AI 進駐製造生產線後 工業機器人安全再升級

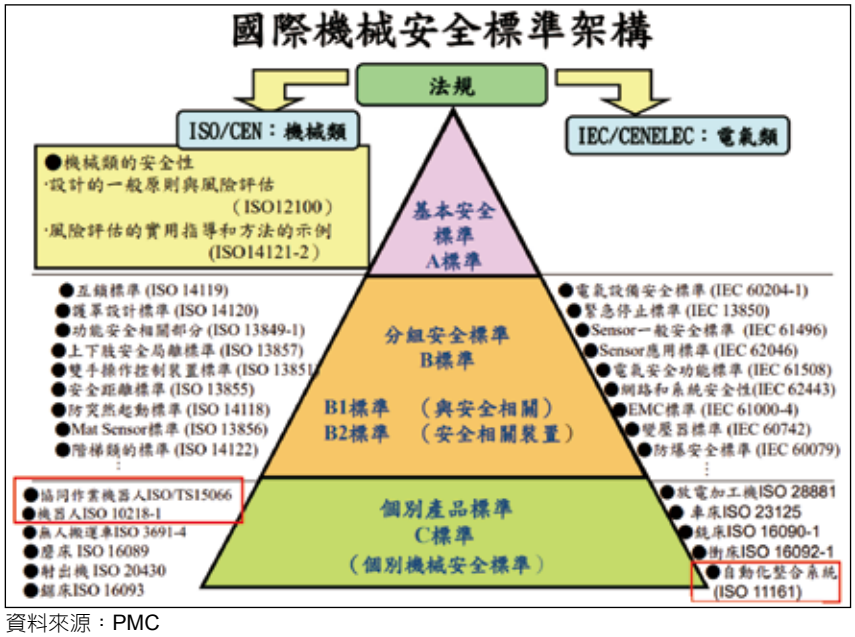
■文：任芷萍

工業機器人／機械手臂一直是工業自動化演進到智慧製造的要角。隨著人工智慧 (AI) 的風起雲湧，促使產業對於這些「必要存在」別有一番新思維。日前由勞動部職安署所舉辦的《工業用機器人安全管理說明會》活動席間，第一線實地參與產業輔導的專家對此有深入解析。

PMC：未來 AI 機器將被視爲「高危害設備」

財團法人精密機械研究發展中心 (PMC) 工業設備安全部副理賴蔚齊表示，勞動部職安署早在 2018 年就計劃對機器人做源頭管理——須經驗證並做登錄，才能讓廠內員工使用機器人，但考慮到有些自動化設備的形式會被定義成機器人的樣態、對經濟層面衝擊過大，故暫予擱置，但未來仍會實施。這是因為國外對工業機器人的定義是：可自動控制、可重新編譯程式以及具多目標用途之三軸或多軸操作機，可依預定程式完成指定作業或工作者即算數，實在有太多自動化設備都將被劃歸在內，甚至連基本的車床都無法豁免。

圖 1：國際機械安全標準法規可概分為「機械」與「電氣」兩大類



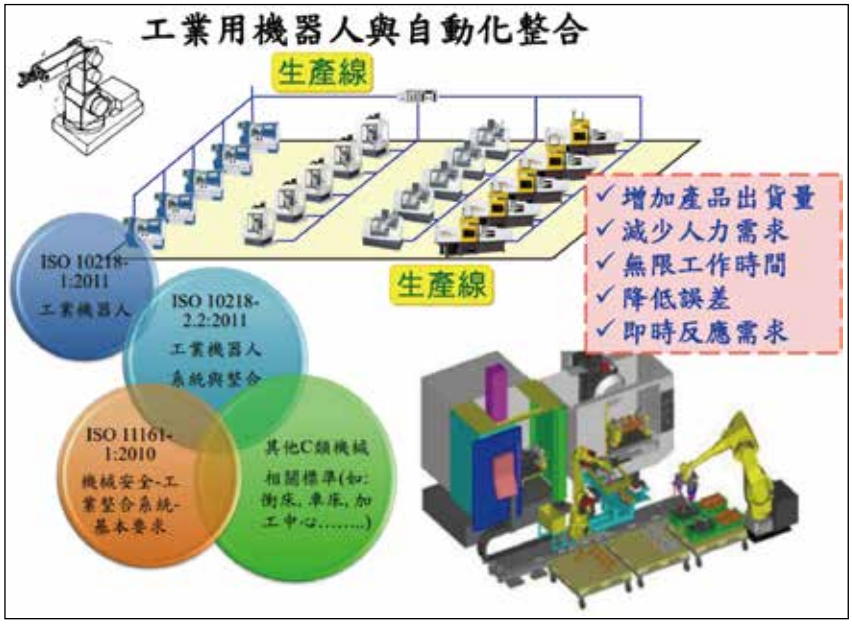
資料來源：PMC

再者，由於部分加總不等於最終結果；例如，車床／銑床和機器人分別符合各自的 ISO 23125/ISO 16090-1 及 ISO 10218-1 標準，但放在同一工作場域，不代表就無安全疑慮，故須就整合後的現況符合 ISO 10218-2 安全標準才可。因此，PMC 正與社團法人台灣智慧自動化與機器人協會 (Tairoa) 研究試行範疇，做場域評估，與國際標準差異多大？可能動搖產業根本有多大？尤其值得留意的是，AI 影響所及，新的歐盟機器指令已決意將 AI 納管；未來但凡有具備自我學習能力的 AI 機器，將會被視為「高危害設備」，必須考慮到安全功能的喪失。

AI 設備須經第三方驗證才能入市

例如，安全與操作便捷性是衝突的，AI 設備會不會自作聰明擅改運作路徑而導致危害？會不會因電磁干擾 (EMI) 而誤動作？會不會有被駭的資安風險？因此，AI 設備將被列入特定安全要求，不能

圖 2：工業機器人 vs. 自動化整合之相對應法規

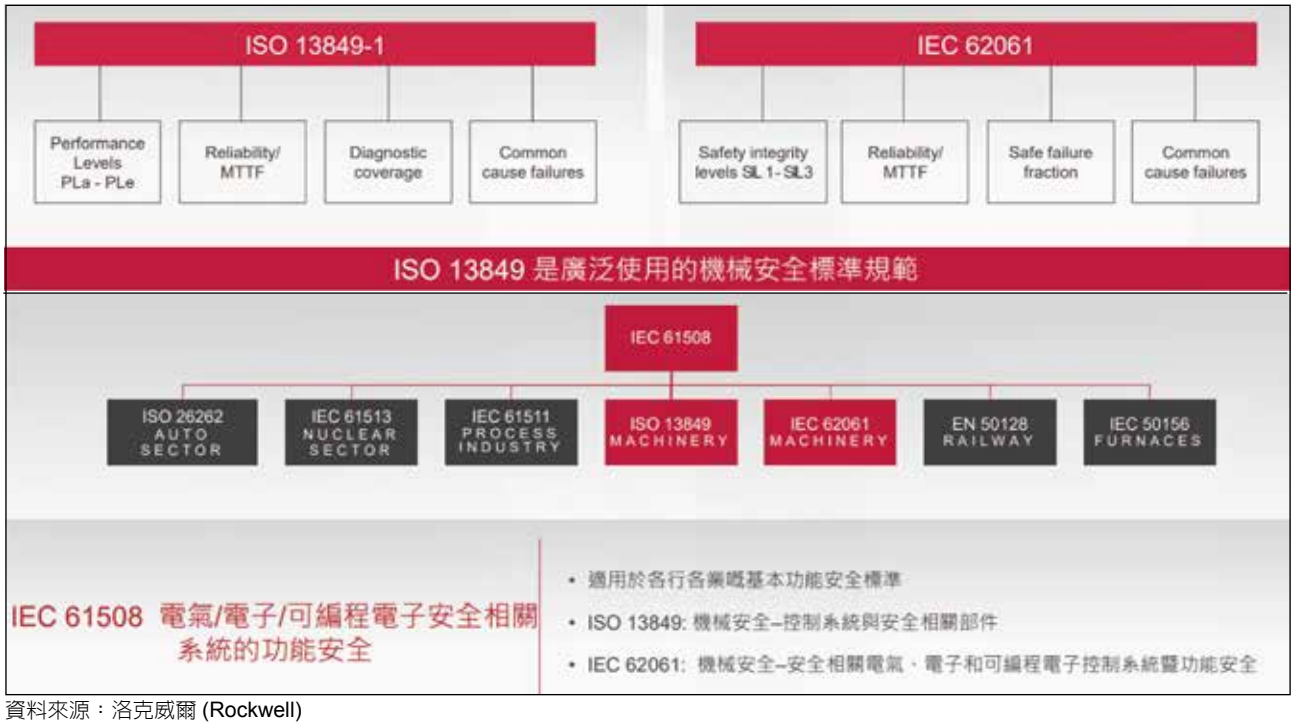


資料來源：PMC

採自我宣告、須經第三方驗證才能入市。國際機械安全標準可概分為 A、B、C 三大類，若須經驗證，會額外對安全迴路可靠度有所要求；例如，ISO 10218-1 明訂要達到 Cat.3 等級 (雙迴路冗餘設計，PL=d)——硬體迴路構造、使用元件壽命、系統偵測能力 (診斷範圍，DVavg)、設計的可靠性 (共因失效，CCF) 為四大考量因子，即 ISO 13849 迴路可靠度條件。

就機器人停止時間狀態系統的本質安全來看，其完全停止時間＝感應器接收到停止命令＋到機器人完全停下來的時間。然而，有些機器人供應商為保護產品元件，會刻意延長機器人煞停、咬住伺服馬達的時間，那麼後端安全裝置的迴路部署也要隨之變大，另動作的可靠度及防護佈置亦是重點。賴蔚齊還提到，不論是新的工具機標準或機器人指令，皆針對遠端遙控的可靠度有額外要求；例如，無線操控緊急停止裝置須符合 ISO 13849 或 IEC 62061 標準及安規測試。最後，在節能減碳及 ESG 浪潮推動下，碳盤查是新型智慧工廠的一大亮點，PMC 也與財團法人全國認證基金會 (TAF) 合作為工具機業者進行相關輔導。

圖 3：國際安全標準規範



資料來源：洛克威爾 (Rockwell)

Rockwell：「安全模組」須獨立於主控 PLC 之外

洛克威爾 (Rockwell) 自動化產品技術顧問高永勳接棒進一步闡述：ISO 13849-1 與 IEC 62061 是兩大主軸，前者聚焦於機械的控制系統與安全相關部件，後者側重電氣、電子和可編程電子控制系統暨功能安全。在滿足這兩個先決條件之下，如何提升設備產能及效率是供應商心心念念的頭等大事——例如，如何應用新的控制器來達陣目標。現場作業員若要完整卸載安防裝置、執行調整、爾後復歸，至少會耗時 5 ～ 10 分鐘不等；若設備嚴重異常、需要更多應對時間，對設備的效率及稼動率影響更鉅！

洛克威爾深耕工廠自動化多年，現今出貨到美國的設備幾乎都能見到他們產品的蹤跡，關於系統規劃及輔導甚有心得。高永勳觀察到，實務上有些廠商會捨棄安全裝置，但這其實是不合規的作法，對出口至歐美市場是一大障礙，只有被打回票的份。他指出，完整的功能安全架構是輸入、安全邏輯裝置 (安全模組)、輸出設備的組合，值得意的是，為避免時間差問題，安全模組通常不會做在 PLC (可程式化邏輯控制器) 上，以便安全圍籬／開關或光柵等感測防護受到觸發時，安全模組可不經由 PLC 直接輸出訊號、命令繼電器 (Relay) 斷電。

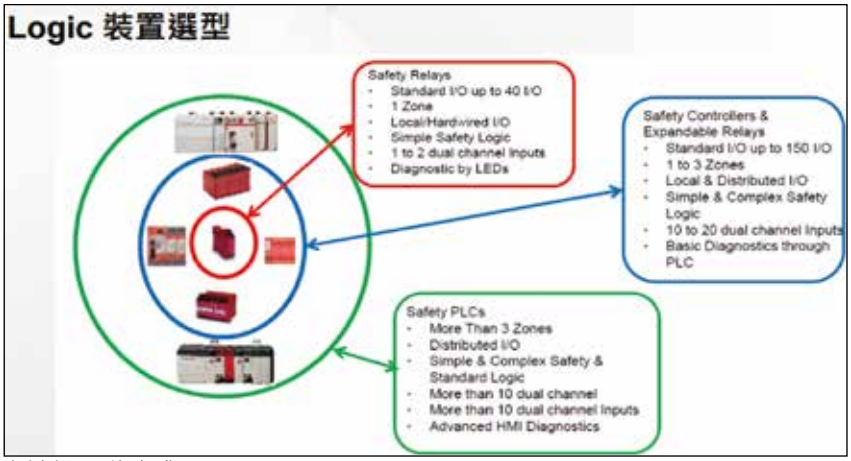
新增「狀態邏輯控制」！Safety PLC 披掛上陣

但這還不能算是安全保證，還須考慮進入危險區間裡調校設備到完成任務離場的安全時間，可惜一般的安全模組並無法實現此目標。於是，有了 Safety PLC 產品的問市，以因應「人機共存」的安全所需。高永勳解釋，相較於一般的 Safety Relay——接收到輸入訊號，只能直接把輸出端裝置關閉，Safety PLC 建構的安全模組能設定更多邏輯程式、實現更多細部要求。例如，當作業員將設備切換到手動模式以排除捲料問題或異常時，Safety PLC 會依人員動作改變設備運行狀態、將伺服馬達降速至安全範圍或將機械手臂退至安全距離，不只有 0、1 二元選項。

高永勳透露，PLC 是數位轉型的要角，有兩大訴求：一是符合安全規範，二是滿足用戶產能需求。據他們實地了解，裝設高性能安全模組的產能表現，一整天下來可較傳統啓／停模式多出 5 ～ 10%——特別是異常狀況多或安全重置的程序很複雜時。他提醒，IEC 61508 之安全完整性等級 (Safety Integrity Level, SIL) 是針對使用者的安全狀態定義、並非產品本身；即使採用最高級的控制器也未必是 SIL3 等級的保證，而是整體電氣維護、電路、功能都必須符合規範才算數。對於在不停機的生產狀態下、進入產線調校機器的場景，尤需安全模組的挹助。

高永勳說明，Safety PLC 內部是雙迴路架構 (類似雙核心)，在單一控制器裡可以跑兩個程式邏輯：一個應對設備運作，一個專責安全工作，兩者存放區壁壘分明，且安全程式等級高於一切！協作時可發揮「判斷」能力，讓操作危害性相對高的重機械也能達到 SIL3 規範。銷往國外市場的機器設備，當中所有程式皆必須羅列出來供檢查。為簡化佈線工程的複雜度、也為便於診斷，現在許多機器通訊 (M2M) 已直接與乙太網串聯；基於資安考量，Safety PLC + Safety I/O 模組的組合正漸受歡迎，且與安全相關的通訊路徑與一般數據封包的傳輸是分開的。 CTA

圖 4：功能安全模組之三大邏輯控制類型——繼電器、簡單控制、狀態條件邏輯控制



資料來源：洛克威爾 (Rockwell)