6G 無線定位應用之人工智慧生命週期治理：ISO/IEC 42001 之應用

Artificial Intelligence Lifecycle Governance in 6G Wireless Positioning Applications: An Application of ISO/IEC 42001

游承翰
明志科技大學電機工程系

劉恩成
明志科技大學電機工程系

摘要

第六代行動通訊（6G）通感一體化架構下的高精度無線定位服務，因深度學習技術的廣泛導入而面臨模型可解釋性不足、位置隱私保護困難與模型漂移監控缺乏等治理挑戰。6G 定位 AI 系統同時面臨無線通道隨機性、位置資料空間連續性、毫秒級即時性約束、跨頻段部署異質性與物理驅動模型漂移等五項特性的交叉疊加效應，其複合治理需求難以由通用框架直接回應。本研究採設計科學研究方法論，以 ISO/IEC 42001:2023 人工智慧管理系統標準為制度基礎，融合 ISO/IEC 22989 生命週期階段劃分，建構適用於 6G 無線定位 AI 系統的全生命週期治理框架。透過控制措施對應分析，將 ISO/IEC 42001:2023 附錄 A（Annex A）各項措施歸入直接適用、情境化調適與領域延伸三類，並辨識出四項超越現行標準條款範圍的領域延伸措施：物理驅動模型漂移之專屬監控機制、空間連續性位置資料之專屬隱私治理機制、即時性約束下人為監督之分級設計，以及跨頻段與跨領域部署之治理一致性管理機制。框架以實際部署於大學校園之 6G AI 室內定位系統進行應用展示，並以智慧工廠作為高風險對照領域檢視跨領域適用性。研究結果顯示，ISO/IEC 42001 經領域情境化調適後具備回應 6G 定位治理需求的制度能力，模組化設計使治理邏輯層在不同風險等級場域間維持結構穩定性。

關鍵詞：6G 無線定位、人工智慧治理、ISO/IEC 42001、AI 生命週期管理、通感一體化、位置隱私保護、模型漂移監控

Abstract

The widespread adoption of deep learning in 6G integrated sensing and communication (ISAC) architectures has introduced governance challenges including insufficient model interpretability, location privacy protection, and model drift monitoring. 6G positioning AI systems face five compounding characteristics—wireless channel stochasticity, spatial continuity of location data, millisecond-level latency constraints, cross-band deployment heterogeneity, and physics-driven model drift—whose composite governance requirements exceed the capacity of general-purpose frameworks.

Using Design Science Research methodology, this study constructs a full-lifecycle governance framework for 6G wireless positioning AI systems grounded in ISO/IEC 42001:2023 and ISO/IEC 22989. A control measure mapping analysis classifies Annex A measures into three categories—directly applicable, contextually adapted, and domain-extended—identifying four domain-extended measures: physics-driven model drift monitoring, spatially continuous location data privacy governance, tiered human oversight under real-time constraints, and governance consistency management for cross-band and cross-domain deployment.

The framework is validated through a campus-deployed 6G AI indoor positioning system, with a smart factory as a high-risk reference domain for cross-domain applicability assessment. Results demonstrate that ISO/IEC 42001, following domain-specific contextual adaptation, maintains structural stability across deployment scenarios of varying risk levels.

Keywords: 6G Wireless Positioning; AI Governance; ISO/IEC 42001; AI Lifecycle Management; Integrated Sensing and Communication (ISAC); Location Privacy Protection; Model Drift Monitoring

1. 緒論

1.1 研究背景

第六代行動通訊（6G）的核心演進方向之一，在於通感一體化（Integrated Sensing and Communication, ISAC）架構的確立。在此架構下，基地台同時承擔資料傳輸與環境感測的雙重功能，而高精度無線定位被視為 ISAC 框架中最具應用前景的感測服務類型 [1, 2]。支撐此願景的硬體技術基礎正趨於成熟：大規模天線陣列

（Massive Multiple-Input Multiple-Output, Massive MIMO）提供高維度空間解析能力，智慧反射面（Reconfigurable Intelligent Surface, RIS）改善非視線傳播條件下的定位可行性，太赫茲頻段以超寬頻寬特性將定位精度推進至公分級水準 [3, 4]。在演算法層面，以 CNN、ResNet 為代表的深度學習模型，已被廣泛應用於從 CSI 中習得與空間座標的非線性映射關係 [5, 6]。

然而，深度學習的廣泛導入也引發不容忽視的治理隱憂：神經網路的黑箱特性使定位決策缺乏可解釋性——終端使用者與系統營運方無從理解推論依據 [7]，位置資訊的高敏感性使傳統匿名化手段難以消除重新識別風險 [8, 9]，模型部署後若精度退化未被及時偵測，可能累積為系統性安全風險。這些治理隱憂並非停留於理論層次的推測——隨著 6G 定位服務從實驗室走向大規模部署，缺乏有效治理機制的後果，將從工程問題演變為社會信任危機。國際社群已對 AI 治理挑戰積極回應：歐盟以《人工智慧法案》[10] 確立基於風險分級的管制模式，高風險 AI 系統須滿足包括資料品質、透明性、人為監督與穩健性在內的嚴格合規要求 [10]；NIST 以 Govern、Map、Measure、Manage 四大模組引導系統性風險管理 [11]；ISO/IEC 則推出首部可認證的 AI 管理系統標準 ISO/IEC 42001，為組織建立 AI 治理提供了結構化且可認證的制度路徑 [12]。這些規範路徑在透明性、公平性、問責性、非惡意與隱私等倫理原則上呈現高度收斂 [13, 14]，但從抽象原則到可落地實踐之間的轉化鴻溝，依然是核心挑戰 [15, 16]。

儘管 AI 治理已進入制度化建構的新階段，6G 無線定位領域的研究幾乎全數集中於演算法效能最佳化——如何在複雜多徑環境中將定位精度推進至更高水準——從治理角度審視 AI 定位系統風險管理需求的論述極為稀少 [8, 17]。這項研究缺口的根本原因在於 6G 定位 AI 系統五項技術特性的交叉疊加效應所產生的複合治理需求，超出了通用治理框架的設計預設範疇，形成了現有治理標準與 6G 定位實務需求之間的結構性落差。

基於上述認識，本研究以 ISO/IEC 42001:2023 為理論基礎與制度骨幹，建構適用於 6G 無線定位 AI 系統的全生命週期治理框架。選擇該標準作為制度骨幹的理由有三：（1）其 PDCA 循環與高階結構使其與既有管理系統具備整合優勢；（2）附錄 A（即 ISO/IEC 42001:2023 之 Annex A [12]）控制措施涵蓋資料品質、模型透明性、人為監督等核心議題；（3）其結構化要求能有效銜接多元區域性法規的遵循需求 [18, 19]。研究依循四個邏輯遞進步驟：（1）從技術文獻萃取治理挑戰並以跨領域比較論證其複合特殊性；（2）逐項審視附錄 A 各控制措施的適用程度，歸入直接適用、情境化調適與領域延伸三類；（3）融合 ISO/IEC 22989 [32] 生命週期階段劃分建立二維對應矩陣；（4）以校園 6G AI 室內定位系統展示操作可行性，輔以智慧工廠檢視泛化潛力。

1.2 研究問題、目的與範圍

本研究聚焦於以下核心研究問題：ISO/IEC 42001:2023 [12] 之通用性管理系統框架，經何種程度與何種形式的領域調適後，能有效覆蓋 6G 無線定位 AI 系統在全生命週期中所面臨的特殊治理需求？此問題進一步分解為三個子問題：第一，6G 定位 AI 系統相較於其他 AI 應用領域，在治理需求的組合形態上呈現何種特殊性？第二，ISO/IEC 42001 附錄 A 各控制措施在 6G 定位脈絡下的適用程度如何分布？第三，標準現有條款未能涵蓋之治理缺口為何，應以何種機制加以補充？

研究目的在於：建構一個以 ISO/IEC 42001 [12] 為制度骨幹、經 6G 定位技術特性情境化調適的全生命週期治理框架，使組織能據此系統性地辨識、評估與回應 6G 定位 AI 系統的治理風險。

研究範圍聚焦於以 AI 技術實現室內高精度定位功能的 6G 通感一體化系統，治理層面以 ISO/IEC 42001 [12]附錄 A 控制措施為分析核心，輔以 ISO/IEC 23894 [51] 與 NIST AI RMF [11] 進行交叉檢核。研究不涵蓋 6G 網路通訊功能本身的治理議題（如頻譜管理、服務品質保障等），亦不處理演算法效能最佳化的技術問題。依 Gregor 與 Hevner [20] 的知識貢獻框架，本研究定位為「改進型」貢獻——針對已知問題領域提出新的解方產出物，且作為此一研究方向的第一輪設計迭代，貢獻定位為概念性框架的建構與初步適用性探索。

2. 文獻探討

2.1 6G 無線定位技術發展

2.1.1 6G 通訊架構與關鍵技術

ISAC 被學界視為第六代行動通訊網路中最具範式變革意義的技術演進方向。在此架構下，基地台從傳統的資料傳輸節點擴展為同時承擔環境感測的雙功能實體，透過對發射訊號回波的系統性分析，實現對周遭環境的主動感知與使用者空間定位 [1, 21]。支撐此技術願景的關鍵硬體技術正趨於成熟。Massive MIMO 賦予基地台高維度的空間解析能力，使系統能在角度域中精細辨別多重訊號路徑，顯著提升到達角估計的準確度。RIS 以可程式化的電磁反射特性，為非視線（Non-Line-of-Sight, NLoS）傳播條件下的定位提供替代性訊號路徑，有效改善遮蔽區域的定位可行性 [4]。太赫茲頻段憑藉超寬頻寬特性，大幅提升時延與角度估計的解析度，為定位精度向

公分級水準推進奠定物理層基礎 [3]。在標準化進程方面，3GPP 已於 Release 17 啟動定位增強研究 [22]，並於 Release 18 將 AI/ML 技術正式納入新無線電空中介面的研究範疇 [23]，同步更新定位功能技術規範 [24]。分散式 MIMO 架構透過多節點的協同感測機制，進一步強化定位覆蓋的空間均勻性與系統在單點故障情境下的穩健性 [2]。

2.1.2 AI 輔助無線定位方法

深度學習的廣泛引入為無線定位帶來質性突破，從根本上改變了定位演算法的設計邏輯。傳統幾何定位方法（如到達時間（Time of Arrival, ToA）/到達角（Angle of Arrival, AoA）三角測量）高度依賴精確的通道模型假設，在複雜多徑環境中效能急遽下降；指紋匹配方法雖能有效規避對通道模型的直接依賴，但線上匹配的運算複雜度與離線指紋庫的持續維護成本，構成規模化部署的瓶頸。卷積神經網路（Convolutional Neural Network, CNN）、ResNet 等深度學習模型從通道狀態資訊（Channel State Information, CSI）等訊號特徵中端到端學習與空間座標的非線性映射關係，在室內環境已實現公分級精度 [5, 25]。注意力機制（attention mechanism）強化了模型對多徑環境中關鍵特徵的辨識能力，使模型能自適應地聚焦於承載最多空間資訊的訊號成分。深度強化學習則被應用於 RIS 輔助 ISAC 系統中的聯合波束成形最佳化 [4]。遷移學習技術被探索用於跨場域的模型遷移，以降低新部署場域的資料採集成本 [6]，但跨場域遷移的效能穩定性仍有待更大規模的實證驗證。

兩項新興技術方向的治理含義尤其值得深入關注。第一，大型無線定位模型（Large Wireless Localization Model, LWLM）仿照大型語言模型的預訓練-微調範式，利用大規模跨場域的通道量測資料進行自監督預訓練，再針對特定場域進行少量樣本微調。此路徑雖能降低新場域的部署成本，但引發資料品質管控——預訓練資料來源的多樣性與品質難以逐一審核——以及智慧財產歸屬——模型權重中跨組織累積的知識歸屬何方——等新治理問題 [26]。第二，聯邦學習（federated learning）在保護原始資料不離開本地端的前提下實現協同模型訓練，為位置隱私保護帶來技術解決路徑，但同時引入模型聚合可信度驗證與跨組織資料主權歸屬等新治理挑戰 [8]。

2.1.3 定位精度與應用場景

垂直應用場景對定位效能的差異化需求直接牽動治理策略的選擇與實施強度。智慧工廠要求公分級精度以支撐自動導引車（Automated Guided Vehicle, AGV）的導航控制與機械手臂的協同作業，定位誤差直接關聯人員安全，屬安全關鍵等級；智慧醫療仰賴即時人員與設備定位提升緊急應變效率，在醫院急診或手術場景中定位失效可能延誤救治；車聯網（Vehicle-to-Everything, V2X）將高精度定位視為感知融合與協同決策的前提，車輛間的相對位置誤差直接影響碰撞迴避決策的有效性 [3, 9]。智慧校園與智慧商業場域的精度需求相對寬鬆（公尺級至次公尺級），但對隱私保護的敏感性可能更高。上述場域對精度、延遲、可靠性及隱私保護的優先排序各異，不僅構成治理框架必須具備場域調適彈性的實務驅動力，更意味著風險分級標準與控制措施的實施深度必須依據應用場景的安全關鍵性進行差異化配置。

2.1.4 6G 定位 AI 系統之技術特性摘要

綜合文獻分析，本節萃取 6G 定位 AI 系統有別於一般 AI 應用的五項關鍵技術特性，作為後續治理框架建構的技術參照基礎。第一，無線通道的高度隨機性與時變性：多徑衰落、遮蔽效應與散射體移動等隨機物理過程，使即便在相同物理位置、不同時刻的量測結果也可能呈現顯著差異，資料品質的可控性面臨結構性挑戰，其根源在於資料來源的物理本質而非管理流程的不完善。第二，位置資料的空間連續性與個資敏感性：空間座標序列的連續性使傳統匿名化技術手段難以有效消除位置軌跡之重新識別風險——攻擊者可藉由軌跡推論與空間模式比對從形式上已匿名化的資料中反向還原個體身份 [27, 28, 29]，此為位置資料有別於其他個資類型的根本屬性。第三，毫秒級即時性約束與人為監督介入需求之間的結構性張力：在安全關鍵應用中，系統幾乎不容許人為審核所致的額外延遲，但完全排除人為監督又與現行治理原則相悖，須發展分級化的監督機制加以調和。第四，跨頻段與跨環境的部署異質性：同一系統在不同頻段（sub-6 GHz、毫米波、太赫茲）與不同場域類型（工廠、醫院、校園、戶外）中面對截然不同的通道特性、干擾模式與風險樣態，使單一模型、單一治理策略的假設不再成立。第五，模型漂移的物理驅動因素：精度退化源於場域結構改變、散射體移動與硬體老化等具體物理成因，而非僅是統計層面的資料分布偏移，偵測與歸因需同時具備通訊工程與 AI 監控的雙重知識 [30, 31]。上述五項特性並非各自獨立存在，而是在實際系統中呈現交叉疊加效應——例如無線通道隨機性加劇資料品質管控困難，而物理驅動漂移的偵測又受制於跨頻段部署異質性——正是這種多維度的耦合複雜度，構成建構領域專屬治理框架的技術基礎與分析起點。

2.2 人工智慧生命週期管理

2.2.1 AI 生命週期於技術標準及治理規範之差異

人工智慧系統的生命週期管理是治理實踐的核心軸線，然而不同規範體系對生命週期的階段劃分與治理介入邏輯並未達成一致。ISO/IEC

22989:2022 [32] 將 AI 系統生命週期劃分為需求分析、設計開發、驗證確認、部署、運營監控與退役六個階段，為生命週期管理建立了術語層面的共同語義基礎 [32]。然而，歐盟《人工智慧法案》將合規義務集中配置於高風險系統的上市前評估與上市後監控兩大節點 [10]，NIST AI RMF 則以四大功能模組橫向貫穿生命週期，不對階段本身施加剛性的合規切分 [11]。此種歧異使組織同時面對多套標準時易遭遇方向矛盾的合規指引。更根本的問題在於，AI 系統高度依賴訓練資料品質、容易因環境變動產生模型漂移、輸出帶有機率性質，這些固有屬性意味著生命週期管理必須以持續監控與迭代改進的姿態貫穿全週期 [33, 34, 35]。

若從生命週期視角切入，6G 定位 AI 系統的風險可沿各階段辨識：需求分析階段的約束條件不足、資料收集的場域偏差與隱私侵害、模型開發的演算法歧視與可解釋性缺失、部署階段的精度劣化、運營期間的模型漂移累積，以及退役階段的資料處置合規問題 [8, 9, 36]。6G 的全球化部署特性更使治理面臨跨司法管轄區的協調難題 [37, 38]，此為本研究選擇具國際共識基礎之 ISO/IEC 42001 [12] 作為框架核心的重要背景。

2.2.2 既有治理框架於 6G 定位領域之適用性缺口分析

為精確定位本研究的學術增量，本節將三個具代表性的既有治理框架逐一置於 6G 無線定位的技術脈絡中進行批判性檢視。首先，Leon [39]的生命週期治理框架雖系統性地將治理機制嵌入 AI 系統的各發展階段，但其監控機制預設模型漂移的主要成因係統計層面的資料分布偏移，機器學習系統在生產環境中普遍面臨的隱性技術債務 [40]，使這項監控挑戰更趨複雜，未能處理 6G 定位中模型漂移的物理驅動因素（場域結構改變、散射體移動與硬體老化等具體物理成因）所致的精度退化。此類漂移要求將物理環境變化事件系統性納入監控觸發條件的設計邏輯，而該框架對此有所欠缺。其次，Mäntymäki 等學者 [36]的沙漏模型所辨識的 67 項治理任務中，涉及資料品質管控、模型監控與隱私管理的關鍵項目，在 6G 定位脈絡下存在需要「重新定義」（如資料品質指標須納入無線通道的時變特性）、「不適用」（如部分預設結構化資料來源的治理假設）或「缺漏」（如缺乏針對空間連續性位置資料的專屬匿名化治理機制）等情形。再者，Mert 等學者 [17]的 6G AI 倫理論述雖正確指出公平性、透明性與問責性在 6G 場域中的重要性，但停留在抽象原則的倡議層次，未提供從倫理原則轉化為可稽核控制措施的操作路徑。這項從原則到實踐的轉化斷裂並非 6G 領域所獨有，而是 AI 治理研究的普遍挑戰——全球已逾 160 份 AI 倫理準則在核心原則上呈現高度收斂，但在實施路徑上卻嚴重分歧 [13, 41]，Fjeld 等學者 [42]的跨文件映射分析亦確認這項「原則豐富、工具貧乏」的結構性失衡。上述三重缺口——物理驅動漂移監控的缺失、通用治理任務的領域適配不足、以及從原則到實踐的轉化斷裂——共同構成本研究建構領域專屬治理框架的直接立論依據。

2.3 ISO/IEC 42001 人工智慧管理系統標準

ISO/IEC 42001:2023 係國際標準化組織與國際電工委員會聯合發布的首部 AI 管理系統（AI Management System, AIMS）標準，為組織建立、實施、維護與持續改進 AI 管理系統提供了可認證的制度框架，以 PDCA 循環為方法論骨幹 [12]。Plan 階段進行組織情境分析、利害關係者需求辨識與 AI 系統風險評鑑，輸出涵蓋治理範圍界定、風險處理計畫與資源配置規劃；Do 階段落實資源配置與運營管理，包括人員能力建設、AI 系統開發與運營的過程管控；Check 階段以內部稽核、管理審查與績效評估確認治理成效，辨識實施落差與改進機會；Act 階段依 Check 發現採取矯正措施推動持續改進，形成閉環管理迴路 [18]。標準主體條款遵循 ISO 高階結構（Harmonized Structure），此一設計選擇使其與 ISO/IEC 27001 [52] 資訊安全管理系統、ISO 9001 [53] 品質管理系統之間天然具備整合基礎——已導入上述管理系統的組織可在既有制度架構上疊加 AI 治理功能，大幅降低導入門檻與重複建置成本 [19]。在風險評鑑方面，標準可追溯至 ISO 31000 通用風險管理框架 [43]，要求組織以系統性方法辨識、分析與評估 AI 系統相關風險，Zicari 等學者 [44] 提出的 Z-Inspection® 流程則為 AI 系統可信度評估提供了可操作的多利害關係者審視架構。

附錄 A 規定了 AI 領域專屬的控制措施集，涵蓋治理架構建立、影響評鑑、資料品質管控、模型透明性、人為監督、供應商管理及持續監控等面向。控制措施採風險導向的彈性設計——組織須依風險評鑑結果判定各措施的實施深度與優先順序 [12]。此設計賦予標準在不同產業場域中廣泛適用的彈性，但也意味著引入高度技術特殊性領域時，可能發現部分治理需求超出現有措施的覆蓋範圍。

在與 6G 技術標準的銜接方面，3GPP 自 Release 18 起將 AI/ML 納入標準化範疇，為 ISO/IEC 42001 [12] 提供技術情境輸入。ISO 體系內部具備豐富互補空間：與 ISO/IEC 27001 [52] 整合可延伸資訊安全控制措施、ISO/IEC 23894 提供風險管理方法論補充、ISO/IEC 22989 [32] 建立跨標準共同語義基礎。學界普遍認為 ISO/IEC 42001 的結構化要求能有效降低組織遵循多元區域性法規時的實務複雜度 [19, 37]，此為本研究選擇該標準作為治理框架核心的關鍵理據。

3. 研究方法

3.1 研究架構與流程

本研究採設計科學研究（Design Science Research, DSR）為方法論取徑 [45, 46]，輔以文獻分析法進行理論基礎萃取，並以校園 6G AI 室內定位系統作為應用展示標的。DSR 的選擇基於研究問題的本質：針對已辨識的治理缺口，設計具操作性的治理制度產出物。依 Gregor 與 Hevner [20]的知識貢獻框架，本研究屬「改進型」貢獻，作為此一研究方向的第一輪設計迭代。在評估策略方面，遵循 Venable 等學者 [47]的 FEDS 框架，採 Quick & Simple 策略——以文獻分析進行形成性評估，以案例展示進行總結性評估，適用於 DSR 早期探索階段。後續研究可依 FEDS 框架升級至 Human Risk & Effectiveness 策略，以行動研究法在真實組織中導入框架並量測治理績效變化。

研究流程依循四個階段循序推進。第一階段為系統性文獻回顧，從三個知識領域——6G 無線定位技術、AI 生命週期管理、ISO/IEC 42001 [12] 人工智慧管理系統標準——進行文獻的系統性蒐集與分析。文獻檢索以 IEEE Xplore、Scopus、Web of Science 與 Google Scholar 四個資料庫為主要來源，檢索時間範圍設定為 2020 年至 2025 年。由於 ISO/IEC 42001 [12] 係 2023 年底始正式發布，相關學術文獻尚在累積階段，本研究亦納入經同儕審查之會議論文與具學術引用價值之預印本作為補充來源。文獻回顧的最終產出包含：6G 定位 AI 系統的關鍵技術特性摘要，以及既有治理框架於 6G 定位領域的適用性缺口分析。

第二階段為治理框架的建構。以 ISO/IEC 42001 [12] 的 AIMS 架構為理論骨幹，融合 ISO/IEC 22989:2022 [32] 所定義的 AI 系統生命週期六階段劃分，以 6G 定位的技術脈絡對各階段進行情境化調適。建構過程同步參照校園定位系統的開發與運營經驗進行交叉校驗，並依第 3.2 節所述方法建立控制措施對應矩陣，同步參照 ISO/IEC 23894 [51] 與 NIST AI RMF [11] 進行交叉檢核。

第三階段為應用展示與適用性評估。以校園 6G AI 室內定位系統為標的，依治理框架逐一展示控制措施的操作方式，屬 DSR 方法論中的「應用展示」（demonstration），旨在說明框架「如何被應用」。

第四階段為跨領域適用性對照分析。選擇智慧工廠作為高風險對照領域，考察框架在風險等級與產業慣例顯著不同的環境中所需進行的調適幅度，藉此初步檢驗框架的泛化潛力。整體研究架構與流程關係如圖 1 所示。

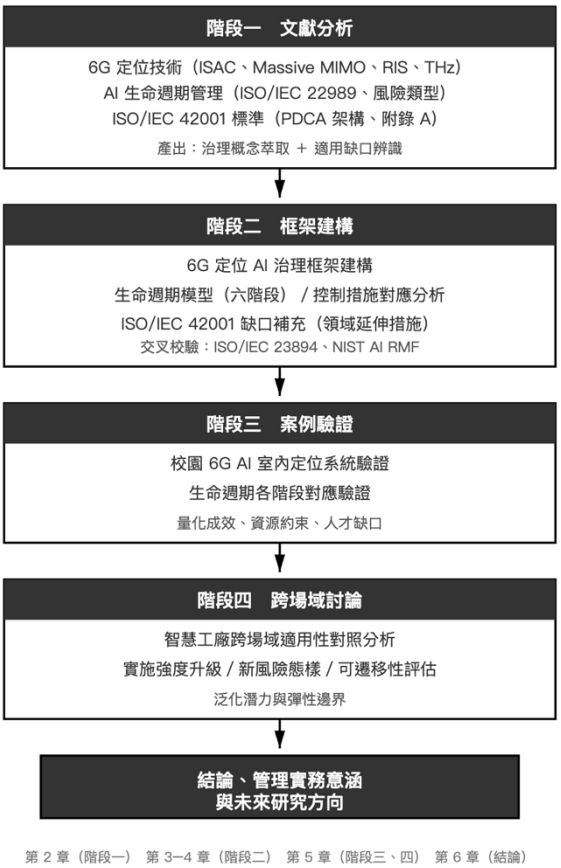

圖 1　研究架構流程圖

3.2 控制措施對應分析方法

本方法旨在系統性建立 ISO/IEC 42001 [12] 附錄 A 控制措施與 6G 定位 AI 系統治理需求間的結構化映射，分三階段推進。

第一階段為適用性分類判定。逐項審視附錄 A 各控制措施的治理目標與規範意圖 [12]，判定適用類型。分析結果歸入三類：「直接適用」指無需實質修改即可套用；「情境化調適」指治理精神不變但實施方式須針對 6G 定位特性調整；「領域延伸」指現有措施未涵蓋之特殊治理需求，須新增領域專屬機制。判定依循四步決策邏輯：第一步判定治理目標在 6G 定位中是否具規範意義；第二步評估實施方式是否可直接套用，若是則歸入「直接適用」；第三步區辨修改性質——若僅涉及既有邏輯框架內的參數調整或程序微調，歸入「情境化調適」；第四步——若需建立附錄 A 未預見的全新治理目標或監控機制，歸入「領域延伸」。關鍵區辨基準在於：「情境化調適」保留原有治理邏輯骨架，僅調整實施參數；「領域延伸」要求全新治理邏輯。

以邊界案例示例：A.7.4 資料品質管控——治理目標完全適用，但實施方式須納入通道時變性指數等領域專屬維度，屬既有邏輯內的擴充，歸入「情境化調適」。物理驅動模型漂移監控——A.10 持續監控條款未涵蓋以物理環境變化為觸發條件的監控邏輯，歸入「領域延伸」。A.6.2

人為監督——治理目標不變，但毫秒級推論延遲須依風險等級設計分級監督；經討論判定其治理目標仍落在 A.6.2 規範意圖內，歸入「情境化調適」，並標註調適幅度偏高。

在品質控制方面，歸類結果提交指導教授獨立審閱，不一致案例逐案討論後以共識定案，並與 ISO/IEC 23894 [51] 及 NIST AI RMF [11] 交叉檢核。本研究未採用雙重編碼程序，亦未實施獨立專家外部評估，此為方法論限制。

第二階段將分類結果結構化為「控制措施群組×生命週期階段」二維矩陣，每一交叉格標示適用類型並附說明，使實務工作者得以辨識各階段治理覆蓋密度。第三階段針對「情境化調適」與「領域延伸」措施提出涵蓋組織、技術與合規三層面的實施建議。

3.3 案例場域系統描述

案例場域為一所綜合型大學之主校區，定位系統覆蓋教學大樓、圖書館與學生活動中心等多棟建築物。各建築在空間結構、樓層配置、建材特性與日常使用樣態上存在顯著差異：教學大樓以走廊串聯多間教室，人員流動呈現隨課程時段變化的週期性模式；圖書館為大跨度開放空間，書架等大型物件構成相對穩定的散射環境；學生活動中心兼具餐飲、社團與休憩等多元功能，人員密度與活動模式的變異幅度最大。這項環境的異質性為定位系統的開發與運營帶來了天然的多樣化測試條件。

系統採分散式 MIMO 架構，將多組天線單元分散部署於各建築物關鍵位置，透過多節點協同感測機制提升定位覆蓋的空間均勻性。部分非視線傳播條件較為嚴苛的區域——如走廊轉角、樓梯間及地下樓層——輔以 RIS 進行覆蓋增強，藉由可程式化的電磁反射特性為定位訊號提供替代性傳播路徑。系統運作於實驗性質的 sub-6 GHz 頻段，以模擬未來 6G 通感一體化場景下的定位服務模式。各天線單元與 RIS 面板透過光纖回傳網路連接至校園機房的集中式運算伺服器，由後端完成訊號處理、特徵萃取與定位推論等運算密集型任務。

AI 模型以 CNN 為核心定位演算法，從 CSI 特徵學習訊號與空間座標的映射關係。模型的輸入為經前處理後的 CSI 振幅與相位矩陣，輸出為二維平面座標估計值。網路架構包含多層卷積層用於自動萃取空間頻率特徵，以及全連接層用於回歸座標輸出，整體設計追求在精度表現與推論延遲之間取得適當平衡。訓練資料透過在場域內預設參考點進行系統性通道量測獲取，各參考點的量測涵蓋不同時段（日間、夜間、上下課高峰期）與不同人員活動密度條件（空置、正常使用、高密度聚集），以確保訓練集的時空覆蓋度。目標精度為次公尺級，係參照校園環境中空間管理、人流分析與緊急疏散等典型應用情境的需求設定。資料生命週期涵蓋原始通道量測採集、前處理（雜訊濾除、缺失值插補、特徵正規化）、模型推論與結果輸出儲存四環節，每一環節均設有品質檢核節點。

利害關係者包括四類：校方資訊中心（營運管理，關切系統可用性）、師生（終端使用者與資料主體，關切定位準確性與隱私保護）、系統開發廠商（技術提供方，關切模型效能與智慧財產保護）、個資保護主管機關（外部監管）。系統已完成初步部署並進入試運營階段。

案例系統雖運作於 sub-6 GHz 而非未來 6G 正式分配之毫米波或太赫茲頻段，但其分散式 MIMO 架構、RIS 輔助覆蓋增強及 CNN 從 CSI 學習空間映射的方法論，均與 6G 願景在架構設計層面具備技術銜接 [8, 48]；現存技術差距（單一頻段、未實現通感一體化波形設計、系統規模為校園級）列為研究限制。

3.4 6G 定位技術標準之不確定性處理

截至本文撰寫時，3GPP 尚未正式發布 6G 技術規範，6G 網路架構、頻譜配置與感測功能整合等關鍵技術參數尚未獲得標準層面的最終確認。該項技術標準的未定性構成本研究在方法論上必須正面處理的不確定性來源。

本研究的技術假設基礎來自兩個層面。第一，3GPP Release 18 與 Release 19 中與 AI/ML 相關之研究項目的階段性產出——3GPP 自 Release 18 起已正式將 AI/ML 納入無線網路功能的標準化範疇，啟動涵蓋定位增強等多個應用場景的研究項目，並在 Release 19 中進一步深化 AI/ML 模型生命週期管理的技術框架討論。第二，學術文獻中對 6G 定位技術發展方向的廣泛共識——ISAC 作為核心架構、Massive MIMO 與 RIS 作為關鍵使能技術、深度學習作為定位演算法主流範式等技術判斷，已在國際研究社群中形成高度共識 [1, 2, 8, 48]。

框架採模組化結構因應此不確定性，刻意區分為兩個可獨立演化的層次。治理邏輯層承載核心治理原則——生命週期階段劃分、三元分類架構、風險分級方法論、PDCA 方法論——植根於 ISO 標準體系，其有效性不依附於特定 6G 技術參數，具備跨技術世代的穩定性。技術參數層承載與特定技術規格耦合的實施細節——頻段選擇對資料品質策略的影響、特定 AI 模型的效能評估指標、通道量測的具體前處理規範、部署場域的效能基線設定。當 3GPP 正式發布 6G 技術規範後，組織僅需更新技術參數層而治理邏輯層不受影響。

然而，若 6G 最終標準在架構層面引入根本性的範式變革——例如完全顛覆 ISAC 概念或採納截然不同的感測技術路線——則治理邏輯層中

與特定架構假設耦合的部分設計仍可能需要結構性修正。本研究對此殘餘不確定性予以明確承認，列為研究限制的討論範疇。

4. 6G 無線定位 AI 系統之 ISO/IEC 42001 治理框架

4.1 6G 定位 AI 系統之治理特殊性分析

本節以跨領域比較矩陣為核心分析工具，將 6G 無線定位與自動駕駛、醫療 AI、智慧製造沿五個治理維度進行系統性比較。維度係基於 ISO/IEC 42001 [12] 附錄 A 的核心治理關切、AI 治理文獻的差異化因素 [11, 36]，以及第 2.1.4 節之五項技術特性。

在資料來源特性方面，6G 定位仰賴的 CSI、接收訊號強度指標（Received Signal Strength Indicator, RSSI）與到達時間等訊號特徵，本質上受制於多徑衰落、遮蔽效應與散射體移動等隨機物理過程，即便在相同物理位置的不同時刻量測結果也可能呈現顯著差異，資料品質管控面臨結構性困難 [48]，根源在於資料來源的物理本質而非管理流程不完善。相較之下，自動駕駛的感測資料主要來自光學攝影機與光達等結構化感測器，資料的可重現性與品質可控性顯著較高；醫療 AI 的輸入資料雖存在標註品質挑戰，但資料採集過程本身具有高度標準化的臨床規範；智慧製造的感測資料多來自受控廠房環境中的工業級感測器，具備相對穩定的訊雜比。

在隱私風險本質方面，位置資料的空間連續性與時序關聯性使傳統匿名化手段面臨根本性限制——攻擊者可藉由軌跡推論從形式上已匿名化的資料中反向還原個體身份 [8]。相較之下，自動駕駛的隱私風險屬離散型視覺問題、醫療 AI 受成熟法規規範 [49]、智慧製造的隱私風險相對較低。6G 定位的特殊性在於資料連續性本質從根本上限制了匿名化有效性，使隱私保護必須從系統架構層級加以設計。

在即時性約束方面，毫秒級推論延遲壓縮了人為監督的介入空間，在安全關鍵應用中系統幾乎不容許人為審核所致的額外延遲。自動駕駛已發展出 SAE 自動化等級的分級監督框架 [50]，醫療 AI 多數情境容許醫師獨立判斷 [49]，但 6G 定位的此項張力在通用治理框架中尚未獲充分設計回應。

在部署環境異質性方面，同一系統在不同頻段與環境類型中所面對的通道特性、干擾模式與風險樣態截然不同 [2, 3]，頻段特性與場域類型的交互作用使治理須具備動態調適彈性。

在模型漂移驅動因素方面，物理驅動因素與無線通道隨機性高度耦合，偵測與歸因需同時具備通訊工程與 AI 監控的雙重知識 [30, 31]，此跨學科監控需求在對照領域中未見同等耦合複雜度。上述五項治理維度的跨場域比較結果，整理如表 1。

表 1　跨場域治理特殊性比較矩陣

圖例：■ 高（深色）　■ 中（灰色）　□ 低（淺色）

場域	D1 資料來源	D2 隱私風險	D3 即時約束	D4 部署異質	D5 漂移驅動	高需求數
6G 無線定位	高	高	高	高	高	5/5
自動駕駛	中	中	高	中	中	2/5
醫療 AI	低	高	低	低	低	1/5
智慧製造	中	低	中	中	中	0/5

4.2 風險評鑑與生命週期治理對應

4.2.1 利害關係者需求分析與風險分級

依 ISO/IEC 42001 第 4 條要求 [12]，6G 定位 AI 系統的利害關係者需求分析須鎖定三個核心議題：位置資料的個資敏感性使隱私保護成為底線要求；特定應用情境的安全關鍵性要求更高可靠性標準；不同垂直領域的法規要求存在實質落差 [18]。利害關係者範圍不應限於直接使用者，尚須涵蓋被動受影響的資料主體、技術供應鏈各環節參與者，以及對定位資料具潛在使用需求的第三方機構（如緊急救難單位）。各利害關係者的需求與風險容忍度可能存在衝突，治理框架須提供結構化的協調與決策機制。

風險分類歸入四類：資料品質風險（場域偏差、標註謬誤、資料代表性不足）、模型風險（效能漂移、對抗脆弱性、可解釋性缺失）、系統風險（精度劣化、服務中斷、安全事故）與合規風險（隱私侵害、跨境規範衝突） [8, 37]。風險分級援引 ISO/IEC 23894:2023 之「發生可能性×影響嚴重度」評估方法論 [51]，影響嚴重度須特別考量位置資料洩露的不可逆性、定位精度退化在安全關鍵應用中的連鎖效應，以及跨境部署中法規差異的合規風險放大效應。評鑑結果決定後續控制措施的實施深度。整體治理生命週期之 PDCA 對應關係，視覺化呈現如圖 2。

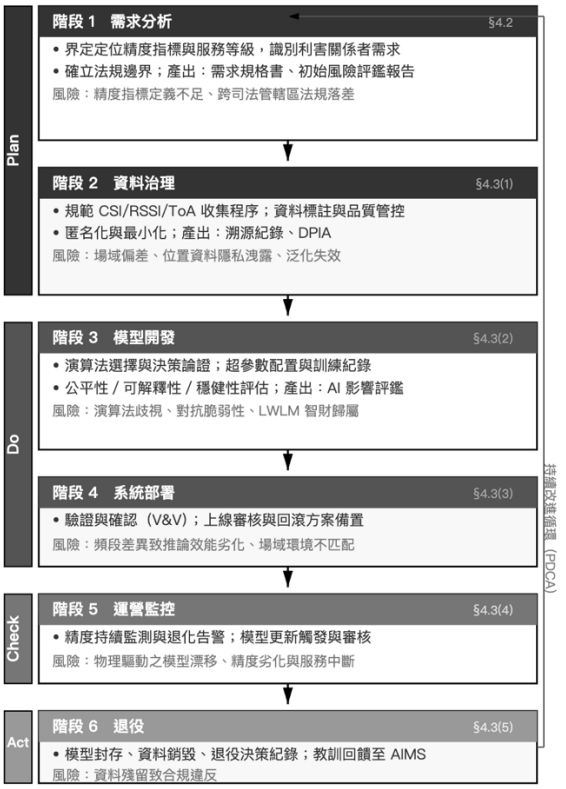

圖 2　6G 定位 AI 治理生命週期模型

4.2.2 生命週期各階段之治理對應

本節依 ISO/IEC 22989 [32] 六階段模型逐階段展開治理對應。

需求分析階段係整體治理週期的起點，須依目標應用領域界定定位精度、延遲容忍、可靠度與覆蓋範圍等關鍵效能指標（Key Performance Indicator, KPI），辨識適用的法律與法規約束（包括個人資料保護法規、電信法規與產業安全規範），完成利害關係者的系統性辨識與需求分析。利害關係者的範圍在 6G 定位脈絡下可能涵蓋終端使用者（被定位者）、場域管理方、系統開發團隊、電信營運商、設備供應商、個資保護主管機關以及可能受定位結果影響的第三方（如室內空間中的訪客）。各利害關係者的需求與期望可能相互衝突——例如場域管理方追求最高精度的人流分析，而被定位者則關注隱私保護與知情同意——須在此階段建立協調機制與優先順序判定準則。

資料治理階段攸關定位 AI 系統的品質根基。須規範 CSI、RSSI 與 ToA 等量測資料的標準化收集程序，明確量測設備校準要求、空間採樣密度與時間採樣策略，維護參考點座標標註的精確性與一致性，並系統性地評估資料集是否充分涵蓋不同時段、人員密度與環境配置等多樣化條件。無線通道的高度隨機性使資料品質管控面臨先天結構性挑戰，須建立品質度量指標與資料溯源（data provenance）機制，完整記錄資料的收集環境、前處理步驟與版本沿革。位置資料的個資敏感性決定了匿名化、去識別化與資料最小化原則不可或缺，組織宜於資料收集之初即依循隱私保護設計（privacy by design）原則將保護機制嵌入管理流程。然而，位置資料的空間連續性使隱私保護不應簡化為一次性匿名化處理——傳統匿名化手段（k-匿名性、空間模糊化）難以抵禦軌跡推論攻擊，差分隱私機制面臨隱私預算校準與效用損耗的權衡困境 [27, 28, 29]，須建立涵蓋匿名化有效性評估、殘餘風險量化與持續監控的多層次防護機制。

模型開發階段須保障每一項設計決策皆留下可追溯紀錄。演算法選擇須附決策論證——例如選擇 CNN 而非傳統指紋匹配方法的理由須涵蓋效能比較數據、計算資源考量與場域適配性分析。訓練過程須完整記錄超參數配置、資料分割策略、收斂軌跡與早停條件。效能評估須跨越多向度：定位精度的統計分析（平均誤差、百分位誤差、累積分布函數）為基礎指標；公平性評鑑考察不同空間區域、不同時段與不同使用者群體間的定位精度是否存在系統性落差；可解釋性分析探究模型所學習的關鍵 CSI 特徵及其與物理傳播路徑的對應關係，協助開發者理解模型決策機制而非僅依賴黑箱輸出；對抗穩健性測試評估模型在惡意干擾（如訊號欺騙攻擊或對抗樣本注入）下的抗擾能力。此外，須依 ISO/IEC 42001 [12] 要求執行 AI 系統影響評鑑，系統性評估定位系統對資料主體、相關利害關係者與社會層面的潛在正面與負面影響。

系統部署階段係 AI 定位系統從開發環境遷移至運營場域的關鍵轉折點。須完成正式驗證與確認（Verification and Validation, V&V）程序，確保系統在目標場域條件下滿足預定效能指標，V&V 結果應明確記錄測試場景、通過準則與實際表現。須建立場域專屬效能基線——此基線不應僅為單一數值，而應包含不同空間區域、不同時段與不同人員密度條件下的分層基線，作為後續運營監控的參照錨點。備妥回滾方案以確保部署失敗或嚴重性能退化時能安全回復至上一穩定版本。頻段差異與場域環境特性對模型推論的影響構成額外的部署評估考量——同一模型在不同頻段或建築結構中的表現可能呈顯著差異 [3]，部署評估須包含場域專屬的適配性驗證，必要時進行遷移學習或微調。使用者告知義務要求向資料主體明確揭露定位服務的存在、資料收集範圍與處理目的；操作能力培訓確保營運人員理解系統的能力邊界與例外處理程序，避免對 AI 輸出的過度信賴或不當使用。

運營監控階段須建立主動式精度持續監測機制，而非被動等待使用者投訴方才啟動排查。場域內物件移動、人員活動模式改變、季節性環境變化（如空調運轉模式切換對電磁環境的影響）與硬體老化（天線增益衰減、RIS 面板反射特性偏移），皆可能使通道特性偏離訓練分布假設。

須明確定義精度退化的告警閾值與模型更新的觸發條件——觸發條件的設計須將物理環境變化納入考量，而非僅依賴統計指標偏移偵測。機器學習系統在生產環境中面臨的隱性技術債務——包括監控盲區、未測試的程式碼路徑與隱式回饋迴路——進一步增加了運營監控的複雜度 [40]。每次模型更新均須經同等嚴謹的驗證程序，包括更新前後的效能對比測試與回歸驗證，確保更新不會在改善特定區域精度的同時引入其他區域的退化 [48]。完整的運營日誌——涵蓋系統效能指標、環境變化事件紀錄與維運操作紀錄——是支持事後稽核與根因追溯的基本條件。

退役階段無論退役原因為何——效能長期未達門檻、替代方案就緒、底層技術汰換或法規環境變遷——決策過程均須經正式記錄與核准，形成可追溯的退役決策文件。退役模型依組織政策妥善封存，保存模型權重、訓練資料描述、版本沿革與效能紀錄，以備後續稽核或法律調查之需。訓練資料的保存期限與銷毀程序須嚴格遵循適用的個資保護法規——位置資料的銷毀須確認涵蓋所有備份副本與衍生資料集。退役過程中的經驗教訓——包括模型在運營期間遭遇的典型漂移模式、曾觸發更新的環境變化事件、隱私治理措施的有效性評估——應有系統地回饋至組織 AI 治理流程，形成 PDCA 循環中 Act 階段的實質輸入，使下一代系統的治理設計能受益於前代系統的運營經驗。

4.3 控制措施對應矩陣與實施指引

「控制措施群組×生命週期階段」二維對應矩陣（如表 2 所示）為本文核心產出之一。矩陣的列對應附錄 A 各控制措施群組，欄對應六個生命週期階段，每一交叉格標示適用類型並附說明，使實務工作者得以全局性掌握治理覆蓋圖像。實施指引從三個層面展開。

表 2　控制措施群組 × 生命週期階段對應矩陣

圖例：● 直接適用　◑ 情境化調適　○ 領域延伸　— 不適用

生命週期階段	G1 政策治理	G2 評鑑透明	G3 資料品質	G4 生命週期	G5 供應監控	G6 安全隱私
1. 需求分析	●	◑	—	●	●	◑
2. 資料治理	●	◑	○	●	◑	○
3. 模型開發	●	●	◑	●	◑	◑
4. 系統部署	●	◑	◑	◑	●	◑
5. 運營監控	●	○	○	◑	●	○
6. 退役	●	●	—	●	◑	○

組織層面：制定正式 AI 治理政策，明確宣示治理目標與適用範圍，建構權責清晰的組織架構。6G 定位 AI 系統的跨領域特性要求人員兼具 AI 技術知識、6G 通訊工程基礎與治理法規素養，組織宜將 AI 倫理原則、ISO/IEC 42001 要求及領域專屬知識納入能力發展計畫 [12, 18]。

技術層面：建置資料目錄與資料血緣追蹤系統，實施角色存取控制與加密保護；將對抗穩健性測試納入標準驗證程序，推論介面防護應防範未經授權的存取與惡意輸入攻擊；所有關鍵系統決策均須完整記錄以支持事後稽核。ISO/IEC 42001 [12] 與 ISO/IEC 27001 的整合優勢於此層面特別顯著——組織可將既有資訊安全控制措施直接延伸至 AI 定位系統 [52]。

合規層面：建立動態法規監測機制，持續追蹤歐盟 AI 法案、各地個資保護法規及 3GPP 標準演進 [10, 38]。內部稽核定期檢視 AIMS 運作成效。6G 定位的跨境特性使同一系統可能同時適用歐盟 GDPR [54]、各國電信監管規範與在地個資保護法規，須在治理規劃之初即納入系統性考量。

4.4 領域延伸措施之論證

本節論證四項超出 ISO/IEC 42001 [12] 現有條款覆蓋範圍、但 6G 定位領域必須額外補充的治理機制。

第一項：物理驅動模型漂移之專屬監控機制。 6G 定位精度退化往往源於場域結構改變、散射體移動與硬體老化等物理成因 [48]。附錄 A 的持續監控條款主要針對一般性模型效能追蹤，未將物理環境變化納入觸發條件。延伸措施要求建立雙軌監控：一軌追蹤統計效能偏移，另一軌系統性記錄與偵測物理環境變化事件——如場域結構改建、大型設備遷移或 RIS 面板配置調整——並將此類事件設為模型重新驗證的強制觸發條件。定位於運營監控階段，但監控參數的初始設定須回溯至部署階段的效能基線建立程序。

第二項：空間連續性位置資料之專屬隱私治理機制。 位置資料的空間連續性使傳統匿名化面臨根本性限制 [8]。附錄 A 的資料管理措施未針對空間連續性資料提供專屬治理設計。延伸措施要求在資料治理階段導入空間匿名化有效性的量化評估程序——以重新識別風險指標衡量殘餘隱私風險，據此決定是否採取差分隱私機制或空間解析度降階。此措施貫穿資料治理與運營監控兩階段。

第三項：即時性約束下人為監督之分級設計。 毫秒級推論延遲與人為監督原則之間存在結構性張力。附錄 A 的人為監督措施未針對即時性極嚴苛的應用情境提供分級化指引。延伸措施依安全關鍵性等級建立三級架構：低關鍵性應用（如校園空間分析）採事後審查模式；中關鍵性應用（如室內導航）採異常觸發介入模式；高關鍵性應用（如緊急救援定位）須設計自動安全降級機制——系統信心度低於閾值時自動切換保守模式或觸發人員確認程序。橫跨模型開發、部署與監控三階段。

第四項：跨頻段與跨領域部署之治理一致性管理機制。 同一系統在不同頻段與場域類型中的通道特性、風險樣態截然不同 [2, 3]。附錄 A 未提供跨異質部署環境維持治理一致性的操作指引。延伸措施要求建立部署環境分類登錄制度，為每一類別設定專屬效能基線、風險評鑑參數與監控閾值。模型跨環境遷移時須啟動遷移適配驗證程序。主要定位於部署與監控階段，但分類架構須在需求分析階段即予規劃。

上述四項措施分別回應模型漂移監控、位置隱私保護、人為監督設計與跨環境部署管理的特殊治理需求，不僅帶來可操作的補充機制，更標示出 ISO/IEC 42001 [12] 在高度技術特殊性場域的適用邊界。

4.5 PDCA 持續改進迴路

PDCA 循環使框架從靜態檢核清單轉化為自我修正的動態迴路，賦予治理體系因應環境變化的持續適應能力。Plan 階段完成風險評鑑與治理規劃，基於利害關係者需求分析與風險分級結果，將四項領域延伸措施連同附錄 A 適用控制措施一併納入適用性聲明（Statement of Applicability），確立治理實施的藍圖。Do 階段依生命週期模型逐階段實施治理活動——從需求分析的約束條件界定、資料治理的品質管控與隱私保護措施建立、模型開發的可追溯紀錄、部署的 V&V 程序，到運營監控的主動式精度追蹤與退役的經驗回饋。Check 階段包含三條並行的回饋路徑：第一，運營監控的漂移偵測觸發模型重新驗證，驗證結果回饋至風險評鑑以更新風險等級——若物理驅動漂移的頻率或嚴重度超出預期，須上調對應風險項目的等級；第二，內部稽核依預定排程檢視控制措施的完整性與有效性，辨識實施落差與改進機會；第三，外部環境變化——如 3GPP 新版規範發布、歐盟 AI 法案 [10] 實施細則更新、地方個資保護法規修訂——觸發風險評鑑的強制更新，確保治理體系與外部規範環境保持同步。Act 階段依 Check 發現採取矯正措施：技術層面啟動模型更新或資料補充，制度層面修訂對應矩陣或補充延伸措施，將改進成果回饋至下一輪 Plan 階段形成閉環。觸發條件的量化閾值設定、稽核頻率最適化與回饋路徑的組織嵌入，有待後續行動研究進一步操作化。

4.6 治理框架量化評估指標

為使框架的治理成效得以系統性量測並回饋至 PDCA 循環之 Check 階段，本節提出五項可量化評估指標，分別對應控制措施實施成熟度、領域延伸措施有效性與整體治理績效三個層次。

第一，控制措施實施覆蓋率（Control Implementation Coverage Rate, CICR）：定義為已實施之控制措施數除以適用清單內控制措施總數，反映 AIMS 的實施完整性。建議目標值 ≥ 90%。

第二，物理驅動漂移觸發響應時間（Physics-driven Drift Response Time, PDRT）：定義為自物理環境變化事件登錄至模型重新驗證啟動之時間差，反映第一項領域延伸措施的運作效能。建議目標值 ≤ 7 日。

第三，重新識別風險指數（Re-identification Risk Index, RRI）：依空間軌跡資料的 k-anonymity 與差分隱私 ε 參數綜合評估，反映第二項領域延伸措施對位置隱私的保護強度。建議閾值由組織依適用法規與資料敏感性決定。

第四，人為監督介入妥適率（Human Oversight Engagement Rate, HOER）：依安全關鍵性等級分層計算實際介入次數佔應介入事件之比例，反映第三項領域延伸措施的設計妥適性。建議低關鍵性 ≥ 95% 事後審查覆蓋、高關鍵性 100% 觸發自動降級。

第五，跨環境治理一致性指數（Cross-environment Governance Consistency Index, CGCI）：以同一 AIMS 下不同部署環境間控制措施實施差異程度衡量，反映第四項領域延伸措施的架構穩定性。

上述指標僅為框架評估的初步量化嘗試，目標值之普適合理性有待進一步多場域實證資料校準，列為研究限制與未來工作之一。

5. 框架應用、跨場域分析與適用性評估

5.1 校園定位系統治理分析

四項領域延伸措施在校園案例中的展示覆蓋程度各異。物理驅動模型漂移監控獲實務觀察支持——學期轉換引發之精度退化時序觀察提供初步實務證據，教學大樓區域於學期中之平均定位誤差，相較寒暑假基線呈現一致性的上升趨勢（基於試運營期間之巡檢式抽樣比對），且退化與恢復的時間節點均與學生人流變化具清晰的時序對應關係。空間連續性隱私治理已有初步實施措施，包含隱私風險評估程序的建立與去識別化設計的導入，但尚未進行量化的重新識別風險評估。人為監督分級設計為概念層面展示——校園定位應用屬中低安全關鍵等級，採事後審查模式即為適當，高關鍵性情境下的自動安全降級機制僅完成設計論證，有待安全關鍵場域的實際驗證。跨頻段治理一致性因系統僅運作於單一 sub-6 GHz 頻段而未能展示實際的跨頻段治理操作，為最主要的覆蓋缺口，此項延伸措施的可操作性須待多頻段部署環境方能獲得實證檢驗。

需要明確指出的限制是，校園定位系統在風險等級上屬中低層級——定位失誤不會直接危及人身安全——因此對框架中高風險治理機制（如自動安全降級與獨立第三方部署審核）的展示深度受到客觀限制，第 5.3 節以智慧工廠進行對照補充。

本節依框架的六階段生命週期結構，逐階段展示控制措施在校園系統中的操作方式。在需求分析方面，利害關係者需求盤點揭示，校方對空間使用數據的管理需求與師生對位置隱私的保護期待之間的平衡，構成最具代表性的治理課題。校方期望藉由定位資料進行教室使用率分析、圖書館座位規劃與緊急疏散動線最佳化，而學生與教職員則對個人行蹤被持續追蹤表達合理疑慮。框架據此要求在需求階段即將隱私保護納入系統設計的核心約束條件，而非事後附加的補救措施。

在資料治理方面，教學大樓走廊在上下課時段的人員密度劇烈波動，導致同一參考點的 CSI 特徵呈顯著差異——上課期間走廊淨空時的通道測量與下課人潮湧出時的測量結果幾乎無法視為同一分布——構成場域偏差的具體樣態；圖書館因書架配置穩定而呈較高資料一致性，但假期閉館期間與學期中開放時段的環境差異仍需納入考量；學生活動中心因兼具餐飲與社團等多元功能，人員密度與活動模式的時間尺度變異（從小時級到學期級）使其成為資料品質管控難度最高的區域。框架要求建立分時段、分區域的資料採集策略——每一區域的採樣計畫須涵蓋典型與非典型使用模式——並維護完整的資料溯源紀錄，確保每筆訓練資料可回溯至其採集時間、環境條件與前處理步驟。隱私保護方面，校方依框架建議採取多層次防護策略：即時定位結果僅以區域層級（如「圖書館二樓」）呈現於管理介面，不向非授權人員揭露精確座標；原始 CSI 資料設定保留期限上限，逾期自動清除；具備存取紀錄的角色型權限控制確保僅授權人員得以接觸原始量測資料。

在模型開發方面，CNN 架構的選擇經記錄決策論證——基於其在多徑環境下從 CSI 特徵學習空間映射的效能優勢，以及在同類研究中已獲廣泛驗證的穩健表現 [5]。決策論證同時記錄了未採用的替代方案（如傳統指紋匹配法、基於圖神經網路的方法）及其未被選擇的具體理由。訓練過程依框架要求完整記錄超參數配置、資料分割策略（按時段與區域分層抽樣）與收斂軌跡。公平性評鑑發現教學大樓走廊與學生活動中心之間存在系統性精度落差——前者的平均定位誤差顯著低於後者——歸因於訓練資料的分布不均衡：教學大樓因結構規律、參考點設置密集而具有較充分的訓練資料覆蓋，學生活動中心因環境複雜度高且人員活動模式多變而資料品質較不穩定。此發現據此回饋至資料治理階段，啟動針對學生活動中心的補充資料採集計畫，展現了框架生命週期各階段之間的回饋機制在實務中的運作。

在運營監控方面，試運營階段的系統資料呈現了具實務參考價值的觀察發現：教學大樓定位精度在學期中與寒暑假期間存在可觀察之差異——學期中日間平均定位誤差較寒暑假基線呈現一致性的上升趨勢（試運營期間巡檢式抽樣觀察所得，未進行系統性量化記錄），且退化在開學後一至兩週逐步浮現，與學生回流的時序吻合；寒暑假開始後約一週精度自行回復至接近基線水準。此為物理驅動模型漂移的實務佐證：精度退化的根源指向物理環境的週期性變化而非模型缺陷，且退化與恢復的時間尺度均與物理環境變化事件具可追溯的對應關係。系統據此設定季節性效能基線調整排程，並將學期轉換視為重新驗證的觸發事件——此為第一項領域延伸措施在真實營運環境中獲得初步實務佐證的具體案例。

5.2 實施效益與挑戰

框架帶來的效益包括：風險前置辨識使組織能在設計階段即嵌入保護措施，降低運營期間隱私侵害或精度退化造成服務中斷的發生機率；PDCA 循環與文件化要求建立了跨部門協調的共同語言與制度化溝通平台，資訊中心、開發團隊與校方管理層得以釐清各自權責與協作介面 [18]；依循 ISO/IEC 42001 [12] 建立治理機制有助鞏固師生對定位服務的信任基礎，透明的治理文件化提供了信任所需的制度性保障。

實施挑戰方面：大學行政資源的配置優先序與營利企業截然不同，專職投入 AI 治理的人力與預算難以獲充足保障；校園環境隨學期節奏劇烈波動增加監控複雜度，如何區分「正常季節

性波動」與「需介入的異常退化」有賴足夠的運營週期經驗校準；6G 定位 AI 系統所需的跨領域人才（通訊工程、AI 技術、法規治理）極為稀缺，短期內依賴跨職能團隊協作較為務實；學術開放文化與位置資料存取控制要求之間存在理念摩擦，須在治理政策中建立透明的例外審查機制加以調和。

5.3 跨領域適用性初探：智慧工廠對照分析

智慧工廠的選取基於兩項考量：（1）風險等級顯著高於校園——AGV 導航定位失誤可能直接造成人員傷害或設備碰撞，屬安全關鍵等級，對治理嚴格度的要求遠高於校園場景；（2）ISO 認證體系接受度高——製造業對 ISO 認證體系的接受度與導入經驗較高，組織已具備管理系統運作的制度基礎。

第一個面向考察控制措施的實施強度升級。部署審核須從校方內部聯合執行升級為獨立第三方驗證，並須依據工業安全標準進行額外的安全性確認；漂移監控告警閾值須更嚴格——校園中次公尺級精度的短暫波動或許僅影響空間分析的參考價值，但工廠中公分級偏移即可能使 AGV 偏離安全路徑或機械手臂錯位；人為監督須採最高等級的自動安全降級機制，系統信心度低於閾值時自動停止 AGV 移動而非僅發出告警。上述升級均不涉及框架結構的重新設計，而是在既有框架的參數空間內調整實施強度，顯示框架具備足夠的彈性範圍。

第二個面向辨識新風險樣態：AGV 碰撞事故的安全責任歸屬需在需求分析階段透過利害關係者協議明確界定——是定位系統提供方、AGV 控制軟體廠商還是工廠營運方承擔主要責任；工業環境的電磁輻射與金屬結構強反射對通道傳播的影響遠較校園劇烈 [48]，可能需要更頻繁的模型重新校準排程；員工定位涉及勞動權益隱私，工會或員工代表的治理參與權可能需要額外的利害關係者協調機制。這些新風險樣態可在既有風險分類架構下增補場域專屬項目，而非需要框架結構的重建，此為模組化設計策略在跨領域遷移中的具體體現。

第三個面向評估跨領域可遷移性。治理邏輯層——生命週期六階段劃分、三元分類架構、PDCA 方法論、四項延伸措施的設計原則——在跨領域遷移時展現高度穩定性。物理驅動漂移監控的設計原則同樣適用於工廠環境，僅需將物理環境變化事件從「學期轉換」替換為「生產線配置調整」或「廠區佈局變更」等製造業特有的觸發事件。空間連續性隱私治理的核心邏輯在員工定位場景中同樣成立；勞動法規對員工監控的額外限制，甚至要求更嚴格的隱私保護措施。主要需再調適的是效能基線、告警閾值、觸發條件與監控頻率等技術參數，依各場域的安全關鍵性等級與產業特性重新校準。此項觀察支持框架「治理邏輯層穩定、技術參數層可調」的模組化設計策略——組織跨場域遷移時，可保留既有的治理流程架構，僅需針對場域專屬風險特性與技術參數進行局部調整，有效降低跨場域導入的邊際成本。

初步論斷：框架在結構設計上具備跨領域可擴展性，模組化設計獲初步實證支持。然而，此項論斷僅基於校園與工廠兩個場域的紙面對照分析，尚未經歷真實工廠環境中的完整導入與迭代驗證。

5.4 與既有文獻之比較

本框架逐項填補第 2.2.2 節辨識之三重缺口。針對 Leon [39]的物理驅動漂移監控缺失，本框架所建構的雙軌監控機制——以統計效能偏移追蹤與物理環境變化事件偵測並行運作——透過將學期節奏性轉換設定為強制重新驗證的觸發條件，使物理驅動的漂移風險獲主動治理回應。校園案例中教學大樓精度隨學期節奏波動的時序觀察，為此一監控設計提供了直接的實證支持，驗證了物理環境的週期性變化確實是定位精度退化的可辨識驅動因素。針對 Mäntymäki 等學者 [36]的領域適配不足，空間連續性隱私治理機制將傳統匿名化的一次性處理升級為涵蓋有效性評估與持續監控的多層次防護，跨頻段治理一致性機制則以部署環境分類登錄與遷移適配驗證回應部署異質性的結構性缺漏，兩項延伸措施分別填補隱私治理與跨環境部署管理的治理空白。針對 Mert 等學者 [17]從原則到實踐的轉化斷裂，框架以控制措施矩陣與三個層面的實施指引建立制度化橋樑——以公平性原則為例，校園案例中據此發現跨區域精度落差並回饋至資料治理階段，使公平性從抽象宣示轉化為「以統計方法比較跨區域精度分布，差異顯著時觸發資料補充與模型重訓練」的可稽核操作程序，展現了框架將倫理原則落地為治理實踐的轉化能力。

6. 結論

本研究以 ISO/IEC 42001:2023 [12] 為制度基礎，建構了適用於 6G 無線定位 AI 系統的全生命週期治理框架，依循「文獻分析→框架建構→應用情境展示→跨領域討論」的邏輯主軸推進。

研究核心發現。 第一，跨領域比較分析表明，6G 定位 AI 系統的五項技術特性——無線通道隨機性、位置資料空間連續性、即時性約束、跨頻段異質性與物理驅動模型漂移——其交叉疊加效應使 6G 無線定位呈現各維度治理需求同時偏高的組合模式，此特徵在對照領域中並未觀察到同等程度的多維度耦合複雜度，為建構領域專屬治理框架提供了充分的必要性基礎。第二，ISO/IEC 42001 [12] 經情境化調適後具備回應 6G 定位治理需求的制度能力——附錄 A 多數控制措

施經調適後能有效覆蓋各生命週期階段的核心治理需求，PDCA 循環為因應無線環境的時變性與 6G 標準的持續演進提供了適切的制度回應機制，此發現確認以 ISO/IEC 42001 為治理錨點的方法論選擇具有合理性。第三，辨識出四項超越現行標準條款範圍的領域延伸措施——物理驅動模型漂移監控、空間連續性位置資料隱私治理、即時性約束下人為監督分級設計、跨頻段與跨領域部署治理一致性管理——標示出通用 AI 管理系統標準在高技術特殊性場域的適用邊界，並就邊界之外提供具體且可操作的補充治理方案。第四，校園展示初步確認框架可操作性——學期轉換引發的精度退化為物理驅動漂移監控提供了初步實務佐證；智慧工廠對照分析支持治理邏輯層的跨領域穩定性，模組化設計使框架能在保留核心結構的前提下適配不同場域需求，但第四項延伸措施（跨頻段治理一致性）仍停留在概念推導階段，尚待多頻段部署環境的實證檢驗。

管理實務意涵。 框架為電信業者與技術服務提供商提供了導入 ISO/IEC 42001 [12] 認證的結構化路徑，控制措施矩陣使組織能系統性辨識治理覆蓋的缺口，並依風險分級配置有限的治理資源。三元分類（直接適用、情境化調適、領域延伸）的設計使組織能依據自身的成熟度與資源條件，採取漸進式的治理導入策略——優先實施「直接適用」類措施以快速建立治理基礎，繼而處理需要專業調適的「情境化調適」類措施，最後投入資源開發「領域延伸」類的專屬治理機制。對 AI 開發團隊而言，生命週期治理對應機制可作為嵌入式治理設計（governance by design）的實務參照，使治理考量從專案後期的合規檢查前移至系統設計階段。對標準制定組織，控制措施對應分析方法提供了可複製的方法論程序，可應用於其他新興技術領域（如邊緣運算 AI、衛星通訊 AI 等）的治理框架建構。

研究限制。 框架評估以應用展示與紙面對照為主，原規劃之領域專家評估未能完成，缺乏外部效度檢核——就 DSR 方法論而言，案例展示已達 FEDS 框架中 Quick & Simple 策略的評估要求，但尚不足以宣稱框架經過完整的外部效度驗證。展示僅涵蓋單一校園領域與非安全關鍵風險等級，高風險治理機制（如自動安全降級與獨立第三方部署審核）的可行性，僅透過工廠場域對照進行了初步推論，尚未經真實安全關鍵環境的實際驗證。分析基於數月試運營資料，長期效應——如多年期硬體老化對模型穩健性的累積影響、隱私治理措施在使用者基數擴大後的承載能力——待追蹤。分類判定未採雙重編碼程序計算編碼者間信度，單一研究者的主觀判斷可能影響邊界案例的歸類一致性。ISO/IEC 42001 [12] 與 3GPP 6G 標準均在演進中，框架的部分技術假設可能需隨標準更新而修正，模組化設計旨在緩解但無法完全消除此項風險。此外，真實安全關鍵環境之實證驗證為本框架完整性之關鍵欠缺：本研究受限於 6G 技術尚未正式商用、智慧工廠等高風險場域導入需取得廠房存取與安全認證等多重門檻，故本輪迭代僅能以紙面對照分析作為跨領域延伸的初步檢驗。完整的真實場域驗證應由產學合作研究項目接續執行，包括：（1）多場域多月期之導入式實驗；（2）AGV 安全事件模擬下的自動降級機制效能驗證；（3）跨頻段（sub-6 GHz、毫米波）部署環境的治理一致性實證。此項驗證工作已列為下一輪設計迭代之核心目標。另就第 5.1 節所述教學大樓學期／假期定位精度差異之觀察，本輪資料係以試運營期間之巡檢式抽樣比對所得，未進行系統性量化記錄、未計算樣本統計量，亦未實施統計顯著性檢定，故僅作為物理驅動模型漂移之趨勢性實務觀察呈現；其精確誤差增幅、信賴區間與時序模型之嚴謹量化，列為下一輪迭代之優先實證項目。

未來研究方向。 第一，邀請具備 AI 治理、6G 通訊與產業實務背景之領域專家，對控制措施矩陣與延伸措施進行獨立適用性評估，補強本研究缺失之外部效度。第二，以行動研究法在多場域（含安全關鍵場域）進行完整導入與迭代改進，對應 FEDS 框架升級至 Human Risk & Effectiveness 策略。第三，開發自動化治理工具——例如與運營監控系統整合的漂移偵測儀表板、自動化合規檢核清單——以降低實施門檻並提升治理效率。第四，將框架擴展至 6G 網路中的其他 AI 應用領域，如 AI 輔助通道估計、AI 驅動網路資源管理等，檢驗治理邏輯層的泛化能力。第五，探索與代理型 AI（agentic AI）治理框架的整合路徑，因應 AI 系統自主性攀升所衍生的治理挑戰——當定位系統從被動推論工具演進為具備自主決策能力的代理時，人為監督的設計邏輯可能需要根本性的重新思考。

綜合而言，本研究的貢獻定位為概念性治理框架的建構與初步適用性探索，係此一研究方向的第一輪設計迭代。在理論層面，本研究為填補 6G 定位技術與 AI 治理標準間的研究空白提供了概念性框架與方法論路徑示範——跨領域比較分析揭示了 6G 定位的複合治理特殊性，控制措施對應分析方法提供了可複製的標準適配方法論，四項領域延伸措施標示了通用標準的適用邊界。在實務層面，控制措施矩陣與三層次實施指引為電信業者、校園管理機構與系統開發商等產業利害關係者提供了可參照的治理架構雛型，模組化設計確保框架能隨 6G 標準演進而持續更新。在標準發展層面，本研究為 ISO/IEC 等國際標準組織未來發展領域專屬實施指引提供了系統性的分析參照，特別是四項延伸措施所揭示的治理缺口可作為標準修訂時的優先考量。

參考文獻

1. Liu F., Cui Y., Masouros C. et al.（2022）, “Integrated sensing and communications: toward dual-functional wireless networks for 6G and beyond.” IEEE Journal on Selected Areas in Communications, Vol.40, No.6, pp.1728-1767.

2. Lu S., Liu F., Li Y. et al.（2024）, “Integrated sensing and communications: recent advances and ten open challenges.” IEEE Internet of Things Journal, Vol.11, No.11, pp.19094-19120.

3. Mogyorósi F., Revisnyei P., Pašić A. et al.（2022）, “Positioning in 5G and 6G networks — a survey.” Sensors, Vol.22, No.13, 4757.

4. Saikia P., Singh K., Huang W.J. et al.（2024）, “Hybrid deep reinforcement learning for enhancing localization and communication efficiency in RIS-aided cooperative ISAC systems.” IEEE Internet of Things Journal, Vol.11, No.17, pp.29494-29510.

5. Chiu C.C., Wu H.Y., Chen P.H., Chao C.E. and Lim E.H.（2024）, “6G technology for indoor localization by deep learning with attention mechanism.” Applied Sciences, Vol.14, No.22, 10395.

6. Sonny A., Kumar A. and Cenkeramaddi L.R.（2024）, “A survey of application of machine learning in wireless indoor positioning systems.” arXiv preprint, arXiv:2403.04333.

7. Arrieta A.B., Díaz-Rodríguez N., Del Ser J. et al.（2020）, “Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI.” Information Fusion, Vol.58, pp.82–115.

8. Pan G., Gao Y., Gao Y., Yu W., Zhong Z., Yang X., Guo X. and Xu S.（2026）, “AI-driven wireless positioning: fundamentals, standards, state-of-the-art, and challenges.” IEEE Communications Surveys & Tutorials, Vol.28, Early Access (2026), IEEE Xplore document 11315904. (具體 No./pp./DOI 待 IEEE 正式刊出後補)

9. Salem H., Sadia H., Quamar M.M., Magad A., Elrashidy M., Saeed N. and Masood M.（2025）, “Data-driven integrated sensing and communication: recent advances, challenges, and future prospects.” ICT Express, Vol.11, No.4, pp.790–808, DOI: 10.1016/j.icte.2025.06.010.

10. European Parliament（2024）, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union.

11. National Institute of Standards and Technology（2023）, Artificial intelligence risk management framework (AI RMF 1.0), NIST AI 100-1, U.S. Department of Commerce.

12. ISO/IEC（2023）, ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system, International Organization for Standardization.

13. Jobin A., Ienca M. and Vayena E.（2019）, “The global landscape of AI ethics guidelines.” Nature Machine Intelligence, Vol.1, pp.389–399.

14. Floridi L., Cowls J., Beltrametti M. et al.（2018）, “AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations.” Minds and Machines, Vol.28, No.4, pp.689–707.

15. Mittelstadt B.（2019）, “Principles alone cannot guarantee ethical AI.” Nature Machine Intelligence, Vol.1, No.11, pp.501–507.

16. Morley J., Floridi L., Kinsey L. and Elhalal A.（2020）, “From what to how: an initial review of publicly available AI ethics tools, methods and research to translate principles into practices.” Science and Engineering Ethics, Vol.26, No.4, pp.2141–2168.

17. Mert M., Öz S. and Mert F.（2025）, “AI ethics for 6G: governance, global alignment, and responsible innovation.” Journal of Industrial Policy and Technology Management, Vol.7, No.2.

18. Benraouane S.A.（2024）, AI management system certification according to the ISO/IEC 42001 standard: how to audit, certify, and build responsible AI systems, Springer.

19. de Borba D. and Brinkhues R.（2025）, “Artificial intelligence in business process management: challenges, opportunities and strategies for alignment with ISO 42001.” Review of Artificial Intelligence in Education, Vol.6, pp.1-19.

20. Gregor S. and Hevner A.R.（2013）, “Positioning and presenting design science research for maximum impact.” MIS Quarterly, Vol.37, No.2, pp.337–355.

21. Qaisar M.U.F., Yuan W., Günlü O., Riihonen T., Cui Y., Zhang L., Gonzalez-Prelcic N., Di Renzo M. and Han Z.（2026）, “The role of ISAC in 6G networks: enabling next-generation wireless systems.” IEEE Transactions on Network Science and Engineering, Vol.13, pp.7825–7861, DOI: 10.1109/TNSE.2026.3666665.

22. 3GPP（2021）, TR 38.857 V17.0.0: Study on NR positioning enhancements, 3rd Generation Partnership Project.

23. 3GPP（2024）, TR 38.843 V18.0.0: Study on artificial intelligence (AI)/machine learning (ML) for NR air interface, 3rd Generation Partnership Project.

24. 3GPP（2024）, TS 38.305 V18.3.0: NG radio access network (NG-RAN); Stage 2 functional

specification of user equipment (UE) positioning in NG-RAN, 3rd Generation Partnership Project.

25. Kotturi S.P. and Ganti R.K.（2024）, “Centimeter positioning accuracy using AI/ML for 6G applications.” 2024 IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN), Stockholm, Sweden, pp.1–2, DOI: 10.1109/ICMLCN59089.2024.10624691.

26. Pan G., Huang K., Chen H. et al.（2025）, “Large wireless localization model (LWLM): a foundation model for positioning in 6G networks.” arXiv preprint, arXiv:2505.10134.

27. Shokri R., Theodorakopoulos G., Le Boudec J.-Y. and Hubaux J.-P.（2011）, “Quantifying location privacy.” Proceedings of the IEEE Symposium on Security and Privacy, pp.247–262.

28. Andrés M.E., Bordenabe N.E., Chatzikokolakis K. and Palamidessi C.（2013）, “Geo-indistinguishability: differential privacy for location-based systems.” Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), pp.901–914.

29. Primault V., Boutet A., Mokhtar S.B. and Brunie L.（2019）, “The long road to computational location privacy: a survey.” IEEE Communications Surveys & Tutorials, Vol.21, No.3, pp.2772–2816.

30. Lu J., Liu A., Dong F., Gu F., Gama J. and Zhang G.（2019）, “Learning under concept drift: a review.” IEEE Transactions on Knowledge and Data Engineering, Vol.31, No.12, pp.2346–2363.

31. Paleyes A., Urma R.-G. and Lawrence N.D.（2022）, “Challenges in deploying machine learning: a survey of case studies.” ACM Computing Surveys, Vol.55, No.6, Article 114.

32. ISO/IEC（2022）, ISO/IEC 22989:2022 Information technology — Artificial intelligence — Concepts and terminology, International Organization for Standardization.

33. Shneiderman B.（2020）, “Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems.” ACM Transactions on Interactive Intelligent Systems, Vol.10, No.4, Article 26.

34. Stahl B.C.（2021）, Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies, Springer.

35. Eitel-Porter R.（2021）, “Beyond the promise: implementing ethical AI.” AI and Ethics, Vol.1, No.1, pp.73–80.

36. Mäntymäki M., Minkkinen M., Birkstedt T. and Viljanen M.（2022）, “Putting AI ethics into practice: the hourglass model of organizational AI governance.” arXiv preprint, arXiv:2206.00335.

37. Liao S.M., Haykel I., Cheung K. and Matalon T.（2025）, “Navigating the complexities of AI and digital governance: the 5W1H framework.” Journal of Responsible Technology, Vol.23, 100127.

38. Buscemi A., Deckenbrunnen T., Kabir F., Mowla N. and Mishchenko K.（2025）, “Assessing high-risk AI systems under the EU AI Act: from legal requirements to technical verification.” arXiv preprint, arXiv:2512.13907v3 (April 2026).

40. Sculley D., Holt G., Golovin D. et al.（2015）, “Hidden technical debt in machine learning systems.” Advances in Neural Information Processing Systems 28 (NeurIPS 2015), pp.2503–2511.

41. Hagendorff T.（2020）, “The ethics of AI ethics: an evaluation of guidelines.” Minds and Machines, Vol.30, No.1, pp.99–120.

39. Leon R.（2025）, “Lifecycle-based governance to build reliable ethical AI systems.” Systems Research and Behavioral Science, Early View (published online 30 January 2026), DOI: 10.1002/sres.70014.

42. Fjeld J., Achten N., Hilligoss H., Nagy A.C. and Srikumar M.（2020）, Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for AI, Berkman Klein Center Research Publication No. 2020-1.

43. ISO（2018）, ISO 31000:2018 Risk management — Guidelines, International Organization for Standardization.

44. Zicari R.V., Brodersen J., Brusseau J. et al.（2021）, “Z-Inspection®: a process to assess trustworthy AI.” IEEE Transactions on Technology and Society, Vol.2, No.2, pp.83–97.

45. Hevner A.R., March S.T., Park J. and Ram S.（2004）, “Design science in information systems research.” MIS Quarterly, Vol.28, No.1, pp.75–105.

46. Peffers K., Tuunanen T., Rothenberger M.A. and Chatterjee S.（2007）, “A design science research methodology for information systems research.” Journal of Management Information Systems, Vol.24, No.3, pp.45–77.

47. Venable J., Pries-Heje J. and Baskerville R.（2016）, “FEDS: a framework for evaluation in design science research.” European Journal of Information Systems, Vol.25, No.1, pp.77–89.

48. Zhang J., Lu W., Xing C., Zhao N., Al-Dhahir N., Karagiannidis G.K. and Yang X.（2025）, “Intelligent integrated sensing and communication: a survey.” Science China Information Sciences, Vol.68, No.3, 131301.

49. Gerke S., Minssen T. and Cohen G.（2020）, “Ethical and legal challenges of artificial intelligence-driven healthcare.” Artificial Intelligence in Healthcare, pp.295–336.

50. SAE International（2021）, SAE J3016: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles, SAE International.

51. ISO/IEC（2023）, ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management, International Organization for Standardization.

52. ISO/IEC（2022）, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, International Organization for Standardization.

53. ISO（2015）, ISO 9001:2015 Quality management systems — Requirements, International Organization for Standardization.

54. European Parliament and Council（2016）, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union.

53. ISO（2015）, ISO 9001:2015 Quality management systems — Requirements, International Organization for Standardization.

54. European Parliament and Council（2016）, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union.