戰術區域通信控制系統備援機制之探討

作者／蘇尚達 少校

提要

戰術區域通信控制系統(CONTACS)負責管制陸軍通資骨幹網路通連重大任務，戰時必定易遭敵摧毀破壞，能否迅速完整回復通資作業能力，全賴各類備援系統是否正常啟動運作。有鑑於此，本論文針對現有備援機制實施探討並研究其不足之處，參考市場上現有通資系統備份運作架構並實施比較，設計修改網管中心現有備援機制，使系統備援機制更趨強化與安全。

壹、前言

臺灣發生的921地震，高雄、竹科大停電；美國911事件發生，兩棟大樓所有電腦資訊瞬間消失，天災人禍對台灣相關產業之影響重大，如何作到不停頓的資訊服務及全面考量無預警的災害發生，降低運作風險所帶來的衝擊，是整體通資安全管理最重要的一環，身為國軍通資電的一員，對於維護系統正常無誤的運作，當從備援機制著手，考量電腦資訊通訊之異地備份、災害復原作業程序與執行速度等多方面架構建立。[1]

戰術區域通信系統(簡稱為陸區)為我陸軍新一代通資骨幹系統，可使戰時快速機動打擊通資系統快速構連，使戰力得以迅速發揚。其所有規劃需倚靠戰術區域通信控制系統(CONTACS)[2]，能否具有高存活力與受創後快速恢復能力，考驗著陸區系統的使用情形。

一、研究動機與目的

陸區系統規劃皆倚靠CONTACS實施分配及運用，如何提高現行安全備援機制，使系統在任何情況發生災害下，能否快速恢復支應作戰任務為主要動機，且通資安全乃現今我通資部隊系統規劃運用時所必須考量之因素，為因應支援各部隊戰術運用需要，也成為現今焦點之一。目前陸區系統以北、中、南三作戰區為劃分，各自配賦CONTACS，各軍團負責管理及規劃所配賦的陸區裝備，隨著戰術運用考量，目前雖已完成北、中、南三軍團的系統介接及平時部署，能夠達成全島系統的運作之功能，但除此之外仍有許多備援機制設計運用，可

1 立法院資訊系統異地備援中心簡介，頁 1，曹志強，2006 年。

2 CONTACS，由CONtrol管制、Tactical戰術、Area區域、Communication通信、Systems系統等字組成。

供未來精進探討設計之研究與分析，故本論文以探討網管中心所設置之各類備援系統，如何實施運用與達成功效，啟動備援管控機制，作為爾後性能與系統安全提升或各類戰術運用時，陸區系統管理者的運用參考方式。

二、研究範圍與限制

本研究僅針對系統安全備份控管部份實施研究，其餘各類系統存活能力與或與國軍網路連接等備援方式不再實施論述，系統內部軟硬體，以不改變現行網管中心內各類伺服器所提供之作業系統為規劃目標，並排除國軍整體軟體採購規劃、特定軟體實施討論及美方合約伺服器內建置之作業系統與軟體問題。

貳、本文

戰術區域通信控制系統(CONTACS)，其功能在執行陸區系統先期(即時)規劃管理、指揮管制、部署監控、作業分析評估，當中包含主要通信作業中心(Primary Communications Operations Center, PCOC)、外接式網路密鑰產生器(Dismounted Network Key Generator, DNKG)及外接式節點管理設備(Dismounted Node Management, DNMF)三部分組成[3]。

一、作業流程及備援設備

(一)作業流程

第一階段，確定任務或作戰需求；如救災、演訓等。上級單位針對本次任務先行實施分析與計畫的擬定。

第二階段，各單位於命令發佈後針對該單位的任務特性與需求，再次擬定相關計畫與命令。單位通信組、幕僚(作業人員)針對此次任務之相關資料交由操作手分別輸入至作業命令管理系統(OP Order Manager)、無線電頻率資源及網路規劃管理軟體(Clear Wave)等軟體並輸出後呈交上級核准/簽署。

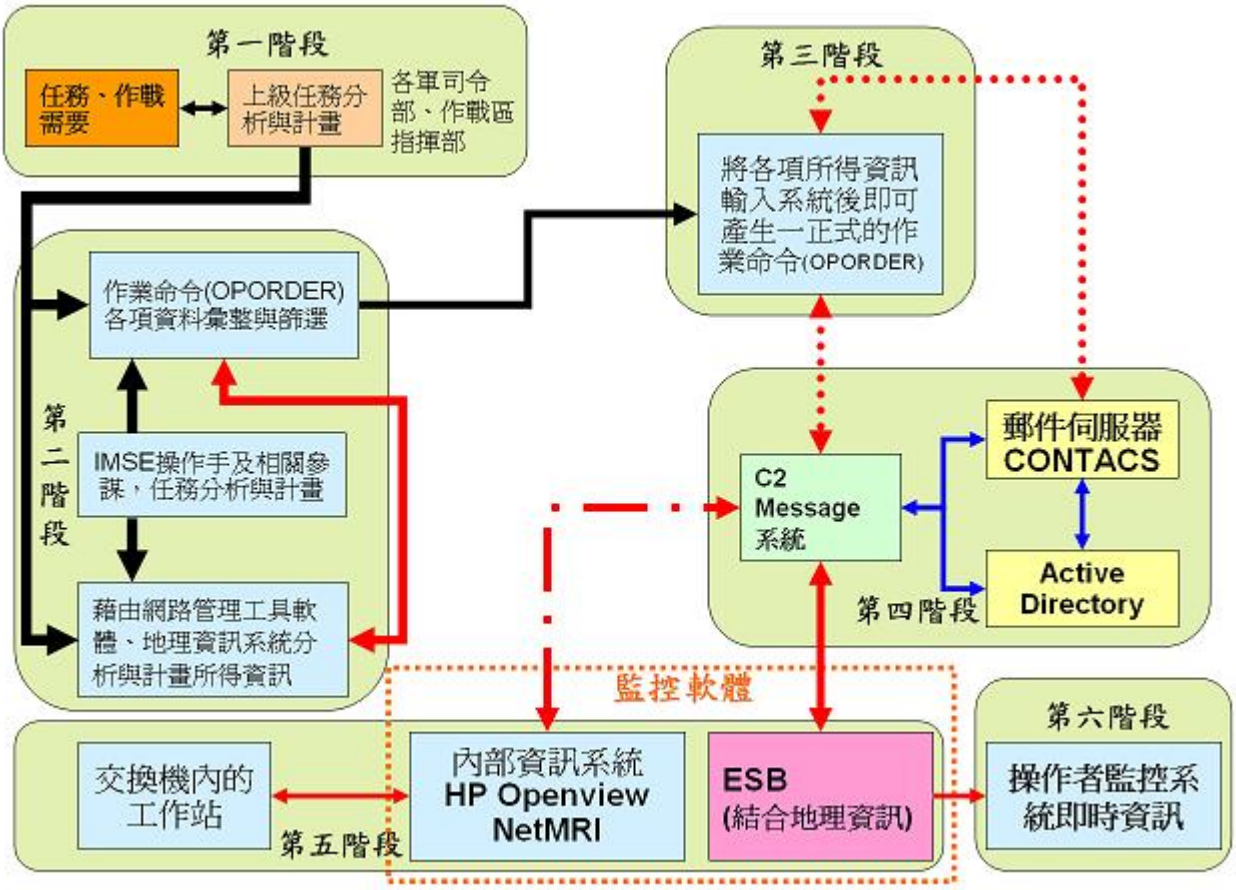
第三階段，任何命令只要經過相關人員核准/簽署後即可發佈至單位執行。

第四階段，接下來操作人員經由動態目錄伺服器(Active Directory)認證後，可透過指管訊息作業系統軟體(Command and Control, C2 Messaging)，對系統進行即時的監控、管理及命令的發佈與回覆。

第五階段，電子狀況顯示板系統軟體(ESB)、內部資訊系統(HP Openview/ NetMRI)，連接 C2 Message 系統、交換機工作站等，藉此掌控系統連接狀況。

第六階段，一般人員可透過電子狀況顯示板系統軟體(ESB)，對系統進行即時的監控。流程示意圖如圖一。

[3] 戰術區域通信系統手冊，第一冊，民國 93 年 6 月 1 日。



圖一 系統整體流程作業圖
（資料來源：作者整理）

(二)伺服器架構與配置

在陸區系統中，PCOC有二部Windows 2000 Advance Server[4]，每一個PCOC均有兩部郵件伺服器所構成的叢集伺服器(Cluster Services)；每一套叢集郵件伺服器，均被視為(設定為)一個站台，以增加作業效率。系統伺服器架構配置圖如圖二。

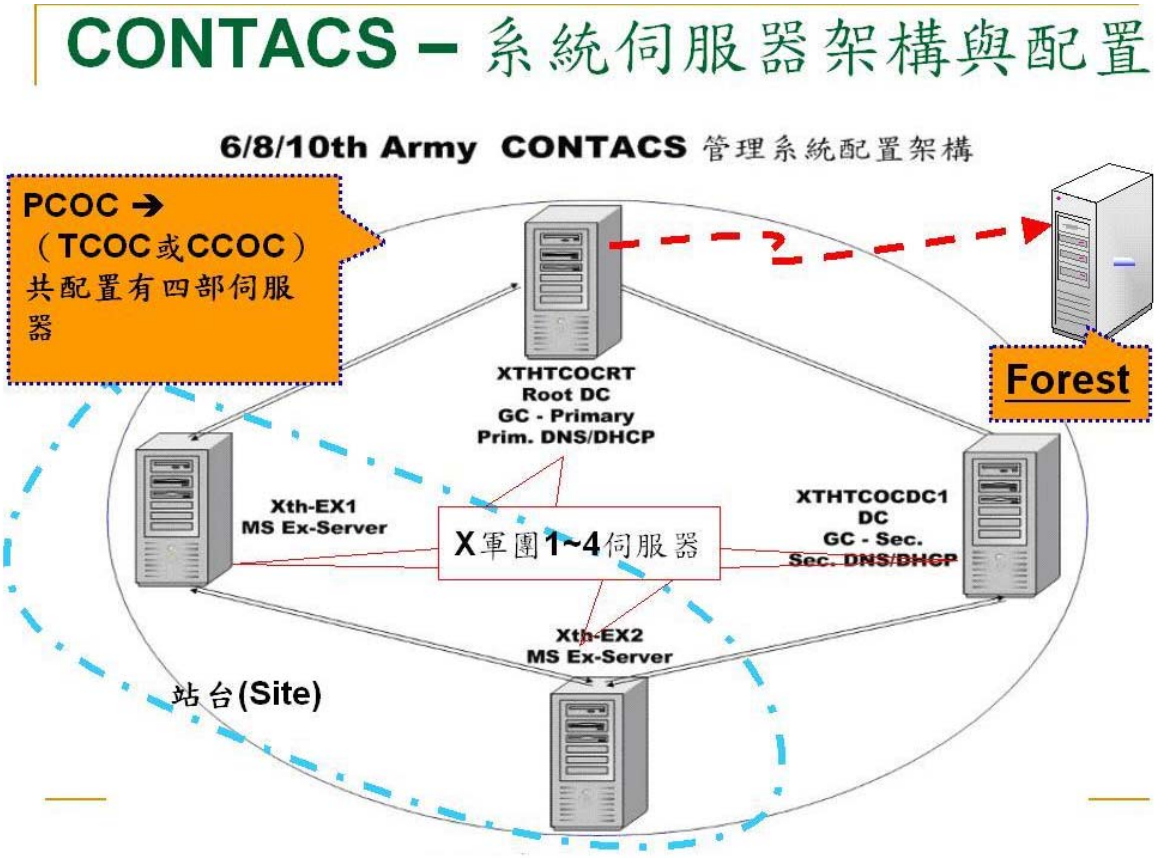
1.系統伺服器

Root是主要的網域伺服器，負責網域名稱伺服器/系統(Domain Name Server/System, DNS)及動態主機構成協定(Dynamic Host Configuration Protocol, DHCP)的工作；DC1為次要的網域伺服器，與主要的網域伺服器彼此互為代理，而EX1(EX2)是網域內主要的郵件伺服器。

Forest伺服器就構起陸區網管系統的伺服器主幹，整個Forest將擁有一個共同的Enterprise Exchange管理群組來負責管理，而每一個網域將有一個Exchange管理群組；而每一個郵件站台將設定為同樣的First Storage Group及

[4] 唯獨 6 軍團 PCOC 有例外狀況，多配賦 1 部於通校，因此有 3 部伺服器。

routing group，每個軍團均配有乙部Forest伺服器，但由於Forest是主幹伺服器，因此在整個系統運作時，僅能乙部Forest伺服器上線運作，避免造成系統混亂無法正常運作。



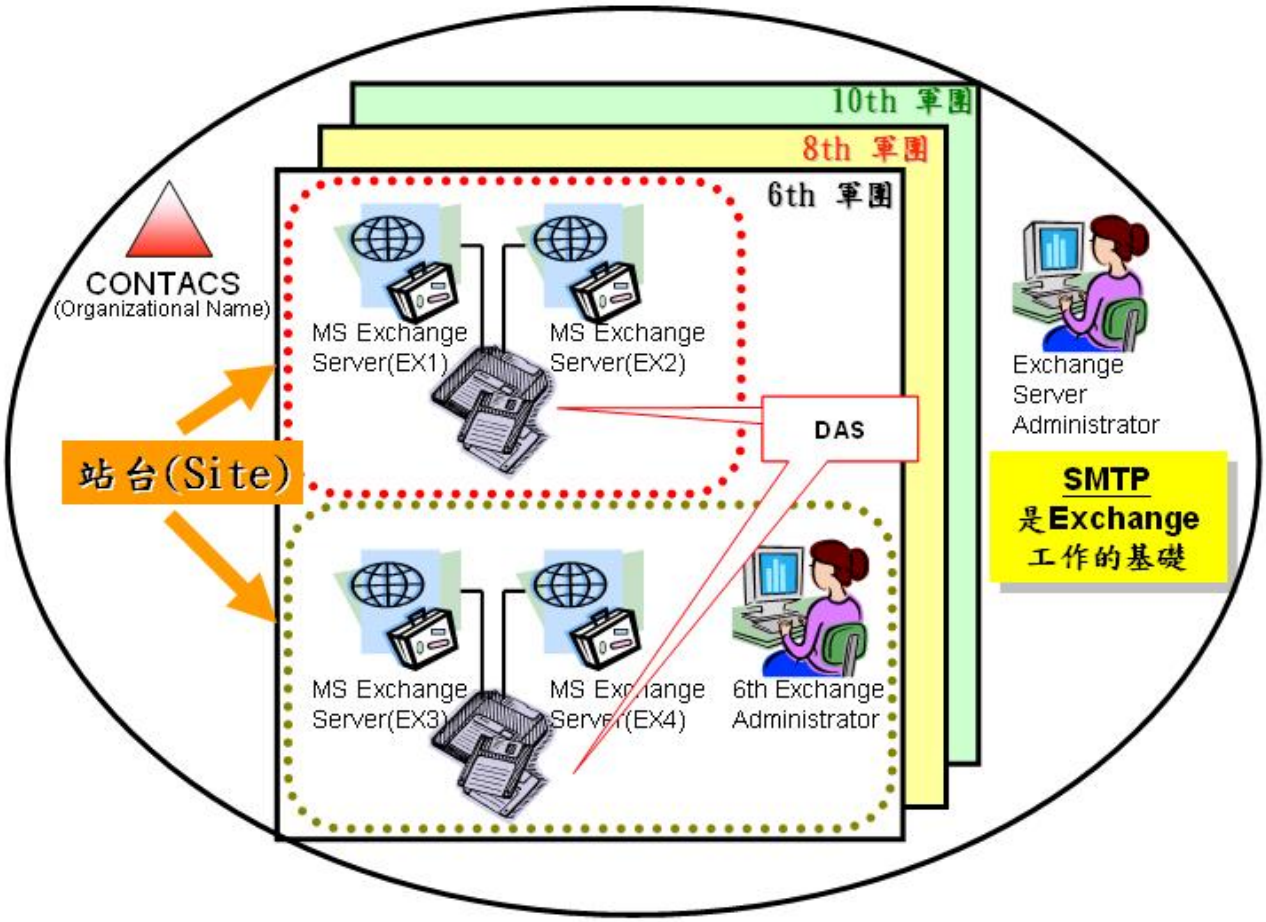
圖二 系統伺服器架構配置圖

(資料來源：戰術區域通信控制系統平台建置，陸軍通資校教案)

2.郵件伺服器

系統中所有的郵件將統一使用一個Exchange的群組(Exchange Organization)；其中劃分為六個站台，每一個軍團二個，但加上通校也自成一個Site，因而實際上陸區系統將擁有七個Site。

每一個站台將包括二部Exchange叢集伺服器及一台DAS(直接附加存取設備)；在實際運作狀況下，所有的郵件都將由SMTP virtual server來負責在站台間互相傳送；每個軍團同時間僅能有一個SMTP virtual server在運作，另一部則負責備援的工作，可隨時經由人工程序取代。郵件伺服器架構配置如圖三。



圖三 郵件伺服器架構配置圖

(資料來源：作者整理)

(三)備援設備

1.伺服器內磁碟陣列(Redundant Array of Independent Disks, RAID[5])機制

(1)網域森林伺服器(Forest Server）具有 2 個 40G硬碟，使用RAID 1[6]方式運作。

(2)根伺服器RT（Root Server）/網域控制伺服器DC（Domain Controller Server）具有兩個 40G系統硬碟，使用RAID 1 方式運作；三個 80G資料硬碟，使用RAID 5+Spare[7]方式運作。

2.DAS 設備與功能

主要為了系統的常態運作及維持，以 RAID 5 的方式實施運作，第八顆硬碟是隨時待命的，可任意抽換七個工作硬碟的任何一個；因此當操作手登入系

[5] RAID，簡單來說就是把許多顆硬碟放在一起，由一個電腦控制器來統一操控，並把所有硬碟整合成一個虛擬的大硬碟，使硬碟的總容量增加，並且提高硬碟的存取速度，安全性、穩定性和執行效率。

[6] RAID1，由兩臺以上的磁碟組成，將資料同時寫入第一組硬碟與第二組硬碟，兩組硬碟上的資料完全相同，所以又稱之為鏡像 (Mirror) 磁碟。

[7] RAID 5+Spare，需要 N+1 個硬碟，方式是將資料切割成數個區段，同位元檢查碼放在每一顆硬碟中，可於任一硬碟發生錯誤後復原，其中增加一備援硬碟，對資料安全多加一層保障。

統時，僅會發現 6*80=480GB；(第七個硬碟 1*80=parity 同位檢查；第八個硬碟 1*80=Spare 備份硬碟)

3.APC UPS

可提供 1500VA 的緊急電源，提供系統一個完善的電源備援系統，確保系統資料的安全。

4.工作站 4 部

提供網管人員執行網路規劃軟體、系統監控使用；節點排長(網管操作人員)執行作業、網路管理、系統訊息回報(C2 Messaging)等功能使用，內部具有 Norton Ghost[8]單機版備份軟體。

5.主要通信作業中心 (PCOC)主備設置

通信作業中心有兩種形態，分別為非戰術型通信作業中心中心(CCOC) 與戰術型通信作業中心(TCOC)，而內部所有伺服器亦分成兩套運作，形成相互備援的機制。

二、備援機制之研究

(一)診斷及分析(Assessments and Analyses)

當各類風險的發生，對資訊安全必會造成相當大的威脅，因此Spruit and Looijen將威脅分類歸納可能使系統停止的原因如下表一，使未來能有更加完善的防護手段。

表一 診斷威脅分析表

問題類別		原因	說明		後果
天然災害	災害	外部自然現象	暴風雨、颱風、水災、火災、濃煙、地震等		資訊服務無法正常
	故障	系統故障	軟體、硬體、網路故障		
人為因素	過失	人為操作故障	疏失	1.操作疏失 2.維護疏失 3.管理疏失	1.無法正常服務 2.影響戰力 3.威脅國軍資訊安全
	故意	故意造成故障	破壞	1.電腦系統遭受破壞 2.資訊設備遭受破壞 3.資料程式遭受破壞 4.資料程式遭受竄改	
			不當使用	1.擅自使用電腦設備 2.未經授權使用 3.不當使用程式、資料	

(資料來源：作者整理)

[8] 軟體廠商 Norton(諾頓)備份軟體產品名稱。

(二)備援方案及架構(Solutions Architecture)

1.系統需求等級

最好的硬體設備、網路架構、技術，通常都需要付出價格不菲的代價，因此在規劃備份方案時，重要的是了解單位實際的需求，選擇適合單位本身的建置方案。單位可以在評估預算時以資料遺失及回復資料時間對單位所造成的損失來規劃，如此可以避免保護不足或過度保護等問題。如網路銀行和單位內部檔案伺服器的重要等級就不同，當兩部主機的回復時間要求就不相同，也影響預算的編列。

2.計劃備份容量

備份的資料量越大小，所需要的時間、硬體、磁帶和網路頻寬；單位底有多少伺服器需要保護？其總資料量有多少？這些伺服器的系統設定檔及應用程式是否需要備份？因此根據過去的經驗，計算合理的資料成長空間，這些數據將提供我們在計算備份的時間及所需工具時重要的參考依據。

3.規劃備份時間

在有限的時間內完成備份且不影響伺服器效能的狀況下，單位必需依照本身的特性找出一個最適合的時間點進行備份，如一般備份執行時間皆會規劃在離峰時間，24 小時運作的服務(如資安管控伺服器等)就規劃在半夜或假日，進而規劃相對所需效能的軟硬體投資。[9]

4.備份方式選擇

(1)完整備份(FullBackup)：簡單的說執行完整備份即對系統進行所有資料的備份。增量備份：可有效率地使用媒體，因為其只備份當天異動的資料，所以相對於完整備份，僅需較少的資料儲存空間。

(2)差異備份(Differential)：只備份當天異動的資料，所以相對於完整備份，僅需較少的資料儲存空間。同時備份所需時間也會比完整備份或差異備份來得少。

(3)增量備份(Incremental)：差異備份是備份從上次進行完整備份後異動的全部檔案。差異備份所需的時間介於增量備份及完整備份之間，但執行資料回復時會比增量備份快速。[10]

5.儲存技術方案

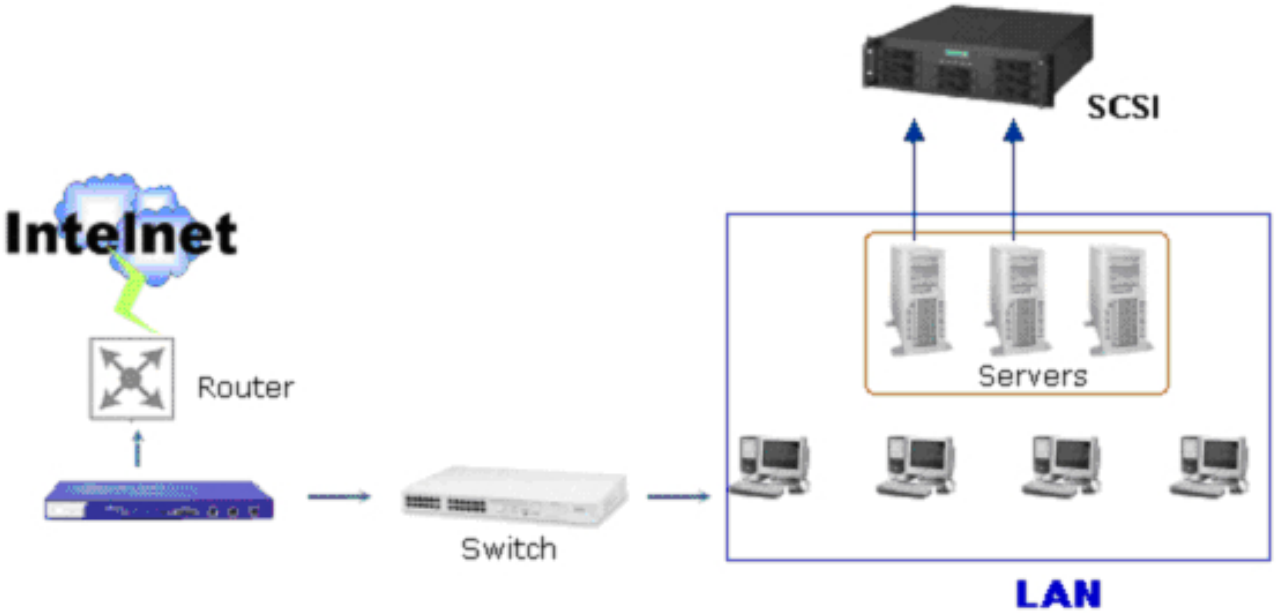
然而一般在建構內部儲存網路時，通常會選擇DAS、NAS與SAN等三種技術方式相互搭配以作為完整的解決方案，以下分別就DAS、NAS與SAN進行

[9] 儲存管理小撇步，頁 2，http://blog.cubo.com.tw/resserver.php?blogId=2&resource=storage_tips_a.pdf .
[10]同駐 9，頁 4。

逐一的介紹與分析比較。

(1)DAS(Direct -Attached Storage，直接連接儲存設備)

此種資料的儲存架構，是最早採行的On Line型儲存設備，主要組成成分包括儲存裝置與作為介面的主機介面卡(Host Bus Adapter，HBA)，大都是採用硬碟(以SCSI、SATA及IDE協定為主)為主要的儲存媒體，對於網路上的檔案共用及資料的存取，皆需透過檔案伺服器(File Server)這個角色。示意圖如圖四。[11]

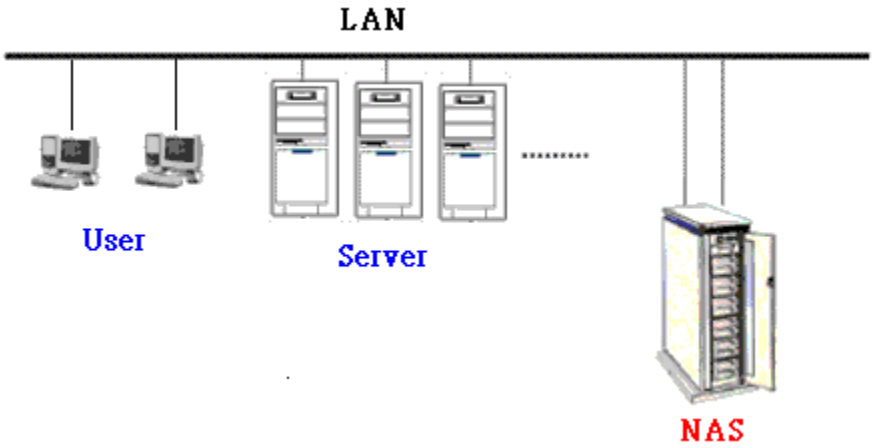


圖四 DAS示意圖
(資料來源：企業儲存架構--DAS、NAS與SAN簡介，http://www.pczone.com.tw/ vbb3/ thread/ 24/29813/。)

(2)NAS(Network Attached Storage，網路附加式儲存裝置)

NAS是一個只專門負責檔案I/O的高效能儲存設備，系統透過特殊專門的檔案伺服器直接連到區域網路上，由於此一伺服器是專門設計用來進行資料存取的動作，因此企業內的其他伺服器便不須同時兼負資料存取的動作，而有更大空間去進行其他的工作。以一種透過網路連結的方式，以提供不同的電腦系統間進行檔案的存取與共用的儲存設備。示意圖如圖五。[12]

[11]企業儲存架構--DAS、NAS 與 SAN 簡介，http://www.pczone.com.tw/ vbb3/ thread/ 24/29813/。
[12]同註 11。

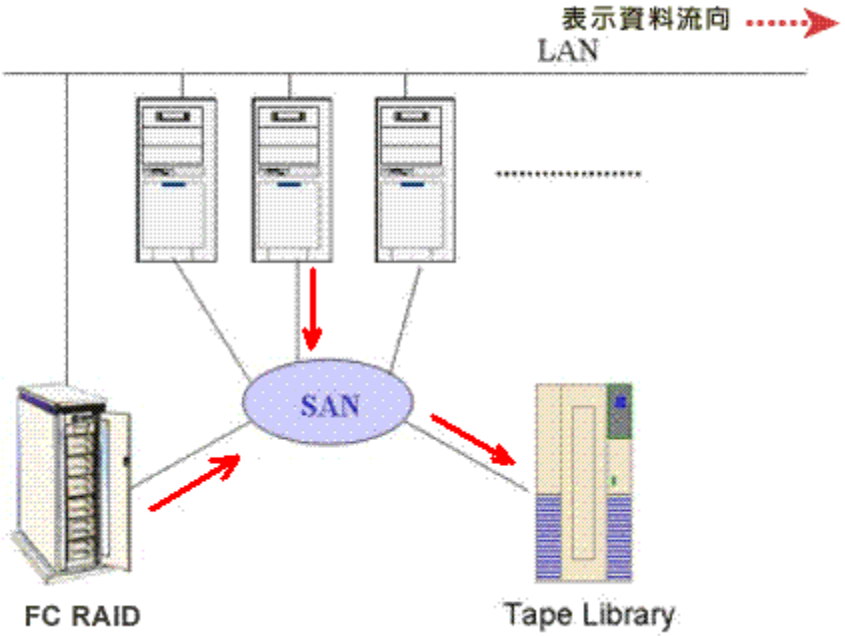


圖五 NAS示意圖

(資料來源：企業儲存架構--DAS、NAS與SAN簡介，http://www.pczone.com.tw/vbb3/ thread/ 24/ 29813/。)

(3)SAN(Storage Area Network，儲存區域網路)

其概念是將伺服器與儲存設備分開，並從區域網路中獨立出來而成為另一個網路，最大的特色即在於得以實現伺服器與儲存設備間有獨立的高速通道，可實現多點對多點的高速連接。這樣一來，伺服器可將其資料儲存這件事完全丟給儲存裝置處理，只要專心於資料的處理工作，同時尚可降低伺服器與伺服器之間的資料流通量，伺服器跟儲存裝置兩者各司其職，以達到一個高效能、高穩定度的儲存環境。示意圖如圖六。[13]



圖六 SAN示意圖

(資料來源：企業儲存架構--DAS、NAS與SAN簡介，http://www.pczone.com.tw/vbb3/ thread/24/29813/。)

[13]同註 11。

(4)DAS、NAS 與 SAN 之比較

DAS的效率不佳、擴充不良等問題，已是不爭的事實，現在大多已由NAS跟SAN來取代，因為NAS與SAN的適用環境有所不同，再加上企業對於成本與實際運作需要的考量不一，因此許多單位經常同時擁有NAS與SAN這兩種儲存架構。然而NAS與SAN架構呈現一種互補、卻又相互競爭的特殊狀況。由於架構與應用技術上的差異，促使NAS與SAN各自有其適用的情況。例如NAS採用的是技術較成熟、且成本低廉的區域網路，但是因為其穩定性不如光纖通道，因此較適合使用於網路目錄服務與檔案服務…等應用程式；至於SAN因為是在專屬的儲存架構上運作，因此諸如主從運算架構應用程式、資料庫…等專屬性或是績效要求高的應用工作，便適合透過SAN的架構才加以實現。[14]

三種備份儲存機制功能，分析整理如下列表一：

表一 備份機制功能分析表

	DAS	NAS	SAN
存取方式	透過網路儲存	透過網路儲存	透過網路儲存
管理方式	較困難	簡單	中
管理界面	須透過 MIS 人員自行設定權限管理	WEB 界面、LCD 控制面版	WEB 界面
效能	主機處理儲存 I/O 的方式，還須負擔相關作業系統的處理程序及服務，造成主機儲存的負荷	只有處理儲存 I/O 的方式，較不會對主機造成效能的負荷	使用光纖介面存取，對不會主機造成效能的負荷
安全性	採用 windows base 的認證方式，病毒防護性較差	透過內建的帳號進行管，較不易中毒	完全小型獨立網路架構，不易中毒或遭入侵破壞
網路協定	支援 TCP/IP，NETWARE，NFS，CFIS，APPLETALK 協定	支援 TCP/IP，NETWARE，NFS，CFIS，APPLETALK 協定	支援 TCP/IP 協定
硬體架構	用 IDE/SATA/SCSI 等界面連接至電腦主機上，供其他人存取	使用 RAID 架構、Ethernet 網路介面組成，以網路方式共同存取	在伺服器與儲存媒體間另成一網路，目前無統一標準架構

(資料來源：作者整理)

6.備援機制分析

備份與備援之目的皆是為了災難復原，兩者之分別在於備份大多指資料或

[14]同註 11。

軟體結構複製的統稱；備援則除了資料、軟體結構外，連同硬體建置另一套相同的系統，但只是復原時間與復原需求不同，一般方式如下：

(1)叢集系統備援架構(Cluster)

由兩套相同的電腦設備與作業系統組成，當一台電腦設備故障時，另一台會自動接手。一般叢集電腦皆在同一機房或同一大樓內，資料隨時透過網路專線，以同步或非同步傳輸至另一設備中。

(2)遠端備援架構(異地備援)

A..以磁碟機為主要備援資料的媒體，利用磁碟機之控制器，將資料複製到異地儲存。

B.利用資料複寫技術，將資料複寫到異地。資料複寫技術的異地備援方式，可分同步及非同步複製資料到異地等兩種方式。[15]

(三)導入管理(Implementation Management)

將備援的程序做成標準作業程序(SOP)，並且依這個 SOP 的方式，以文件方式作為實施依據與方式，其方式要點如下：

1.預防作業

主要目的在於日常備援備份作業，並提供系統運作之日常監控。

2.緊急應變

重點在於系統異常狀況發生後之應變作業，並採取損害評估作業程序，確保應變作業順利進行。

3.災難復原

系統發生重度災難或特殊異常狀況時，進行系統復原作業，以確保系統的持續運作。

4.教育訓練及執行

實施 SOP 訓練，使人員可快速有效按程序執行。

(四)測試及維護

系統完成後，在不影響運作的情形下進行模擬演練，達成不停頓的目標。

三、現行備援機制運作方式

(一)非戰術型通信作業中心(CCOC)與戰術型通信作業中心(TCOC)

現行以複式配置方式達到備援效果建構兩套中心，於平時使用CCOC，進入戰備階段時，隨著軍團指揮所開設地點變換，使用TCOC，其CCOC與TCOC兩者的差異，在於前者開設作業於固定掩體中，而後者開設於野戰帳篷當中，其

[15] 台灣凌越，http://www.lyserp.com/TWindex.htm。

中所有的電腦設備，僅隨著系統的開設，而僅有乙套存在與運作。換言之就是說當CCOC開設時，所有的電腦都在CCOC中，但須開設TCOC時，就將所有電腦設備移動至TCOC當中，CCOC內就無任何設備存在。

(二)伺服器備援機制

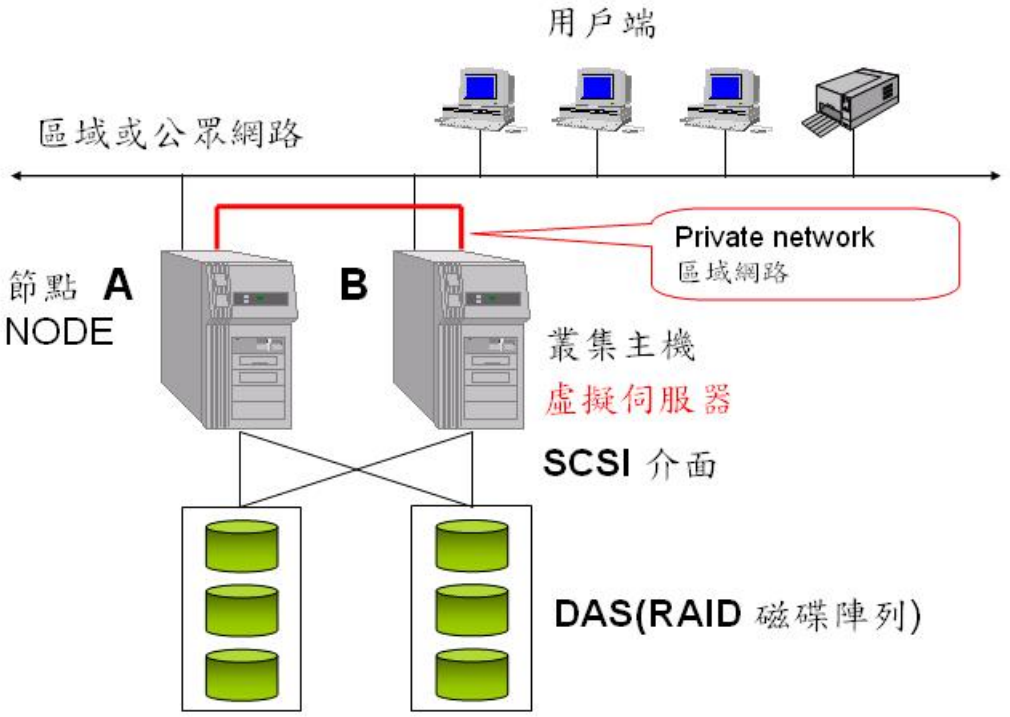
伺服器區分為AD伺服器與郵件伺服器兩類，其中AD伺服器有兩部，分別為RT與DC，同時開啟運作，彼此相互備份系統內部資料，成為兩部AD架構相同的主機，但僅有乙部有主控權，可管制、變更、儲存整個架構資料。

郵件伺服器所運作的軟體為Microsoft Exchange，分別為EX1至EX4，但僅有兩部同時開啟並以叢集的方式運作，可增加相同服務的伺服器，提供更多的使用者使用，減輕伺服器運作時的負載，並達到服務備援的功能。

(三)資料儲存備援

內部建立乙部DAS，以RAID 5的方式實施運作，降低硬體設備損壞時的衝擊，線上工作硬碟1個損壞時，仍可正常工作，再加上系統有8個硬碟，僅7個運作，1個備用，可防止2個以內的硬碟同時損壞的情形發生。

此外叢集架構可使系統永不停頓，有分散資料風險、彈性儲存的特性，不論彈性增加或減少主機，對外而言，服務絲毫不受影響中斷或改變。圖七即為叢集伺服器備份架構並結合DAS備援系統工作示意圖。

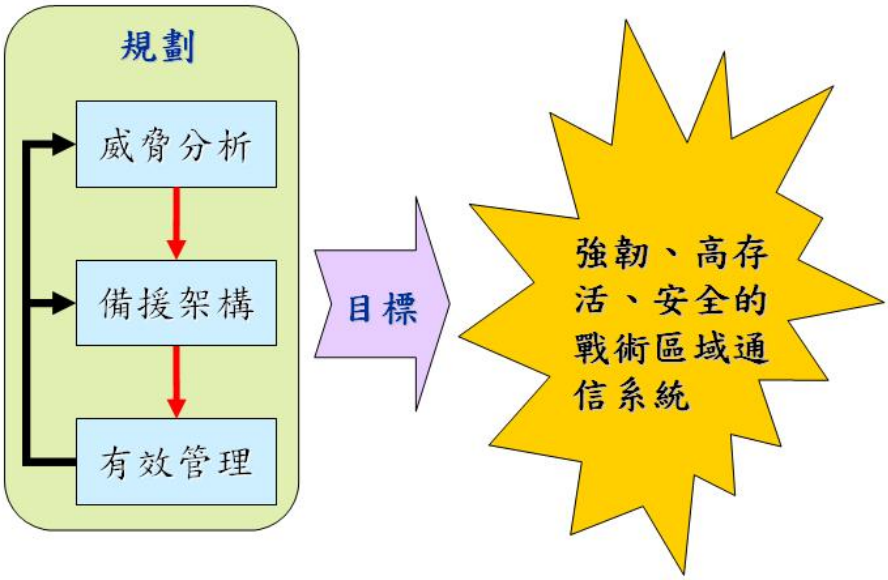


圖七 伺服器備援架構

(資料來源：作者整理)

四、規劃建議及作法

面對我新一帶戰術區域通信系統越來越趨於資訊化的環境，各項危安事件的發生，包含了天災、人禍及電腦系統不正常的故障，都足以危害我陸區系統存活造成重大損失，並影響我建軍備戰之戰力發揮，因此針對現行安全備援架構提出精進作法，運用規劃分析方法，致使現行架構能更趨完整與安全。



圖八 建議作法流程圖
(資料來源：作者整理)

(一)威脅分析

1.分析目前戰術區域通信控制系統配置情況，可能發生故障情形如下：

(1)操作人員訓練不足，因動作不熟悉或未按規定流程作業，以錯誤的方式實施操作，將對系統或資料造成損壞。

(2)網路上存在的電腦病毒、惡意程式、木馬入侵、網路飽和攻擊，對現有程式系統造成破壞或嚴重影響效能，致使伺服器無法正常運作。

(3)各類自然天象等情形所造成的損害，如豪雨、潮濕、雷擊、等天然災害；突然電力中斷的非人為因素；北部多雨、南部天熱，造成內部線路易潮濕短路或過熱而當機，這些情形皆會造成硬體設備故障情形發生。

(4)通信管制、網路管理、頻率分配、密鑰分配、備份資訊等系重要系統資料，並無流程規範安全儲存備份方式，若遭遇損害時，系統無法迅速有效恢復，對整體架構安全有重大之影響。

2.彙整經常發生之各項災害足以影響整體系統安全之因素，並分析現行架構與伺服器上已有備份機制使用與存在作業情形，作為備援機制精進之分析因素，將其中未盡完善、安全防護不足部份，共列出以下四點：

(1)AD伺服器內資料，如Schema、帳號密碼、權限管理等。

(2)系統通聯所需參數，如無線電入口(Radio Access Point, RAP/Radio Access Unit, RAU)的頻率計劃、涵蓋面積半徑、UHF多波道鏈路使用頻率、資訊路由的設定參數、通阻流量狀況紀錄資料、鏈路數位傳輸群組(Digital Transmission Group, DTG)[16]管理分配計劃與作戰計畫命令等。

(3)作業系統或或資料毀損或故障而無法正常工作時，必須以手動啟動還原作業。

(4)現用磁碟陣列櫃內使用RAID5 +Spare備份機制的方式運作，但架構以DAS方式連接，必須在連線伺服器正常運作下方能使用。

(二)備援架構

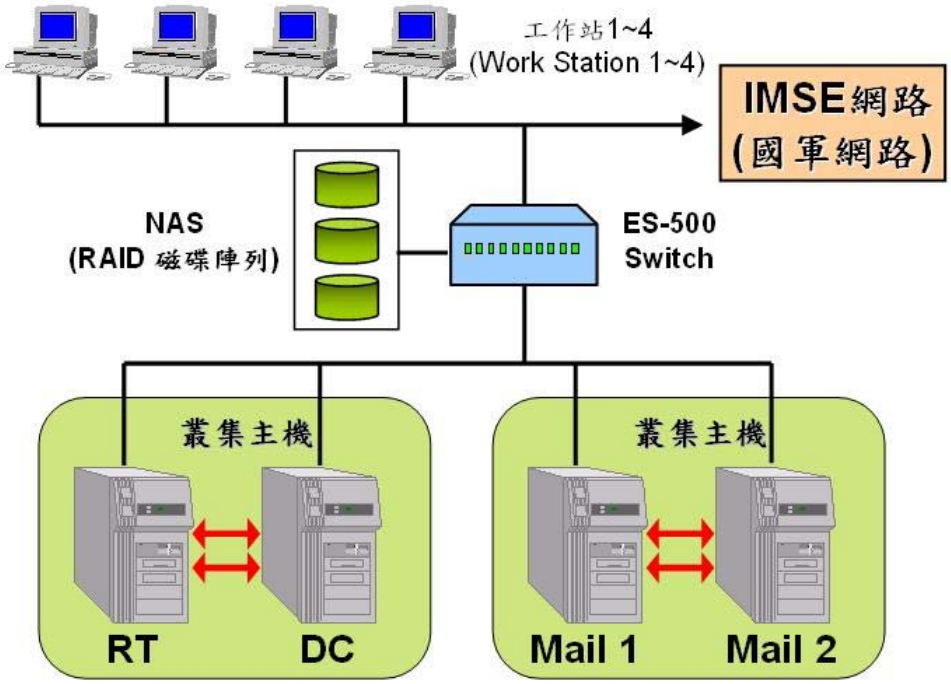
針對現有的戰術區域通信控制系統提供精進作法，但因伺服器礙於仍由美方合約問題，所使用之作業系統及內部軟體，無法實施更換或在中增添其他軟體，因此在有限條件下，對現有系統安全備份架構實施性能提昇，以不對現有架構龐大更動，避免增加系統複雜度，建議方式說明如下：

1.將磁碟陣列櫃連接方式由DAS更換成NAS

現有備援機制下，各伺服器、工作站對連接做資料存取，都必須透過郵件伺服器的線路連接，但只要郵件伺服器有任何問題，進而使得磁碟陣列櫃無法存取，影響資料備份安全性及儲存便利性，然SAN架構運作，係因型態對現有系統網路架構變動大，所有網路存取界面必須更換，對日後系統介面透通性有所限制，因此改用NAS架構後，除可避免上述而之情形發生，並使儲存方式擴充，增加備份的彈性，只要能夠用乙太網路介面連接的設備，就能對磁碟陣列櫃實施存取。

而各伺服器內RAID機制無需再作更動，因市場上現有備份機制除RAID 5外，已有更進步安全的技術，如RAID 6、RAID 1+0等，但在效益上並無太大的提升與幫助，以保持原有的RAID機制為主要規劃。PCOC備份架構圖如圖八。

[16] 戰術區域通信系統交換機傳送信號格式名稱。



圖八 PCOC備份架構圖

（資料來源：作者整理）

2.資料異地備援

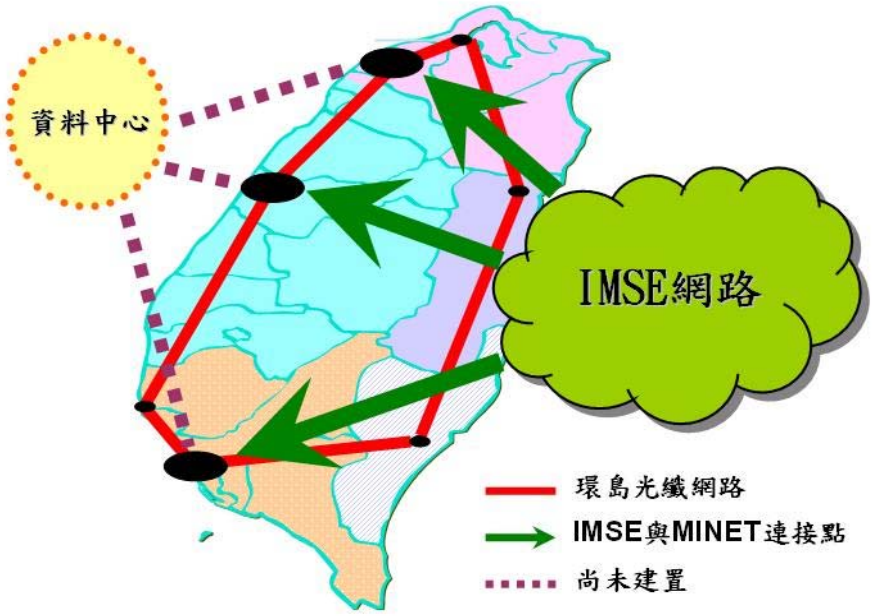
AD伺服器資料、工作站製作而成的參數或管制系統而產生之記錄檔等資料，均可藉由連接至通信作業中心的NAS中，將資料存放至其中，使得伺服器及工作站中存有乙份，NAS中亦存有乙份，使得磁碟陣列櫃若損壞，仍可於工作站中取得資料持續工作。

除此之外，備份資料可經由陸區網路[17]傳送至其他的通信作業中心(PCOC)而儲存，因此每個PCOC除了自己本身，同時也擁有別的PCOC備份資料，可在任一PCOC無法工作時，替代而起之工作。

戰術區域通信系統除自己本身網路外，分別於北、中、南三個軍團中與國軍骨幹網路連接，能夠將戰術區域通信系統服務，運用國軍骨光纖幹網路傳遞，同時也能使用國軍網路中各項服務，因此備份資料傳遞除了陸區網路外，也可透過國軍光纖骨幹網路，形成多重鏈路備援架構。

然而所有的通信控制中心的地點，相距都在50公里外，超出一般企業界規劃設置的考量，但若就在國軍未來資料中心建置完成，於特定地點可提供的資料儲存服務，必對此備援架構能有更多一層的保護。異地備援架構圖如圖九。

[17] IMSE 網路可提供節點對節點網路傳輸頻寬為 4~8Mbps。



圖九 異地備援架構圖
（資料來源：作者整理）

(三)有效管理

系統中均有設置還原軟體，可將作業系統或資料製作成還原映像檔，但卻未規劃使用備份方式、備份時間、備份範圍？因此如何制定完整備份計畫、啟動備援步驟、建立SOP，使得備援機制得以完整發揮，全有賴有效管理的方式。

1.依據系統優先順序，按照關鍵性、重要度區分，將資料依項目分類實施備份，可減少備份工作產生的人力負擔，使備援效果能更為完善。建議備份方式如表四。

表四 建議備份方式表

分類 / 項目	作業系統	製作參數	郵件資料	作業命令
備份方式	完整備份	差異備份	差異備份	完整備份
備份時間	系統架構或伺服器網目更動	每個月或每次參數製作後[18]	每小時	每小時

（資料來源：作者整理）

2.現有叢集的方式已可運作正常，但在更改儲存架構後，其工作方式勢必有所更動；運用網路的異地備援方式，當中的作業程序也必須制定，才能有完整的備援的機制。管理驗證方向如下：

(1)叢集機制(Cluster)中，任一主機停止運作，接替而起的作業方式與效果。

(2)任一軍團所配置之PCOC遭敵破壞摧毀後，能否經由陸區網路代理其監

[18] IMSE 密鑰最短期限為 1 個月

控管制的工作。

(3)驗證陸區網路、國軍骨幹網路當中備份資料能否順利傳遞，以及任一線路斷線後，能否經由其他網路繼續工作。

3.運用各項操演結合平時戰備任務訓練，實際運做備援系統的標準作業程序(SOP)程序，動員相關人員以進行資訊系統災害復原SOP及緊急動員演練作業，演練作業旨在提升網管人員在面臨各種突發狀況時之通報與應變能力，完成緊急應變下實際作業需求，驗證戰術區域通信控制系統備援機制的效果。

結論

一、未來研究方向

(一)陸區系統通資安全

陸區系統內以有各類的加密機制、系統備援方式與通資安全執行方法，但係屬美軍早期規劃方向，與國軍現行通資安全政策仍有部份無法完全相符與執行，且通資技術日新月異，此方向未來仍有很大的研究空間。

(二)後勤維保

陸區系統由美方協助我建置，因此後勤維保能量仍有大部份掌握於美方手上，且備援系統設置，必定會對網管中心設備有所更動，因此如何規劃我軍建立更完整的後勤維保體制，除可支應我作戰持續力與存活力，對通資安全與備援架構強化，能有更大的幫助。

(三)國軍骨幹網路結合與應用

未來國軍資料中心建立，能否順利提供相關服務支應戰術區域通信系統備援或傳遞儲存資料，仍是一未知的考驗。

二、結語

期許能讓現有備份架構在此架構下具有更強韌與快速恢復的能力，使戰術區域通信系統於戰場上的存活力更強，系統資料具多重備份而更為完善，人員更能容易迅速的操作。而宏觀的系統規劃輔助適當的資料回復演習訓練，將能協助跨越可預見的瓶頸，可使我戰術區域通信系統更具有長久持續作戰能力，並將我軍部隊戰力完整發揚，但系統安全的考量是全面必需兼顧，否則在無網管中心的管控下，作戰如同摸黑走路般，無所適從，隨時可能被敵殲滅而全面作戰失敗，因此發展資訊系統備援服務與應變措施作業機制，全有賴通資系統快速靈活運用，於未來各項資訊通訊與應用服務，均能確保永續運作與資料完整，建立更優質安全的通資電環境。