ICS 49.140

中華民國國家標準

C N S

太空系統－形態管理

Space systems－Configuration management

CNS 草-制 1150009:2026
D1

中華民國　年　月　日制定公布
Date of Promulgation:　-　-

目錄

前言

本標準係依據 2019 年發行之第 1 版 ISO 21866，不變更技術內容，制定成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

太空系統是一個複雜系統，需要形態管理確保其成功。形態管理建立並維護產品功能及實體特性，與其設計及運作要求事項比較之一致性紀錄，以便允許參與人員隨時使用已核准文件瞭解產品之技術說明，及在任何時間點瞭解產品運作之可能性及限制。

1. 適用範圍

本標準定義太空專案形態管理之內容、方法及要求事項，及相關方之職責及權限。

本標準可與ISO 14300-1：2011第10節一起使用。

本標準適用於太空專案從任務分析階段至處置階段之形態管理。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

CNS 14238 品質管理系統－形態管理指導綱要

ISO 14300-1 Space systems－Programme management－Part 1: Structuring of a project

ISO 10795 Space systems－Programme management and quality－Vocabulary

3. 用語及定義

CNS 14238、ISO 14300-1及ISO 10795之用語及定義及下列用語及定義適用於本標準。

3.1 形態(configuration)

形態資訊中定義之產品或服務的相互關聯功能及實體特性。

3.1.1 功能特性(functional characteristic)

待實現或要求之性能參數及設計限制，包括運作及邏輯參數及其各自之許可差。

備考：功能特性包括所有性能參數，如範圍、速率、毀壞性、可靠度、可維護性及安全性。

3.1.2 實體特性(physical characteristic)

產品及其許可差之定量及定性表達。

例：機械、電氣、化學或生物特性。

3.2 形態管理(configuration management)

建立並維護與產品設計及運作要求事項相比，產品性能參數與其功能及實體屬性狀況及變更之一致性紀錄的活動。

備考：形態管理貫穿產品整個壽命週期(即開發、生產、部署、運作及處置)。

3.3 形態項目(configuration item)

指定用於形態管理並在形態管理(3.2)過程中視為單一實體之硬體、軟體、加工材料、服務或其任何獨立部分之集合。

備考：一個形態項目可包含其他形態項目。

3.4 形態文件(configuration document)

定義形態項目(3.3)功能、設計、建造、生產及查證要求事項之文件。

備考：對於太空系統，形態文件可包括與形態項目運作及處置相關之文件。

3.5 形態基線(configuration baseline)

產品要求事項及設計在專案關鍵里程碑之核准狀況，可作為產品整個壽命週期活

動之參考。

3.6 變更管制(change control)

在產品形態基線(3.5)正式核准後，管制產品變更、偏差/豁免之活動。

3.7 變更(change)

對文件或其任何部分進行正式依編號發布之修改，通常由於條件改變或更完整之資訊所引起。

備考1. 〝1類〞(主要)變更是指衝擊專案與其顧客間達成之合約/技術協議之變更。此類變更必須在實施前提交顧客審查及核准。

備考2. 〝2類〞(次要)變更是指未衝擊顧客合約，且為專案及其供應鏈符合技術/合約要求事項及規定所需之變更。此類變更可於形態管制委員會(configuration control board, CCB)核准後實施。

4. 一般

4.1 形態管理建立並維護與產品設計及運作要求事項比較之產品功能及實體特性的一致性紀錄。形態管理應應用於產品整個壽命週期，並隨著專案發展而不斷改進。

4.2 依據形態項目之複雜性及其在專案分解結構中之位置，建立由相關領域代表組成之形態管制委員會(CCB)。CCB由所有計畫或專案專業領域之固定代表組成，負責變更之審查及評估。CCB成員擁有決策權。

4.3 每一供應者應依據顧客之形態管理要求事項產出形態管理計畫書(CM計畫書)。CM計畫書應規定整個壽命週期內每一階段之目標、任務、職責及要求事項，並依據專案發展過程中之具體情況進行必要的修訂。

4.4 形態管理與工程、產品保證、製造及生產介接，並藉由識別與商業協議條款相關所有限制，為計畫或專案組織及其執行進度做出貢獻。

5. 形態管理規劃

5.1 一般

形態管理規劃針對特定之形態項目。有效之形態管理規劃能夠在產品壽命週期之特定環境中協調形態管理活動，並應於專案初始階段執行。

形態管理規劃應：

(a) 確保形態管理過程能夠全面且精確地記錄及管制產品形態之演進。

(b) 確保參與人員隨時瞭解產品正確形態文件。

(c) 確保所使用之形態文件完整、正確、受控且經核准。

(d) 確保形態演進之可追溯性。

(e) 確保產品內部與外部介面之一致性。

(f) 確保受檢驗產品之形態與技術文件要求事項的一致性。

5.2 形態管理計畫書

5.2.1 形態管理計畫書是規定組織及其職責、實施形態管理程序、資源及方法之文件。形態管理規劃之輸出是形態管理計畫書。供應者應依據提交顧客核准之要求事

項準備形態管理計畫書。

5.2.2 對於形態項目，形態管理計畫書應：

(a) 符合合約要求事項。

(b) 建立實施形態管理之總體目標及階段目標。

(c) 規定實施形態管理之職責及權限。

(d) 建立實施形態管理之程序及方法。

(e) 遵守顧客定義之形態要求事項。

(f) 明確介面管制要求事項。

(g) 確保形態管理過程處於受控狀態。

5.2.3 附錄A提供形態管理計畫書之架構及基本內容。

5.3 形態管理介面

形態管理是專案管理不可或缺之一部分。形態管理過程應與工程管理、產品保證、產品製造及資訊/文件管理介接。在形態管理活動之定義及分階段實施方面，形態管理亦應考慮合約規定及時間表。

6. 形態識別

6.1 一般

形態識別應逐步建立並發布管制文件，以識別產品之形態特性，直至產品完全定義其預期功能及實體特性。形態識別為形態管制、現況彙整、查證及稽核建立並維護文件之基礎，並為實施形態管理之基礎。形態文件之管理宜納入資訊/文件管理過程，其關係詳述於附錄B。

6.2 形態識別之主要活動

形態識別之主要活動包括：

(a) 基於專案分解結構及產品樹選擇形態項目。專案分解結構之過程及要求事項依據ISO 27026執行。

(b) 決定不同階段產生之形態文件(包括內部及外部介面文件)，並形成初步形態文件清單。

(c) 規定形態項目及形態文件之識別符。

(d) 基於核准之形態文件清單產生形態文件。

(e) 建立形態基線。

(f) 文件化形態變更資訊並提供其識別符。

6.3 產品樹

6.3.1 供應者應依據一級(level 1)顧客定義之可靠邏輯及要求事項，從功能要求事項開始分解專案任務。供應者應基於專案分解結構，決定專案結構層級及相應之工作，並依據每一產品之功能要求事項，完成對應之產品樹。

6.3.2 產品樹基於已核准之最終功能，將系統分解為連續之層級，定義產品由上而下之架構框架，如系統層級、次系統層級、單元層級等。

6.3.3 供應者應確保產品樹能全面說明產品之連續分解、產品之組成及其位置並實現產品功能所需之形態項目。

6.3.4 產品樹是基於專案過程中所獲得之歷史資訊或知識而建立。產品樹應在形態管制下進行更新。

6.4 形態項目

6.4.1 形態項目之選擇是基於專案分解結構及產品樹。形態項目與產品樹結構相對應，並於產品樹不同層級上識別。

6.4.2 形態項目分為二類：已開發形態項目及未開發形態項目。已開發形態項目是指正在開發中，且為該計劃或專案而全部或部分設計之形態項目。而非開發形態項目是指標準化或〝現成(off-the-shelf)〞之產品，並非專門為計畫或專案開發。此二類形態項目均應遵循形態管理之要求事項進行管理。

6.5 形態項目之選擇

6.5.1 儘早選擇形態項目。上層(系統及次系統層級)之形態項目應於早期定義階段加以選擇。下層(單元層級)之形態項目應於其壽命週期之初始階段加以選擇。

6.5.2 所選形態項目之數量應考慮管理效果、成本、風險(包括安全性及安保性)及開發時間等，以最大化提高組織之專案管制能力。

6.5.3 組織應依據明確之選擇準則以決定形態項目。選定形態項目通常為：

(a) 功能及實體特性可單獨管理之形態項目。

(b) 系統層級、次系統層級或跨單元、跨部門開發之形態項目。

(c) 從安全性、風險及任務成功觀點而言，具有關鍵特性之形態項目。

(d) 採用新設計、技術或方法之形態。

(e) 與其他項目介接之項目。

(f) 指定單獨採購之形態項目。

(g) 對使用及安保性關鍵之形態項目。

6.5.4 對於顧客管制之形態項目及其相關基線審查，顧客及供應者應相互協商，以決定形態管理計畫書中應定義之原則。

6.5.5 已確認之形態項目清單應提交顧客核准。清單應指出形態項目之結構(系統、次系統及單元)、名稱及識別符。

6.5.6 隨著專案演進，對形態項目進行審查並更新。

6.6 形態文件清單

6.6.1 每一供應者應決定在產品整個壽命週期內需要準備與設計、製造、測試、運作、維護、儲存等相關之形態文件(包括內部及外部介面文件)。形態文件清單應隨著組態識別活動之演進而不斷改進及更新。

6.6.2 形態文件清單應包括：

(a) 文件標題及識別符。

(b) 文件類型。

(c) 壽命週期期間中之階段。

(d) 預期發布時間(由階段及供應者時間表決定)。

(e) 準備公司及文件狀況。

(f) 類別(公開、保密)等。

6.6.3 供應者準備之形態文件清單應提交顧客核准。

6.7 識別標記

6.7.1 一般

對於已確認之形態項目，其識別標記主要包括形態項目識別符及形態文件識別符。

6.7.2 形態項目識別符

6.7.2.1 形態項目識別符是用以指示項目(產品)稱號及類型之代碼，應由顧客、供應者或相關方依據其來源及分解結構(如系統、次系統、單元等)產生。

6.7.2.2 形態項目識別符應具有唯一性。形態項目識別符應包括：

(a) 型號識別符。

(b) 序號。

(c) 形態項目識別符。

(d) 製造者識別符。

(e) 產品名稱等。

6.7.2.3 標準產品及現貨產品之識別符應符合相關標準及要求事項。

6.7.3 形態文件識別符

6.6.3.1 形態文件識別符是用於指示所述實體及文件類型之代碼，通常由供應者依據內部規定產生。

6.7.3.2 形態文件識別符應具唯一性。

備考：為避免不同產品(項目)可能存在相同之識別符，通常之做法是在識別符前加上企業識別符。

6.7.3.3 形態文件識別符通常包括：發布者名稱、文件識別符、階段識別符、狀況識別符、文件變更或修訂識別符等，並應於技術文件之特定位置(例：標題列)進行標記：

(a) 發布者名稱：文件發布者之名稱或名稱縮寫。

(b) 文件識別符：文件編號由產品識別符、實體代碼、代碼及文件類別號碼組成，其中：

(1) 產品(項目)識別符是為區分不同產品而規定之符號。

(2) 實體代碼是為區分不同類型產品技術文件而規定之代碼，通常包括型號產品代碼、設計序號等。

(3) 代碼是依據特定規則，依據產品之層級關係或技術特性而規定之代碼。

(4) 文件類別號碼是區分不同類型文件而規定之代碼。

(5) 企業代碼是供應者為區分不同供應者而規定之代碼。說明同一形態項目之文件應連續編號。

(c) 階段識別符：用於識別形成之文件在產品整個壽命週期中所處階段。階段劃分參照ISO 14300-1。

(d) 狀況識別符：用於指示實體之狀況，例：M表示模型衛星，F表示任務衛星。

(e) 文件變更實施識別符：實施文件變更識別符包含實施文件編號之變更及標記之變更。

6.8 形態文件

6.8.1 組織應依據壽命週期期間各階段所需之形態文件清單，準備一套完整之形態文件。

6.8.2 在專案開發期間中，應文件化所有每一形態項目之所有功能特性、實體特性、介面、變更及其他資訊，並為其指定唯一識別符。

6.8.3 形態項目資訊通常於下列文件中說明：

(a) 規格：定義要求事項之文件，包括功能規格及技術規格(如系統規格、開發規格、產品規格、製程規格、材料規格等)。功能規格及技術規格應依據ISO 21351準備。

(b) 圖面：使用圖形及(或)規定符號展示產品結構、組成、形狀及其他資訊之文件，包括圖面及示圖。

(c) 清單：使用表格或清單說明產品或文件之組成及數量的文件，包括總結清單、支援清單及成套文件清單等。

(d) 程序及手冊：規定執行某項活動或程序之方法及要求事項的文件，如操作程序、操作及維護手冊等。

6.8.4 專案開發期間目標之實現，通常由三類形態文件定義：功能形態文件、開發形態文件及產品形態文件。

6.8.4.1 功能形態文件定義顧客之任務需求，規定整體功能要求事項、任務要求事項、介面要求事項、設計限制、允收及運作要求事項。功能形態文件通常以功能規格及(或)系統規格之形式表達。

功能形態文件通常包括：

(a) 任務定義。

(b) 性能、風險、要求事項及目標。

(c) 主系統或次系統之功能及實體特性。

(d) 內部及外部介面要求事項。

(e) 設計準則、條件及運作限制。

(f) 試驗及可靠度要求事項。

(g) 組織、成本、時程等。

6.8.4.2 開發形態文件定義上層形態項目分配之組成及項目的功能要求事項、任務要求事項、介面要求事項、設計限制、允收及運作要求事項。開發形態文件通常以開發規格形式表達。

開發形態文件通常包括：

(a) 系統、次系統或單元之功能特性要求事項。

(b) 系統、次系統或單元之主要實體特性。

(c) 系統、次系統或單元之內部及外部介面要求事項。

(d) 所有查證設計所需之試驗或審查要求事項。

(e) 設計準則、設計限制等。

6.8.4.3 產品形態文件定義特定項目之功能特性、實體特性、檢驗及允收要求事項。產品形態文件包含完整之技術文件，說明交付產品之設計、製造、允收、運作、支援及介面。產品形態文件通常以產品規格、物料規格、程序規格、圖面、示圖、清單等形式表示。

6.8.4.4 在壽命週期期間之每一階段，均要準備、審查及維護功能、開發及產品形態文件。此三類文件應逐步擴展、細化、協調一致且可追溯。

6.8.4.5 當功能、開發及產品形態文件間發生衝突時，其優先順序為：功能形態文件、開發形態文件、產品形態文件。

6.9 形態基線

6.9.1 為實現總體目標，專案通常分為幾個階段。每一階段均有各自之目標及任務。在形態管理中，每一階段之目標均藉由建立形態基準實現。

6.9.2 形態基準包括在專案開發期間某些時間點正式核准之文件。該文件被指定為後續開發及生產活動之基線。此基線由供應者及顧客共同決定，並應作為形態管制之起點。

6.9.3 在產品壽命週期期間，形態基準應依下列順序制定：

(a) 從可行性階段(階段A)開始，在早期定義階段(階段B)建立功能基線。當顧客核准關於功能、性能及介面指標之整體要求事項文件時，功能基線即完成。

(b) 從早期定義階段(即功能基線建立後)開始，在後期定義階段(階段B)建立開發基線。當低層形態項目之功能、性能及介面要求事項文件經供應者確認後，開發基線即完成。

(c) 產品基線在生產後期(階段D)及產品合格後建立。產品基線包括產品製造、組裝、測試、允收及運作所需之文件及已核准之所需變更。

6.9.4 對於系統、次系統及低層級，可依據項目之複雜性及任務進度新增新的形態管制點。例：設計基線可於開發早期(階段C)及關鍵設計審查後建立。設計基線包括供應者準備之技術規格及設計資料文件，及低層級形態項目之相應文件。

6.10 形態變更文件

6.10.1 基線建立後，所有基線之後的變更均應文件化，每一文件應具唯一識別符，以

保持文件及實體間之一致性。

6.10.2 形態變更文件包括變更請求、變更提案(change proposal, CP)、偏差及豁免申請及核准後之相關實施文件。

6.10.3 實施文件之識別符通常應包括變更實施文件編號、變更頻率及變更之處等。

6.11 形態文件之發布及維護

應於規定時間前提交經核准之形態文件以供發布。供應者應保存並管制所有形態文件之原始副本。

7. 形態管制

7.1 一般

形態管制是管制已同意基線演變或偏離/豁免之過程。其包括工程及合約變更、偏差及豁免之準備、合理說明、評估、處置及實施。

7.2 形態管制要求事項

7.2.1 為維持形態文件與實體間之一致性，供應者應執行形態變更管制，以管制已同意基線之演變或偏離/豁免。

7.2.2 形態管制從功能基線建立時開始，並於專案整個壽命週期期間執行。形態管制通常包括：

(a) 決定形態管制之類別。

(b) 決定形態管制實施之程序、職責、方法及要求事項。

(c) 實施對形態變更之管制。

(d) 追蹤並查證已核准變更之實施情況。

7.2.3 對於任何變更、偏差或豁免，應說明其對較高層級及相關形態項目之影響。由於共同變更需求而導致多個產品之相關變更應同時處理。涉及多個產品共同要素之變更，應提交所有相關方進行影響評鑑。

7.3 變更

變更是指在專案開發期間中對已正式核准形態文件案進行之修改。顧客及供應者均可提出〝變更請求〞。對於顧客提出之〝變更請求〞應以書面形式通知供應者，並在實施前一定時間內獲得供應者以經核准之〝變更提案〞形式答覆。對於會影響合約及/或技術要求事項之〝變更提案〞，應在實施前提交至顧客層級形態管制委員會審查並核准。

7.3.1 變更分類

7.3.1.1 變更分為二類：I類變更與II類變更。供應者可依據管理要求事項，在變更受控之前提下，進一步細化變更內容。

7.3.1.2 I類變更包括：

(a) 顧客規定且會影響合約要求事項之變更：

(1) 成本。

(2) 保固條款。

(3) 交付要求事項。

(4) 重大事件安排。

(b) 功能及(或)開發形態文件之變更，導致下述要求事項超出規定值：

(1) 功能及性能定義。

(2) 可靠度、可維護性、安全性、生存性、環境適應性及電磁相容性等。

(3) 介面特性。

(4) 關鍵實體特性，如結構大小、質量、轉動慣量。

(5) 其他對專案成功有直接衝擊之要求事項。

(c) 對下述有顯著衝擊之產品形態文件變更：

(1) 上述(a)及(b)規定之功能及(或)開發形態文件。

(2) 支援設備及應用軟體。

(3) 形態項目及其組成之互換性。

(4) 已交付之操作及維護手冊。

(5) 已交付項目等。

I類變更應提交相應層級之形態管制委員會進行審查。I類變更必須在獲得形態管制委員會核准後才能實施。

7.3.1.3 II類變更不符合I類變更之準則，且是供應者為符合合約及/或技術要求事項與法規所必需。供應者應針對II類變更實施內部控制。

7.3.2 變更程序

7.3.2.1 決定變更之必要性

任何形態項目之變更均應於提交前，由請求方進行說明及證明正當。

7.3.2.2 變更分類

在提交變更前，依據7.3.1.2中之規定對變更進行分類(I類變更及II類變更)。

7.3.2.3 變更開始

對於I類變更，請求方應起草變更提案(或變更請求)，並提供必要之證明資料，並提交相應之形態管制委員會進行審查。對於II類變更，供應者應依規定實施內部控制。

7.3.2.4 變更評鑑

變更評鑑應由相應之形態管制委員會依據變更類別、介面及階段進行。評鑑主要包括：

(a) 變更之必要性與可行性。

(b) 變更影響之相關項目及文件。

(c) 對介面、互換性、安全性及可靠性之衝擊。

(d) 對生產、測試及檢驗之衝擊。

(e) 對採購及儲存之衝擊。

(f) 對運作、維護及更換零件之衝擊。

(g) 對合約、後勤支援及成本等之衝擊。

7.3.2.5 變更處置

所有變更應由相應之形態管制委員會依下述方式之一處置：

(a) 核准，定義演進之適用性及相關實施模式。

(b) 否決，並提供支持性理由。

(c) 延後，直至提供更多資訊。

7.3.2.6 變更核准

變更提案應由相應形態管制委員會成員中之適當人員核准。

7.3.2.7 實施及查證

7.3.3 對於已核准之變更，供應者應準備變更實施文件(如變更通知)，並發布給相關方實施，並應查證實施情況。變更提案/請求。

對於I類變更，供應者完成其審查及核准過程後，應將變更提案/請求提交至相應之形態管制委員會進行審查。變更提案/請求應包括：

(a) 變更提案/請求編號。

(b) 公司名稱及變更提案/請求之提交日期。

(c) 變更之形態項目及形態文件之標題及編號。

(d) 變更類別。

(e) 變更之必要性及原因。

(f) 變更內容。

(g) 變更之衝擊(受影響之項目、文件、性能參數、時間表、介面等)。

(h) 變更實施計畫書。

(i) 變更費用預算等。

7.4 偏差/豁免

7.4.1 偏差/豁免要求事項

為達到預期目標或特定目的，與形態文件之偏差應於產品製造前經過申請程序。

若成品或製造過程中之產品超出形態文件規定允許值，則應申請豁免。

除特殊情況外，不得申請涉及安全、對運作及維護有致命缺陷或衝擊之偏差。

涉及人員健康、功能、可靠度、維護性、互換性及關鍵實體特性之豁免應經顧客核准。

經核准之偏差/豁免僅適用於指定之背景及時間段，且不變更形態文件。

供應者應對偏差/豁免實施內部控制。為避免豁免再次發生，供應者應分析根本原因，採取矯正措施，並將有效措施納入相應文件。

7.4.2 偏差/豁免分類

偏差/豁免可分為主要偏差/豁免及次要偏差/豁免。主要偏差/豁免涉及：

(a) 功能特性及性能定義。

(b) 關鍵實體特性(結構大小、質量、轉動慣量)。

(c) 介面。

(d) 產品互換性、可靠度、安全性、保安性、電磁相容性及環境適應性。

(e) 人員健康與安全。

(f) 產品之使用及維護性。

次要偏差/豁免為不符合主要偏差/豁免之準則。

7.4.3 偏差/豁免申請

偏差/豁免申請通常包括：

(a) 申請編號。

(b) 公司名稱及提交日期。

(c) 偏差/豁免類別。

(d) 偏差之必要性或豁免原因。

(e) 偏差/豁免說明。

(f) 受影響之形態項目及文件編號及標題。

(g) 對功能、性能參數、進度、介面之衝擊(包括改進)。

(h) 偏差範圍(數量及批次)。

(i) 實施計劃書。

(j) 費用預算等。

供應者應提供偏差/豁免申請所採用之特定文件。

7.4.4 偏差及豁免管制程序

7.4.4.1 偏差管制程序

(a) 決定偏差之必要性

供應者應於提交任何形態項目偏差前，對其進行說明並證明正當。

(b) 偏差分類

供應者應依據7.4.2決定偏差類別。

(c) 偏差申請

對於主要偏差，向相應之形態管制委員會提交偏差申請進行審查。對於次要偏差，供應者應實施內部控制。

(d) 偏差申請審查

相應之形態管制委員會應依據產品等級及介面要求事項進行偏差審查。審查主要包括：

(1) 偏差之必要性及可行性。

(2) 對專案、介面、互換性、安全性及可靠度之衝擊。

(3) 對生產、測試及檢驗設備之衝擊。

(4) 對運作及維護設備及替換零件之衝擊。

(5) 對合約進度、後勤支援及成本等之衝擊。

(6) 決定偏差類別。

(e) 偏差申請核准

形態管制委員會應依據評估結果決定偏差類別，並提出是否核准偏差申請之建議。若否決，應提供支持性理由。若有異議，應協商解決或呈報較高層級裁定。

(f) 實施及查證

對於已核准之偏差，供應者應準備偏差實施文件(如技術通知)，並向相關方發布實施。準備相應之製程規格，並採用相應之製程設備及方法，以確保偏差之正確實施。查證並記錄偏差之實施及符合性。

7.4.4.2 豁免管制程序

豁免程序應與不符合管制系統一致。

(a) 決定豁免狀況

製造商應評鑑豁免程度、豁免原因及其造成之影響，以正確判定豁免狀況。

(b) 豁免分類

供應者應依據7.4.2並基於判定結果決定豁免類別。

(c) 豁免申請

對於已確認之主要豁免，製造商應提出豁免申請，並依規定逐級審查後，提交相應之形態管制委員會審查。對於已確認之次要豁免，供應者應實施內部控制(重工、維修、降級及報廢)。

(d) 豁免申請審查

(1) 豁免申請理由之充分性。

(2) 豁免對產品介面、互換性、安全性及可靠度之衝擊。

(3) 實施方案之可行性。

(4) 對合約、後勤支援及成本等之衝擊。

(e) 核准豁免申請

依據審查結果，對提交之豁免申請提出是否核准的建議，並將要求及時回覆提案者。否決豁免應提供否決理由。

(f) 豁免允收

供應者應依據審查結果對不符合產品實施豁免允收。

7.5 介面管制

7.5.1 介面是二個或多個物件間之共同邊界。介面管制是以適當且可追溯之方式管制介面變更。

7.5.2 介面管制是形態管制之一部分。介面管制應確保：

(a) 獨立開發及製造之項目，能與其他項目正確地介接並適當地工作。

(b) 當項目改變時，對應介面之功能及實體介面亦能隨之改變。

7.5.3 形態介面管理要求通常應於形態管理計畫書中規定。若專案涉及多個介面，則

應各別準備文件(如協議及合約)。

7.5.4 通常形態介面具下述類型。

(a) 依介面特性，分為功能介面及實體介面：

(1) 功能介面：互連項目協同工作，以實現相同之功能目標。

(2) 實體介面：互連項目之實體邊界相互相容，以實現整體結構之完整性。

(b) 依介面位置，分為內部介面及外部介面：

(1) 內部介面：同一項目各部分間之介面。

(2) 外部介面：不同項目間之介面。

(c) 依介面層級，分為系統及單元介面：

(1) 系統介面：系統層級項目間之介面。

(2) 單元介面：低於系統層級項目間之介面。

7.5.5 供應者應對所有類型之介面進行管制，以確保介面定義資料與產品形態一致。

8. 形態現況彙整(configuration status accounting)(CNS 14238, 3.7)用語參考審完刪

8.1 一般

形態現況彙整記錄並報告已確認形態項目、形態文件、變更提案、偏差與豁免及實施已核准變更及偏差之核准文件。形態現況彙整提供已核准形態之可見性、形態基線演進之可追溯性及與實際建造形態之比較。

形態現況彙整包括：

(a) 已核准形態項目之開發及相關形態文件的資訊。

(b) 變更、審查及實施之狀況。

(c) 偏差與豁免之審查及實施狀況。

(d) 形態稽核資訊，包括稽核概述、稽核結果、不符合項目處理及結果追蹤。

形態現況彙整是依據形態之一般管理計畫(計畫書)及顧客、供應者/分包者之要求事項執行。(原文Discount of configuration state...錯誤應為configuration status accounting....)

8.2 形態現況彙整要求事項

8.2.1 供應者應收集所有形態項目資訊，產出正式紀錄並報告給相關方，以便為相關參與人員提供精確且所需之資訊，以確保專案開發。

8.2.2 形態現況彙整從第一份形態文件開始，貫穿產品開發整個過程。形態現況彙整應精確且全面地記錄相關資訊，以確保形態演進之可追溯性。

8.3 形態現況彙整過程

8.3.1 一般

形態現況彙整過程包括形態文件之累積與交接、資料收集、形態狀況記錄與報告及形態現況彙整系統分析。

8.3.2 形態文件累積

形態經理準備形態文件應從第一份形態文件建立起累積所有形態文件，並依產

生時間或文件類別登錄所有文件，以產出形態文件清單。

8.3.3 形態文件交接

8.3.3.1 形態經理準備形態文件應定期將累積之形態文件移交給形態管理部門。文件應整潔、完整且與形態文件清單保持一致。

8.3.3.2 形態經理應依規定對文件進行查證並完成文件交接程序。

8.3.4 資料收集

8.3.4.1 資料收集為形態項目狀況之記錄及報告提供輸入，其應遵守資料收集規定，並符合資訊/文件管理系統之要求。

8.3.4.2 資料收集應考慮文件產出部門、文件類別(如文字、圖及表)及文件特性。所收集之資料應完整、真實及統一。

8.3.4.3 形態經理負責資料收集，收集之資料通常包括：

(a) 文件標題及編號。

(b) 文件發布日期及版次。

(c) 文件產出部門及負責人。

(d) 核准變更及生效日等。

8.3.5 形態狀況之紀錄

形態狀態紀錄是指形態經理依據不同使用端及目標，整理收集之資料，形成正式紀錄及報告之過程。紀錄及報告應輸入形態現況彙整系統。紀錄及報告應確保：

(a) 所收集資料之精確性、可靠性及完整性。

(b) 所收集資料應及時更新，並妥善保存原始資料。

8.3.6 形態狀況之報告

形態經理應依據顧客、供應者/分包者之要求及管理要求事項，定期向其發布/發送形態現況彙整報告(參照附錄C)。報告通常包括：

(a) 形態項目開發狀況。

(b) 形態基線文件清單。

(c) 主要變更、偏差及豁免及其實施及查證之狀況。

(d) 形態稽核狀況、提出之主要問題、稽核結論及問題處理結果。

8.3.7 形態現況彙整系統分析

形態經理應分析並改善形態現況彙整，以符合使用者要求。

9. 形態查證

9.1 一般

形態查證是查證所分析產品目前形態狀況，並建立形態基線之過程。形態查證包括產品形態定義查證及產品形態查證。

9.2 產品形態定義查證

9.2.1 在系統要求事項審查(system requirements review, SRR)中，應對任務目標查證

功能形態定義。

9.2.2 在初步設計審查(preliminary design review, PDR)中，應對適用之技術規格查證開發形態定義。

9.2.3 在關鍵設計審查(critical design review, CDR)中，應對相關設計文件查證設計定義。

9.2.4 若查證失敗，則採取相應之改進措施。

9.3 產品形態之查證

9.3.1 供應者應藉由系統性比較執行形態查證，比較形態項目之〝實際建造(as-built)〞形態與其〝實際設計(as designed)〞形態。為進行此比較，供應者應於階段審查會議上準備〝實際設計形態清單(as-designed configuration list, ADCL)〞及〝實際建造形態清單(as-built configuration list, ABCL)〞以供審查。

9.3.2 對於原型，功能特性項目中之形態應於合格審查(qualification review, QR)中進行查證。實體特性項目中之形態應於允收審查(acceptance review, AR)中進行查證。

9.3.3 對於量產，功能形態驗證(functional configuration verification, FCV)應從首件試驗資料收集開始進行。實體形態驗證(physical configuration verification, PCV)應與產品資格審查一起執行或與FCV同時執行。

10. 形態稽核

10.1 一般

形態稽核是一種正式檢驗，用以決定形態項目與其形態文件間之一致性。藉由稽核度量形態管理系統之有效性，以查證於產品壽命週期內是否依據顧客規定正確應用形態管理要求事項。形態稽核包括功能形態稽核及實體形態稽核。

10.2 形態稽核要求事項

10.2.1 成立形態稽核團隊，對每一形態項目進行功能及實體形態稽核。

10.2.2 形態稽核通常在供應者或分包者營業場址以會議形式進行。上層級應稽核下層級。

10.2.3 形態稽核為：

(a) 審查形態文件之正確性及完整性。

(b) 審查形態項目與形態文件之一致性。

(c) 審查形態項目之功能及實體特性是否符合合約、時間表及運作要求事項。

(d) 審查形態識別之正確性與形態管制之有效性。

10.2.4 產出稽核結論。對於發現之問題，設定改正期限。

10.3 形態稽核團隊

10.3.1 形態稽核團隊由顧客及供應者之代表組成。通常情況下，由顧客代表擔任領導者，由供應者代表擔任副領導者。

10.3.2 形態稽核團隊代表應具備一定之資格，並參與專案開發。

10.4 供應者及顧客之職責

10.4.1 在形態稽核中，供應者應負責：

(a) 與顧客協調稽核時間表、地點及要求事項。

(b) 準備稽核計畫書。

(c) 指定形態稽核小組副領導者及供應者參與人員。

(d) 確保分包者參與必要之稽核。

(e) 準備形態稽核計畫書要求之會議文件。

(f) 向形態稽核小組及參與人員提供稽核所需之文件及設備清單。

(g) 提供稽核所需之資源及設備。

(h) 起草會議紀錄。

10.4.2 在形態稽核中，顧客應負責：

(a) 指定形態稽核團隊領導者及顧客參與人員。

(b) 審查會議紀錄，確保其反映顧客提出之所有重要意見。

(c) 提供稽核結論：認可、有條件認可或不認可。

10.5 會議紀錄

10.5.1 會議紀錄應由供應者起草，並精確地反映會議內容。

10.5.2 通常會議紀錄應包括：

(a) 會議日期、地點、主持人、參與者及記錄者。

(b) 會議議程。

(c) 提出之問題、建議、解決方案或要求事項。

(d) 結論及改正期限。

10.5.3 經形態稽核團隊領導者核准後形成紀錄。

10.6 功能形態稽核

10.6.1 功能形態稽核是為查證形態項目之功能特性(性能指標、設計限制、運作保證要求事項)是否符合功能形態文件及開發形態文件中規定之要求事項而進行的檢驗。

10.6.2 功能形態稽核之資料應從原型試驗資料中取得。若未製造原型，則應從首件產品之試驗資料中取得。

10.6.3 功能形態稽核應與原型試驗結合，亦可隨設計要求事項之開發逐步完成。

10.6.4 通常功能形態稽核包括：

(a) 供應者之試驗程序及結果是否符合功能及(或)開發形態文件中規定之要求事項。

(b) 開發試驗計畫書及試驗規格之實施。試驗結果之完整性及精確性。試驗報告是否能精確反映試驗情況。

(c) 已核准之變更是否已納入相應之形態文件並已實施。

(d) 對於無法藉由試驗完全查證之要求事項，確認分析或模擬結果可確保功能

形態符合形態文件規定之要求事項。

(e) 對未符合要求事項之形態項目，是否已進行原因分析並採取相應之矯正措施。

(f) 重大偏差、豁免等技術問題是否已妥善處理。

(g) 對於軟體，除上述稽核外，亦應依據其自身特性進行必要之補充稽核。

10.7 實體形態稽核

10.7.1 實體形態稽核是為查證已完成之形態項目是否符合功能、開發及產品形態文件之要求事項而進行的最終檢驗。

10.7.2 實體形態稽核之資料應從正式製程製造之首件產品的試驗及(或)檢驗資料中取得。

10.7.3 實體形態稽核通常在功能形態審查之後，與產品合格審查同時進行。實體形態稽核後建立產品基線。

10.7.4 通常實體形態稽核包括：

(a) 對顧客規定之每一硬體形態，檢驗足夠之產品規格、圖面、清單及相關製程規格之樣品，以查驗其精確性及完整性，包括形態文件及實體產品上反映之變更。

(b) 檢驗足夠之樣品，以確保依生產製程製造之形態項目符合形態文件中之要求事項。

(c) 審查形態項目之允收程序及試驗資料是否符合產品規格中之要求事項。不符合要求事項之形態項目應由供應者重新試驗，且需要時應重新審查。

(d) 審查分包者之產品品質證明文件及試驗紀錄是否精確。

(e) 審查功能形態稽核遺留問題是否已妥善處理。

(f) 對於軟體，除上述稽核外，亦應依據其自身特性進行必要之補充稽核。

10.8 其他

功能及實體形態稽核完成後，供應者應：

(a) 發布功能或實體形態稽核結果。

(b) 將稽核結果輸入形態現況彙整系統中。

(c) 指定負責人員完成所有遺留工作。

11. 形態管制委員會

11.1 形態管制委員會是由技術及管理專家組成之權責主體，對產品形態狀況擁有決策權。任何負有設計責任及權限之組織均應設立形態管制委員會。

11.2 組織應依形態項目之層級、介面、特性及複雜程度，於每一專案層級設立形態管制委員會。

11.3 當規定職責及權限時，應考慮下述事項：

(a) 專案之複雜性與特性。

(b) 專案各階段之要求事項。

(c) 專案開發所涉及之各方。

(d) 形態管理期間活動之介面。

(e) 管理組織之結構。

11.4 形態管制委員會之主要職責包括：

(a) 審查變更之必要性。

(b) 確保變更提案之正確性、協調性及有效性。

(c) 評估變更所帶來之影響。

(d) 對是否核准變更提案(變更請求)、偏差/豁免提出建議。

(e) 監督已核准變更之實施。

附錄 A
(參考)
形態管理計畫書之結構及內容

A.1 一般

形態管理計畫書之結構宜包含獨立章節，分別討論A.2至A.7中列出之主題，亦提供有關內容之指引。

A.2 一般資訊

形態管理計畫書宜包含一個介紹章節，提供一般資訊。該章節通常涵蓋下述主題：

(a) 形態管理計畫書之目的及適用範圍。

(b) 該計劃書適用產品及形態項目之說明。

(c) 提供重要形態管理活動時間表指引之進度。

(d) 形態管理工具(例：資訊科技)之說明。

(e) 相關文件(例：供應者提供之形態管理計畫書)。

(f) 相關文件及其相互關係之清單。

A.3 政策

形態管理計畫書宜詳述顧客或供應者同意之形態管理政策。此宜為合約中之形態管理活動提供根據，如

(a) 形態管理實務及相關管理活動之政策。

(b) 相關利害關係方之組織、職責及權限。

(c) 資格鑑定及訓練。

(d) 選擇形態項目之準則。

(e) 內部及顧客報告之頻率、分發及管制。

(f) 專門用語。

A.4 形態識別

形態管理計畫書宜詳述下列事項：

(a) 形態項目、規格及其他文件之族譜。

(b) 規格、圖面、認可及變更採用之編號慣例。

(c) 修訂狀況之識別方法：

(1) 欲建立之形態基線、進度及應包含之產品形態資訊類型。

(2) 序號或其他可追溯性識別之使用及分配。

(3) 產品形態文件之發布程序。

A.5 變更管制

形態管理計書宜詳述下列事項：

(a) 組織CCB與其他相關方之關係。

(b) 建立合約形態基線前之管制變更程序。

(c) 處理變更(包括由顧客或供應者發起之變更)及認可之方法。

A.6 形態現況彙整

形態管理計書宜詳述下列事項：

(a) 收集、記錄、處理及維護產生形態現況彙整紀錄所需資料之方法。

(b) 所有形態現況彙整報告之內容及格式的定義。

A.7 形態稽核

形態管理計畫書宜詳述下列事項：

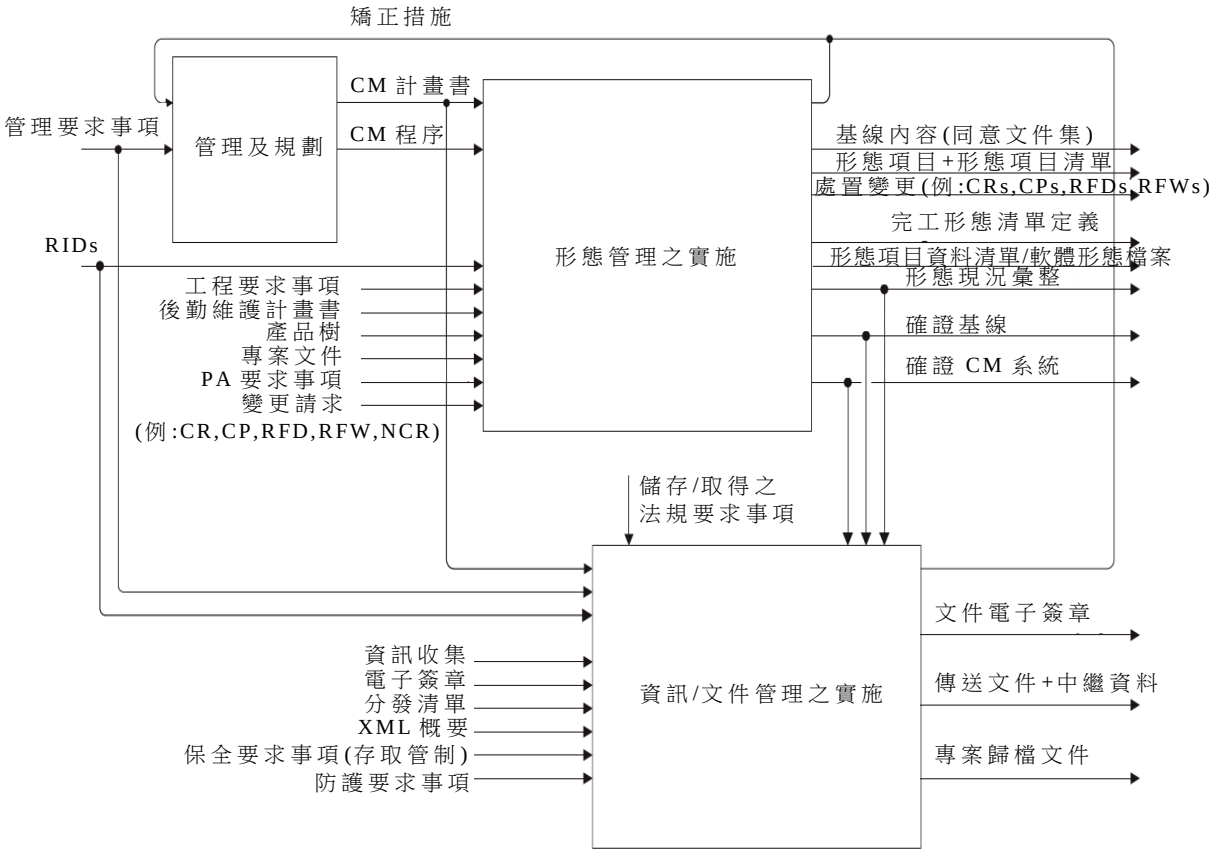
(a) 欲執行之稽核清單及其在專案時間表出現之處。

(b) 欲使用之形態稽核程序。

(c) 與相關方(組織內部與外部)有關之權限。

(d) 稽核報告格式之定義。

附錄 B
(參考)
形態管理



備考：矯正措施是依據專案經驗學習及任何回饋意見對過程本身之改進。

圖B.1 形態管理及資訊/文件管理

附錄 C
(參考)
形態現況彙整報告

C.1 目的及目標

形態現況彙整報告之目的是提供可信賴的形態資訊來源，以支援所有計劃或專案活動。其提供執行形態管理所需之知識基礎。

C.2 期望響應

C.2.1 適用範圍及內容

(1) 簡介

簡介宜說明形態現況彙整報告之目的及目標。

(2) 適用文件及參考文件

形態現況彙整報告宜列出支援文件產出所需之適用文件及參考文件。

(3) 說明

形態現況彙整報告宜包含下述資訊：

(i) 文件索引及狀況清單

(a) 文件識別。

(b) 發布及修訂。

(c) 發布及修訂日期。

(d) 標題。

(e) 備考。

(f) 作廢文件之識別。

(ii) 圖面索引及狀況清單

(a) 圖面識別。

(b) 發布及修訂。

(c) 發布及修訂日期。

(d) 標題。

(e) 備考。

(f) 圖面之模型適用性。

(iii) 偏差索引及狀況清單要求

(a) 偏差文件編號。

(b) 發布及修訂。

(c) 發布及修訂日期。

(d) 標題。

(e) 受影響之文件或要求。

(f) 受影響之形態項目。

(g) 核准狀態。

(iv) 豁免索引及狀況清單要求

(a) 豁免文件編號。

(b) 發布及修訂。

(c) 發布及修訂日期。

(d) 標題。

(e) 受影響之文件或要求。

(f) 發起豁免之NCR。

(g) 受影響之形態項目序號。

(h) 核准狀態。

(v) 變更提案(CP)索引及狀況清單

(a) 變更提案(CP)文件編號。

(b) 發布及修訂。

(c) 發布及修訂日期。

(d) 標題。

(e) 發起變更之變更請求。

(f) 受影響之形態項目。

(g) 核准狀況。

(vi) 審查項目不一致(review item discrepancies, RID)索引及狀況清單

(a) 設計審查識別。

(b) RID識別。

(c) 不一致之標題。

(d) 受影響之文件編號及發布。

(e) 受影響之段落。

(f) RID狀況。

(g) 指派行動之識別。

(h) RID結束日期。

(i) 備考。

C.2.2 特定備考

無。

參考資料

[1] ISO 21351 Space systems－Functional and technical specifications

[2] ISO 27026 Space systems－Programme management－Breakdown of project management structures

[3] MIL-STD-HDBK-61 Military handbook: Configuration management guidance

[4] MIL-STD-973 Military standard: Configuration management

[5] ECSS-M-ST-40C Rev.1 Configuration and information management

相對應國際標準

ISO 21349：2019 Space systems－Configuration management

ICS 49.140

中華民國國家標準

C N S

太空專案–計畫管理–可信性保證要求事項

Space projects – Programme management – Dependability assurance requirements

CNS 草-制 1150010:2026
D1

中華民國　年　月　日制定公布
Date of Promulgation:　-　-

目錄

前言

本標準係依據 2023 年發行之第 2 版 ISO 23460，不變更技術內容，制定成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

可信性保證之目標是在所有相互競爭技術、排程及財務限制下，藉由最佳化系統可信性，以確保任務成功。

可信性保證是貫穿整個專案壽命週期之連續及迭代過程，採用定量及定性方法，確保符合可靠度、可用性及可維護性要求事項。

1. 適用範圍

本標準規定太空專案可信性(可靠度、可用性及可維護性)保證計畫之要求事項。

本標準定義太空產品於軟體內實施之系統功能及硬體與軟體間互動之可信性的要求事項。

本標準適用於所有計畫階段。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

CNS 17666　太空系統－風險管理

ISO 10795　Space systems－Programme management and quality－Vocabulary

ISO 15865　Space systems－Qualification assessment

ISO 16192　Space systems－Experience gained in space projects (lessons learned) －Principles and guidelines

3. 用語及定義

ISO 10795之用語及定義及下列用語及定義適用於本標準。

3.1 危害度(criticality)

依據功能、軟體、硬體或操作之潛在失效後果嚴重度類別。

備考：此危害度概念應用於功能、軟體、硬體或操作時，僅考慮嚴重度，不同於失效或失效模式(或風險)之危害度，後者亦考慮發生之可能性或機率。

3.2 失效情境(failure scenario)

事件從初始根本原因至最終失效之狀態及序列。

4. 政策及原則

4.1 基本方法

為實現可信性目標，可信性保證應依據邏輯過程實施。

此過程從概念設計階段開始，於功能樹最高層級，由上而下地定義待實施之任務及要求事項。功能樹所有層級之結果，均以由下而上之方法進行管制及使用，以鞏固產品之可信性保證。附錄A提供可信性活動與計畫階段間之關係。

此過程包括下列類型之活動：

(a) 可信性計畫之定義、組織與實施(定義參照第5節)。

(b) 可信性之風險識別、降低與控制(定義參照第6節)。

(c) 可信性工程(定義參照第7節)。

(d) 可信性分析(定義參照第8節)。

(e) 可信性之測試、證明及資料收集(定義參照第9節)。

4.2 裁適

當從特定專案背景而言，本標準定義之要求事項宜進行裁適，以符合特定專案輪廓及情況之實際要求事項。

5. 可信性計畫管理

5.1 組織

承包者應實施可信性(可靠度、可用性及可維護性)保證，以作為產品保證專業領域之組成部分。

5.2 可信性計畫規劃

承包者應開發、維護並實施涵蓋所有計畫階段之可信性計畫書，該計畫書應說明如何證明符合可信性計畫要求事項。該計畫書應涵蓋本標準之適用要求事項。

附錄B提供文件要求清單(document requirement list, DRL)內容，作為整個專案文件要求(document requirement, DR)之可信性計畫輸入。

對於每一產品，可信性保證之應用程度應適合系統層級失效結果之嚴重度(定義參照7.3.1)。為此目的，產品應依據專案之風險政策劃分為適當的類別。

承包者應將失效識別為不符合，並應依據品質管理系統中之不符合項目管制系統，執行一系列管制活動，如報告、分析及預防。

5.3 可信性關鍵項目

為支援執行專案風險降低及控制過程，應藉由執行可信性分析以識別可信性關鍵項目。識別可信性關鍵項目之準則參照6.4。

可信性關鍵項目應接受風險評鑑及關鍵項目管制。

管制措施應包括：

(a) 審查與關鍵功能、關鍵項目及程序相關之所有設計、製造及試驗文件，以確保採取適當措施管制與其危害度相關之項目。

(b) 參與不符合審查委員會(nonconformity review boards, NRB)、失效審查委員會(failure review board, FRB)、形態管制委員會(configuration control boards, CCB)及試驗審查委員會(test review boards, TRB)之可信性工作，及豁免與偏差之核准過程，以確保可信性關鍵項目之處置充分考慮其危害度。

應於可信性關鍵項目整個查證過程中考慮可信性，直至結束為止。

5.4 設計審查

承包者宜以ISO 21349作為指引，建立並實施正式之排程及文件化設計審查。

承包者應確保設計審查所有可信性資料完整，詳細程度與審查目標一致，並依據專案審查時間表提交給顧客。

承包者應確保在所有設計審查中充分考慮可信性。

提交之所有可信性資料應清楚地指明其所依據之設計基線，並應與所有其他支援性技術文件保持一致。

應評鑑所有設計變更對可信性之影響，必要時，對變更後之設計進行可信性再評鑑。

5.5 稽核

稽核應包括可信性活動，以查證是否符合專案可信性計畫書及要求事項。

5.6 使用先前設計、製造、合格或飛行之項目

若承包者擬在系統中使用先前設計、製造、合格或飛行之元件，則應證明擬用之元件符合設計規格之可信性保證要求事項。

應識別不符合可信性保證要求事項，並提供豁免請求說明保留未解決不符合之理由。

5.7 分包者管制

承包者應負責確保從分包者處取得之產品，以符合整個系統規定之可信性要求事項。

5.8 進度報告

承包者應向顧客報告可信性進度，以作為產品保證之一部分。

5.9 文件

承包者應維護用於可信性計畫之所有資料。該檔案至少應包含下述內容：

(a) 可信性分析、清單、報告及輸入資料。

(b) 可信性建議狀況日誌。

依據商業協議，顧客可在提出要求時取得專案可信性資料。

6. 可信性風險降低及控制

6.1 一般

作為依據CNS 17666於專案中實施風險管理過程之一部分，承包者應分析、降低及控制所有導致不符合可信性要求事項之可信性風險，即所有導致產品要求技術性能降低或喪失之風險。

可信性風險分析、降低及控制應包括下述步驟：

(a) 依據不符合事件後果之嚴重度進行識別及分類。

(b) 分析失效情境，決定相關失效模式、失效起源或根本原因。

(c) 將各項功能及相關產品依其危害度類別類別，以便依據其危害度制定裁適之風險降低措施。

(d) 定義詳細之風險評鑑、風險消除或風險降低並控制至可接受位準之行動及建議。

(e) 實施風險降低措施。

(f) 作出風險降低及風險接受之決策。

(g) 查證風險降低及評鑑殘餘風險。

6.2 不良事件之識別與分類

承包者應識別導致技術性能喪失或劣化之不良事件，並依據其後果嚴重度將其分類(參照7.3.1)。

不良事件之初步識別及分類應從概念設計及初步設計階段，藉由分析任務成功準則決定。在最高產品層級(整個系統包括太空及地面段)中需要考慮之不良事件，其發生可能危及、連累或劣化任務之成功。在產品樹較低層級(太空段、地面段、

次組合件及設備)中，需考慮之不良事件，應為會導致在最高產品層級所識別不良事件之產品失效效應。

在評鑑失效情境後，應整合不良事件之識別及類別(參照6.3)。

6.3 失效情境之評鑑

承包者應調查可能導致不良事件發生之情境，並識別相關之失效模式、失效起源與根本原因及詳細之失效影響。

在概念設計及初步設計階段應執行下述分析，以初步決定及評鑑失效情境。

(a) 使用功能失效模式效應分析(failure modes effects analysis, FMEA)(定義參照8.2.2)分析功能失效(即與實現產品任務相關之功能失效)，以決定每項功能之效應(導致風險)：喪失、劣化及不適時發生。各項功能應預先定義(功能分析可用於此目的)。

(b) 應在產品壽命週期之每一階段進行功能失效分析，考慮所有運作模式在整個任務期間之實際執行順序，以識別由錯誤排序導致之不良事件(例：同步喪失及不適時運作)。

(c) 分析待調查不同功能間失效之潛在傳播。

(d) 分析運作性能中與人為因素相關之失效模式。

(e) 分析過去類似產品或任務經驗中，觀察到之典型失效模式對產品潛在應用。

在細部設計階段，應藉由考慮下述附加貢獻以加強失效情境評鑑：

— 分析選定設計導致無法藉由功能失效分析偵測到之特定失效模式及失效效應。

— 分析以偵測由元件接近所導致之潛在失效傳播路徑。

6.4 功能及產品之危害度類別

在初步設計階段，承包者應將功能、運作及產品分類至危害度類別中。

功能及運作之危害度類別應與功能或運作失效導致之後果嚴重度直接相關(例：若某個功能失效導致災難性後果，則應將其分類至最高危害度等級)。

產品(硬體及軟體)之危害度類別應為與產品相關功能之最高危害度類別。

危害度分類應用於將工作聚焦於最關鍵領域。

6.5 風險降低之行動及建議

承包者應定義風險降低之行動及建議，使其達到可接受程度。在風險降低方面，應考慮下述措施：

(a) 基於專用可信性分析之性能及於特定情況下之可信性試驗，進行詳細風險評鑑。第8節所述之可信性分析的選擇及裁適，應依據產品本質及危害度類別進行定義。

(b) 依據7.3.2及7.3.3所述之設計或運作規格，消除失效原因、降低失效發生機率、減少失效效應並監控及控制失效情境。

6.6 風險決定

承包者應制定並文件化關於風險接受度及降低風險行動之決定。

決定應基於專案風險政策中定義之已建立準則，並考慮技術及計畫之影響。

應於專案適用之風險管理過程中做出決定並予以管制及實施。

6.7 風險降低之查證

承包者應進行適當之查證，以確保識別出之風險已被消除或降低至可接受程度。

查證應包括：

(a) 監控並完成行動及建議之查證。

(b) 審查可信性分析之詳細風險評鑑。

(c) 參考專案風險政策中定義之適用準則，重新評鑑殘餘風險並查證可接受性。

(d) 識別問題區域。

結果應向專案風險管理部門報告，以作為接受或補充之決定。

6.8 文件

在整個專案實施過程中，應建立、管制及維護關於可信性風險分析降低及控制之文件，以便：

(a) 使風險識別、評鑑及降低之結果及進度具可見性。

(b) 定義產品樹較低層級之適用要求事項。

(c) 對降低風險及接受風險之決定提供適當的正當理由。

(d) 確保每一風險可追溯至所有恰當之分析、結果、資料、決定及結束狀態。

文件應包括：

(a) 不良事件之識別及分類。

(b) 失效情境、失效模式、根本原因及效應之識別。

(c) 功能及產品之危害度分類。

(d) 產品樹較低層級之要求事項。

(e) 行動及建議之定義。

(f) 為風險評鑑及降低所需而進行之可信性分析。

(g) 風險降低狀況。

(h) 風險降低紀錄及其相關理由。

7. 可信性工程

7.1 在專案中可信性之整合

可信性是系統或產品之固有特性。在設計過程中，可信性應與安全性整合。在設計最佳化過程中，可信性特性應與其他系統屬性(如質量、大小、成本及性能)進行交換。

從概念階段開始，所有交換及專案所有階段均應考慮可信性問題。製造、組裝、整合、試驗及運作皆不得降低設計中導入之可信性屬性。

可信性分析、試驗及證明之結果，均應於設計、試驗及所有製造/整合過程中適時地反覆做，直至所有對可信性目標之威脅均已消除，或已提供可接受剩餘威脅之

理由。

可信性保證之重點應置於設計或製造過程，具體取決於專案階段。

7.2 技術規格中之可信性要求事項

在準備及審查設計與試驗規格期間，應考慮可信性要求事項。主要目標應為實施可信性分析之發現，並查證已接受之可信性工程建議，已納入相關技術規格中。此等規格應包括：

(a) 功能、運作及環境要求事項。

(b) 試驗要求事項，包括應力位準、試驗參數及允收/拒絕準則。

(c) 在規定環境條件下之設計性能裕度、降額係數、定量可信性要求事項及定性可信性要求事項(不良事件之識別及分類)。

(d) 人為因素，其中人為錯誤是任務成功之考量。

(e) 設計對硬體或軟體失效之容忍程度。

(f) 系統失效之偵測、隔離、診斷、恢復及系統復原至可接受狀態。

(g) 預防跨介面失效造成不可接受之後果。

(h) 維護概念之定義。

(i) 維護任務及特殊技能要求事項。

(j) 預防性維護、專用工具及專用試驗設備之要求事項。

7.3 可信性設計準則

7.3.1 後果類別及嚴重度

應依據表1，對已識別之每一失效模式進行嚴重度分類，並依據失效效應(後果)進行分析。

表1 後果嚴重度

嚴重度	等級	可信性	安全
致命	1	失效傳播(僅適用於系統層級以下分析)	喪失生命、危及生命或永久致殘傷害或職業病 系統喪失 載人飛行介接系統喪失 發射場設施喪失 嚴重有害環境效應
關鍵	2	任務完全喪失	暫時致殘但不危及生命之傷害或暫時性職業病 飛行介接系統重大損壞 地面設施重大損壞 公共或私人財產重大損壞 重大有害環境效應

主要	3	主要任務劣化	
次要或可忽略	4	次要任務劣化或其他任何效應	

7.3.2 失效容限

承包者應依據性能規格中定義之失效容限要求事項，查證設計承受單一或多個失效之能力。

此查證應涵蓋所有失效模式，其後果嚴重度依據專案風險政策分為致命、關鍵及主要。

7.3.3 設計方法

承包者應開發並實施設計準則以改善可靠度，並促進在預測環境中之維護行動。在建立可靠度及可維護性設計準則時，承包者應在有適當可用資料時，使用先前計畫中獲得之資料。

承包者應確保使用容錯及設計裕度時，將可靠度融入設計中。承包者應評鑑系統之失效特性，以識別設計中之弱點並提出改善辦法。

在將可用性及可靠性融入設計中時，應採用下述方法。

(a) 功能設計：

— 實施失效容限。

— 實施故障偵測、隔離及恢復，藉由專門之飛行及地面措施進行適當的失效處理，並考慮最不利條件下事件傳播時間與偵測或重新配置時間之關係。

— 實施對任務執行至關重要之參數監控，考慮系統失效模式與偵測裝置實際能力之關係，並考慮產品維持之可接受環境條件。

(b) 實體設計：

— 應用經過證明之設計規則。

— 優先使用在預期任務環境中已成功執行之設計。

— 選擇適當品質等級之零件。

— 使用電機、電子及機電(electrical, electronic and electromechanical, EEE)零件，並降低機械零件之降額及應力裕度。

— 最佳地使用冗餘設計技術(同時盡可能降低系統設計之複雜性)。

— 最大限度地提高內建設備之可檢查性及可試驗性。

— 提供設備之可及性。

7.4 參與試驗定義

依據ISO 15865，承包者應確保所有開發、合格鑑定及允收試驗之規劃及審查工作均涵蓋可信性方面，包括準備試驗規格與程序及評估試驗結果。合格鑑定應能查證零件、材料及製程之可信性要求事項。

可信性專業領域應支援：

(a) 定義試驗特性及試驗目標。

(b) 選擇量測參數。

(c) 試驗結果之統計分析。

8. 可信性分析

8.1 可信性分析及專案壽命週期

所有太空專案均應於整個專案壽命週期內進行可信性分析，以支持第5節規定之任務及要求事項。

可信性分析應首先用於建立概念設計及系統要求事項。之後，應進行分析以支持設計之概念、初步及細部開發及最佳化，包括最終獲得設計合格鑑定之測試階段。

應實施可信性分析，以便：

(a) 確保符合可靠度、可用性及可維護性要求事項。

(b) 識別所有可能導致不符合可信性要求事項之潛在失效模式及技術風險，並依據專案實施之風險管理過程，提供風險評鑑、風險降低及控制措施。

可信性分析結果應納入設計合理化檔案。

8.2 可信性分析方法

8.2.1 一般

應於太空系統所有適當層級進行可信性分析。

所有可信性分析之主要目的是藉由及時向設計人員提供回饋以改善設計，降低產品實現過程中之風險，並查證是否符合規定之可信性要求。

應使用並裁適8.2.2至8.2.4所識別之方法，匹配每一專案之要求事項，以解決構成系統之硬體、軟體及人為功能。基於附加價值及成本衝擊，應於專案早期定義從此等子節中選擇之一組一致性分析。

8.2.2 可靠度分析

此等分析亦可用於決定可維護性及可用性之目標及任務。下述用於可信性分析之分析亦可用於決定可維護性及可用性要求事項及任務。

(a) 設計階段開始後，應立即進行初步風險分析，以便從系統擔心之事件中識別出可能失效之根本原因。應考慮下述可能之根本原因：硬體、軟體及人為。

(b) 失效模式效應分析(FMEA)及失效模式與效應關鍵性分析(FMECA)。

(1) 應針對功能及實體設計(分別為功能FMEA/FMECA及硬體FMEA/FMECA)及用於實現最終產品之過程(FMECA過程)進行FMEA及FMECA。

(2) 應識別所有潛在失效模式，並依據其後果之嚴重度(FMEA)或危害度(FMECA)進行分類。應在分析中提出措施，並將其導入產品設計及製程

管制中，以使所有此類後果為專案所接受。

(3) 當進行任何設計或過程變更時，應更新FMEA/FMECA，並評鑑變更導致之新失效模式效應。

(4) 失效偵測及恢復行動規定應作為FMEA/FMECA一部分。

(5) FMEA/FMECA應用於支援可信性建模及可信性及安全性分析。

(c) 應進行軟體硬體互動分析，以確保軟體設計能以可接受之方式對硬體失效做出反應。此分析應於軟體技術規格之層面進行。軟硬體互動分析可包含在FMEA/FMECA中。

(d) 應進行偶發事故分析，以識別所有由系統失效引起之偶發事故。此分析應識別預防、抑制及限制每一偶發事故之方法，並偵測及診斷偶發事故，以將系統恢復到正常狀態或降級狀態。

備考：偶發事故分析是一系統層級之任務。

(e) 應使用故障樹分析(fault-tree analysis, FTA)查證設計是否符合失效組合之失效容限要求事項。

原始承包者應執行故障樹分析(FTA)，以識別導致不良最終事件〝任務喪失〞之可能事件組合。次系統承包者應針對頂級事件建立次系統層級之故障樹分析(FTA)，以支援此活動：

— 次系統功能喪失。

— 次系統功能意外啟動。

(f) 應針對可靠度及安全關鍵項目執行共模分析及共因分析，以識別可能導致失效容限位準無效之根本原因(參照7.3.2)。此分析可作為FMEA/FMECA或FTA之一部分完成。

(g) 可靠度要求事項應分配至較低層級產品設定之可靠度要求事項中。

(h) 應使用可靠度預測技術以優化設計在相互衝突約束條件(如成本及品質)下之可靠度，預測產品使用時之可靠度，並為目的(如風險評鑑)提供失效機率資料。

可靠度預測中使用之失效率及方法應符合顧客規定。應建立可靠度模型以支援預測及失效模式效應分析(FMEA)及失效模式與效應關鍵性分析(FMECA)。

(i) 應於電子/電機設備上執行最不利情況分析(worst-case analyses, WCA)，以證明其性能符合規格，即使其組成部分之參數及施加之環境存在特定變化。WCA應於設備層級完成。

(j) 應執行零件降額分析，以確保施加於所有EEE零件之應力位準均在專案規定限值範圍內。零件降額分析應在設備層級進行。

(k) 應使用區域分析以確保不存在失效傳播。

(l) 應在系統層級執行失效偵測、隔離及復原(failure detection isolation and

recovery, FDIR)，以確保滿足自主性及失效容限要求事項。

8.2.3 可維護性分析

應分配可維護性要求事項，以設定較低等級產品之可維護性要求事項，使其符合系統之維護概念及可維護性要求事項。

應於系統層級執行可維護性預測，並將其作為設計工具，依據規定之可維護性量化要求事項評鑑及比較設計選擇。

執行此等分析時應考慮下述：

(a) 診斷(即偵測及隔離)項目失效所需之時間。

(b) 移除及更換缺陷項目所需之時間。

(c) 將系統或次系統恢復至其正常形態，並執行必要檢查所需之時間。

(d) 項目失效率。

應在系統層級執行排程之維護分析，以決定最佳之排程維護計畫書，以最小化減少維持所需安全程度及任務能力所需之支援資源，並最小化停工期。

每一預防維護行動應基於經顧客核准之系統決策邏輯的應用結果。

應在系統層面進行區域分析，以決定每一產品在可及性、可試驗性及可修復性之最佳位置。

可維護性分析應識別可維護性關鍵項目，此等項目至少應包括整合後無法檢查及試驗之產品、有限壽命產品、不符合或無法確證是否符合適用可維護性要求事項之產品。

8.2.4 可用性分析

承包者應執行可用性分析或模擬，以評鑑系統之可用性。分析結果用於：

(a) 從設計、運作及維護方面最佳化系統概念。

(b) 查證是否符合可用性要求事項。

(c) 提供輸入以估算系統運作之總成本。

承包者為可用性分析提供輸入資料應執行停運分析(outage analyses)。分析輸出包括已識別之所有潛在停運(如專案定義)之清單、根本原因、發生機率及持續時間。可提供與停運相關之失效率，而非停運機率。此外，分析中應識別停運偵測及恢復方法。

應使用系統可靠度及可維護性模型及停運分析資料，於系統層級進行可用性預測/評鑑。

8.3 生產文件中設計特性之分類

為支援對可信性關鍵項目實施之風險降低及控制過程，承包者應對產品之設計特性進行分類，以突顯產品中需要特別關注、管制或查證之處。此為可信性及品質保證(quality assurance, QA)專業領域之整合工作。

設計特性之分類及排序旨在：

(a) 引起工程、生產及試驗人員對產品正確運作至關重要之特性的關注。

(b) 定義應用之適當整合、試驗及檢驗方法、技術及資源，並依據設計特性選擇生產設施。

(c) 採取一切預防措施以符合設計特性之要求事項，例：環境控制。

(d) 對不合格、變更及豁免進行適當且一致之分類及處理。

顧客應於專案要求文件中定義分類準則，或經協商，承包者亦可在產品保證計畫書中提出分類準則。

8.4 關鍵項目清單

藉由各種可信性分析識別之所有關鍵項目應記錄在關鍵項目清單中，並接受管理及管制。每一關鍵項目之文件應包含保留該項目經顧客核准之理由。

至少應將單點失效且失效後果嚴重度至少為致命、關鍵或主要之項目列為關鍵項目。

整合後無法檢查及試驗之產品、無法進行端對端試驗之功能或產品、有限壽命產品、不符合或無法查證是否符合適用可維護性要求事項之產品列為關鍵項目。

顧客應依據專案定義之風險管理政策，決定進一步之分類(例：不符合降額要求事項之零件、磨損時間、有限壽命項目或失效機率極高之項目)。

9. 可信性測試、證明及資料收集

9.1 可信性測試及證明

9.1.1 可靠度

可靠度測試及查證應依據專案要求文件進行，以便：

(a) 確證失效模式及效應。

(b) 檢查失效容限、失效偵測及恢復。

(c) 取得統計失效資料以支援預測及風險評鑑。

(d) 加強可靠度評鑑。

(e) 確證硬體與軟體協同運作或依據規格進行人工操作之能力。

(f) 證明關鍵項目之可靠度。

(g) 確證或證明用於理論證明之資料庫。

9.1.2 可維護性

應藉由查證適用之可維護性要求事項證明可維護性，並確保在維護概念範圍內成功執行預防及矯正維護活動。

可維護性證明應查證下述能力：

(a) 偵測、診斷及隔離每一故障線路可更換單元或軌道可更換單元。

(b) 移除及更換每一線路可更換單元或軌道可更換單元。

(c) 執行不預期藉由更換完成之任務必要維修。

(d) 檢查維護行動完成後產品完全作用。

(e) 證明維護行動不會導入安全危害。

(f) 證明維護作業可在適用限制(例：時間、數量或可及性)內進行。此應包括在

發射活動期間準備系統所需作業，例:〝飛行前移除〞項目或更換電池。

9.1.3 可用性

應依據專案要求事項執行可用性測試及證明，並使用可靠度及可維護性測試及證明。

9.2 可信性資料收集及可信性成長

在太空系統開發期間應從來源(如不符合、問題或失效報告及維護報告)收集可信性資料。此等資料應基於實際試驗或飛行經驗，並應包括所用項目之數量及模式，包括其應力及運作概況。可信性資料亦應藉由協議或規定之模型，用於可信性性能監控及可信性成長監控。

10. 經驗學習活動

應組織符合ISO 16192之經驗學習活動，藉由記錄、分類及標記適當之資訊，以保護所有可信性知識，進而造福未來太空專案。

附錄 A
(參考)
可信性活動與專案階段之關係

A.1 可行性階段(階段A)

在此階段，可信性保證任務是為：

(a) 開發及建立專案可信性政策，以滿足可信性要求事項。

(b) 支援設計權衡，並進行初步可信性分析，以識別及比較每一設計方案之可信性關鍵，並當需要時進行初步可用性評鑑。

(c) 進行初步風險識別及分類。

(d) 規劃專案定義階段之可信性保證任務。

A.2 初步定義階段(階段B)

在此階段，可信性保證任務是為：

(a) 繼續支援權衡研究，以選擇初步設計。

(b) 建立專案失效效應嚴重度類別，並將量化之可信性要求事項分配至系統所有層級。

(c) 對風險情境進行初步評鑑。

(d) 建立適當之失效容限要求事項。

(e) 進行初步可信性分析。

(f) 藉由提供初步關鍵項目清單，定義降低風險之行動及建議。

(g) 提供功能及產品之危害度分類。

(h) 支援維護概念及維護計畫書之定義。

(i) 規劃細部設計及開發階段之可信性保證任務，並準備可信性計畫書作為產品保證(PA)計畫書之一部分。

A.3 細部定義及生產階段(階段C/D)

在此階段，可信性保證任務是為：

(a) 執行詳細風險評鑑及詳細可信性分析。

(b) 細化功能及產品之危害度分類。

(c) 藉由執行風險降低查證，定義風險降低之行動及建議。

(d) 更新及細化可信性關鍵項目清單及其(保留)理由。

(e) 定義可靠度及可維護性設計準則。

(f) 支援關鍵及強制檢驗點的識別，識別可信性關鍵項目之關鍵參數，並啟動及監控可信性關鍵項目管制計畫。

(g) 與設計及運作工程合作執行偶發事故分析。

(h) 支援設計審查，並監控變更對可信性之衝擊。

(i) 定義工具要求事項，並執行可維護性訓練及可維護性證明。

(j) 支援製造、整合及試驗過程中之品質保證。

(k) 支援不符合審查委員會(NRB)及失效審查委員會(FRB)。

(l) 審查設計、試驗規格及程序。

(m) 審查運作程序，以評估與人機介面(human-machine interface, HMI)相關之人為可靠度問題，檢查與可信性分析準備過程中所做假設之相容性，或決定不相容性之衝擊。

(n) 監督可信性資料之收集。

A.4 利用階段(階段E)

在此階段，可信性保證任務是為：

(a) 支援飛行準備就緒審查。

(b) 支援地面及飛行運作。

(c) 監控設計變更流量及其因設計演變而對可信性之衝擊。

(d) 調查與可信性相關之飛行異常。

(e) 監督運作期間可信性資料之收集。

附錄 B
(參考)
文件要求清單(DRL)

文件要求清單(document requirement list, DRL)用作可信性計畫之輸入，用於整個專案之DRL。

建議之做法是檢查可信性及安全計畫中，承包者產生之文件是否重複。

顧客可規定或同意將二個或多個文件項目合併為一份報告。

下列清單涵蓋本文件規定之合約文件要求事項：

(a) 可信性計畫書。

(b) 失效模式、效應(及危害度)分析(FMEA或FMECA)。

(c) 硬體-軟體互動分析。

(d) 共模及共因分析。

(e) 故障樹分析。

(f) 偶發事故分析。

(g) 排程維護分析。

(h) 區域分析。

(i) 可信性分配。

(j) 可信性評鑑。

(k) 停運分析。

(l) 最不利情況分析。

(m) 零件降額分析。

(n) 可靠度關鍵項目清單。

(o) 風險識別、評鑑、降低及控制報告。

參考資料

[1] CNS 12680 品質管理系統－基本原理與詞彙

[2] ISO 21349 Space systems－Project reviews

相對應國際標準

ISO 23460：2023 Space projects – Programme management – Dependability assurance requirements