

未來通訊環境，將由陸上行動通訊結合衛星通訊，以達到全球無縫隙的傳輸環境，而衛星通訊更是未來通訊服務的重要一環。為了達到在此通訊環境的通訊安全要求，存取控制機制的設計就成為重要的議題。

一個好的存取控制模式，除了要能保證可使通過授權的使用者存取所被授予權限範圍內的資料，又不能讓使用者獲得不需要或者有機會造成問題的權限。因此事前的風險管理分析就在這邊彰顯出它的重要性，因為透過風險管理分析我們才能清楚詳細的知道哪些行為屬於哪些權限跟角色集合，而這些權限跟角色集合又與哪些使用者有所關聯。若在系統設計與開發階段就導入風險管理分析的方法，找出上述的關係，將有助於整個存取控制模式運作時更有效率及更加安全。

又本研究動態指派權限之存取控制的觀念，是以地理位置為基礎結合憑證鏈的觀念，再導入風險分析與管理，使得本研究所提的存取控制機制未來在實務應用上更為安全可行，並且具備一定程度上的彈性，讓使用者可以在嚴格的控制條件下，只要滿足系統提高安全性的要求時就不會受到原先安全性過低的影響，因此更能適用於衛星通訊如此開放的環境。

本論文未來的研究方向，將針對各個風險管理分析模式應用在存取控制模式之適用性分析；以及考量未來衛星它是可能具備可以線上處理能力(On-line Based Processing)的條件下探討安全性問題；另外也可以針對風險分析評估與信賴度之計算公式加以改善。

參考文獻

[1] J.O. Aagedal, F.D. Braber, T. Dimitrakos, B.A. Gran, D. Raptis, and K. Stolen, "Model-based Risk Assessment to Improvement Enterprise Security," Proceedings Sixth International Enterprise Distributed Object Computing Conference (EDOC'02), 17-20 Sept. 2002, pp.51-62.

[2] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: A Spatially Aware RBAC," In Proc. Of the 10th ACM Symp. On Access Control Models and Technologies (SACMAT05), pp.29-37.

[3] Rebecca S. Diercks, "3G Technology As A Fixed Wireless Solution", May 2000

[4] Peter Fenelon, Barry Hebbron, "Applying HAZOP to Software Engineering Models"

[5] Jose Antonio Bogarin Geymayr, Nelson Francisco Favilla Ebecken, "Fault-Tree Analysis: A Knowledge-Engineering Approach", IEEE Transactions on Reliability, vol 44, NO.1, 1995 March

[6] Frode Hansen and Vladimir Oleshchuk, "SRBAC: A Spatial Role-Based Access Control Model for Mobile Systems",

[7] T. Jaeger and J. Tidswell, "Practical Safety in Flexible Access Control Models," ACM Transactions on Information and System Security, Vol.4, No.2, 2001, pp.158-190.

[8] Pradip Lamsal, Understanding Trust and Security, October 2001

[9] Minsoo Lee, Jintaek Kim, Sehyun Park, Ohyoung Song, and Sungik Jun, "A Location-Aware Secure Interworking Architecture Between 3GPP and WLAN System

[10] Ilari Lehti and Pekka Nikander, "Certifying Trust"

[11] Stephen Paul Marsh, "Formalising Trust as a Computational Concept", April 1994

[12] Gary Stonebuner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for information technology system", NIST Special Publication 800-30, July 2002

[13] Nimal Nissanke and Etienne J. Khayat, "Risk Based Security Analysis of Permissions in RBAC"

[14] Tero Ojanperä, Ramjee Prasad, "An Overview of Third-Generation Wireless Personal Communications: A European Perspective"

[15] R. Sandhu, E.J. Coyne, and C.E. Youman, “Role-based Access Models,” IEEE Computer, Vol.29, No.2, Feb. 1996, pp. 38-47.

[16] K. Stolen, F.D. Brber, T. Dimitrakos, R. Fredriksen, B.A. Gran, S.H. Houmb, M.S. Lund, Y.C. Stamatiou, and J.O. Aagedal, “Model-based risk assessment – the CORAS approach”, 2003.

[17] Jianyun Zhou, Tor Stålhane, “Using FMEA for early robustness analysis of Web-based systems”, Computer Software and Applications Conference, 2004. COMPSAC 2004. Proceedings of the 28th Annual International

[18] MIL-STD-1629A, “Procedures for Performing a Failure Mode Effects and Criticality Analysis. U.S. Department of Defense,” Washington, D.C., November 28, 1984.

[19] ACUTech, “The HAZOP (Hazard and Operability) Method”, http://www.acusafe.com/Hazard_Analysis/HAZOP_Technique.pdf

[20] Packeteer, Inc., “Accelerating Application Delivery For Satellite Networks”, http://www.sonet.at/dsdsl-vpn/dsdsl-vpn.htm

[21] 王秀文，一個針對共通作業環境中資訊資產風險評估模式，國立交通大學資訊管理研究所碩士論文，民 92 年。

[22] 林千代，可攜性 RBAC 資訊系統架構之研究，朝陽科技大學資訊管理系碩士論文，民 92 年。

[23] 曾俊豪，以角色為基礎作網頁伺服器的存取控制之系統設計與實作，國立台灣大學資訊工程研究所碩士論文，民 88 年。

附錄 A

虛擬碼(Pseudo Code)

使用者申請角色實體部分：

Build session

Receive user apply role (u, r, l, p)

If ($UserApplyRole_u(r) = \{u \in USERS \mid (u, r) \in UA\}$)

Calculate $CV(l) \rightarrow SecurityLV(l)$

For each permission of the role which user required

If ($PRMSAss_p(r, l) = \{p \in PRMS \mid (p, r, l) \in PA\}$ *AND*

$PRMSEnable(l, p) = \{l \in LOC \mid p \in PRMS \mid SecurityLV(l) \geq SecurityLV(p)\}$

)

Assign the permission to the role

Else

Remove the permission from the role

End If

Send the role to the user

Else

Drop the user's request

Terminate session

End If

End Procedure

使用者存取資源部分：

Receive user request resource (r, p, l)

If ($p \supseteq PRMS(r) \times SecurityLV(l)$)

Request granted

Processing the request operation

Return the result to the user

Else If ($CFT(p,l) \in CFTRULES$)

Enter exception handling

Ask the user enforce environment security

Rebuild session

If ($p \subseteq PRMS(r) \times SecurityLV'(l)$)

Resend the updated role instance to the user

Else

Drop the request

End If

Close exception handling

Else

Drop the request

End If

End Procedure