功能安全進入新階段

■文：編輯部

人工智慧、物聯網、數位孿生等新興技術的快速發展，傳統的功能安全標準體系和技術架構面臨著根本性挑戰。2024 年下半年至 2025 年 11 月期間，國際標準組織密集發佈了多項關鍵技術規範，行業領先企業在安全架構創新、驗證測試方法、AI 融合應用等領域取得了突破性進展。

國際標準體系的全面更新與演進

1. IEC 61508 系列標準的重大突破

IEC 61508 作為電氣 / 電子 / 可程式設計電子安全相關系統功能安全的基礎標準，在 2024-2025 年期間迎來了重要的技術更新。IEC TS 61508-3-2:2024 於 2024 年 8 月正式發佈，這是該系列標準中首次專門針對數學和邏輯技術在安全關鍵軟體中應用的技術規範。該標準為建立軟體及其文檔的精確特性提供了詳細的數學和邏輯技術要求，特別針對按照 E/E/PE 軟體功能安全標準 IEC 61508-3 開發的安全相關軟體。

更為重要的是，IEC TR 61508-3-3:2025 於 2025 年 7 月 1 日發佈，7 月 16 日正式實施，這是關於安全相關系統中物件導向軟體的技術報告。該技術報告提出了在設計物件導向軟體時應考慮的主題以及確保功能安全應用中適當品質的方法和技術建議，為現代軟體架構設計提供了重要指導。

在標準體系的整體發展方面，IEC 61508 第三版的開發工作已經啟動，目前處於委員會草案 (CD) 階段，預期將在 2027 年發佈。第三版將重點強化對 AI 系統的安全要求，擴展數位孿生和邊緣計算應用指導，這標誌著功能安全標準正在向智慧化、網路化方向全面演進。

2. 汽車功能安全標準的 AI 融合

汽車行業的功能安全標準正在經歷最為深刻的變革。ISO 26262 第三版的開發工作於 2023 年 10 月啟動，截至 2025 年 7 月，內部工作草案正在委員會層面積極討論，預期於 2027 年 10 月發佈。這一版本的核心變化是首次正式定義了 "自動駕駛系統 (ADS)" 和 "故障運行 (Fail-operational)" 等關鍵術語，並將安全手冊定義為規範性工作產品。

更為創新的是，ISO/PAS 8800:2024《道路車輛 —— 安全和人工智慧》於 2024 年 12 月正式發佈，旨在填補汽車領域人工智慧安全應用的國際標準空白。該標準圍繞 AI 系統的全生命週期構建安全管理體系，涵蓋需求分析、系統設計、資料管理、驗證測試到部署運維的完整流程，強調每個階段的安全目標與交付物。

例如中國的吉利汽車於 2025 年 8 月獲得了全球首個

ISO/PAS 8800:2024 AI 安全認證，標誌著該標準已經進入實際應用階段。ISO/PAS 8800 採用三層防護架構：硬體層 (ASIL) 防隨機失效、系統層 (SOTIF) 防功能不足、AI 層防演算法風險，這種創新的架構設計為 AI 驅動的汽車系統提供了全面的安全保障。

3. 醫療設備與機械安全標準的強化

醫療設備安全標準在 2024-2025 年期間也進行了重要更新。IEC 60601-2-40 第三版於 2024 年 12 月發佈，新增了恒壓刺激器要求，澄清了視覺刺激器要求。

在機械安全領域，ISO 13849-1 第四版於 2023 年發佈，取消並替代了 2015 年的第三版，進行了技術修訂。主要變化包括：整個文檔重新組織以更好地遵循控制系統的設計和開發過程；增加了與 ISO 12100 風險評估的直接關聯；詳細規範了安全功能和安全需求規範 (SRS)；增加了對軟體要求的全新條款。

中國也發佈了相應的國家標準 GB/T 16855.1-2025，於 2025 年 8 月 29 日發佈並實施，增加了子功能交叉監控、平均失效間隔時間等術語定義，進一步完善了機械安全標準體系。

技術創新與架構突破

1. AI 與功能安全融合的革命性架構

AI 技術與功能安全的融合正在催生全新的系統架構設計理念。在硬體層面，最新的處理器採用了更為先進的鎖步架構，更為創新的是多樣化鎖步技術的出現。與傳統鎖步架構使用相同核心不同，多樣化鎖步技術使用兩個不同的核心，採用不同的架構和指令完成相同的整體任務，提供卓越的錯誤檢測能力，有效緩解共模故障。這種技術在自動駕駛車輛的電子控制單元 (ECU) 中得到廣泛應用，能夠即時檢測異常，即使在輕微硬體或軟體故障的情況下也能讓車輛安全運行。

在系統架構層面，業者正在探索三域分離架構：主計算域 (DNN 模型)、監控域 (輸出驗證)、安全域 (形式化驗證控制演算法)，這種架構已在特斯拉 FSD 等系統中應用。同時，風險緩解機制也在不斷完善，包括多樣化冗餘 (雙 AI 系統遵循 " 開發團隊獨立、訓練資料隔離、硬體平臺差異 " 原則)、安全邊界 (Safe Envelope) 限制 AI 操作範圍、混合決策 (非 AI 元件作為 " 安全網 ") 等。

2. 驗證測試技術的智慧化革新

驗證測試技術正在經歷從傳統方法向 AI 驅動的智慧化方法轉變。在 AI 輔助安全分析方面，研究人員提出了基於大語言模型 (LLM) 的 FMEA 框架，使用 GPT-3.5、GPT-4、GPT-4o 和 Gemini 1.5 FLASH 進行案例研究，結果顯示在分析速度、準確性和可靠性方面相比傳統方法有顯著提升。

數位孿生驗證技術在功能安全領域的應用也取得了突破性進展。ANSYS 數位孿生技術被比亞迪用於汽車研發的功能安全驗證，根據 ISO 26262 標準，功能安全等級 ASIL-D 的驗證次數需達到 10^6 次，而通過數位孿生技術，比亞迪將驗證效率提升了 300 倍。

3. 雲端協同驗證的產業化應用

雲端協同驗證技術正在成為功能安全驗證的重要趨勢。Ansys 虛擬認證工具鏈於 2024 年 12 月發佈，與微軟、TÜV SÜD 和 Kontrol 合作開發，專為軟體定義車輛、ADAS、電動出行等設計，使用微軟 Azure 雲平臺基礎設施和 AI 驅動的分析，為法拉利、紅牛、保時捷等車隊縮短了設計週期並降低了開發成本。

在 AI 輔助測試診斷方面，DiaVio 系統通過利用大語言模型自動診斷模擬測試中的安全

違規，基於特定領域語言 (DSL) 將自然語言描述的真實世界事故報告與模擬測試中的違規場景對齊，通過微調基礎 LLM 學習診斷能力。

AI 驅動的測試用例生成技術也在快速發展，通過分析歷史測試資料和系統行為模式預測潛在故障點並生成針對性測試用例，實現主動測試，專注於最高風險區域，提高測試過程的效率和有效性。

行業應用的標杆案例與技術實踐

1. 自動駕駛領域的安全架構革新

自動駕駛領域在 2024-2025 年期間實現了功能安全技術的重大突破。特斯拉 FSD V14 在 2025 年推出，作為自 V12 以來最大的升級，參數增加 10 倍，目標是到 2025 年實現 " 感知 " 行為並提高安全性。FSD V14 的 " 可解釋中間層 " 提供了監管和驗證基礎，系統在輸出控制動作前，會同時生成佔用網格、語義圖、語言推理結果等多模態信號，這些中間結果不僅可用於車機視覺化，也便於開發者與監管機構審查決策邏輯。

在安全架構方面，特斯拉採用雙晶片平行計算架構 (總算力 72TOPS)，配備定制神經網路加速單元和硬體安全島設計 (ASIL-D 認證)，通過 " 影子模式 " 持續進化策略，在保持現有安全框架的前提下，通過海量真實場景資料構建閉環訓練體系，形成 " 感知 - 決策 - 控制 " 全鏈路的自進化能力。

中國的蔚來汽車在 2024 年 7 月推出了行業首個基於端到端模型化架構的自動緊急制動 (AEB) 系統，成為行業首家使用端到端模型化架構來做主動安全的車企。該系統前向形成了 240° 環繞防衛圈，可以處理更多二輪車路口穿行場景，路口性能相比規則時代的 AEB 提升了 5.2 倍，對前向障礙物和全角度切入障礙物的事故減損分別達到了 51% 和 35%。

2. 工業自動化的智慧安全升級

工業自動化領域的功能安全技術正在向智慧化、網路化方向全面升級。

施耐德電氣 EcoStruxure Triconex 安全儀錶系統 (SIS) 在安全完整性等級方面表現卓越，支援 SIL 1、SIL 2 和 SIL 3 安全和關鍵控制應用，是高可用性、高完整性、容錯控制器。Tricon CX 作為 Triconex 最強大的安全系統，利用現場驗證的 Tricon、Trident 和 Tri-GP 系統的傳統優勢，當安全性和盈利能力是關鍵成功因素時是最佳選擇。

在網路安全方面，2025 年 10 月，西門子推出了 SINEC Secure Connect 平臺，採用創新的零信任架構，在現有 OT 基礎設施之上創建安全的虛擬覆蓋網路，解決了工業網路互聯的安全挑戰。

3. 醫療設備的精准安全控制

醫療設備領域的功能安全技術在 2024-2025 年期間實現了重大突破。達芬奇 5 手術機器人於 2024 年 3 月獲得 FDA 批准，具有 150 多項增強功能，包括全新的外科醫生控制台、強大的震顫控制能力、最高品質且最自然的 3D 成像系統，引入力回饋技術，能夠幫助手術效率大幅提高，被稱為迄今運行最流暢、操作精度最高的手術平臺。

醫療機器人也取得了重要進展。CARINA TM 平臺輔助腎部分切除術的初步研究表明，術中操作穩定、靈活、延遲低，該平臺輔助的部分腎切除術是安全可行的。

在植入式設備方面，雖然參考資料中未提供具體的起搏器功能安全案例，但根據 ISO 26262 標準的發展趨勢，醫療設備正在採用 V 模型開發流程，左側包含技術安全要求的

定義、系統架構、系統設計和實現，右側包含集成、驗證、確認和功能安全評估。

4. 新興領域的功能安全拓展

功能安全技術正在向無人機、協作機器人等新興領域快速拓展。在無人機安全標準方面，ISO 正在推進關鍵標準的第三版，與 JARUS 引入的開放、特定和認證類別對齊，2019 年在歐洲採用，2024 年被國際民航組織 (ICAO) 全球認可。

歐盟航空安全局 (EASA) 完成了 SAIL III 無人機系統的合規手段，完成了在聲明框架下運行無人機所需的技術框架 (在特定運行風險評估 - SORA 下分類為特定保證和完整性級別 (SAIL) III)。

在協作機器人領域，2024 年國際標準組織發佈了更新的安全標準 ISO 10218，對工業機器人安全功能提出更清晰、更嚴格的規定，同時要求達到 SIL2/PLd/Cat.3 級別。新的 ISO 10218 完全納入了先前的 ISO/TS 15066，現在規範協作應用的要求，即人機協作，允許與移動機器人直接交互。

歐姆龍 TM S 系列協作機器人配備 31 個安全功能，符合 ISO 13849-1 Cat.3 PLd 和 ISO 10218-1 安全標準，獲得 TÜV Nord 認證和 SGS 的 UL/CSA 認證，代表了協作機器人安全技術的最新水準。

功能安全市場正在迎來高增長時代

1. 市場規模的高速增長預測

根據多家權威機構的預測，全球功能安全市場規模在 2025 年為 70 億美元，預計到 2030 年將達到 115.3 億美元，2025-2030 年複合年增長率 (CAGR) 為 10.48%。

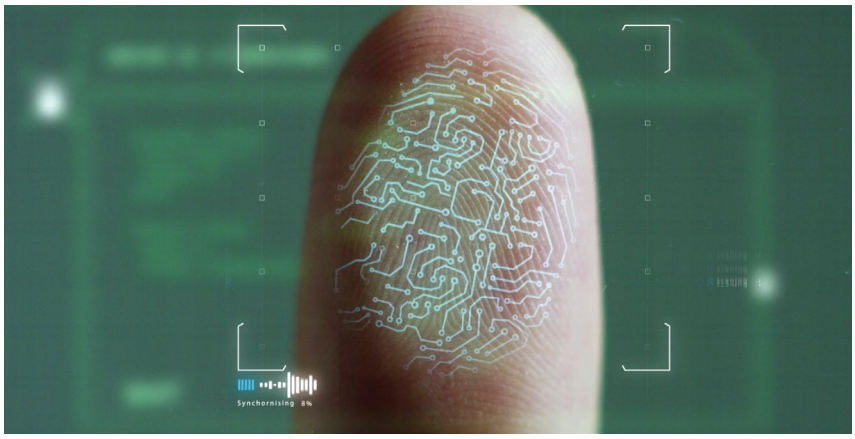
更為樂觀的預測顯示，市場規模將從 2025 年的 157.87 億美元增長到 2033 年的 360.43 億美元，2025-2033 年 CAGR 高達 10.87%。這種高速增長主要受到 AI、物聯網和自主系統等下一代技術的推動，功能安全解決方案成為這些技術不可或缺的組成部分。

在細分市場方面，緊急停機系統 (ESD) 預計在 2030 年佔據最高市場份額，CAGR 為 10.05%，因為 ESD 能夠保護人員、環境和其他重要資產，特別在石油天然氣等高風險行業需求旺盛。

2. AI 融合與零信任架構的發展趨勢

"AI + 安全 " 融合正在成為功能安全技術發展的核心趨勢。2026 年市場規模將超百億，AI 不僅用於安全分析，更將成為安全機制核心元件。AI 和 ML 與功能安全系統的集成提高了工作執行和品質，同時減少了人工交互需求，這種集成增加了工作執行和品質，同時減少了人工交互要求。

零信任架構在功能安全領域的應用前景廣闊。零信任架構通過 " 永不信任，始終驗證



" 的核心理念，正重塑工業資料安全防護體系，需要實現設備身份認證、動態存取控制與區塊鏈存證的協同聯動。

在技術實現方面，零信任架構基於 " 默認不信任 " 原則，要求對網路內外的任何實體都不給予預設信任，關鍵技術包括多因素認證 (MFA) 和生物識別技術確保用戶合法性。零信任架構不是假設內部流量是安全的，而是在授予存取權限之前持續認證、授權和監控所有訪問請求 —— 每個使用者、設備、應用程式和交易，無論網路位置如何。

3. 供應鏈安全與監管政策的演進

供應鏈安全管理正在成為功能安全的重要組成部分。中國發佈的 GB/T 45953-2025 供應鏈安全管理體系規範於 2025 年 8 月 1 日發佈，11 月 1 日實施，規定了供應鏈安全管理體系的組織環境、領導力、規劃、支持、運作、績效評估和改進等要求。

全球供應鏈安全市場也在快速增長，2024 年價值 24.7 億美元，預計 2025 年達到 27.6 億美元，CAGR 為 12.55%，到 2030 年將達到 50.2 億美元。區塊鏈技術因其透明度和防篡改能力而受到關注，預計到 2025 年將被廣泛採用用於可追溯性，確保供應鏈中的安全資料共用。

在監管政策方面，各國正在加強對自動駕駛等新興技術的安全監管。中國工信部 2025 年汽車標準化工作要點明確提出，加快自動駕駛系統安全要求強制性國家標準研製，構建自動駕駛系統安全基線；同時，推動《汽車駕駛自動化分級》(GB/T 40429-2021) 等標準的實施，明確 L3-L5 級自動駕駛的技術要求與駕駛員義務。

美國交通部於 2025 年 4 月 24 日宣佈了新的 NHTSA 自動駕駛車輛框架，作為交通部促進國內創新議程的一部分。北京也於 2025 年 1 月 2 日批准了自動駕駛車輛新法規，將於 4 月 1 日生效，標誌著中國在支持自動駕駛技術方面取得重大進展。

結語

設備功能安全相關技術正在走出傳統領域，擁抱更多新興技術和新興市場，呈現出以下三個趨勢

- ■技術創新不斷：晶片多樣化鎖步技術、AI 輔助驗證等創新方法不斷湧現；
- ■標準體系加速整合：IEC 61508、ISO 26262 等核心標準正在融合 AI 安全、數位孿生等新技術要求；
- ■應用場景不斷擴展：從傳統汽車、工業向醫療、無人機、協作機器人等新興領域快速延伸。

展望未來，設備的功能安全將從 " 合規要求 " 轉向 " 市場競爭力 "，成為產品差異化的重要要素。

參考資料

基於國際電子電機委員會 (IEC)、國際標準組織 (ISO) 等權威機構的最新報告，以及特斯拉、西門子、施耐德等企業的公開技術檔。 CTA