

# 應用 IDEF 於系統運維期之軟體支援流程建模

管孟忠

開南大學專案管理研究所  
mjkuan@mal.knu.edu.tw

劉璧如

開南大學資訊管理研究所  
e09707012@mal.knu.edu.tw

## 摘要

鑑於 2009 年中正機場入出境管制系統大當機與台北捷運文湖線通車後多起事故的兩大事件所引發的政府重大公共工程如何有效運維之議題，並吸取 1997 年馬特拉公司無預警撤離木柵線維護的應變處理中獲得國軍科技單位協助的正面經驗。本文針對國軍之「佈署後軟體支援」模型，參照論者所建議，將原本配合軟體發展軍規運作的武器系統軟體支援模式，加上軟體生命週期過程國家標準 CNS14837 所提供之指導，在既有的活動架構下，規劃軟體於運維期之支援過程活動一般模型，並以 IDEF0 流程建模方法實作之。

**關鍵詞：**軟體支援、流程建模、軟體生命週期過程、IDEF。

## 1. 前言

2009 年台灣發生了兩起令人矚目的政府重大公共工程事件。首先是元月 3 日，桃園國際機場二期航站的入出境管制電腦系統接連發生兩次當機，事件發生後，剛得標接手負責該系統運維，惟尚未完成簽約及責任交接之某廠商雖旋即派員前往處理，然均搶救無效，直到內政部派遣負責原系統建置之工程人員進駐機場後才逐步恢復正常[7]。

其次是 7 月初，與文山線串連後稱為文湖線的台北捷運內湖線正式通車，然自風光通車營運以來，除了系統的能量及穩定度遭到質疑外，更是大小故障問題不斷，還曾經發生一日三次當機且停擺多日的嚴重情況[2]。

更早之前，文山線(原稱為木柵線)更是飽受爭議。除了土建工程出現瑕疵外，亦出現試車時兩度發生火燒車及電聯車爆胎等重大事故。負責文山線機電工程的法商馬特拉公司更在營運兩個月後無預警撤離，並禁止下包商出售備品零件給台北捷運公司，導致行控電腦大當機。事發後，北市政府向軍方尋求諮詢及協助，在某科技單位派員協助並獲得正面結果的

支撐下，讓市府吃下一顆定心丸，決定自己來克服種種問題。

中正機場與台北捷運系統的大當機事件除了背後隱藏了公共事務的故事與艱困外，亦突顯出高科技與高精度之系統及/或軟體其支援能量之重要性與關鍵地位，以及從系統工程發展、建置到佈署營運過程，若干具任務關鍵性之系統在其籌獲生命週期中有關的「軟體支援」議題：

- (1). 開發(建置)期的軟體支援
- (2). 從開發(建置)完成到運維之間的系統營運及軟體支援移轉
- (3). 運維期的軟體支援工作

在內政部移民署入出境管制電腦系統當機事件後，現任國家標準技術委員會資訊與通訊分組委員林泰龍先生曾以該事件作為引子，發表針對軟體系統之有效維運研究，檢討及提出包括 ISO/IEC 12207 軟體生命週期過程在內的各種建議[3][4]。而從過去軍方協助台北捷運木柵線應變處理的往事，可以看出有著完整後勤支援體系的軍方科技單位，在「軟體支援」方面所展現出來的能量，確有諸多可供借鏡之處。

本文即從以上兩點出發，以國軍科技單位參照美軍 [34]及國軍[10]，針對「武器系統軟體支援研究」[12]中的「佈署後軟體支援」(Post-Deployment Software Support, PDSS) 模式作為客體，考量引進可與 ISO/IEC 12207 軟體生命週期過程等效之 CNS14837[1]中適用的各種生命週期過程，並以 IDEF0 流程建模方法[17]實作此一軟體支援模型。

## 2. 背景與方法論

### 2.1 軟體生命週期過程

DOD-STD-2167A[21] 是美國國防部於 1988 年配合當時美軍國防系統籌獲之政策指導[19]而改版，將屬「關鍵性任務電腦資源」(mission critical computer resource, MCCR)之國防軟體發展的活動與交付文件作一標準化的規定，圖 1 即為此軍規之一般要求與細部要

求的文件架構，其中橫軸代表系統/軟體的 8 個發展過程；縱軸表示「軟體項目」發展的 6 項功能領域。1988 後的若干年期間，新立案的 MCCR 系統電腦(含軟體)籌獲均採行 DOD-STD-2167A 標準。例子如目前美國最先進戰機 F-22A[18]。

1994 年 8 月，美國國防部長 Dr. Perry 發表一份對採用國防部標準及規格之政策備忘錄[35]，要求國防部各級管理者在籌獲產品與服務時儘可能採用商用標準。基於此一政策，美國國防部決定將 DOD-STD-2167A 與「電腦資訊處理標準」(Information Processing Standards for Computers, IPSC)的文件標準 DOD-STD-7935A[22]合而為一，使其能用於任意形式軟體。此項合併工作之成果即為 1994 年 12 月頒佈的美軍軟體發展暨文件標準—MIL-STD-498[34]。

同一段時期，由 IEEE 與 EIA 所共同主持的計畫，將正準備發佈的 MIL-STD-498 轉換成「非官方」的商用標準。惟因配合 1995 年國際標準組織公佈的軟體生命週期過程標準 ISO/IEC 12207:1995[28]，IEEE/EIA 於 1996 年及 1998 年分別公佈了 IEEE/EIA 12207.0、IEEE/EIA 12207.1、IEEE/EIA 12207.2、與 IEEE/EIA J-std-016 等標準[24][25][26][27]。

其間，我國防部亦以 MIL-STD-498 作為藍本，配合當時的國軍武器系統研製政策規定[9]及相關之(含軍品)採購法規等指導，於民國 85 年六月完成「國軍軟體發展規範(草案)」[10]之編撰。

依據中華民國軟體品質協會公佈的訊息[5]，前述 ISO/IEC 12207:1995[28]分別於 2002 年及 2004 年提出過兩次修正案[29][30]，並將其修正內容納在 2008 年第二次改版中。至於取材自 ISO/IEC 12207 的我國軟體生命週期過程國家標準 CNS14837[1] 於 94 年 7 月修訂公佈時，即已將 ISO/IEC 12207 的兩次修正案內容納入。

CNS14837 將各種須在軟體生命週期間實行的活動劃分為 5 項主要過程、8 項支援性過程及 4 項組織性過程，分別記載於該標準的第 5、6、7 節。其中，主要生命週期過程的 5 項過程為：獲取、供應、發展、營運、維護；支援性生命週期過程的 8 項過程為：文件活動、組態管理、品質保證、查證、確認、聯合審查、稽核、和問題解決。各生命週期過程均可區分成一組活動；而組織內生命週期過程所含的 4 項過程則為：管理、基礎建設、改善、訓練等。

前述 17 個過程之每一過程均含有若干活動，而每一活動又可再區分成一組工作，各過程所含之活動及工作數統計節要於表 1。

## 2.2 軟體支援(Software Support)

DOD-STD-2167A 對「軟體支援」之定義為：為確保已實作及分發使用之軟體，能持續支援該軟體的作戰任務所採行的活動之總合。MIL-HDBK-347[32]將簡單區分為「佈署前軟體支援」(Pre-Deployment Software Support)及「佈署後軟體支援」(Post-Deployment Software Support, PDSS)，提出「佈署前軟體支援」與 PDSS 的功能活動模式，說明軟體支援機構(Software Support Agent, SSA)於「佈署前」及「佈署後」的「軟體支援」及 SSA 的角色、地位與活動，隨系統/軟體的進展的演化。

「國軍軟體發展規範(草案)」將「軟體支援」定義成：一套工作項目，其為確保軟體安裝在系統運作時，能按照要求持續進行其工作，且符合其角色要求所進行的一套包括軟體的維護、對使用者的協助、及其他相關的工作項目。「武器系統軟體支援」[13]一文即採取此「一套工作項目」之精神，將「武器系統軟體支援」視同「武器系統軟體的後勤支援」，結合了國軍當時的軟體發展與整體後勤體系規範[6][14][15]，保留 MIL-HDBK-347 的「佈署前軟體支援」與 PDSS 的功能活動模式為經，「國軍軟體發展規範(草案)」的過程為緯，試圖探討出可供國軍及研發單位參考運用的「軟體支援」方向，並曾在進一步的內部研究中[12]，將這個初步想法落實，提出了可對應的「武器系統軟體支援」模式。民國 96 年 12 月出版的「專案計畫軟體後勤支援作業規定」[8]已正式將「軟體支援」視同「整體後勤支援」之一環的構想納入。

## 2.3 IDEF 建模方法[17]

IDEF 的含義是集成電腦輔助製造(Integrated Computer-Aided Manufacturing, ICAM DEfinition)，是一種應用廣泛的企業建模方法，源自於 SofTech 公司的 Structured Analysis and Design Technique (SADT)方法論，後經美國空軍加以改良，取其功能模式發展而成。為促進企業程序改進，美國國防部採用 IDEF 模式技術及作業制成本分攤制，現已成功使用於私人企業及政府部門，用來定義與企業活動及個體的高階觀念、技巧與程序，以發展出對企業程序的邏輯模式。

IDEF 最初開發了 3 種方法：系統功能架構建模(IDEF0)、資訊建模(IDEF1)、系統動態建模(IDEF2)，後來，隨著資訊系統相繼開發，又開發出系統資料建模(IDEF1X)、系統過程描述獲取方法(IDEF3)、面向物件設計(IDEF4)、實體描述獲取方法(IDEF5)、設計理論獲取方法(IDEF6)、人/系統交互設計方法(IDEF8)、業務約束發現方法(IDEF9)、網路設計方法(IDEF14)等。

所謂 IDEF0 方法，是美國空軍為提高製程效率，提供共同通用語言所發展出來的工具，期理論基礎是建構於系統分析與設計技術上。其分析是由上而下局部細分活動內容，逐步將實體系統分解，使得一個複雜的系統能以系統化的方式加以表達，分析者不但可以在分析過程中使得各工程彼此協調溝通，為共同目標合作。IDEF 模式由圖形、文字與詞彙等三種資訊形式所組成，其彼此交互參考，每張 IDEF 圖形通常包含 3 至 6 個斜狀排列之方塊，這些方塊與週邊箭頭組合成一個 ICOM (input、control、output、mechanism)圖，分別包含輸入、控制、輸出及機制等項目，每一個 ICOM 圖又可再細分成若干個子圖(參閱圖 2)。

### 3. 運維期軟體支援模型解析與規劃

本文軟體支援者採用之「運維期軟體支援活動模型」(以下簡稱本模型)係沿用國防科技單位「武器系統軟體支援」的佈署後軟體支援模型第二層(圖 3)，並參照「武器系統軟體支援研究」[12]，將之再擴展至第三層(圖 4)。

為與模型實作採用之方法論一致，本文在模型解析時即採用 IDEF0 之編碼方式：

- A 代表活動(Activity)
- C 代表活動之控制(Control)
- M 代表活動之機制(Mechanism)
- I 代表活動之輸入(Input)
- O 代表活動之輸出(Output)

#### 3.1 活動之控制規劃

本模型軟體支援活動之控制係以參照 CNS14837[1]附錄 C，對於過程與組織之指導(參閱圖 5 及圖 6)，採用下列程序組合作為模型中各項活動之控制規則：

C1 型管作業規定：實現支援性生命期過程(第 6 章)中之組態過程(節 6.2)。本文假設本模型仍沿用「武器系統軟體支援研究」[12]之型管流程，故相關表單如「問題/變更報告」、「變更狀態報告」(Change,

Status Report, CSR)、「工程變更申請」(Engineering Change Proposal, ECP)、規格變更通知書(SCN's)、「功能構型稽核」(Functional Configuration Audit, FCA)與「實體構型稽核」(Physical Configuration Audit, PCA)等，本模型均加以保留。

C2 軟體支援程序：實現主要生命期過程的維護過程(節 5.5)，分成以下次程序：

C2.1 問題及修改分析程序：實現維護過程之問題及修改分析(段落 5.5.2)活動

C2.2 軟體發展程序：實現維護過程之修改實作(段落 5.5.3)並依段落 5.5.3.2 進入發展過程(5.3 節)

C2.3 軟體需求分析程序：實現發展過程之軟體需求分析(段落 5.3.4)

C2.4 軟體設計程序：實現發展過程之軟體架構設計(段落 5.3.5)與軟體細部設計(段落 5.3.6)

C2.5 軟體建置及單元測試程序：實現發展過程之軟體編碼與測試(段落 5.3.7)

C2.6 軟體整合與測試程序：實現發展過程之軟體整合(段落 5.3.8)

C2.7 軟體鑑定測試程序：實現發展過程之軟體資格測試(段落 5.3.9)

C2.8 系統整合與鑑定測試程序：包含兩個子程序：

C2.8.1. 系統整合程序：實現發展過程之系統整合(段落 5.3.10)

C2.8.2. 系統鑑定測試程序：實現發展過程之系統資格測試(段落 5.3.11)

C2.9 軟體驗收支援程序：實現軟體驗收支援(段落 5.3.13)

C2.10 產品驗證程序：實現維護過程之維護審查/驗收(段落 5.5.4)

C3 文件產製程序：實現文件活動過程(6.1 節)之產製(段落 6.1.3)。

C4 技術審查程序：實現支援性過程之聯合審查(節 6.6)中的技術審查活動(段落 6.6.3)，並引用 DOD-STD-2167A[21]的相關技術審查項目，次程序如下：

C4.1. 需求審查程序：實現 DOD-STD-2167A 的軟體規格審查(Software Specification Review(s), SSR)

C4.2. 軟體設計審查程序：實現 DOD-STD-2167A 的初步設計審查(Preliminary Design Review, PDR)

與關鍵設計審查(Critical Design Review, CDR)

C4.3.測試備便審查程序：實現 DOD-STD-2167A 的測試備便審查 (Test Readiness Review, TRR)

C5 交付與結案程序：實現主要生命期過程中，供應過程(5.2 節)之交付與結案(段落 5.2.7)

### 3.2 活動之機制規劃

MIL-HDBK-347[34]及「武器系統軟體支援之研究」[12]分別配合 DOD-STD-2167A[23]與取法自 MIL-STD-498[36]的「國軍軟體發展規範草案」(85 年版)[10]而作。在不失一般性的原則考量下，本文參考 CNS14837[1]附錄 C，對軟體生命週期過程角色與關係之指導(圖 5)將本模型之軟體支援者的主要活動機制簡單劃分為管理、工程與支援等三個部門。

M1 管理部門：引用圖 5 管理觀點，擔任軟體生命週期過程之「管理者」角色，主導「管理過程」。此可對照於 DOD-STD-2167A 的「軟體發展管理」以及「國軍軟體發展規範草案」的「管理」過程。由於軟體組態管理之各種決策可視同一種管理功能，故將之納在管理功能並整合於其中。

M2 工程部門：引用圖 5 工程觀點，擔任軟體生命週期過程之「維護者」角色，執行「維護過程」並運用「發展過程」。就 DOD-STD-2167A 過程言，此可對應於圖 1 之「軟體發展工程」與「軟體鑑定測試」；事實上，CNS14837 將軟體鑑定測試與軟體發展工程均納為工程功能，此對「國軍軟體發展規範草案」來說，其與圖 3 之「發展」過程完全相容。

M3 支援部門：引用圖 5 支援觀點，擔任軟體生命週期過程之「支援過程之運用者」角色，負責「支援過程」。

### 3.3 活動模型架構解析

依照圖 3 及圖 4，PDSS 過程區分為初期分析(A1)、軟體項目發展(A2)、系統整合與測試(A3)、以及生產支援(A4)等功能活動。每一次由「問題/變更報告」發起的 PDSS 工作到產出「交付套包」為止的活動均含此 4 項活動、且因其與 CNS14837[1]之工程觀點，以「維護者」角色執行「維護過程」並運用「發展過程」之過程運用相容，本模型文流程建模亦加以採納並沿用。以下分別對各項活動及其 ICOM 進行細部解析：

#### 3.3.1 進行初期分析(A1)

初期分析可再細分成：識別問題/變更(A11)、分派衝擊分析任務(A12)、分析問題/變更之衝擊(A13)、核可/否決問題/變更(A14)、與記錄及納管問題/變更報告狀況(A15)等 5 個下一層活動，各活動分述如下

##### 3.3.1.1 A11 識別問題/變更

活動內容：對問題/變更報告進行登錄及識別。本活動之 ICOM 分別為：

輸入(I)：問題/變更報告

控制(C)：型管作業規定

輸出(O)：已識別之問題/變更報告、CSR

機制(M)：支援部門(型管人員)

##### 3.3.1.2 A12 分派衝擊分析任務

活動內容：審查所提議之變更事項，驗證其類別，並採取適當之行動。本活動之 ICOM 分別為：

輸入(I)：已完成識別之問題/變更報告

控制(C)：型管作業規定

輸出(O)：衝擊性分析之任務分派、決定不予執行的問題/變更報告

機制(M)：管理部門

##### 3.3.1.3 A13 分析問題/變更之衝擊

活動內容：分析問題/變更事項對管理、工程及支援等層面造成之衝擊。本活動之 ICOM 分別為：

輸入(I)：已完成識別之問題/變更報告、衝擊性分析之任務分派

控制(C)：問題及修改分析程序

輸出(O)：衝擊性分析報告與成本估算

機制(M)：管理部門、工程部門、支援部門

##### 3.3.1.4 A14 核可/否決問題/變更

活動內容：假如所申請的變更事項為重大變更，即需提交一份 ECP 初稿(或正式)版本給管理決策者，並附上衝擊性分析與成本估算。本活動之 ICOM 分別為：

輸入(I)：衝擊性分析報告與成本估算

控制(C)：問題及修改分析程序

輸出(O)：經核可的問題/變更報告及建議的交付時程、決定不執行的問題/變更報告

機制(M)：管理部門

##### 3.3.1.5 A15 記錄及納管問題/變更報告狀況

活動內容：依據型管規定更新電腦軟體構型索引及 CSR，以反映經核可的問題/變更報

告及其現狀。本活動之 ICOM 分別為：

輸入(I)：經核可的問題/變更報告及建議的交付時程、決定不予執行的問題/變更報告、CSR；

控制(C)：型管作業規定；

輸出(O)：經核可的問題/變更報告及其電腦軟體構型索引與 CSR；

機制(M)：支援部門

### 3.3.2 軟體發展(A2) 之細部解析

軟體發展可再細分成：分析軟體需求(A21)、設計軟體(A22)、建置及測試軟體單元(A23)、整合與測試軟體單元(A24)、進行軟體鑑定測試(A25)、與發布決策(A26)等 6 個下一層活動，各活動分述如下

#### 3.3.2.1 A21 分析軟體需求

活動內容：問題/變更事項若涉及軟體需求，則執行細對軟體變更事項的細部分析，並進行對軟體項目工程需求任何變更事項的完整定義，將之記載在適當的軟體需求文件如「軟體需求規格書」(Software Requirements Specifications, SRS)及(或)「介面需求規格書」(Interface Requirements Specifications, IRS)等。本活動亦識別出各項規定的測試文件與各項必要的測試變更，以用來驗證此一實作的變更。按照軟體需求分析程序要求，將更新的軟體項目鑑定需求紀錄在測試規劃文件紀錄，如「軟體測試計畫書」(Software Test Plan, STP)。本活動之 ICOM 分別為：

輸入(I)：經核可的問題/變更報告、變更前之軟體 SRS/IRS 與 STP

控制(C)：軟體需求分析程序、需求審查程序

輸出(O)：已更新完成配置之構型識別、SRS/IRS 及其 STP

機制(M)：工程部門

#### 3.3.2.2 A22 設計軟體

活動內容：問題/變更事項若涉及軟體的設計便啟動本活動。軟體的設計包括軟體層面設計架構設計與細部設計。成果記錄在適當的設計說明紀錄，如「軟體設計說明書」(Software Design Description, SDD)。於必要時更新 STP 以反映出軟體設計決策對 SDD 所做的變更。本活動之 ICOM 分別為：

輸入(I)：已更新完成配置之構型識別、SRS/IRS 及其 STP、軟體設計問題/變更、變更前之軟體 SDD/IDD 與 STD

控制(C)：軟體設計程序、軟體設計審查程序

輸出(O)：已更新完成之 SDD/IDD 與 STD

機制(M)：工程部門

#### 3.3.2.3 A23 建置及測試軟體單元

活動內容：目的在進行各軟體單元的建置及其測試工作，以確定各軟體單元的演算法及其邏輯為正確，且滿足既定之設計需求。各軟體單元的「軟體發展檔」(Software Development, Files, SDFs) (如有的話)皆要依照要求被更新，包括新的測試需求、個案、程序及其結果。此新的原始軟體碼報表將納入合適的發展構型。本活動之 ICOM 分別為：

輸入(I)：已更新完成之 SDD/IDD 與 STD、軟體單元建置/變更、變更前之軟體單元 SDFs

控制(C)：軟體建置及單元測試程序

輸出(O)：工程部門

機制(M)：新的發展構型及更新後的軟體單元 SDFs

#### 3.3.2.4 A24 整合與測試軟體單元

活動內容：整合兩個(或以上)之單元，測試此軟體以確保其正確工作，直到所有軟體單元皆完成整合及測試為止。修訂及更新可供軟體單元整合與測試用之各項測試個案、測試程序、與測試資料等，於需要時進行改版及再測試。本活動之 ICOM 分別為：

輸入(I)：新的發展構型及更新後的軟體單元 SDFs、已更新完成之 SDD/IDD 與 STD、變更前之軟體組件 SDFs

控制(C)：軟體整合與測試程序、測試備便審查程序

輸出(O)：新的發展構型及更新之組件 SDFs、以及更新後之 STD

機制(M)：工程部門

#### 3.3.2.5 A25 進行軟體鑑定測試

活動內容：依據 STD 中被更新後的程序在發展構型上執行，在各軟體項目上執行的「軟體鑑定測試」皆要準備一份可供永久保存的「軟體測試報告」(STR)。本活動之 ICOM 分別為：

輸入(I)：已更新完成配置之構型識別、SRS/IRS 及其 STP、以及已更新完成配置之構型識別、SRS/IRS 及其 STP

控制(C)：軟體鑑定測試程序

輸出(O)：軟體測試報告(STR)

機制(M)：工程部門

### 3.3.2.6 A26 發布決策

活動內容：包括 STR 的審查，發展構型的確認與鑑識以及將發展構型(有時稱為「測試版本」)釋出供系統整合與測試。管理決策者宜在釋出給系統整合與測試之前確定測試版本已符合需求。本活動之 ICOM 分別為：

輸入(I)：軟體測試報告(STR)

控制(C)：型管作業規定

輸出(O)：經鑑識完成釋出供系統整合與測試(發展構型)之軟體項目測試版本

機制(M)：管理部門

### 3.3.3 系統整合與測試(A3) 之細部解析

整合與測試可再細分成：整合(A31)、測試(A32)、審查及釋出測試版本(A33)、構型稽核(A34)、發展資料套包(A35)、構型管制決策(A36)、與發佈決策(A37)等 7 個下一層活動，各活動分述如下：

#### 3.3.3.1 A31 整合

活動內容：合併各軟體項目使之成為一經整合後的軟體系統。本活動之 ICOM 分別為：

輸入(I)：經鑑識完成之軟體項目測試版本

控制(C)：型管作業規定、系統整合程序

輸出(O)：(中間)測試版本

機制(M)：工程部門

#### 3.3.3.2 A32 測試

活動內容：正規的測試工作宜包括在每一個層次上的「迴歸測試」與軟體項目介面測試，並且要有見證。整合與測試循環經常重覆許多(若干)次，直到完全的軟體程式被產生且完成測試為止。本活動之 ICOM 分別為：

輸入(I)：經鑑識完成之軟體項目測試版本

控制(C)：系統鑑定測試程序

輸出(O)：(中間)測試版本

機制(M)：工程部門

#### 3.3.3.3 A33 審查及釋出測試版本

活動內容：審查各測試結果、確認需求、及釋出此測試版本(發展到構型)。本活動之 ICOM 分別為：

輸入(I)：經鑑識完成之軟體項目測試版本

控制(C)：系統鑑定測試程序

輸出(O)：各項測試結果

機制(M)：工程部門

#### 3.3.3.4 A34 構型稽核

活動內容：在權限範圍內，執行其獨立的

FCA 與 PCA 工作。在測試版本核可之前宜執行構型稽核。本模型雖規定在系統整合與測試之後舉行構型稽核。然無論如何，各項稽核均得在「軟體鑑定測試」後舉行。當稽核在「軟體鑑定測試」之後舉行時，整合與測試工作過程的備便事項為一經核可的軟體版本與其所伴隨之構型識別。本活動之 ICOM 分別為：

輸入(I)：可供「構型稽核」之軟體程式測試版本、現行之構型識別

控制(C)：型管作業規定

輸出(O)：稽核結果

機制(M)：管理部門

#### 3.3.3.5 A35 發展資料套包

活動內容：受到本項已實施之問題/變更報告所影響的每一份規格或納管下之文件，皆要個別準備一份 SCN。文件生產工作包括對有變更之頁次或文件改版之「照像製版」成已可出版形式的發展技術編輯、驗證與生產。本活動之 ICOM 分別為：

輸入(I)：規格變更通知書(SCN's)草稿或改版

控制(C)：型管作業規定

輸出(O)：正式之 SCN's 或改版

機制(M)：支援部門

#### 3.3.3.6 A36 構型管制決策

活動內容：依照變更的層級及獲得授權之權限，可採取下列行動，為(a)核轉此測試版本、測試結果及稽核結果，附加上一份意見；(b)核可測試版本及所伴隨對構型識別之變更申請；(c)駁回測試版本，不予核可。一旦建立更新之構型識別，針對每一項所規定之變更事項發佈一份 SCN。本活動之 ICOM 分別為：

輸入(I)：正式之 SCN's 或改版、稽核結果、各項測試結果

控制(C)：型管作業規定

輸出(O)：經核可之軟體版本、以及藉由 SCN's 更新之構型識別發佈文件

機制(M)：管理部門

#### 3.3.3.7 A37 發佈決策

活動內容：將已核可之軟體版本釋出交給使用者(即運作發佈決策)。國防系統中某些具任務關鍵性系統會要求在將某一新軟體版本釋出給作戰部隊之前，進行「作戰測試與評估」(Operational Test and Evaluation, OT&E)。在 OT&E 結果審查之後，便可依據該部門之規定下達釋出決策。本活動之 ICOM 分別為：

輸入(I)：經核可之軟體版本、以及藉由 SCN's

更新之構型識別發佈文件

控制(C)：型管作業規定

輸出(O)：暫訂交付時程及運作版本

機制(M)：管理部門

### 3.3.4 產品後勤(A4) 之細部解析

產品後勤可再細分成：建構交付模型(A41)、驗證(A42)、產製各類手冊(A43)、建置交付套包(A44)、協調交付(A45)、及分發與使用者訓練(A46)等 6 個下一層活動，各活動分述如下：

#### 3.3.4.1 A41 建構交付模型

活動內容：隨不同硬體、基(場)地、或模型調適資料。亦包括模型交付套包(包括在任何形式媒體之已核可軟體版本，使用者/操作者手冊變更頁次或改版、韌體或 IC 板，以及新的診斷軟體)的製造或初期生產與驗證。每一交付項目之模型要在大量生產之前完成其建構及驗證工作。本活動之 ICOM 分別為：  
輸入(I)：運作版本  
控制(C)：型管作業規定  
輸出(O)：各種交付模型  
機制(M)：支援部門

#### 3.3.4.2 A42 驗證

活動內容：本項工作包括對交付套包各組件之完整性與正確性之最終檢查與驗證。本活動之 ICOM 分別為：  
輸入(I)：各種交付模型  
控制(C)：產品驗證程序  
輸出(O)：經驗證之交付套包  
機制(M)：支援部門

#### 3.3.4.3 A43 產製各類手冊

活動內容：本項工作可視為「建置交付套包」的一項工作組件。手冊的生產工作宜包括之任務要項諸如：文件驗證、技術編輯、插圖與生產等工作項目。初期對手冊生產之規劃工作宜包括：人力需求、經費需求、以及前置時間需求。宜將照像製版、插圖與圖形皆保留下來以供未來之用。本活動之 ICOM 分別為：  
輸入(I)：經驗證之交付套包  
控制(C)：文件產製程序  
輸出(O)：各類手冊  
機制(M)：支援部門

#### 3.3.4.4 A44 建置交付套包

活動內容：本項工作包括交付套包之生產

所伴隨的任務要項，例如可包括磁性媒體、韌體、IC 卡、使用者手冊、課程網大綱、學生文件、維護工具包、診斷工具包等之裝配、製作或生產。本活動之 ICOM 分別為：

輸入(I)：經驗證之交付套包、各類手冊

控制(C)：型管作業規定

輸出(O)：交付套包

機制(M)：支援部門

#### 3.3.4.5 A45 協調交付

活動內容：本項工作實際包含所有最終之交付準備工作。本活動之 ICOM 分別為：

輸入(I)：交付套包、暫訂之交付時程

控制(C)：交付與結案程序

輸出(O)：經協調後之生產/出版及交付時程，以及完整的交付套包

機制(M)：管理部門

#### 3.3.4.6 A46 分發與使用者訓練

活動內容：現場交付的不只是轉(替)換成新的軟體版本而已。支援部門派往交付的人員在每一個交付場地至少要完成下列五件事：

- (1). 換上並證實交付套裝的接收條(據)。
- (2). 換下過期的交付套裝。
- (3). 安裝軟體。
- (4). 訓練強調新功能之能量，與人機界面的變更，以及
- (5). 更新(任何的)電腦輔助指導軟體。

本活動之 ICOM 分別為：

輸入(I)：核可的交付時程與經驗證完畢之交付套包

控制(C)：交付與結案程序、軟體驗收支援程序

輸出(O)：正式的交付套包

機制(M)：支援部門

## 4. 模型實作

以 IDEF0 方法實作前述運維期軟體支援模型之結果參見圖 6~圖 11

圖 6 為本模型之全景，顯示出原有運作中版本的交付軟體套包從問題/變更報告起透過整個運維其支援活動修改成新的交付套包。

圖 7 為圖 6 的第一層展開，其中之 A1~A4 等四項活動表示每一次由「問題/變更報告」發起的運維期軟體支援到產出「交付套包」為止所需的活動。

圖 8 為圖 6 中初步分析(A1)的 5 個下一層活動展開(A11~A15)，表示由收到「問題/變更報告」開始將問題登錄，直到產出經核可的



問題/變更報告及其電腦軟體構型索引與 CSR 為止所必需的活動。其中亦顯示出一旦決定不執行此「問題/變更報告」亦會由記錄及納管問題/變更報告狀況(A15)加以處理。

圖 9 為圖 6 中軟體發展(A2)的 6 個下一層活動展開(A21~A26)，表示從分析軟體需求(A21)到發布決策釋出測試版本的細部活動過程。其中，啟始的軟體發展活動將依問題報告屬性而定。例如，問題/變更如為設計而不涉及軟體需求異動者，其軟體發展活動即由軟體設計(A22)開始。吾人可由圖 9 觀察到 SRS/IRS、SDD/IDD、SDP、STD、STR 及 SDF's 等各項軟體文件/紀錄在這些細部活動流程中的變化(異動)。

圖 10 為圖 6 中系統整合與測試(A3)的 7 個下一層活動展開(A31~A37)，表示從軟體系統之整合(A31)到發佈決策(A37)釋出暫訂交付時程及運作版本的細部活動過程。

圖 11 為圖 6 中產品後勤(A4)的 6 個下一層活動展開(A41~A46)，表示從建構交付模型(A41)到分發與使用者訓練(A46) 支援部門派往交付的人員在每一個交付場地進行軟體更新與必要的使用者支援(如教育訓練)的細部活動過程。

## 5. 檢討與結論

本文係針對 2009 年機場入出境管制系統於交付營運後不久即出現大當機及台北捷運文湖線通車後多起事故的兩大事件，所引發對政府重大公共工程如何有效運維議題之探討。

有鑑於過去馬特拉公司無預警撤離木柵線維護的應變處理中獲得軍方科技單位協助的正面經驗。本文針對運維期的軟體支援，嚐試將原本配合軟體發展軍規運作的武器系統軟體支援模式改以配合軟體生命週期過程國家標準 CNS14837 所提供之指導，在既有的活動架構下，規劃成軟體於運維期之軟體支援過程活動一般模型，並以 IDEF0 流程建模方法實作之。檢討如下：

### 5.1 壽期涵蓋之檢討

從全系統壽期之時間座標考量，任何系統之軟體支援均至少含括

- (1). 開發(建置)期的軟體支援
- (2). 從開發(建置)完成到運維之間的系統營運及軟體支援移轉
- (3). 運維期的軟體支援工作

本文範圍僅及於其中項次(3)之運維期軟體支援模型。由於此三個時期的軟體支援關係

環環相扣，為完整化考量，未來宜以系統全壽期之格局考量，將開發(建置)期及移轉至運維期的軟體支援一併納入。

此外，軍方科技單位亦曾針對項次(2)的軟體支援移轉做過探討，其以某專案個案之實例，提出了第三者、三階段軟體支援移轉之模式 [11]，此移轉模式成功之實例顯示各系統軟體支援移轉實際可有相當大之彈性空間供吾人進一步研究。

### 5.2 方法論選用之檢討

本文採用之 IDEF0 方法論可分成兩個層面檢討：

- (1). 引用其它方法論建模及其與 IDEF 間的比較檢討
- (2). 引用 IDEF 方法論體系中的其他方法論(如 IDEF1x)以進一步檢討

就前者之不同方法論體系之建模檢討，整合性資訊系統架構 (ARchitecture of integrated Information Systems, ARIS)與本模型採用之 IDEF 正是現今流程建模的兩大方法論體系。就方法論本身而言，已有學者[17]以適用範圍、特點、對於管理的應用、與實踐應用範圍、進行過比較；而應用軟體工具方面，亦以有效的知識管理、圖示明確化、能支援團隊合作工作、共通資料庫、跨平台、及價格等各種指標作為檢討。採 ARIS 方法論與工具對本模型建模並以前述各項指標驗證，將是吾人未來可以進行的方向。

### 參考文獻

- [1] CNS14837，資訊技術—軟體生命週期過程，*中華民國國家標準*，民國 94 年 7 月 26 日修訂公佈。
- [2] 林恕暉，”柵湖線明晚提前收班 六、日停駛”，*自由時報電子報*，2009 年 8 月 20 日。  
<http://www.libertytimes.com.tw/2009/new/au/20/today-life2.htm>
- [3] 林泰龍，”使軟體系統有效維運應依循之過程與建議(上)”，*數揚資訊經營決策論壇*，56 期，2009 年 5 月 1 日。  
<http://www.gss.com.tw/tw/eispage/vol56/eispage5604.htm>
- [4] 林泰龍，”使軟體系統有效維運應依循之過程與建議(下)”，*數揚資訊經營決策論壇*，57 期，2009 年 8 月 1 日。  
<http://www.gss.com.tw/tw/eispage/vol57/eispage5703.htm>



- [5] 林泰龍，「新版ISO/IEC 12207:2008(12207 第二版)已發行」，**中華民國資訊軟體品質協會知識論壇**，民國 97 年 7 月 1 日  
[http://www.csqa.org.tw/portal/modules/newb/viewtopic.php?topic\\_id=384&forum=1](http://www.csqa.org.tw/portal/modules/newb/viewtopic.php?topic_id=384&forum=1)
- [6] 吳正信編撰，**整體後勤支援作業手冊**，系統維護中心，中山科學研究院，民國 80 年 11 月 14 日。
- [7] 姚介修、羅添斌、吳正庭，”桃園機場電腦當機 境管門戶洞開”，**自由時報電子報**，2009 年 1 月 6 日。  
<http://www.libertytimes.com.tw/2009/new/jan/6/today-life6.htm>
- [8] 高進登，**專案計畫軟體後勤支援作業規定**，系統維護中心，中山科學研究院，民國 96 年 12 月。
- [9] 國防部，**國軍主要武器系統研製管理作業規定**。
- [10] 國軍軟體發展規範編撰小組，**國軍軟體發展規範(草案)**，國防部計畫次長室，民國 85 年 6 月 30 日。
- [11] 陳鳳榮、黃昭熙、張孔夏，”佈署前後軟體支援的關鍵--軟體移轉”，**軟體工程通報**，157 期，資訊管理中心，中山科學研究院，民國 90 年 9 月。
- [12] 張孔夏，**武器系統軟體支援研究**，中山科學研究院，內部研究報告，日期不詳。
- [13] 黃昭熙、王平、張孔夏，”武器系統軟體支援”，**軟體工程通報**，146 期，資訊管理中心，中山科學研究院，民國 89 年 10 月。
- [14] 黃昭熙，**軟體維護指引**，V1.0，SE-G0043，軟體工程與資訊中心，中山科學研究院，民國 81 年 9 月。
- [15] 黃昭熙，**軟體發展計畫書指引**，V1.1，SE-G0040，軟體工程與資訊中心，中山科學研究院，民國 83 年 1 月。
- [16] 黃昭熙，**國軍軟體發展規範(草案)簡介**，**軟體工程通報**，97 期，軟體工程與資訊中心，中山科學研究院，民國 85 年 9 月。
- [17] 管孟忠，**策略專案管理系統建模與決策**，初版，博頓策略顧問股份有限公司，pp.54-62，民國 97 年 2 月。
- [18] Budlong, F.C. and Stanko, J.J., “Using software document evaluations to enhance software supportability,” **Digital Avionics Systems Conference**, 1993. 12th DASC., AIAA/IEEE, Volume , Issue , pp.433 – 438, 25-28 Oct 1993.
- [19] DOD Directive 5000.1, **Defense Acquisition**.
- [20] DOD STANDARDS (MILITARY/FEDERAL SPECS) - Procedures Collection, <http://aero-defense.ihs.com/collections/dod/ds6.htm>
- [21] DOD-STD-2167A, **Defense System Software Development**, 1988.
- [22] DoD-STD-7935A, **DoD Automated Information Systems (AIS) Documentation Standards**
- [23] Faye Budlong and Reed Sorensen, “Software Document Evaluation Guidelines for DOD-STD-2167A,” **CrossTalk**, June 1996.
- [24] IEEE/EIA 12207.0-1996, **IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC12207:1995 and (ISO/IEC 12207) Standard for Information Technology—Software life cycle processes –Description**, 1996.
- [25] IEEE/EIA 12207.1-1997, **Industry implementation of International Standard ISO/IEC 12207: 1995. (ISO/IEC 12207) standard for information technology - software life cycle processes - life cycle data**, 1998.
- [26] IEEE/EIA12207.2-1997, **IEEE/EIA Guide Software life cycle processes — Implementation considerations – Description**, 1998.
- [27] IEEE/EIA J-STD-016-1995, **Interim Standard for Information Technology - Software Life Cycle Processes - Software Development - Acquirer-Supplier Agreement** , 30 September 1995.
- [28] **ISO/IEC 12207: 1995, Information technology -- Software life cycle processes**, 1995.
- [29] ISO/IEC 12207:1995/Amd 1, **Information technology -- Software life cycle processes**, 2002.
- [30] ISO/IEC 12207:1995/Amd 2, **Information technology -- Software life cycle processes**, 2004.
- [31] ISO/IEC 12207:2008(E), **IEEE Std 12207™-2008, Systems and software engineering — Software life cycle processes**, Feb. 2008.

[32] MIL-HDBK-347, *Mission Critical Computer Resources Software Support*, 1990  
 [33] *MIL-STD-498 Overview & Tailoring Guidebook*, 31 Jan 1996.  
 [34] MIL-STD-498, *Software Development*

*and Documentation*, 1994.  
 [35] William J. Perry (1994), *Specifications & Standards - A New Way of Doing Business, Memorandum for Secretaries of the Military Departments*, 29 June 1994.

功能領域	一般需求	系統需求分析設計	軟體需求分析	軟體初步設計	軟體細部設計	程式製作 元件測試	件整合測試	軟體構型 項目測試	系統整合 測試
軟體發展管理	4.1	5.1.1	5.2.1	5.3.1	5.4.1	無需求	5.6.1	5.7.1	5.8.1
軟體發展工程	4.2	5.1.2	5.2.2	5.3.2	5.4.2	5.5.2	5.6.2	5.7.2	5.8.2
軟體鑑定測試	4.3	5.1.3	5.2.3	5.3.3	5.4.3	無需求	5.6.3	5.7.3	5.8.3
軟體產品評估	4.4	5.1.4	5.2.4	5.3.4	5.4.4	5.5.4	5.6.4	5.7.4	5.8.4
軟體構型管理	4.5	5.1.5	5.2.5	5.3.5	5.4.5	5.5.5	5.6.5	5.7.5	5.8.5
移交軟體支援	4.6								

圖 1 DOD-STD-2167A 文件架構

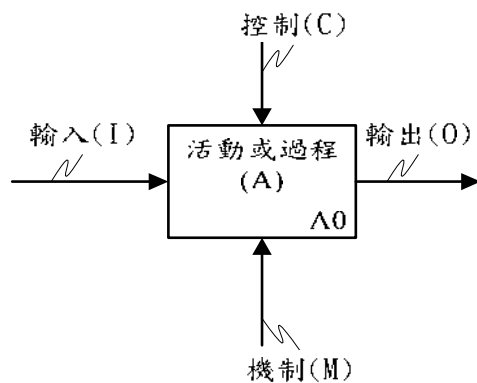


圖 2 IDEF0 結構表示圖

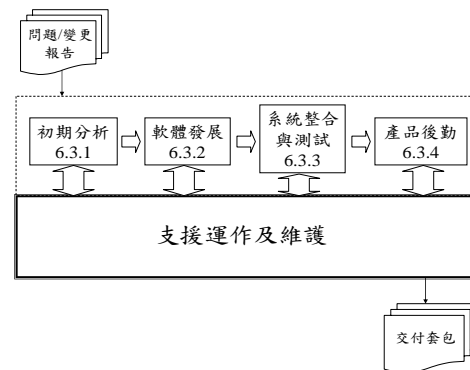


圖 3 PDSS 共通模式

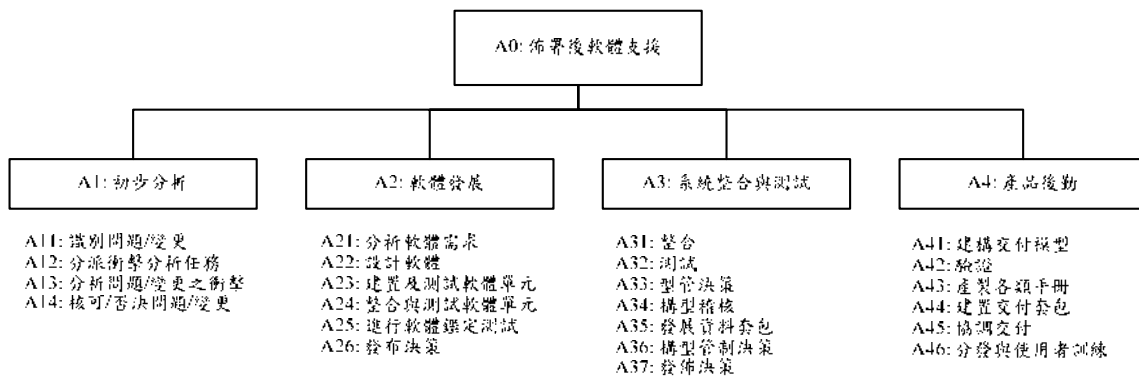


圖 4 PDSS 活動結構

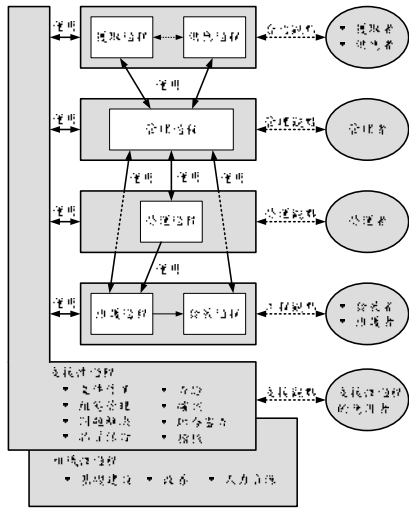


圖 5 軟體生命週期過程—角色與關係

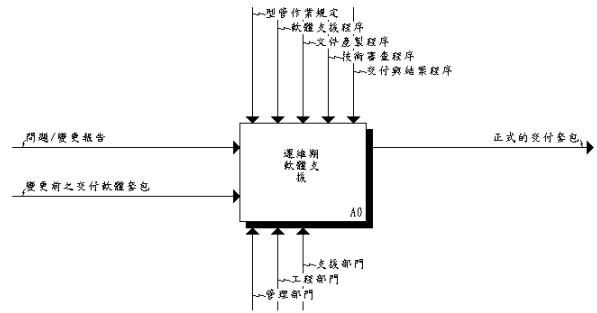


圖 6 運維期軟體支援模型全景

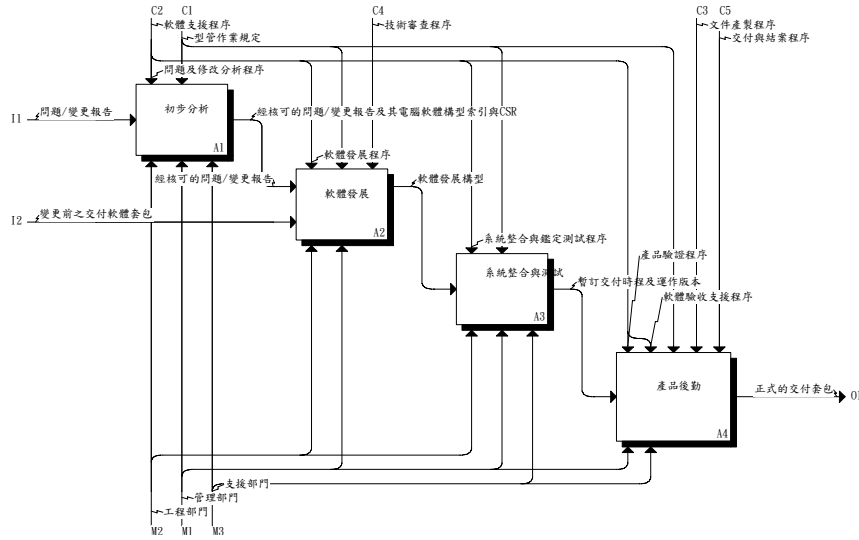


圖 7 運維期軟體支援之第一層活動模型 IDEF0 實作

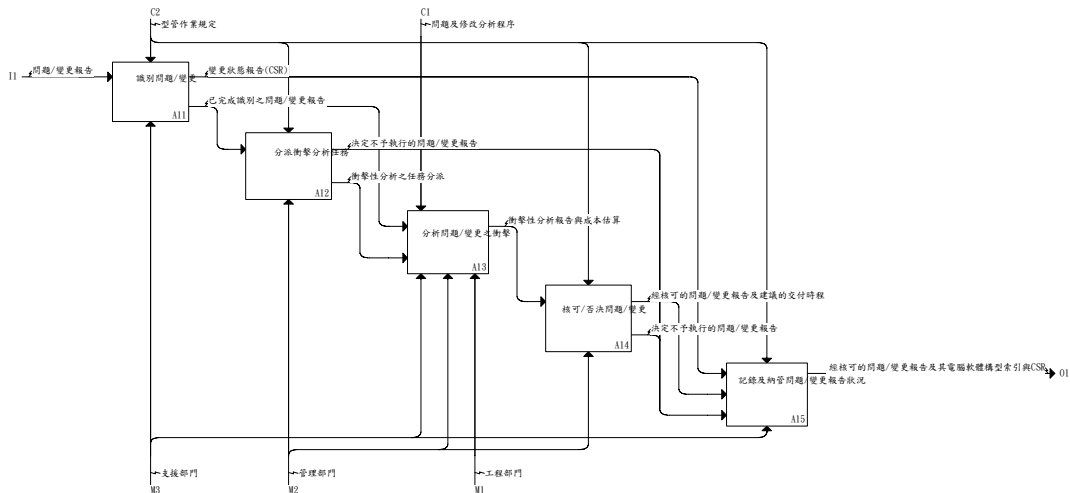


圖 8 初步分析(A1)之下層活動模型 IDEF0 實作

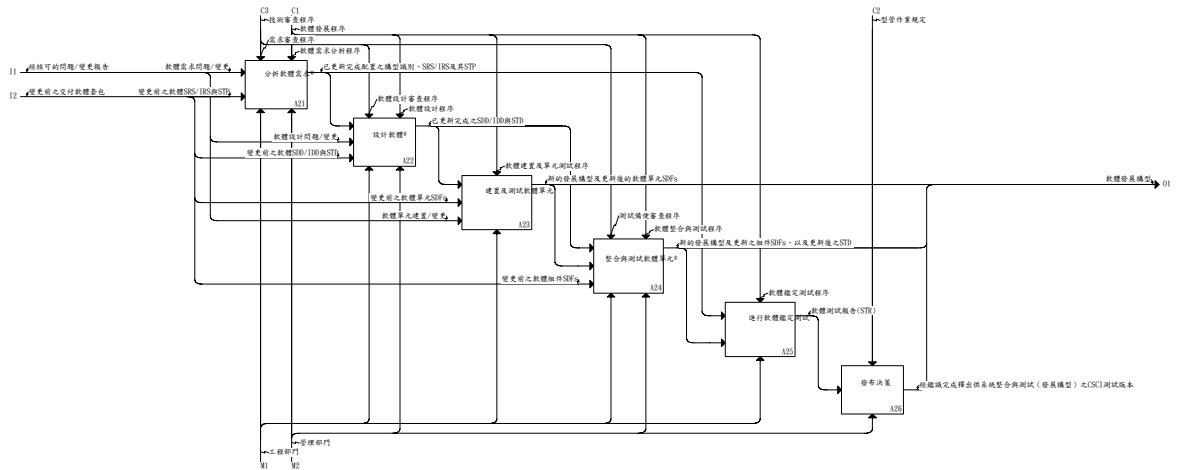


圖 9 軟體發展(A2)下層活動模型 IDEF0 實作

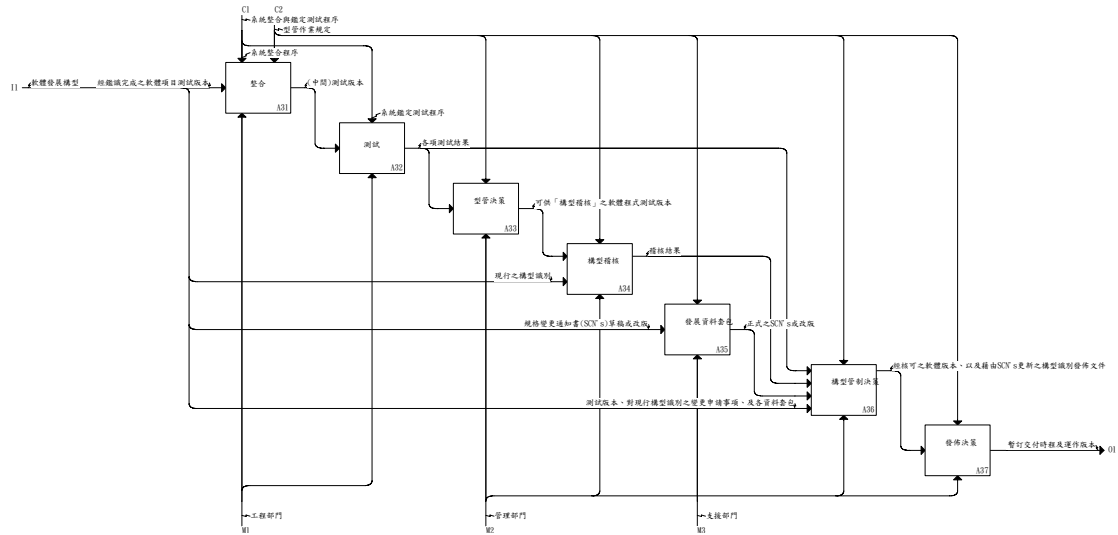


圖 10 系統整合與測試(A3)之下層活動模型 IDEF0 實作

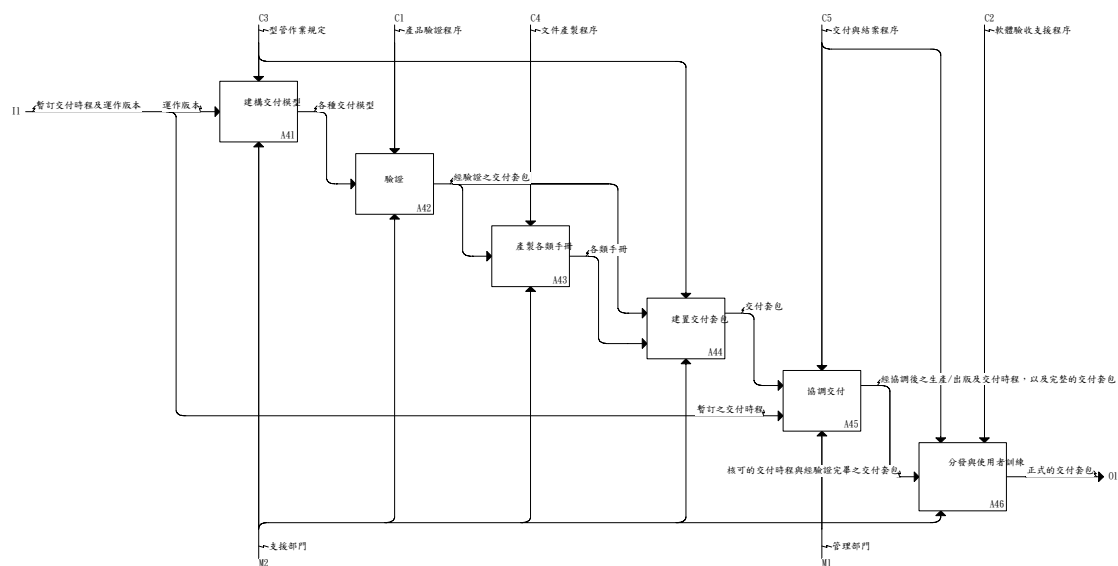


圖 11 產品後勤(A4)之下層活動模型 IDEF0 實作

表 1 CNS14837 各過程之活動與工作統計

軟體生命週期過程	過程	活動	工作
5 主要過程	5.1 獲取(Acquisition)	5	23
	5.2 供應(Supply)	7	24
	5.3 發展(Development)	13	55
	5.4 營運(Operation)	4	9
	5.5 維護(Maintenance)	6	24
6 支援性過程	6.1 文件活動(Documentation)	4	7
	6.2 組態管理(Configuration Management)	6	6
	6.3 品質保證(Quality Assurance)	4	16
	6.4 查證(Verification)	2	13
	6.5 確認(Validation)	2	10
	6.6 聯合審查(Joint Review)	3	8
	6.7 稽核(Audit)	2	8
	6.8 問題解決(Problem Resolution)	2	2
7 組織內過程	7.1 管理(Management)	5	12
	7.2 基礎建設(Infra Structure)	3	5
	7.3 改善(Improvement)	3	6
	7.4 訓練(Training)	3	4