交通部臺灣鐵路管理局

票務系統整合再造計畫書

中華民國 106 年 3 月 30 日

第10章 替選方案之分析及評估

10.1 網路訂票租用與自建分析

一、票務資訊雲端技術方案分析

票務資訊系統適合以雲端技術方案處理作業依，在訂售票階段依對外與內部作業，可再區分為使用者服務(包括：訂票請求接收、訂票確認、付款/取票方式確認)與可售班次座位查對兩類作業(即時資料處理與歷史資料處理)，各類作業分別具有快速大量資料、處理量變動大等作業特性，建議運用雲端技術執行前述作業，藉由雲端技術的高擴充彈性、高可用性與資源共享運用等技術特性，以經濟、可靠的方案滿足票務資訊系統的運作需求。

1. 訂售票—使用者服務：訂售票-使用者服務運作時，主要透過網頁或網路通訊與使用者或語音系統互動，作業具一致性，運用負載平衡方案可在服務尖峰時期分散大量接收與回覆的作業量、維持服務應符合之效能；訂售票—使用者服務所需作業資源，透過虛擬化管理因應服務作業量彈性增減(scaleout、scalein)。
2. 訂售票—班次座位查對：訂售票-班次座位查對運作時，必須於大範圍資料內即時篩檢出可供販售的班次、座位，為避免篩檢、搜尋過程過多的硬碟讀寫動作延緩處理速度，運用分散式記憶體內運算技術(DistributedInMemoryComputing)，除可減低作業時間即時完成班次座位的查對之外，在尖峰作業期間也可將大量查對作業分散處理、維持查對作業效能；訂售票—班次座位查對所需作業資源，可透過虛擬化管理彈性因應查對作業量進行增減。

表13 票務資訊服務雲主要作業解決方案建議

資訊作業	相關資料	作業特性	因應方式	技術方案	品牌參考
訂售票—使用者服務	訂票紀錄(要求、取票方式) 班次座位	尖峰/非尖峰服務量變動大	運用負載平衡技術分散服務作業量 運用雲端資源共享與快速部署的特性，快速因應資料接收量的變動增、減資料接收所需運算資源	負載平衡 資源虛擬化	F5 A10 Citrix Microsoft VMware
訂售票—班次座位查對	訂票要求 列車售票現況	尖峰/非尖峰處理量變動大 快速大量資料查對	運用記憶體內運算降低硬碟資料存取的的次數，加快運算速度 運用雲端資源共享與快速部署的特性，快速因應資料接收量的變動，增、減資料接收所需運算資源	分散式運算 記憶體運算 資源虛擬化	IBM Oracle Microsoft VMware

二、大量即時訂票技術分析

處理大量且需即時的訂票作業，有別於傳統資料庫管理系統(RDBMS，RelationalDatabaseManagementSystem)，快速資料 FastData 技術強調資料處理的速度，在許多應用功能回應時間就代表著民眾滿意度，如何縮短資料處理的時間，透過即時資訊來加速決策執行，也是企業改善營運甚至創造新業務模式的重要手段之一。

本局於 103 年 1 月 7 日上午所公布的春節東部訂票情況，在「第 1 分鐘」完成 6 萬 7000 筆、15 萬 2000 多張訂票；針對瞬間大量且快速需求的訂票服務必須考量雲端運算特性處理以下需求：

1. 訂票期間拉長，資料量處理量增加
2. 使用者瞬間訂票需求量極大，並於極短時間內處理完成
3. 跨幹線訂票需求，資料處理的複雜性

4. 因應前述巨量票務需求，並維持系統高可用性(Availability)與高穩定性(Reliability)，且不影響既有系統運作效能之情況下，將搭配雲端系統資源之動態調派彈性，有效利用雲端系統環境運算及儲存資源，快速解決系統應用負載之擴增需求、尖離峰高低需求與資料儲存需求，以確保系統高延展性(Scalability)。由於網路訂票系統負責即時接收外部瞬間大量的查、訂票作業，並須於限定時間內回覆作業結果，為因應此一大量且具時效性及資料量變動大的資料處理需求，為利於平行且分散之 DataDriven 運算，建議運用具備分散作業能力的 InMemoryComputingFastData 技術，藉由減低 DiskI/O 次數，加快運算速度以符合時效性的要求；應用 InMemoryComputing 可彈性不停機調配運算單元的能力，可因應資料接收量的大小彈性有效的應用系統運算資源。

表14 傳統資料庫與網格資料庫比較表

		RDBMS（現行網路訂票模式）	FastData（本案規劃模式）
授權方式	Free	MySQL、PostgreSQL	連線限制 2 個
	商業版	Oracle、DB2、MSSQLServer	SAP-HANA、ORACLE-Coherenc、Vmware-Gemfire
Client 連線方式(Java)		JDBC	ClientCache
Server 管理工具		豐富完整的 GUI 介面	cmd，shell
資料模型(DataModel)		定義結構化資料(tableschema)	Key-Value
儲存模型(Storagemodel)		DBFile	Memory(RAM) (可設定 DB 實體備存)
一致性模型(consistencymodel)		嚴格一致性(tableschema)	可一致也可不一致
實體模型(physicalmodel)		DBcluster	分散式主機
I/O(Read/Write)		DBFile	MemoryCache
索引(Index)		支援最豐富	支援
錯誤處理			可設定多台複製分散儲存
負載平衡		(DBcluster)	datalocator
可擴展性			可擴充
啟動速度		Fast	Nomral
寫入速度(Insert/Delete/Update)		Normal (若物件定義為關聯資料表，速度較慢)	Fast (可直接儲存物件)
SQL 語法支援		有	有

三、未來本局實際需求分析

1. 現有大量訂票業務量，網路訂票需 20 分鐘才能完全消化：

本局目前網路訂票委託中華電信承接相關系統業務，以103年春節為例東幹開放訂票1小時內，30分鐘內總訂票筆數為162,400(351,076張票)。30分鐘後為零星訂票，表示熱門車次已完售，旅客亦不再積極訂票。東西線30分鐘合計完成258,519筆訂票記錄(518,913張票)。

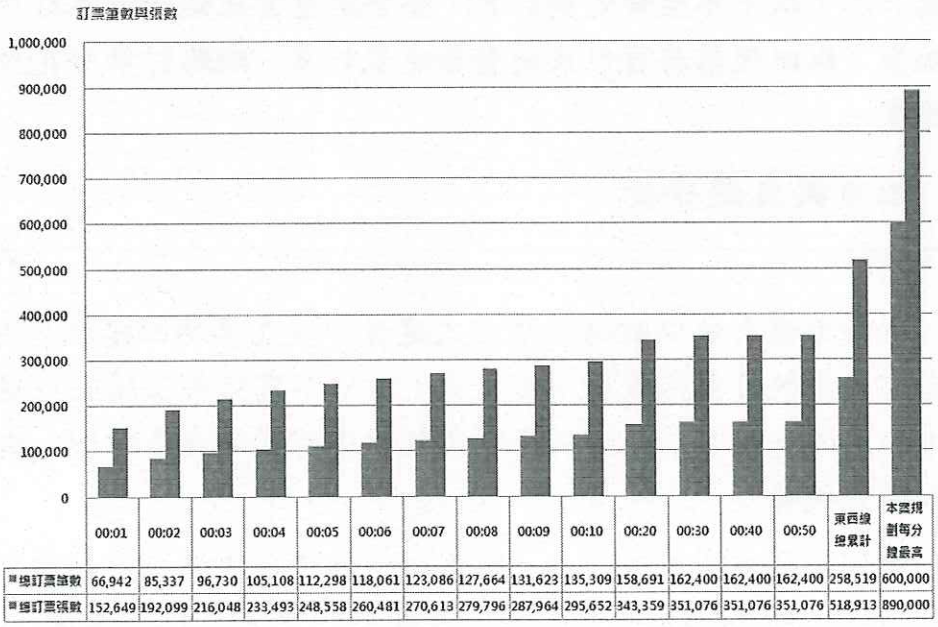
2. 因應未來本局 10 年內列車運能成長，本案網路訂票服務水準為：

(1) 每分鐘可完成40萬筆交易（61萬張票）

(2) 彈性至60萬筆交易（89萬張票）

(3) 上述指標經過本局委託規劃廠商採用 FastData 與 IMC 技術，建立網路訂票雛形系統，並通過經濟部雲端開發平台見證。

3. 整體分析如下圖所示



	00:01	00:02	00:03	00:04	00:05	00:06	00:07	00:08	00:09	00:10	00:20	00:30	00:40	00:50	東西線總累計	本案規劃每分鐘最高
總訂票筆數	66,942	85,337	96,730	105,108	112,298	118,061	123,086	127,664	131,623	135,309	158,691	162,400	162,400	162,400	258,519	600,000
總訂票張數	152,649	192,099	216,048	233,493	248,558	260,481	270,613	279,796	287,964	295,652	343,359	351,076	351,076	351,076	518,913	890,000

圖9　103 年春節東幹線、全線網路訂票交易量與本案規劃比較

四、網路訂票整合建置分析

1. 既有網路訂票無法滿旅客所需

由圖9可看出，整體東幹線網路訂票在開始訂票後20分鐘趨緩，總計有158,691筆交易與343,359訂票張數需求。因此可推斷出旅客春

節大量訂票需求需滿足至少1分鐘158,691筆交易，方能使旅客不至感受到網路壅塞與系統忙碌之感。

以現階段而言，既有網路訂票系統採用傳統技術無法滿足旅客需求，因此必須採用新技術方能滿足旅客所需。以本局委託規劃廠商雲端技術雛形系統實測，每分鐘最高可滿足60萬筆訂票交易，足以因應東西幹線合併訂票與未來10年成長所需。

2. 既有網路訂票與票務系統為獨立系統架構不利營運

第四代票務資訊系統中一項關鍵工作為導入收益管理系統，收益管理中動態依照旅客需求與收益原則配位。目前網路訂票系統與票務系統為獨立架構，窗口售票無法與網路訂票共用配位資訊，因此網路訂票在架構上必須與票務系統合為一體，方能順利施行收益管理。

3. 成本效益分析

本局初步估算網路訂票整合建置預估經費約為6仟萬~1億，每年維運與相關網路費用約10~15%。如以目前每年網路訂票費用3仟~5仟萬計算，以十年生命週期計算，整合建置實比現行網路訂票方式節省經費；以四代票務資訊系統整合建置計算，網路訂票所花預算應更為節省。

10.2 租用與自建分析

一、現況分析

現行票務系統以財務採購方式建置於臺北車站四樓機房內，網路暨語音訂票系統目前採服務租賃方式，由中華電信將相關服務建置於新北市永和區國光機房內。時刻查詢系統由臺灣世曦負責維運，機房亦位於永和國光機房

現行本局預約訂票系統，係委託中華電信代管於永和國光機房，主要提供網路訂票(railway.hinet.net)與語音訂票(412-1111)服務，目前應用伺服器計有網路訂票 14 部與語音訂票 4 部，資料庫伺服器共有 3 部(1 部服務、1 部備援與 1 部同步)。採用 Apache 與 Java 中介軟體、Oracle 資料庫、RedHat 作業系統。預約訂票系統係針對既有票務系統開發，由於依存度高且因瞬間大量訂票特性限制，在考量系統穩定性與使用習慣接受度的前提下，較不易增加新功能。

二、可行性分析

根據現有實際維運的若干系統所對應之可行方案，分別從具有代表性的專案、計價單位、優缺點等面向比較分析彙總如表 15。未來機房、設備或服務欲採用租用或自建之建置模式分別詳述如后。

表15 建置模式比較表

	方案	專案代表	計價單位	優點	缺點
1	機房自建 設備自購	財政部 臺電 本局	總包價法	自主性高 時效性高	政策不鼓勵 建置成本高
2	機房租賃 設備自購	經濟部工商 E 網通	機房空間 7U=3000 元(GSN)	機房專業性高	建置成本次高 時效性次高
3	機房自建 設備租賃	臺水	每年租金	自主性高 掌握度高 時效性高	政策不鼓勵 建置成本高 乙方中止租約
4	虛擬資源 租賃	實價登錄網	VM/小時	建置成本低 資源彈性調度	自主性低 責任難釐清
5	服務租賃	採購網	以案件 計價	建置成本低	合約難週全 自主性低

1. 機房自建＋設備自購

由於高可靠度的資訊系統有賴於穩定的機房設施及硬體設備，至少包括空間、電力(雙電力迴路、不斷電系統、發電機、足夠燃油)、空調、網路佈線、消防、照明、保全設施等，因此透過妥善的規劃與高度自主性的建置，可以依照客製化需求完成最符合自身業務之資訊系統。後續亦可根據未來業務發展需求，機動性調整已建置之資訊系統。雖然機房自建期初成本耗費最高，但本模式有最高度的維護自主性與服務可近性。以本案為例，本局機房均位於環島光纖網路上，有著絕佳的網路可用性。過去受限於各車站每年電力歲修需斷電四小時議題，如今台北車站已可透過防災中心的獨立電力供應，解決歲修停電議題，因此本選項將列入重點規劃方向。

2. 機房租賃＋設備自購

依研考會與中華電信簽定之 GSN 服務合約，可提供高可靠的機房設施與100Mbps 的網路頻寬，大幅節省機房建置成本，並保留資訊設備的自主性，在無法取得完備機房設施或自行建置機房的情況下，由於透過設備自購亦可以依照客製化需求完成最符合自身業務之資訊系統，後續亦可根據未來業務發展需求，機動性調整已建置之資訊

系統。由於電信機房並無駐點人員辦公空間，因此系統異常時，機房所在的位置與相關維護人員間之距離與交通時間問題須列入考慮。以現在本局網路與語音預約訂票代管機房－中華電信國光機房為例，國光機房位於新北市永和區國光路8號5樓，該處為專業電信機房，並不提供廠商駐點辦公，機房距離台北車站4.6公里，距離最近的頂溪捷運站950公尺，當異常發生時，維護人員由台北車站移動至國光機房5樓至少需時30分鐘，如果該異常狀況，將導致全省售票與驗票服務停擺，風險能否承受，列入方案評估與決策重點。

3. 機房自建＋設備租賃

由於整體資訊系統建置成本主要是在機房建置，包括用地取得與機房設施建置。相對來說，本模式有最高的建置成本(機房)，以及最大維護風險(廠商中止租約)。不過，如果將設備安裝在既有機房，且預算不足須分年編列時，本選項亦為可行方案之一。

4. 虛擬資源＋租賃

所有機房與資訊設備皆向電信業者租賃，或是透過系統整合廠商協助整合相關資源，對於資訊系統生命週期較短，或是資訊系統資源需求異動頻率較高，甚至是尖離峰資源耗用比例懸殊的情況來說，本模式是較佳可行方案。不過，當系統發生異常或效能不穩定時，虛擬資源較難釐清問題所在。

5. 服務租賃

在資訊系統功能具有普遍性的方式，且運作穩定與客製化需求較少的情況下，租賃服務以便對外提供服務將是不錯的選擇。透過完善的合約內容確保租賃服務達到預期的服務水準，同時也擬定合適替代方案，可充分發揮服務租賃帶來的好處。透過本模式至少可有效降低建置成本，以及專業資訊人員的人事成本。不過，由於租賃的服務內容通常不易變更，服務需求變更所衍生的費用，以及系統持續的穩定度有待運作時間考驗，再加上擬定租賃合約需要熟悉業務內容的專業人員，以及專業資訊人員充分提供意見，以便擬定最適化之租賃合約，因此在合約草擬時投入大量資源，以便確保合約內容切實可行且有助於推展業務。

三、建議方案

票務核心系統與全國民生息息相關，**且須與全國各車站售票周邊設備直接連線並與本局內部資訊系統介接大量資料（如採租賃機房方式，則票務網路所負擔租借線路頻寬費用成本將增加）**，為避免發生服務停止或故障難以釐清事件發生，建議採用方案為機房由本局現有資訊機房擴建，以提高系統發展自主性、擴充性與時效性，並規劃異地備援機房租賃運用；當主中心機房異常時，異地備援機房可暫時提供線上即時服務相關所需的系統資源。同時本局未來發展其它系統時，亦可在票務機房與雲端資訊中心擴充，節省經費與資源使用。

費用分析：

機房擴建費用預估為 2,600 萬元（每年維護費約 210 萬元）；機房租用每年約為 1,013 萬元。若機房使用三年以上，租用機房成本即已超過自建機房成本，本案預估生命週期為 10 年以上，故採自建機房可大幅節省成本。

針對機房建置的各種可行性經過評估後，整理如表 16。建議由現有機房擴建機房，可由防災中心獨立電源供機房歲修時使用，以避免歲修斷電情事。建議於既有四樓機房旁之儲藏室擴建機房（可避免影響既有機房運作與粉塵污染），以滿足本系統高可用與低風險之需求。

表16　機房建議方案比較表

解決方案	改建現有機房	建置新機房	租用IDC機房
水電費用	自行負擔	自行負擔	包含於租金內
門禁控管	自行管控	自行管控	由IDC協助管理
環控機制	自行管控	自行管控	視各IDC所提供之服務而定
頻寬需求	訂票系統皆使用自有網路，無額外費用	訂票系統皆使用自有網路，無額外費用	需與IDC租用大頻寬連接台鐵及IDC機房
風險評估	改建過程對於現有機房影響難料，如粉塵汙染及空調電力問題	無	需面臨機房管理問題以及斷線造成的系統停擺問題
費用	一次性費用 NTD：45,000,000	一次性費用 NTD：55,650,000	按月付費,每月支出約100萬

10.3 備援方案分析

一、現況分析

現行第三代票務資訊系統僅在本局大樓資料中心機房建置同地高可用架構，尚未具備異地備援與異地備份之相關機制。

二、可行性分析

由於票務資訊系統在上線運作後會遭遇何種災難，基本上難以完全預測，至於其損失程度與影響範圍也很難精確估計。不過當遭遇嚴重災難時，如何有效降低損失程度與縮小影響範圍，卻是在規劃災難復原或備援機制時必須審慎評估，評估依據至少包括：架構特徵、建置成本、營運成本、資料回復時間、系統切換時間等因素。

在建置災難復原或備援解決方案時，首先應對票務資訊系統相關應用程式或服務進行評估，具體釐清哪些為具有關鍵性的應用程式或服務，並對其執行環境進行評估，判斷產生災難的可能性有多少。如果發生災難的話，這些具有關鍵性的應用程式或服務中斷執行的時間有多長、中斷後對整體業務的影響範圍有多大、哪些資料可能會因此遺失、有沒有妥適解決的辦法與措施等。由於這些判斷過程非常複雜且耗時，因此更應審慎挑選適合保護資料安全的災難復原或備援解決方案，使得具關鍵性的應用程式或服務、資料庫充分具備完整的高可用性與災難復原能力，以便讓票務資訊系統建立完善的備援架構與迅速的災難復原機制，藉此確保票務資訊系統的永續維運。表 17 為可行備援模式分析。

1. 異地備份：提供異地資料存放機制，不提供資料處理設備，通常以「週」為備份單位，透過磁帶異地存放或設置異地儲存設備，以網路方式進行備份。
2. 異地備援：在異地機房設置資料處理與異地儲存設備，以「日」為單位進行資料同步，當主機房停止運作時，可透過機房切換機制，約 1~4 小時後，由異地機房接手主機房，繼續提供服務。
3. 雙中心：規劃主機房與異地機房以「交易」為單位進行資料同步機制，並同時提供服務，當任一機房中斷服務時，另一機房可即時接手服務，使用者不會有服務中斷的感覺。

表17　備援模式比較表

	異地備份	異地備援	雙中心
架構特徵	主機房(提供服務) 備份機房(資料備份)	主機房(提供服務) 備援機房(資料同步) 主機房停止時, 備援機房接手服務	主機房(提供服務) 備援機房(資料同步) 主機房+備援機房 同時提供服務
建置成本	低	中	高
營運成本	低	中	高
資料回復時間	長	中	短
系統切換時間	1-2天	1-4小時	0-5分鐘

將服務依據不同的應用特性，規劃不同的備份與備援服務，分析各備援模式如下表。

表18　備份備援模式建議

	異地備份	異地備援(A/S)	雙中心(A/A)
網路訂票			★★★★★
人工售票			★★★★★
電腦售票			★★★★★
收益管理		★★★★★	★★★
旅客資訊		★★★★★	★★★
資料倉儲	★★★★★	★★★	★
商業智慧/決策支援	★★★★★	★★★	★
智慧營運管理儀表版		★★★	★★★★
整合入口網		★★★	★★★★★
行動應用			★★★★★
行銷餐旅	★★★	★★	★
資訊服務交換		★★★★★	★★★
金流服務			★★★★★
營運管理		★★★★★	

三、建議方案：建議依各系統之重要性定義不同的異地備援等級。重要核心系統透過 Active-Active 的規劃設計，提供不間斷的 24 小時服務能力，非核心系統則採 Active-Standby 的設計，提供足夠的資料安全防護措施，而諸如共用軟體與資料處理的工具程式類型，則因系統特性，並無實質

儲存資料的行為，而以雙中心各自獨立運作，此類型系統建議以系統備份方式規劃。

四、採取異地備援之優點評估

1. 建立雙中心以增加票務處理績效

臺鐵利用網路將兩地的票務中心彼此連接，將工作負載分攤給兩個中心的方式，一則可以將票處理的績效大幅提升，增加訂票乘客的滿意度；二則減少因災害發生時主、副中心轉換所需的時間。同時仍將資料以網路進行備份管理外，也保留備援磁碟機供資料備份儲存之用。

在電子化作業頻繁的情況下，若遭恐怖攻擊、地震等災害，資料中心所記錄的交易資料損毀後，消費者所持有的資產、身份等將變得很難被證實，因此離線的實體磁帶備份仍是相當重要的，企業在利用網路進行備份時，也要以實體的磁帶運送備份資料以確保備份資料的保留完整。

進一步配合業務持續管理(Business Continuity Management，BCM)策略，除了資料中心的備援需求外，員工業務運作所需的備援辦公能力，也需要同時考量在內。

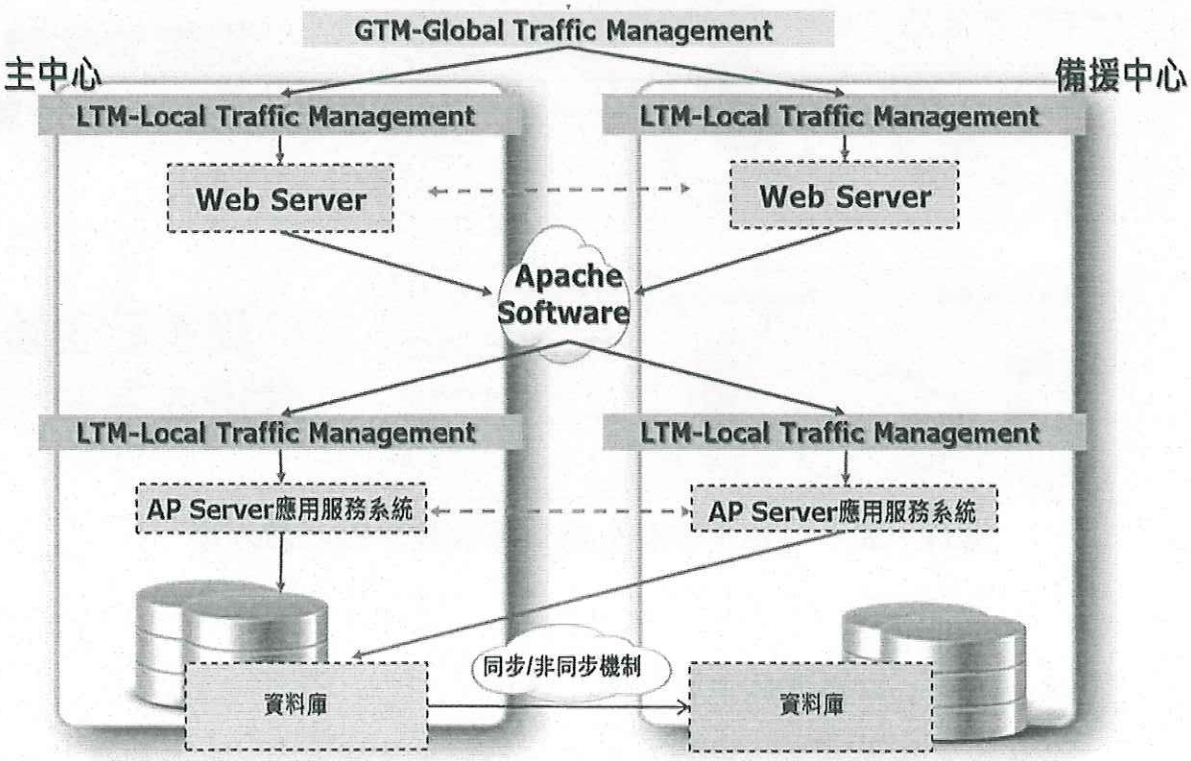


圖10　以雙中心增加票務處理績效之架構圖

2. 建立雙中以心避免重大災害影臺鐵業務

目前臺鐵票務中心主要機房位於台北車站之內，位處整個車站的核心之中，雖然位置交通便利，也因環境的複雜而相對的較易曝露在危險之中。傳統觀念認為只要系統規劃有考慮高可用性 HA-High Avalability 即可，但是那是以保護系統的運作為主，如果有災難發生，例如台北車站被攻擊而癱瘓、因地震而坍塌、因颱風水災而淹沒、因火災而全棟建築燒毀，這時就需規劃災難復原機制。所謂災難復原(Disaster Recovery；DR)，是針對企業資訊架構進行異地備援。它是主系統外的另一套系統，當主系統中斷後，這套備用設備可以立刻接手，企業不需等待原有系統修復，只需將作業環境切換，即可持續正常的工作，讓業務不中斷（Business Continuity）的目標得以達成。

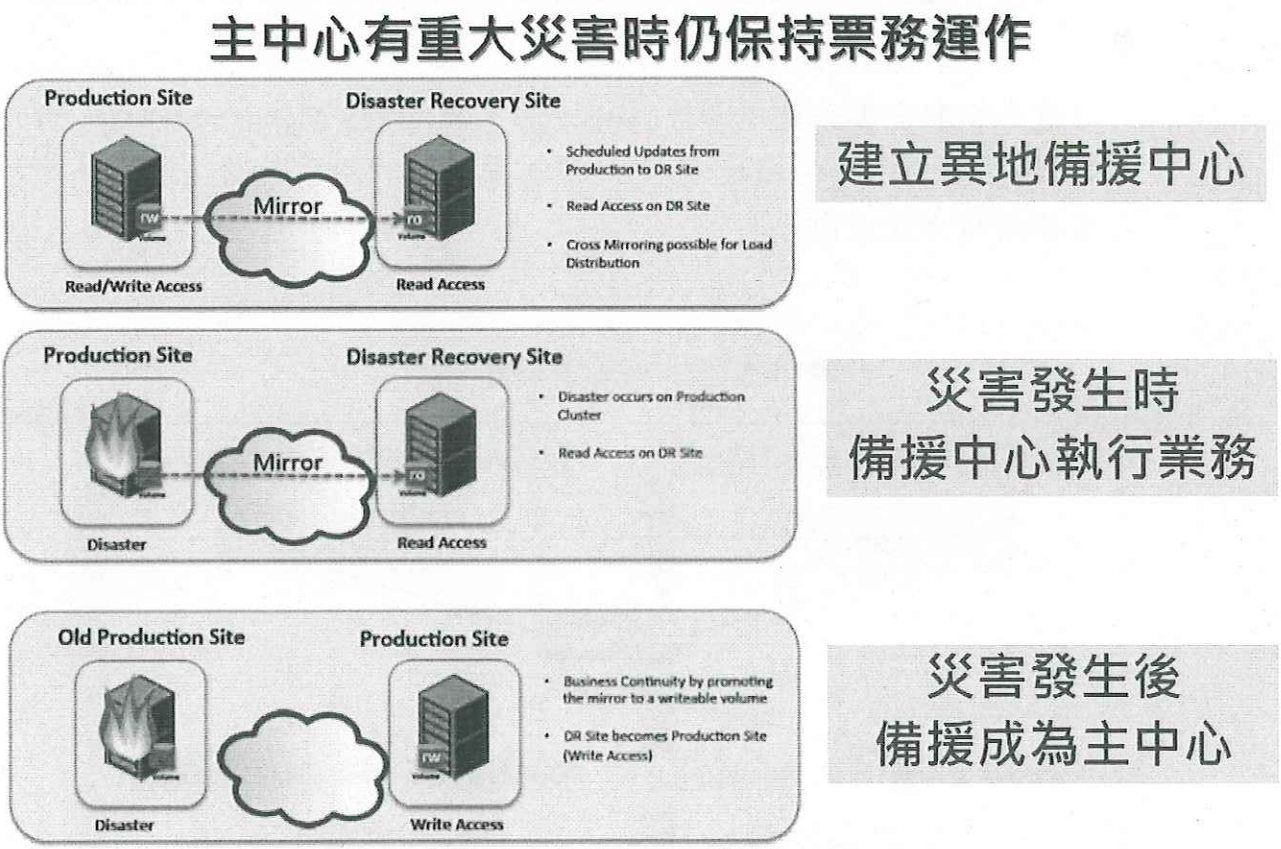


圖11　主中心在災害發生時切換備援中心之程序圖

3. 建立雙中心以提高維運彈性

目前臺鐵票務中心之主要機房位於台北車站之內，如果因為某些因素需要搬遷，可能是政府徵收用地、可能是租金太高、可能是整體組織

重整等因素，這是所有的業務系統都常會發生的事情。例如：目前臺鐵票務中心亦已規劃未來會將主要機房遷移到另一安全地點(目前規劃為南港)。

但是搬遷必定會影響業務的運作，甚至倉促進行時會造成重要資料的遺失或是系統的損壞。這對臺鐵的聲譽影響很大。

因此建立異地備援中心的優勢之一，就是將來在進行資料中心搬遷時，可以將服務的影響降到最低。也就是在搬遷時，先將主中心的運作切換到備援中心，然後可以按部就班地將主中心進行搬遷，待一切的搬遷完成就定位且測試完成時，再將備援中心切換到新的主中心。

當然，新機房的搬遷也需要有效率地進行，畢竟只有一個中心在運行，仍然是有風險的。需要盡早回復雙中心才能保證業務運行萬無一失。

4. 雙中心 Active-Active 模式可以完善保護 IT 投資

備援中心與主要中心之主要票務服務系統會採最高等級之 Active-Active 架構設計，在進行二地資料中心切換時，主要對外票務服務將不會受到影響。而 Active-Active 運作模式可保護 IT 投資，避免浪費。

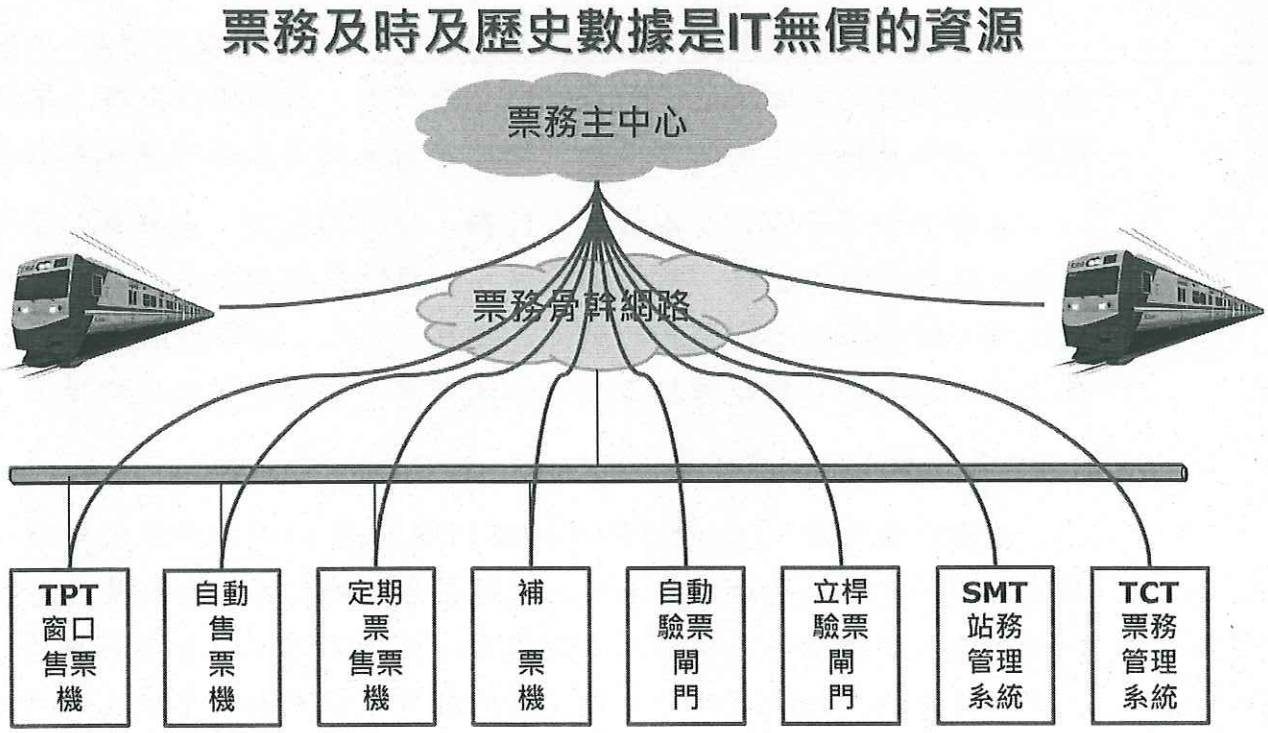


圖12　票務中心長短期資料的價值之說明圖

5. 雙中心建立高信任感的企業形象與承擔社會責任的能力

臺鐵運輸系統為重要之交通設施，機關能永續經營，除了追求經濟利益的同時，也需致力於民眾與旅客之間互動與互信，並取得平衡。而IT技術在機關永續經營方面，須能協助日常維運，並於災難回復扮演重要角色，以健全組織的發展，實現機關社會責任。

五、異地備援規劃原則

1. 備援中心規模規劃

備援中心之整體系統規模，依據前節之需求「備援中心建置規模規劃與主中心相同」之原則規劃，備援中心軟硬體架構可用性達到服務水準(SLA) 99.95%，以符合 Active-Active 資料雙中心的規劃需求。

2. 異地備援任務與目標的考慮

(1) Active-Active 資料中心與災難復原能力與成本的考慮

企業的系統、資料要達到最佳保護狀態，自然就是盡可能縮短系統中斷到回復的時間，且將系統中斷所造成的資料損失降到最低。不過，這也代表企業必須支付相當的金錢代價。在金錢與保護間要達到怎樣的平衡，並無定論，還是要回歸到業務面的考量。

企業資訊系統面臨的風險可概略分天災與人禍。天災從地震、水災、到各種無預警的災難屬之；而人禍則包括火災、人為操作失誤、惡意破壞等。這些災難發生的頻率不一，但都會對系統造成不可彌補的損傷。

在當下企業營運已全由資訊來啟動、維持的狀況，包括客戶資料、財會、稅務與庫存記錄、訂單細節等，全部儲存在系統中，若沒有足夠的保護，將直接影響到企業的運作與獲利。因此，企業對備援解決方案的需求，在兼顧災難復原能力與成本的考慮下需要更周全地評估。

(2) 異地備援的主要任務

所謂災難復原（Disaster Recovery；DR），是針對企業資訊架構進行異地備援，也稱為異地備援系統。它是主系統外的另一套系統，當主系統中斷後，這套備用設備可以立刻接手，企業不需等待原有系統修復，只需將作業環境切換，即可持續正常的工作，讓業務不中斷（Business Continuity）的目標得以達成。切換的方式與停機的時間，依選擇的解決方案不同而會有所不同。

異地備援與企業系統所使用的叢集式架構（Cluster）不同，它具備資料叢集特性的資料，可以讓多台伺服器主機同時透過光纖（Fiber）或SCSI介面來存取、使用。

一般來說，企業針對本地的系統，都會建立叢集式架構，讓多組設備共同支援一個工作，以便在其中一組設備中斷時，其他設備可以接手。但叢集式架構，不管以軟體、伺服器來做，都是在相鄰近的區域、機房進行，系統內只存有一份資料，如果此機房遭到不可測的意外，工作一樣會中斷。

但是異地備援不等於系統的高可用性架構(High Availability；HA)，所謂的高可用性運算環境，是指在伺服器主機或儲存設備端，提供冗餘（Redundancy）的各種元件，讓系統不會因為單點失效（Single Point of Failure）造成存取動作中斷，但在HA架構下，系統中的資料仍然只是存有一份。

技術的發展，讓主機端的HA，已經開發出結合資料異地複製的進階技術，可做到在異地端也產生一個資料副本，當災難發生時，可透過HA的軟體，將系統服務從本地端切換到異地端，達到異地備援的目的。

企業比較熟悉的資料保護是備份（Backup），備份針對的是企業資料的保護，而備援則是確認這些資料，不只被保護，且能夠繼續作業、使用，對業務的支援程度遠大於備份。

備援最主要目的，就是讓另一套設備，將原來系統的工作拯救回來。建立一套異地備援系統，除了伺服器主機，至少必須具備相對應的作業系統（Unix、Window、Linux）、磁碟陣列、磁帶機，其他包括風扇、電源供應器等元件，傳輸資料的網路，都得一應俱全，更重要的是，必須選擇適當的地點，放置這些設備。

3. 異地備援的任務分級

根據目前常用的任務分級，災難復原系統可依照對系統保護的程度與等級，分七個層次。這七個層級基本上是以復原恢復的速度及完整性來區分。如果考慮不同的運作功能時，可以區分為即時處理系統、非在線處理系統、伺服器層次、儲存設備層次。

這七個層級的定義，是由系統中斷到重新回復間隔的時間、資料可能遺漏的程度，以及建置系統所花費的成本等因素來定義的。第一層級

所需的恢復時間最長，但成本最少；而第七層級正好相反，恢復系統運作的時間幾近於0，不過建置成本相對來說非常高。

表19 異地備援重要等級參考表

等級	RPO (hr)	RTO (hr)	建制內容	建置費用
0	不明確	不明確	做資料備份設備的費用	較低
1	24-48	48 以上	做資料備份設備的費用、運送及儲存備份資料的費用	低
2	12-24	24 以上	做資料備份設備的費用、快遞、備援中心租金、儲存備份資料的設備、備援中心的基本設備	中
3	4-12	12-24	做資料備份設備的費用、電信網路租金、備援中心租金、儲存備份資料的設備、備援中心的基本設備	中
4	2-8	4-12	做資料備份設備的費用、寬頻電信網路租金、備援中心租金、儲存備份資料的設備、備援中心的基本設備、異地備援軟體。	高
5	0.5-2	4-12	做資料備份設備的費用、寬頻電信網路租金、備援中心租金、儲存備份資料的設備、備援中心的基本設備、異地備援軟體、資料異動更新軟體	高
6	0.1-1	0.5-4	做資料備份設備的費用、高寬頻電信網路租金、備援中心租金、儲存備份資料的設備、儲存檔案及記錄的設備、備援中心的基本設備、異地備援軟體、資料異動更新軟體	很高
7	0-0.1	0.1-0.5	做資料備份設備的費用、高寬頻電信網路租金、備援中心租金、儲存備份資料的設備、儲存檔案及記錄的設備、備援中心的基本設備、異地備援軟體、資料異動更新軟體、資料 AA 機制軟體硬體、應用系統 AA 機制軟體硬體	很高

完全自動、同步的系統之所以昂貴，例如以資料完全不遺漏的同步儲存來考慮，系統所產生的每一筆資料，都必須直接對兩地的系統寫入，因此第二地異地備援系統需要另外購買資料庫虛擬軟體（如：Oracle RAC），為第二地系統虛擬出寫入窗口，此外，由於兩邊的資料庫是同時運作，因此資料庫軟體得購買兩倍的數量，加上頻寬租賃費用，自然非常可觀。

(1) 業務運作是決定備援重要層級的關鍵

業務運作需求是決定備援系統層級的關鍵因素。

到底要做到哪一層次的備援，企業最重視的仍然在總體持有成本（Total Cost）。決定異地備援系統成本的兩個重要因素，為回復所需時間（Recovery Time Objective；RTO）和資料損失量（Recovery Point Objective；RPO）。RTO 計算的是系統中斷到重新啟動間所經歷的時間；RPO 則是指在系統中斷時間間隔中，資料損失的狀況。

如果企業的系統、資料要達到最佳保護狀態，自然就是系統中斷時間到回復時間盡可能縮短，且因系統中斷所造成的資料損失降到最低，這也代表企業必須支付相當的金錢代價，而這個代價是否值得就需要一些評估與分析。這樣的評估與分析是個複雜且動態的過程，需要業主與廠商通力合作。

金錢與保護間要達到怎樣的平衡，並無定論；企業型態不同，所需要的備援系統也大相逕庭；一般說來，金融、電信、高科技產業，因為系統必須達到不間斷服務的需求，因此無論是 RTO 或 RPO，都需要達到最短、最少的目標，甚至必須達到第七層級的最高可用性（即 99.99999%的可靠性），也就是容錯式架構（Fault Tolerable；FA）。

有些系統不需要時刻維持服務，就可以用伺服器層次的解決方案；對於沒有線上服務的中小企業，則只需將資料挽救回來即可。

要針對哪些系統建置異地備援，也是決定建置預算的要素。為了控制成本，企業多會針對重要的系統來作。以製造業為例，生產製造執行系統是最重要的，因為這個系統中的任何一個模組，諸如：CP(Circuit Probing 圓晶針測)、WAT(Wafer Accept Test 晶片驗收測試)、DDMS(Dalvik Debugging Monitoring Server 效能剖析工具)、RTD(Real Time Dispatching 即時排貨系統)、EDA(Electronic Design Automation 自動化設計工具)，若發生問題，生產線必然無法繼續運作，因此多數高科技製造業的備援，

會以此為主；而在金融業或電信業，帳務、交易、櫃臺系統的備援則特別重要；如果是零售業，前端銷售系統（Point of Sales；POS）的備援就是最先被考量的了。

如果針對鐵路局票務業務來說，票務處理攸關乘客即時訂位的相關交易處理，可以考慮為較高的層級。關於網路管理、伺服器管理、效能管理、監測管理等不影響票務的即時運作，可以考慮稍低一些的層級。關於各種訊息及事件的收集與分析報告，是以長期的營運業務分析為目標或是短期事件對未來營運有衝擊的分析，這些可以考慮更低一些的層級。不過以上的考慮需要業務、財務、營運等各單位共同評估，因為各企業都有不同的經營策略，一切的可慮都要有相同的策略脈絡。

(2) RTO/RPO 的指標分析

為避免災害發生而致票務系統業務中斷，首先需保存票務系統服務資訊，其次為回復可接受的票務業務，使得票務系統能持續於異地營運，將此二項參數以 RPO 及 RTO 表示：

A. RPO (Recovery Point Objective)

災害事故發生時最大可容忍的資料遺失。例如，只能接受遺失 2 小時資料，則 RPO 值為 2 小時；無法接受任何資料遺失，則 RPO 值為 0。

B. RTO (Recovery Time Objective)

災害事故發生後，最大可容忍的業務回復時間。RTO 值越小，需更快還原資料，但同時增加票務系統建置與維護成本。

建置異地備援的目標是希望降低資料損失(RPO)及盡快回復營運(RTO)，惟 RPO 及 RTO 值越小，其建置與為運費用隨之增加，因此，週期性地分析災害及服務損失、進行備援演練及檢討缺失、預算規劃，做為調整異地備援原則及應變計畫內容，確保票務系統服務受災害影響降低至可接受範圍內，因此，企業可將業務依據需要及費用，將不同資訊服務系統分類，規劃可接受的 RPO 與 RTO。

本計畫所訂定之復原時間目標(RPO)、復原點目標(RTP)及相關服務水準協議(SLA)指標詳見 2.11 服務水準之表 4(系統可用性)與表 5 (系統效能水準)。

六、災害回復測試與演練

由於環境可能持續的改變，因此應當定期對災害回復計畫進行檢核、測試與演練，當票務資訊系統於新建立或上線一段時間後發生變更時，應評估對災害回復計畫之影響以修改計畫內容，並進行異地備援功能測試及演練。目前業界趨勢是強調“演練”的重要性，演練帶來的壓力較小，集中性更強，並能夠最終推動整體執行效率。每次對計畫進行測試和演練後，通常都可以從中找到改進和提高效率的方法，能夠獲得越來越好的結果。因此，建立定期演練和維護計畫的任務至關重要，應專門指定給特定小組，以負責組織機構內業務連續性、災害回復等任務。

大多數機關承受不起因為災害回復測試而中斷或服務所造成的損失，因此可選擇部分系統或特定的時間內進行測試，這就需要制定災害回復測試計畫，對整個災害回復計畫中的特定弱點進行測試，這種測試不須涉及所有員工，而是從相關部門選取一小組員工，直至小組成員都確實清楚各自的任務為止。接下來就可以進行大規模的演練，依據這樣的模式則公司的整體運作就不會受到負面影響。透過演練可從中發現問題和錯誤，並重新檢視改良災害回復計畫，從而在真正的災難發生時更有效地完成票務系統服務的回復。

1. 災害回復測試

備援中心建置完成後，應完成主中心與備援中心網路介接及異地備援測試，以測試異地備援之機制正常運作，其系統績效達到預期結果，以建立災害發生時之應變能力，使票務系統服務能持續營運。

(1) 定期對災害回復計畫進行測試，可針對整體或部分資訊系統及於特定時間進行，避免影響整體票務系統服務水準。

(2) 訂定備援回復績效評估項目及標準，以確保異地備援災害回復服務水準。

(3) 訂定災害回復測試計畫，並檢討缺失後改進以符合績效評估標準。

(4) 災害回復測試應於系統上線前完成測試，可避免上線後需進行過多的測試，全部或大多數系統應於上線完成測試。測試完成後，將結果交由災害回復演練規劃人員進行災害回復演練規劃。

(5) 災害回復測試應於系統經過變更，且對災害回復計畫有影響之情況下，進行受影響子系統之測試，測試完成後，將結果交由災害回復演練規劃人員進行災害回復演練規劃。

2. 災害回復演練

定期進行災害回復演練，以提升新票務系統之服務持續性，藉由災害回復演練可有效提高災害回復組員之災害回復程序熟悉度，當實際發生重大災害時能依照預定目標達到災害回復使票務系統回復至預期的狀態。災害回復演練建議事項如下：

(1) 災害回復演練應至少每年定期執行一次。

(2) 災害回復演練應避免影響現有系統服務水準，以免造成客戶權益受損。

(3) 應訂定災害回復演練計畫，規範演練之腳本、人員、時程、地點與範圍等。

(4) 災害回復演練應依照災害回復計畫之程序，由災害回復小組執行。

(5) 災害回復小組需接受災害回復教育訓練，才能夠參與災害回復演練。

(6) 災害回復演練應有演練成果評估報告，以檢視與災害回復計畫之差異，並交由災害回復計畫小組分析，並改進災害回復程序或加強人員訓練以符合災害回復程序。