飛行軟體

Flight Software

孟效智
Hsiao-Chih Meng

福衛五號衛星為第一枚由台灣本土團隊自行研發之遙測衛星，運行軌道為 720 公里高之太陽同步圓形軌道。其主酬載為自行研發之遙測影像儀，可提供 2 米解析度之全色影像和 4 米解析度之多光譜彩色影像。福衛五號飛行軟體以韌體形式儲存運行於衛星電腦，共同組成衛星之神經中樞並扮演如同人類大腦的角色。 福衛五號衛星整體之關鍵系統功能運作，均仰賴飛行軟體之規劃／協調／執行／監控，其層面涵蓋衛星本體之熱控制次系統、電力次系統、姿態與軌道控制次系統、反應控制次系統、指令與資料管理電腦次系統、無線通訊等次系統功能。本文將介紹福衛五號衛星飛行軟體設計與測試驗證技術，以及發展過程所面對的困難與挑戰。

FORMOSAT-5 Flight Software and the Flight Computer compose of the central nervous system of the FORMOSAT-5 satellite. They play the role in the satellite as the brain does in human body. All vital satellite subsystem functions are under the persistent planning/coordination/execution/monitoring of the flight software. These vital functions include the Thermal Control Subsystem (TCS), Electrical Power Subsystem (EPS), Attitude & Orbit Control Subsystem (AOCS), Reaction Control Subsystem (RCS), Command & Data Handling Subsystem (C&DH), Telemetry Telecommand and Control (TT&C). This paper introduces the development, verifications and validations strategies taken by the flight software team in developing the FORMOSAT-5 flight software, as well as the difficulties and challenges encountered during the development phase.

一、福衛五號飛行軟體概述

福衛五號飛行軟體以韌體形式儲存運行於衛星電腦，共同組成衛星之神經中樞並扮演如同人類大腦的角色。 飛行軟體技術為衛星計畫敏感技術項目之一，其研發成果決定衛星是否能成功運作，也是台灣能否完全掌握衛星核心控制技術的指標。福衛五號飛行軟體為國家太空中心首次自主發展之高解析度／高機動性遙測衛星控制軟體。發展團隊已完全掌握衛星系統與飛行元件控制技術，及飛行軟體整套開發與驗證作業，完成一套可跨衛星計畫傳承之衛星軟體平台架構。 此通用平台架構可應用於後續衛星系統發展，或在技術完全自主之優勢條件下結合產業界進行商業化營運。

飛行軟體內建即時作業系統，以規劃／協調／執行／監控衛星整體之關鍵系統功能運作，其層面涵蓋衛星本體之熱控制次系統、電力次系統、姿態與軌道控制次系統、反應控制次系統、指令與資料

管理電腦次系統、無線通訊等次系統功能。飛行軟體之發展過程，從需求分析定義、軟體設計、程式碼開發及驗證測試，各個環節皆遵循最嚴格的品質規範。 福衛五號飛行軟體可同時提供 256 個衛星絕對時間指令、10,000 個姿態控制相對時間指令與 20,000 個酬載相對時間指令之儲存空間，並同時監控 512 個衛星健康狀態點。飛行軟體原始程式碼達 120,000 行，執行檔大小達 750 K 位元組，存放於衛星電腦記憶體，必要時能透過地面控制站，將軌道上之飛行軟體進行遠端更新，提供即時韌體升級與高度任務彈性需求。

二、飛行軟體特性

衛星飛行軟體具備以下運作特性，使其能承擔衛星自主控制之重要角色：

特性	說明
可預測性	相同之執行情境導致相同之執行結果
決定性	I/O 管理、控制演算法、時間管理、任務管理隨著時間演進穩定反覆執行
迅速反應	對即時事件立刻反應
可靠度	無軟體錯誤
強健度	可承受衛星在軌時遭遇之異常狀況
可重設構型	可以不同模式或使用不同資料應對相同執行情境
可維護性	支援遠端 (地面控制站) 讀取軟體內部狀態值或低階硬體資料，並提供遠端對衛星軟體之修改機制
安全性	支援遠端控制指令之加／解密機制，保護其不受惡意干擾

三、飛行軟體系統失效回復策略

飛行軟體提供高度自主化系統錯誤偵測、錯誤隔離與系統回復能力。可確保在極端太空環境運作條件下，即使遭遇嚴重系統錯誤時衛星仍能自錯誤狀態回復至安全模式。 衛星在安全模式下衛星可長期運作，電力、熱控與軌道飛行姿態完全由軟體自主掌控，無須地面介入。加上具高容錯能力之衛星軟硬體架構，使衛星不會因任何單一軟/硬體錯誤造成無法挽回之全系統功能失效，此點對衛星生存能力極為重要。

當衛星發生異常時，飛行軟體可視其性質而定，選擇性執行回復程序以防止失效作用擴散至全系統，並進一步將系統回復至全功能或部分功能(系統安全考量)：

(1) 重設出現錯誤之軟體狀態。
(2) 重設出現錯誤之通訊埠。
(3) 關閉故障硬體並切換至備用硬體。
(4) 重組衛星硬體構型至次佳構型。

如系統不支援前述回復程序類型、或失效狀況嚴重時，飛行軟體可進一步將全系統重新啟動，並保留失效事件記錄供地面人員除錯。通常系統重新啟動後進入「安全模式」，在地面人員排除故障前衛星仍可長期在此模式下安全運行。

四、飛行軟體架構

福衛五號飛行軟體採用階層式、模組化架構(圖 1)。衛星所有次系統與設備皆可對應至特定軟體模組，並由軟體模組提供其專屬之通訊／控制功能。

<table>
<tr><td colspan="5">衛星系統管理</td><td rowspan="2">應用軟體層</td></tr>
<tr><td colspan="2">姿態與姿態與軌道控制
次系統</td><td>電力
次系統</td><td>熱控制
次系統</td><td>酬載管理</td></tr>
<tr><td>地面指令</td><td>遙測資料</td><td>衛星電腦管理</td><td>系統監控</td><td>其它服務</td><td>服務軟體層</td></tr>
<tr><td>實時作業
系統</td><td>共用資料區</td><td>事件記錄</td><td>時間管理</td><td>硬體驅動程式</td><td>核心軟體層</td></tr>
</table>

圖 1. 飛行軟體架構。

五、核心軟體層 (kernel layer)

飛行軟體核心層包括實時作業系統 (Real-Time Operating System, RTOS)、共用資料區 (Data Pool)、事件紀錄功能、時間管理及硬體驅動程式功能。

六、服務軟體層 (service layer)

服務軟體功能泛指衛星系統維持系統運作所需之通用性服務項目，或支援次系統／酬載軟體運行所需任務性服務項目。 內容包括地面指令 (Tele-Command, TC) 服務功能、遙測資料 (Telemetry, TM) 服務功能、衛星電腦管理服務功能、系統監控服務功能及其它功能。

七、應用軟體層 (applications layer)

應用軟體層提供整個衛星系統運作所需之高階次系統控制功能 (圖 2)。最上位者為總管整個衛星系統之衛星系統管理 (System Management) 功能，旗下則為各次系統控制軟體功能如姿態與軌道控制次系統 (Attitude & Orbit Control Subsystem, AOCS)、電力次系統 (Electrical Power Subsystem, EPS)、熱控制次系統 (Thermal Control Subsystem, TCS) 及酬載管理 (Payload Management) 功能。

(1) 衛星系統管理軟體：提供衛星模態管理／處理功能、指令介面管理功能與系統層級失效偵測／隔離／回復機制。 所有其它次系統軟體功能皆從屬於衛星系統管理功能並受其管制。當次系統功能出現異常時，亦由系統管理軟體統籌

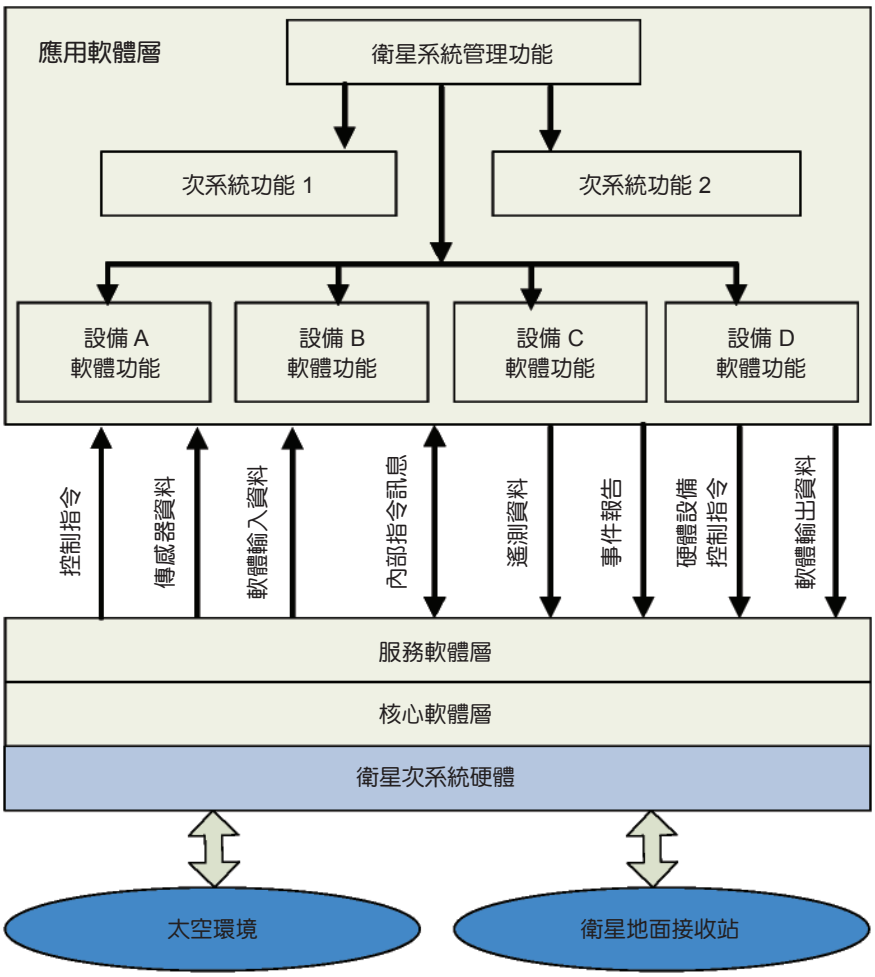

圖 2. 飛行軟體系統管理。

執行對應之系統層級故障排除或保護機制。例如：重啟衛星系統並將之置於安全模式。

(2) 姿態與軌道控制次系統軟體：提供飛行模式管理／處理功能、衛星飛行姿態估測與控制、衛星軌道計算與控制、感測器／致動器資料處理與控制，以及姿態與軌道控制次系統層級失效偵測／隔離/回復機制。例如：飛行姿態異常保護及感測器/致動器異常保護。

(3) 電力次系統軟體：提供衛星電力控制模式管理／處理功能、衛星電池充放電控制，以及電力次系統層級失效偵測／隔離／回復機制。例如：電力負載過電流保護與電池低電壓保護。

(4) 熱控次系統軟體：提供衛星溫度計／電熱器構型管理功能、溫度計讀值處理／監控、電熱器開／關作動，以及熱控次系統層級失效偵測／隔離／回復機制。例如：局部溫度異常之保護。

(5) 酬載管理軟體：提供衛星酬載控制模式管理功能、酬載構型管理，以及酬載層級失效偵測/隔離／回復機制。例如：酬載通訊異常之保護。

八、飛行軟體發展策略

人造衛星是一套極其複雜的電機系統，而其所處之工作環境非常嚴苛的太空物理環境 (高度真空、急遽溫度變化、大量電磁輻射)。在此前提下如要確保飛行軟體能完全正確無誤執行系統控制之核心工作，飛行軟體的發展過程，從需求分析定義、軟體設計、程式碼開發及驗證與確認測試之各個環節皆需遵循最嚴格的品質規範。

從飛行軟體發展工程實務面觀之，在衛星計畫早期階段，其硬體規格與軟體需求尚不明確，導致軟體設計與飛行電腦設計工作或硬體輸出／入界面定義工作出現平行發展之狀況，因此軟體發展測試團隊面臨以下之困境：

- 經常需以尚在發展中硬體 (航電系統) 測試軟體。
- 需應用邏輯分析儀、軟／硬體模擬器等各類進階測試工具。
- 測試時偶發事件之綜合效應可能引發未知之軟／硬體衝突，非常不易除錯。
- 幾乎不可能同時控制多項測試資料輸入介面以達成完全可受控之測試環境。
- 實作大量 (但未必足夠) 測試情境會過度耗費計畫資源 (時程)。

為克服諸多不利於飛行軟體研發工作推展之困難，飛行軟體團隊須遵循嚴謹軟體發展流程，採行以下發展步驟完成發展工作：

(1) 軟體工程師全面性參與任務發展定義。

(2) 審慎規劃/定義軟體需求規格。

(3) 先完善設計架構，再著手發展程式碼。

(4) 完整驗證軟體程式碼及設計，盡可能以實際硬體測試飛行軟體。

步驟一：飛行軟體功能需求定義

分析衛星系統層級需求文件，並將之轉化成飛行軟體高階軟體需求，例如：

(1) 衛星系統需求及規格分析。

(2) 酬載系統介面規格及操作程序。

(3) 星-地通訊協定分析。

(4) 系統失效偵測、隔離及回復程序分析。

步驟二：飛行軟體設計規格發展

全面分析衛星電腦之設計規格、衛星內部／外部所有通訊協定、 各次系統功能控制邏輯與硬體裝置之設計，進一步發展對應之軟體控制架構與細部設計：

(1) 核心及服務層軟體發展。

(2) 系統管理 (System Management) 軟體發展。

(3) 姿態與軌道控制次系統 (AOCS) 軟體發展。

(4) 電力控制次系統 (EPS) 軟體發展。

(5) 熱控次系統 (TCS) 軟體發展。

(6) 酬載管理 (Payload Management) 軟體發展。

步驟三：飛行軟體程式碼撰寫

以遞增方式建構軟體程式碼， 配合衛星及酬載系統設計製造進度將軟體分為若干建構 (build) 版本。每一建構版本皆為可執行之飛行軟體版本，次系統軟體功能則隨著建構版本之演進而逐漸完備。

例如：

建構版本 1：系統管理功能、系統核心服務程式及驅動程式。

建構版本 2：衛星安全模式飛行控制功能及電力控制／熱控制功能。

建構版本 3：衛星正常模式飛行控制功能。

建構版本 4：衛星系統失效偵測、隔離及回復功能

建構版本 5：任務酬載控制功能與科學酬載控制功能。

步驟四：飛行軟體功能驗證與確認

飛行軟體後期發展階段，最重要工作為軟體驗證與確認。飛行軟體須通過至少三階段基本測試考驗，才能實際安裝使用於衛星飛行電腦上：

第一階段測試為軟體模組測試。此時龐大之飛行軟體被化為單一或數個相關軟體功能模組，個別的進行局部功能及界面之測試。 測試過程中將儘可能運用白箱測試方式，即軟體模組程式碼執行狀態可為測試人員掌握。如此可充分確認個別程式模組與所屬設計規範為一致且正確。此階段測試工作如果完善，可早期檢出大部份程式碼錯誤，大幅提高後續進階功能整合測試之執行效率，並降低後期發現錯誤而衍生之修正成本 (圖 3)。

第二階段為次系統功能層級之功能驗證測試。其代表者為姿態與軌道控制次系統軟體控制功能驗證。 利用特殊「軟體功能驗證平台」，將待測飛行軟體功能模組與獨立發展之軟體姿軌控制模擬器結合，進行高精度軟體模擬測試、功能檢查、除錯與驗證等工作。「軟體功能驗證平台」主要由三層軟體工具環境組合而成，此三層工具環境分別為上層姿軌控制飛行軟體模組，中層功能驗證測試環境與資料介面層，以及底層姿軌控制模擬器。其中最重要的是功能驗證測試環境層，它提供一套完整飛行軟體作業系統執行核心及 IO 模擬環境。該模擬環境可在一般的電腦平台上運行 (例如：Windows / LINUX/UNIX)，並提供高階飛行軟體應用程式的執行環境。從軟體功能驗證測試目的而言，此平台不僅可以節省購置真實衛星電腦硬體環境的高昂成本，且可提供軟體變數資料的檢查與輸出介面，以支援精確測試數據分析。大幅降低功能驗證平台、軟體測試驗證平台與衛星工程體軟體驗證測試時除錯之困難與複雜度 (圖 4)。

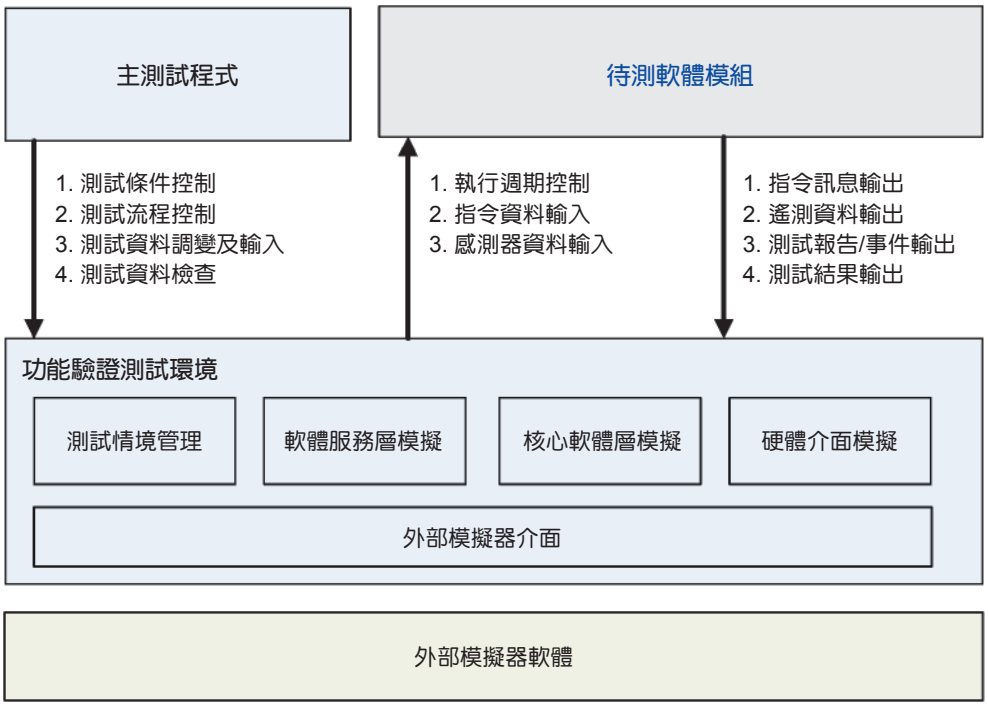

圖 3. 飛行軟體模組測試環境。

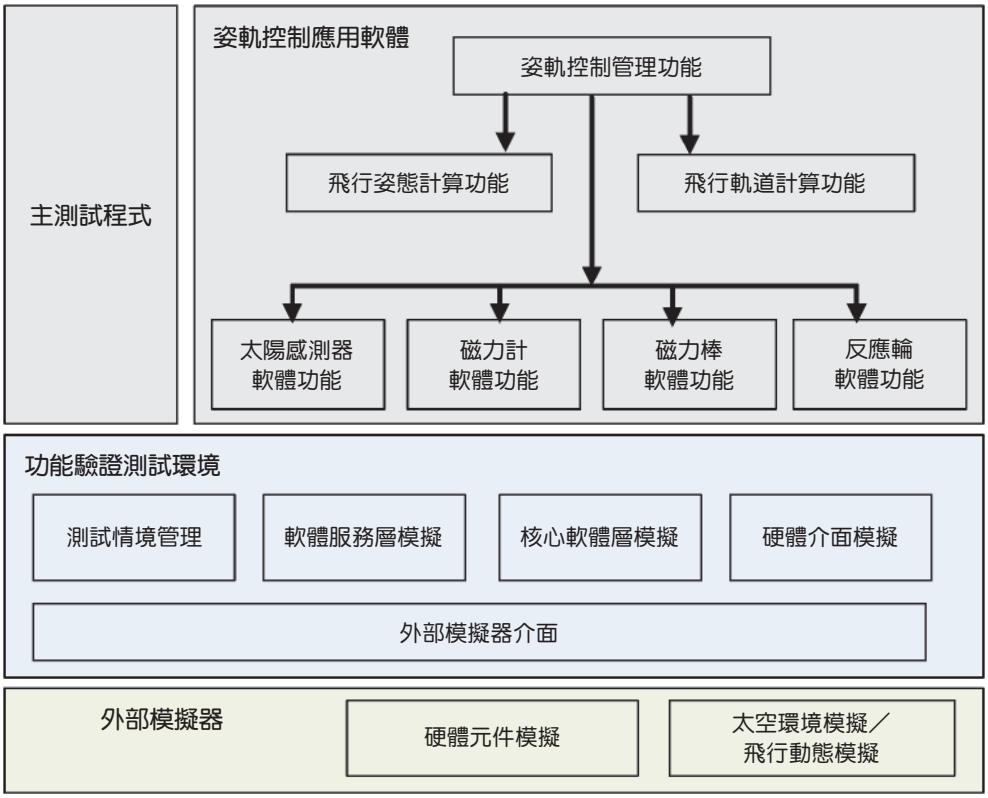

圖 4. 姿軌控制軟體功能驗證測試。

第三階段為衛星工程體層級驗證測試。此階段利用與真實之飛行電腦相同功能之飛行軟體測試平台，並結合其它衛星次系統軟／硬體模擬器進行接近全功能軟體驗證測試 (圖 5)。

圖 5. 衛星工程體驗證測試。

透過以上之三階段歷程，由點 (模組測試) 而線 (次系統功能驗證測試)，再推展至全面 (衛星工程體測試)，即可逐步完成飛行軟體驗證測試工作。 而通過層層考驗之飛行軟體產品，才算取得合格之品質與功能標章，可安全進入衛星發射前最終階段之整合測試工作。

孟效智先生為美國德州大學奧斯丁分校航太工程碩士，現為國家實驗研究院國家太空中心衛星飛行軟體部門經理。

Hsiao-Chih Meng received his M.S. in aerospace engineering from the University of Texas at Austin. He is currently the Flight Software department manager of the National Space Organization, NARLabs