國營臺灣鐵路股份有限公司

臺鐵電務智慧化提升計畫－第三代中央行車控制中心暨相關系統整合統包工程採購案

統 包 工 程 採 購 特 定 條 款

第 參 章　系 統 保 證 要 求

(草 稿)

中華民國 113 年 1 月

統包工程採購契約特定條款(稿)

第參章　系統保證要求

目錄

統包工程採購契約特定條款(稿)

第參章 系統保證要求

1 系統保證作業

1.1 工作範圍與規定

1.1.1 廠商應就本工程第三代 CTC 系統及電力 SCADA 系統工作範圍，執行系統保證作業。

1.1.2 廠商應於設計、製造、施工、安裝、測試、驗收、商業運轉之保固期間等階段執行系統保證作業，亦即可靠度（Reliability）、可用度（Availability）、可維修度（Maintainability）、安全（Safety）相關分析、驗證與展現等作業（以下簡稱 RAMS），以確保 RAMS 均已完整地納入設計與設計變更之中。

1.1.3 廠商應以邏輯化及系統化的方法來規劃與執行系統保證作業，並展現本規範中所約定的安全需求及其他需求均已充分地融入於設計中。

1.1.4 系統保證之工作應包含系統安全、RAM 作業及提供相關之報告。系統保證之工作應符合以下之規範要求:

1.1.4.1 IEC 62278(EN 50126)：軌道應用標準—可靠度、可用度、可維修度與安全性之規範與展現（Railway Applications –The Specification and Demonstration of Reliability, Availability, Maintainability and Safety）。

1.1.4.2 IEC 62279(EN 50128)：軌道應用標準—通訊、號誌及處理系統—鐵路控制與防護系統之軟體（Railway Applications – Communications, Signalling and Processing Systems – Software for Railway Control and Protection Systems）。

1.1.4.3 IEC 62425(EN 50129)：軌道應用標準—通訊、號誌及處理系統—號誌安全相關電子系統（Railway Applications – Communication, Signalling and Processing systems – Safety Related Electronic Systems for Signalling）。

1.1.4.4 IEC 61508：電氣/電子/可編程電子安全相關系統的功能安全(Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems)。

1.1.4.5 廠商應指派系統保證組長，負責統籌系統保證工作，同時該系統保證組長應至少有五年以上於軌道系統的系統保證工作經驗。

1.1.4.6 在第三代 CTC 系統及電力 SCADA 系統正式切換前，廠商須提供本公司所有系統保證之文件、軟體和程序，以使本公司能夠：

(1) 持續對系統之營運執行系統保證管理作業。

(2) 於系統有修正或擴充時能持續執行系統保證管理作業。

1.1.4.7 廠商應依據所提出並經本公司核定之系統 RAM 計畫及系統安全計畫來執行系統保證工作。

1.1.4.8 無論是廠商所完成之系統 RAM 計畫、系統安全計畫或系統保證相關的報告和文件，均應視為一份可持續修訂的文件，並於契約期間內，經本公司之核定後視需要予以修訂。

1.1.4.9 在契約期間，廠商應定期召開系統保證工作會議，以確保所有與系統保證相關工作均已於要求的時間點執行完成，同時廠商應配合進度執行新危害的辨識、確認與登錄、剩餘風險容忍度的評估、分析與修正，並如期提供本公司有關系統保證趨勢之進展。

1.1.4.10 本公司將對廠商及其下包商之系統 RAM 計畫及系統安全計畫執行稽查作業，並評估相關計畫作業的工作內容與進度。

1.1.4.11 廠商應負責對其系統及設備承商之系統 RAM 計畫及系統安全計畫之審查與核定，以使能與廠商所提送之系統 RAM 計畫及系統安全計畫一致。廠商應監督其系統及設備廠商在其系統 RAM 計畫及系統安全計畫中所規範的系統保證工作。

1.1.5 RAM 需求

1.1.5.1 一般規定

(1) 廠商應藉由下列各項作法，使系統可靠度、可維修度及可用度獲致最佳化之結果：

A. 提供高可靠度及可用度。

B. 減少維修及故障之停機時間。

C. 排除或降低所有經過確認的危險。

D. 對於可能引起乘客或人員傷害以及設備損壞，且無法完全避免之意外事件，如果不能完全消除，須減少受害範圍及降低其嚴重性。

E. 減少人機介面問題。所有相關定義、作業方式、報告內容及分析格式，應依國際間系統保證相關標準、準則及規範，以及契約相關規定辦理。

(2) 系統應提供診斷數據，以識別故障的影響以及多種故障的潛在風險。

(3) 第三代 CTC 系統之系統的可用度應至少為 99.9%。

(4) 電力 SCADA 系統之系統的可用度應至少為 99.5%。

1.1.5.2 系統 RAM 計畫

(1) 廠商應參考 IEC62278(EN50126)、IEC62279(EN50128)、IEC62425(EN50129)與 IEC61508 等標準，並依據本規範對系統保證工作之要求提送「系統 RAM 計畫(System RAM Plan)」，經本公司核可後據以執行相關作業。並應於契約履行

階段保存相關的紀錄。

(2) 系統 RAM 計畫中應包含可靠度、可維修度及可用度(Reliability, Availability and Maintainability, RAM)之執行計畫，並說明下列內容：

A. 計畫目標。

B. 計畫組織，包括人員權限、職務、資格及其責任。

C. 介面組織，應確認各作業與相關支援人力、組織間之關係。

D. 作業及程序，包括：

(A) 設計及分析技術。

(B) 測試、檢查，以及各階段之驗證。

(C) 設計及施工之掌控。

(D) 確認、評估、報告、追蹤、更正危險缺失等之方法。

(E) 參與設計審查及設計變更需求之掌控。

(F) 稽查。

(G) 記錄、資料及證明文件。

(H) 提供系統保證需求予分包廠商，並自分包廠商處得知其作業現況之方法。

E. 配合計畫之里程碑，提送 RAM 作業時程。

F. 設置 1 名系統 RAM 作業之負責人，需有 3 年以上系統機電系統保證執行經驗。

G. 廠商之系統 RAM 計畫中所訂定之各項工作，應依據各個不同的計畫階段予以區分。

1.1.5.3 可靠度分析

(1) 可靠度分析應在開工日即開始進行，並持續維持及更新，直至設計及可用度驗證完成為止。這些分析將是預估系統是否能符合本規範與招標文件需求的基礎。

(2) 分析應就會影響系統保證之各系統、設備及元件，執行並提出下列項目(包含但不限於)：

A. 功能描述，包含概要圖說及功能、流程圖等。

B. 可靠度方塊圖。

C. 可靠度配當。

D. 可靠度預估。

E. 失效模式、影響與關鍵性分析(Failure Modes , Effects and Criticality Analysis, FMECA)。

F. 可靠度關鍵項目清冊。

G. 分析所需及供證明用之資料。以上所述之各系統、設備及元件，其對象應至線上維修更換件(Line Replacement Unit, LRU)，且 LRU 的清單應經本公司核可。

1.1.5.4 可維修度分析

(1) 維修度分析應在開工日即開始進行，並持續維持及更新，直至設計及可用度驗可證完成為止。這些分析將是預估系統是否能符合契約需求的基礎。

(2) 分析應就會影響系統保證之第三代 CTC 系統及電力 SCADA 系統之子系統、設備及元件進行，以確保系統與子系統之維修成本與失效時間降至最低，其結果應能指出進行各項故障檢修所需之人時。提出文件中應含括分析所需及供證明用之可維修度資料。

(3) 以上所述之各子系統、設備及元件，其對象應至 LRU，且 LRU 的清單應經本公司核可。

1.1.5.5 可用度分析

可用度分析結果應符合招標文件相關規定，並依規定測試、展現、驗證與確認。

1.1.5.6 失效報告及矯正行動系統 (Failure Reporting and Corrective Action System，FRACAS)

(1) FRACAS 應由廠商執行與建立，並提供一份在製造、施工、安裝、測試與展現等階段，發生問題原因和失效處理的歷史紀錄文件。

(2) 廠商須應在製造、施工、安裝、測試與展現等階段，透過操作與維修資訊回饋的作為，用 FRACAS 來監控設備安全與 RAM 之性能。

(3) FRACAS 應用來監控設備組件之性能與確認其失效的模式及採行的改正行動。

(4) FRACAS 應被用於:

A. 提升設備之可靠度成長，以超越規範之目標值水準。

B. 併同設備之失效資料作為設計審查之參考。

C. 在測試驗證與保固期間，驗證設備可靠度的能力及可能的衰退，以確保設備能維持其可靠度之水準。

1.1.5.7 RAM 展現

(1) 於設計階段結束前應依「系統 RAM 計畫」提出「RAM 展現計畫」，應包含可用度、可靠度及可維護度的展現，以作為後續執行 RAM 展現或子系統/設備相關工作的依循。除載明執行期程與方法外，應敘明依據的標準與展現方法，以

證明其能滿足 RAM 目標。

(2) 廠商應依據「RAM 展現計畫」具體執行 RAM 展現，並於展現完成後 30 天內提送「RAM 展現報告」。

1.1.6 系統安全需求

1.1.6.1 一般規定

(1) 廠商應依本規範之系統安全要求，以及國際間安全管理相關標準、準則及規範，即時確認潛在風險與實際危害，以採取必要行動，降低或消除這些風險與危害。

(2) 第三代 CTC 系統及電力 SCADA 系統於計畫各階段作業中，應分別確認其過程與結果均能達成招標文件規定之系統安全目標。

(3) 系統安全準則，至少應包括下列各項：

(4) 當所有系統元件均正常運作時，整個系統及每一功能性單元，於所有操作狀況下，均須安全地運作。

(5) 就分析中所確認之潛在風險或實際危害，應依以下優先順序予以降低或消除：

A. 採具最低風險與危害之設計。

B. 設置安全裝置、系統或設備。

C. 設置警報或警告裝置、設備。

D. 使用特殊程序。

(6) 安全關鍵項目：於設計階段，廠商應分別執行第三代 CTC 系統及電力 SCADA 系統之安全關鍵項目分析，並經本公司審查與核可。

A. 就分析確定之安全關鍵項目，所關連之系統或設備，不得具有會導致重大或致命危害的失效模式或組合失效模式。

B. 此等關鍵系統或設備，應具故障自趨安全之設計或採複置裝置檢查，俾使任何故障或功能喪失時，皆不會導致不安全狀況。

C. 當任何系統、設備及元件之故障，會導致人員受傷、主要系統損壞或營運中斷時，則廠商應採複聯裝置、熱機自動備援，或依故障自趨安全原則進行設計。

(7) 失效自趨安全原則：

A. 一般準則：

(A) 元件故障或喪失輸入訊號，不得造成危害；

(B) 併發其他故障時，亦不得造成危害；

(C) 相同原因或相關原因，所造成之多重元件同時故障，不得導致危害；

(D) 單點故障不得造成安全保護喪失。

B. 電力/電子電路準則：

(A) 電線斷裂、受損或接點、電驛不潔，造成通電後沒有反應，於斷電或重新接通電路，均不得造成危害。

(B) 建立電子電路之故障自趨安全準則時，應考慮元件可能因開路或短路的故障。

(C) 具多重端子之裝置，應假設可能因端子開路、短路，或端子間部份短路的各種組合狀況的故障。

(8) 警告標誌設置原則：

A. 對可能危害乘客及營運、維修人員之狀況，均應設置警告標誌。

B. 必要之安全符號、警告標誌皆應納入維修程序中，並張貼在各相關使用設備附近、設備房入口，如：高壓電源危險、高溫危險及高速機械裝置危險。

C. 操作、維修設備之人員，不得曝露於不合理的風險與危害中。

(9) 安全裝置防護原則：

A. 任何非依規定順序操作將會導致之風險與危害，於系統設計中即應包含元件間之聯鎖。

B. 第三代 CTC 系統及電力 SCADA 系統之所有設備均應有適當防護措施，以防止玩弄及破壞。

C. 電纜應佈設於適度加蓋之電纜槽內，或予足夠的安全遮蔽、保護。

(10) 複式元件或電路故障時，應可立即警示，或由廠商定出定期檢查時程及程序。

1.1.6.2 系統安全計畫

(1) 廠商應參考 IEC62278(EN50126)、IEC62279(EN50128)、IEC62425(EN50129)與 IEC61508 等標準，並依據本規範對系統保證工作之要求提送「系統安全計畫(System Safety Plan)」，經本公司核可後據以執行作業。並應於契約履行階段應保存相關的紀錄。

(2) 系統安全計畫中應就工作範圍，規劃系統安全分析、管理與驗證之執行計畫及依據，並說明下列內容：

(A) 計畫目標。

(B) 計畫組織，包括人員權限、職務、資格及其責任。

(C) 介面組織，應確認各作業與相關支援人力、組織間之關係。

(D) 作業及程序，包括：

a. 設計及分析技術。

b. 測試、檢查，以及各階段之驗證。

c. 設計及施工之掌控。

d. 確認、評估、報告、追蹤、更正危險缺失等之方法。

e. 參與設計審查及設計變更需求之掌控。

f. 稽查。

g. 記錄、資料及證明文件。

h. 提供安全需求予分包廠商，並自分包廠商處得知其作業現況之方法。

(E) 配合設計、施工及計畫之里程碑，提送安全作業時程。

(F) 設置 1 名安全作業之負責人，需有 3 年以上系統機電系統保證執行經驗。

(G) 系統安全準則。

(H) 廠商應對安全設定目標與承諾，制定書面說明之安全政策，並由資深的管理階層簽署。

(I) 廠商之系統安全計畫中所訂定之各項工作，應依據各個不同的計畫階段予以區分。

1.1.6.3 系統安全分析

A. 安全與風險接受準則

(A) 廠商應參照 6.3.1、(4)所訂定之規範，對危害嚴重等級、危害發生頻率和危害忍受度劃分之定義及本公司確認之表格來執行危害嚴重等級、危害頻率和危害容忍度分析作業。對於風險可容忍度(Risk Tolerability)之訂定，至少須符合國際上目前已經開始營運之現代化類似軌道系統之標準。

(B) 廠商就危害登記冊所登錄之危害，應提出減輕措施，並經本公司之檢核及認可。且應依危害嚴重等級、危害發生頻率和危害忍受度，提出風險接受準則。對於意外傷亡之風險(Risk of Fatalities)之訂定，至少須降低至國際上目前已經開始營運之現代化類似軌道系統之標準。

(C) 廠商應對本公司提出營運階段持續性安全管理之整體安全準則及安全需求。

B. 危害分析

(A) 危害分析的目的是為辨識與紀錄所有有關本第三代 CTC 系統及電力 SCADA 系統營運時可能發生之危害，並評估其危害風險。

(B) 廠商應對所有相關權責單位所執行的危害辨識過程及其初步風險評估進行管理。

(C) 廠商應將危害分析的結果，使用危害登記冊紀錄，需能對危害減輕納入設計

做追蹤，並對未來營運階段任何工作地點所發生的危害，及所有的作業行動，提供簡易存取的功能。

(D) 廠商應定期維護危害登記冊，並對所有相關單位所提出的危害減輕措施，進行完整之辨識和紀錄作業。

(E) 對於所有相關單位所辨識出之減輕措施及其執行結果，廠商應提供完整之工作紀錄及進度報告予本公司。

(F) 廠商應製作應用於營運與保固期間之變更及維修等各階段之危害檢核流程，包含製作危害登記冊所完成之新增危害及其減輕措施之辨識過程。

(G) 最終風險評估、危害減輕的接受及危害的結案，需要符合已核定之安全及風險接受準則。

(H) 於本系統切換測試開始前，須完成危害登記冊，並須於本系統正式切換前提送予本公司。危害登記冊建置軟體之選用，應考量後續營運單位維護與更新需求，如使用專用軟體，須提供本公司所有的密碼、支援軟體和使用手冊，以供本系統營運時使用及後續發展。

(I) 危害分析應包含但不限於：

a. 初步危害分析 (Preliminary Hazard Analysis, PHA)。

b. 系統危害分析 (System Hazard Analysis, SHA)：廠商應就系統整合時以及各系統介面間，所可能產生之危害進行分析。

c. 子系統危害分析 (Subsystem Hazard Analysis, SSHA)：廠商應分別就各子系統進行分析。

d. 操作及支援危害分析 (Operation & Support Hazard Analysis, OSHA)：廠商應發展出營運前之安全分析，以推論系統之營運安全。

e. 介面危害分析(Interface Hazard Analysis, IHA)：分析各子系統間之介面及外在介面所可能產生之危害進行分析。

f. 危害登記冊(Hazard Log)。

g. 所有危害分析文件均應清楚描述目的、範圍、方法、以及與其他文件相互間之關係。其中，相關欄位應載明所引用之相關細部設計文件，或/及操作手冊、維修手冊名稱，以及廠商相關文件之參考編碼。

h. 遇有重大/致命且無法解決之危害，或在系統測試至保固期間發生之重大意外，廠商須另提送故障樹分析(Fault Tree Analysis, FTA)予本公司核可。

C. 設計安全研究

(A) 設計安全研究的目的是為設計流程提供安全分析的文件，以確保能將危害減輕措施優先納入於設計。

(B) 設計安全研究應對關鍵性系統/子系統/設備有完整之說明，並對可能會影響到系統與子系統安全之硬體與軟體之細部設計，進行詳細之危害分析。

(C) 設計安全研究應以系統層級的危害分析流程及危害登記冊為基礎來製作。設計安全研究亦應使用被認可或特別規範要求之定量及定性分析技術來執行：

a. 危害及作業能力研究(Hazard and Operability Studies, HAZOP)。

b. 故障樹分析(Fault Tree Analysis, FTA)。

c. 事件樹分析(Event Tree Analysis, ETA)。

d. 失效模式、影響及關鍵性分析(Failure Mode Effects Criticality Analysis, FMECA)。

e. 量化風險分析(Quantified Risk Analysis, QRA)。

(D) 設計安全研究應特別指出由下列環境所產生的危害：

a. 包含維修作業的正常操作。

b. 降級操作模式。

c. 緊急情況。

d. 對天然危害所特別提出之特殊或有效的減輕措施。

(E) 設計安全研究應考量：

a. 操作方式。

b. 系統可靠度、可用度和可維修度（RAM）。

c. 營運階段所預期的維護方式及其持續性。

d. 營運階段人員之標準。

(F) 安全關鍵項目清冊。

(G) CTC 系統的 SIL 等級需求如下：

a. CTC 系統應符合 IEC 62278(EN 50126)、IEC 62425(EN 50129)與 IEC 61508 標準定義之 SIL2 等級，其內建之軟體應符合 IEC 62279(EN 50128)與 IEC 61508 標準定義之 SIL2 等級。

b. CTC 系統之各項軟體修改工具應符合 IEC 62279(EN 50128)與 IEC 61508 標準之相關規定，以確保經軟體工具產出之機械碼於執行階段不會危及安全完整性等級。

c. 使用之通訊協定應符合 IEC 62280(EN 50159)與 IEC 61508 標準之規定，以確保 SIL 之符合性。

d. 除本規範所要求之安全完整性等級外，廠商應依據 IEC 62278(EN 50126)、IEC 62279(EN 50128)、IEC 62425(EN 50129)與 IEC61508(或同等級之其他標準)執行 SIL 分配，並制定各子系統之安全完整性等級。

e. 廠商應依據 IEC 62278(EN 50126)、IEC 62279(EN 50128)、IEC 62425(EN 50129)與 IEC 61508 之規定委託第三方單位執行獨立安全評估(ISA)，並出具安全評估報告以說明能達成 SIL 需求。

f. ISA 應具備 ISO/IEC 17020 認可之資格，而 ISA 評估的範圍至少應包含：

(a) 系統設計及開發過程。

(b) 廠商的品質管理及安全管理。

(c) 設計文件、測試文件及安全相關文件(如：本工程相關的危害分析、風險量化分析 QRA 等)。

(d) 生產檢查。

(e) 現場安裝及現場測試見證。

D. 安全驗證

(A) 於設計階段結束前應依「系統安全計畫」提出本工程「安全驗證計畫」，以驗證系統符合營運安全需求，計畫中除載明執行期程與方法外，並敘明依據的標準與評估方法，以證明其能滿足本契約要求的安全需求。

(B) 於製造、施工、安裝與測試等階段，廠商應依據「安全驗證計畫」具體執行驗證，並將各階段驗證結果紀錄於本工程「安全驗證報告」提送審查。

1.1.6.4 系統安全管理

A. 系統安全資料及程序，應納入訓練教材以及操作手冊、維修手冊中。其內容應包括但不限於：正常及緊急操作下，營運、維修人員所使用之保護裝置及緊急設備。

B. 廠商之系統安全組織應參與設計審查。其系統安全工程師應提供危害輸入、危害分類，並提出審查意見，評估所作設計是否符合安全需求/準則，並擇優提出適當建議。

C. 與安全相關文件(包括但不限於設計完成、設計變更，以及測試計畫、操作手冊、維修手冊等文件)於發佈前，均應經廠商之系統安全工程師審查及核准。

1.1.6.5 安全風險管理

A. 安全風險管理應包含與死亡、受傷以及財務損失(包含財產的損失和/或環境的破壞)相關之預防措施。

B. 任何合理實際的使用情況下，廠商應對危害執行辨識、確認及登錄，並在設計階段中加以消除。對於不能在設計階段中合理實際被消除的危害，廠商應執行風險評估，以確保剩餘危害風險能符合：

(A) 在設計階段中能對危害盡可能減到最小。

(B) 在後續階段中儘可能再減輕。

(C) 能對危害執行後續的管理作業。

C. 安全風險管理之準則應遵循 IEC 62278(EN 50126)規範中所定義之低到合理可行(ALARP)的原則。

D. 廠商應確認所有內、外部相關介面以及設備操作與維修所產生之風險，並應提出本公司所認可且能將風險降低到合理可行程度的各種可能方法。

E. 廠商應發展和維護所有已經辨識與確認危害之危害登記冊，此危害登記冊應是安全證明文件的一部分。

1.1.6.6 符合管理

A. 廠商應確保危害登記冊之內容能符合所有操作與維修安全法規之要求。

B. 在本規範所提出的所有慣例、標準及規格規範，在危害登記冊中也應參考並確認符合需求。

1.1.6.7 安全證明

A. 廠商應於細部設計完成後，提供設計安全證明文件(Design Safety Case)，於系統整合測試完成後，提供營運安全證明文件(Pre Operational Safety Case)。

B. 安全證明文件(Safety Case)應建立具體之佐證資料，以證明第三代 CTC 系統及電力 SCADA 系統之系統安全已滿足本規範之要求。廠商應參考 IEC 62425(EN 50129)之規定建構安全證明文件，其組成應至少包含但不限下列之必要部分。

(A) 系統定義。

(B) 系統品質管理。

(C) 系統之安全需求與安全管理(含 Hazard Log 及 SIL 說明)。

(D) 系統之技術安全。

(E) 系統其他關聯安全證明實例。

(F) 系統安全之結論。

1.2 查證與確證管理(Verification and Validation)

1.2.1 廠商應提送查證與確證管理計畫供本公司審查，經本公司核定後，始能進行設計、製造、安裝、系統測試與切換等程序，於契約履行階段應保存相關的紀錄。

1.2.2 查證與確證管理計畫之擬訂應參考 IEC 62278(EN 50126)標準，依系統生命週期概

念，詳細規劃各階段之查證與確證管理作業。其內容應包括但不限於以下部分：

1.2.2.1 負責執行查證與確證管理計畫之廠商組織、人員之適任說明(例如個人之詳細學經歷資料)。

1.2.2.2 查證與確證管理相關職權與責任。

1.2.2.3 查證與確證管理工作執行範圍。

1.2.2.4 第三代 CTC 系統及電力 SCADA 系統之查證與確證管理需求與目標。

1.2.2.5 查證與確證管理機制與作業程序。

1.2.2.6 查證與確證工作項目與文件交付之時程。

1.2.2.7 介面需求之分配、追蹤、管控作業等之執行辦法。

1.2.2.8 查證與確證作業稽核辦法。

1.2.2.9 管理查證與確證作業之軟體說明。

1.2.3 廠商應說明及證明需求之可追溯性，不只於兩階段間，更要廠商證明所使用之系統/軟體可以在簡單、快速、易懂、容易操作的情況，證明如何於向後續階段追溯，並應可向先前各階段回溯。

1.2.4 上述之可追溯性，須能夠在簡單、易懂、易操作，且於同一軟體/系統、文件、檔案內來呈現。其證據須為提送本公司之文件，並在本公司要求審查時提供，不得拒絕。

1.2.5 廠商針對需求所提出的證據，若是為文件，其文號、版次、章節、描述及內部審查證據須清楚記錄在系統/軟體裡，並在需要列印紙本報告的情況下能夠呈現上述細節。若提出證據為圖說則需提供其文號、圖號與版次。

1.2.6 廠商應說明將會如何追蹤介面需求，在查證與確證管理系統/軟體內如何追蹤各系統功能介面需求。介面需求與一般需求所須提供證據以及管理方式相同。

1.2.7 廠商的查證與確證應將所有需求分配給適當的系統同時確保每個介面需求都被該介面系統納入設計考量。

1.2.8 廠商應於每階段提供兩次查證與確證報告，第一份報告為該階段的需求以及其相對應之上階段需求(於前一階段結束前提送)，第二份報告為該階段需求以及其完整證據供本公司審查(於該階段結束前提送)。

1.2.9 廠商需在各階段查證與確證報告提送之前持續進行查證與確證作業，本公司將會不定期要求檢查/稽核廠商查證與確證作業進度，廠商需配合並提供所需之相關證據。

1.2.10 查證與確證成員需在提出查證與確證報告時，負責審查該系統各階段所提供之證據是否滿足相關需求。

1.3 應配合獨立查證與確證(IV&V)執行需求，提供所需文件、參與稽核、執行相關檢驗與測試等工作，並應配合 IV&V 開立缺失於期限內完成改善，直至該缺失結案為止。所衍生之人力成本、時間與費用等，均屬本契約之工作範圍，由廠商自行負擔。