



歐盟網路韌性法（CRA） 工具機產業因應指南

Cyber Resilience Act

法規重點 · 短中長期路線圖 · 輔導與驗證資源

製作單位 | 台灣工具機暨零組件工業同業公會

2026.08

CRA 簡介 | 產品資安成為歐盟市場准入條件



Regulation (EU) 2024/2847 將「具數位元素產品」的資安責任，延伸至設計、上市與整個支援期。



誰需要注意

- 在歐盟市場提供、可直接 / 間接連線的硬體、軟體與獨立元件。
- 含遠端資料處理解決方案；醫療、航空、汽車等已有同等專法者多屬排除。
- 工具機控制器、HMI、閘道器與遠端維護功能，應先做產品邊界判定。



全生命週期義務

上市前

風險評估、安全設計 / 預設、技術文件與 SBOM

上市時

符合性評定、EU 符合性聲明、CE 與支援期資訊

上市後

監測漏洞、提供安全更新，保留修補與揭露證據



評定與事件通報

- 一般產品多可自評；重要 / 關鍵類產品依分類與標準，可能需公告機構。
- 2026.09.11 起，活躍利用漏洞與重大資安事件須透過CRA單一平台通報。
- 24h 早期預警、72h 完整通知；後續再依規定提交最終報告。

工具機現在先做：盤點可連網產品與軟體組成 → 建立 PSIRT / SBOM → 定義更新支援期與通報演練。

PSIRT | Product Security Incident Response Team

產品資安事件應變團隊：接收與評估產品漏洞 / 事件，協調修補、回應及對外通報。

SBOM | Software Bill of Materials

軟體物料清單：列出軟體、版本、相依與開源元件，支援弱點比對及供應鏈追溯。

工具機廠 CRA 範圍 | 產品邊界與零組件協作



每一層直接對應「是否納入」與「工具機廠責任」；由產品本體一路判定到外部環境。

產品 / 服務層	包含項目	責任判定 燈號	工具機廠負責到哪裡
 產品本體 / 內建軟體 工具機廠投放市場的核心產品	CNC / Motion · PLC / Safety HMI / IPC · Firmware / SW	一定納入 核心產品	整機邊界、設計安全、技術文件、支援期與最終符合性
 產品內建連線 / 更新 隨產品交付並由廠商維護	Edge Gateway · Protocol Stack Update Agent · Remote Access	通常納入 隨產品交付 / 維護	權限與介面安全、安全更新、弱點處理及維護入口
 遠端資料處理服務 是否為產品功能所必要是關鍵	OEM Service · Cloud Analytics Update Service · Remote Processing	視功能納入 缺少即無法達成預期功能	若屬必要功能或由廠商控制，納入產品邊界、風險評估與支援
 客戶廠內環境軟體 通常由終端使用者配置管理	Factory LAN · MES / SCADA Local Server · Asset Mgmt.	通常不納入 客戶配置管理	不視為同一產品；仍須定義介面假設、安裝條件與整合風險



零組件協作

證據交付 → 整機承擔

零組件廠交付

型號 / 版本、SBOM、支援期限、安全介面，以及
漏洞與修補資訊



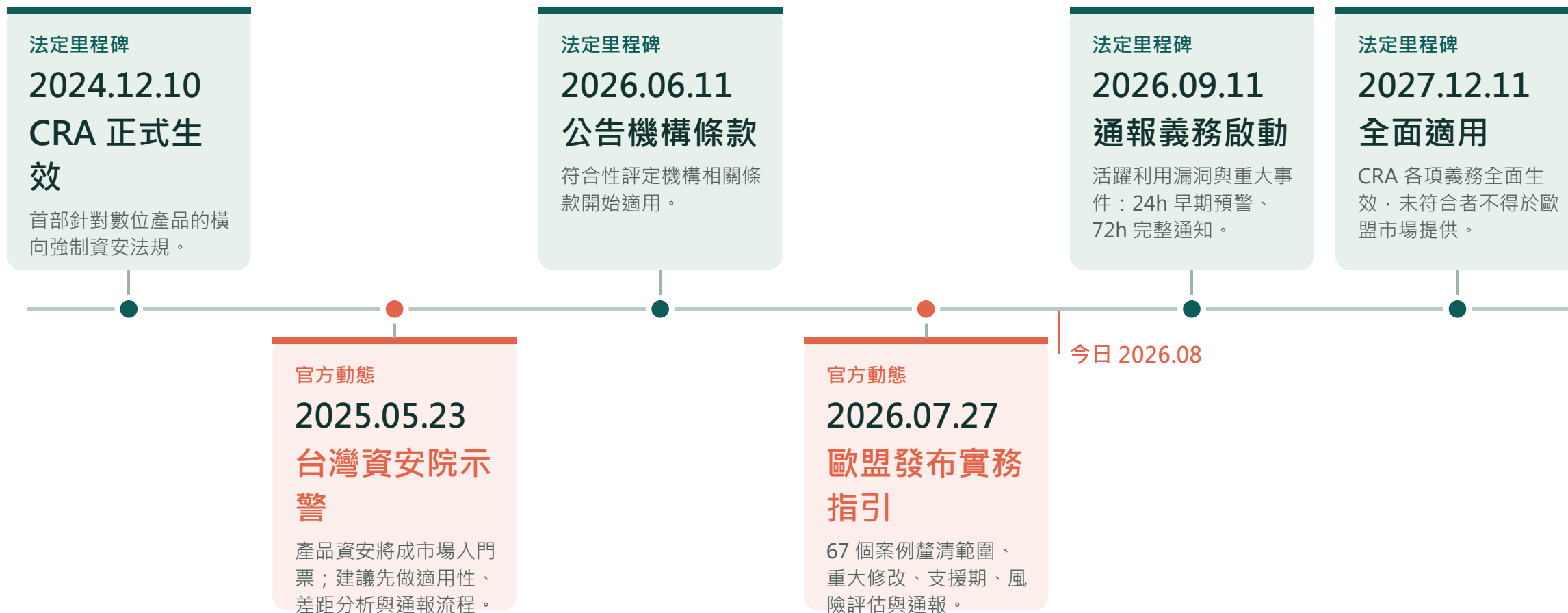
工具機廠整合 / 承擔

圈定整機邊界、驗證權限 / 介面 / 遠端功能，承擔整機風險與最終符合性

CRA 時間軸 | 法定里程碑與官方動態



從 CRA 生效到全面適用，法定里程碑（上）與官方動態（下）併於同一條時間軸。



官方來源：EUR-Lex 2024/2847；歐盟執委會 CRA Summary / Manufacturers / Guidance (2026-07-27)；國家資通安全研究院 (2025-05-23)。查詢日 2026-07-30。

法規原文優先 | 摘要非法律意見

台灣工具機與零組件廠 | CRA 對應路線圖



輔導



測試 / 驗證



先輔導建制度，再以測試 / 驗證確認證據；**第三方評定依產品分類與法定路徑。**



01 短期

2026.08 - 09

先具備辨識與通報能力



需要輔導

整機廠

盤點銷歐型號、控制器 / HMI、遠端維護與雲端服務，判定產品邊界。

零組件廠

建立初版 SBOM、CVE 接收窗口；
指定 CRA 負責人 / PSIRT 並完成通報 SOP。



需要測試 / 驗證

- 控制器、HMI、遠端介面先做弱點掃描與基線滲透測試。
- 檢核清冊、SBOM 與 24 小時 / 72 小時 通報演練紀錄；此階段測試不等同法定 CRA 驗證。

交付 | 清冊 | ARCI | SOP | 初版 SBOM



02 中期

2026.10 - 2027.06

建立產品與供應鏈證據



需要輔導

整機廠

完成風險評估、附錄 I 映射、安全預設、更新機制與支援期。

零組件廠

合約納入 SBOM / VEX、漏洞回應 SLA、版本與重大變更通知。



需要測試 / 驗證

- 依產品角色執行工業控制系統資安標準 IEC 62443-4-1 流程審查、IEC 62443-4-2 或適用標準測試。
- 驗證韌體簽章、更新、存取控制與漏洞修補；補齊測試報告與追溯證據。

IEC 62443-4-1

| 看流程：安全需求、設計、測試、漏洞處理與更新維護。

IEC 62443-4-2

| 看產品：身分驗證、權限控管、資料保護與事件記錄。

交付 | 風險檔案 | 要求矩陣 | 供應商證據包

CRA 對應路線圖 | 長期與名詞對照



輔導



測試 / 驗證



先輔導建制度，再以測試 / 驗證確認證據；**第三方評定依產品分類與法定路徑。**



03 長期

2027.07 - 12

完成評定與持續維護



需要輔導

整機廠

鎖定產品分類與符合性評定路徑，完成**技術文件**、DoC、CE 與上市後流程。

零組件廠

承諾支援期、更新與稽核配合；維持版本及漏洞處理**可追溯**。



需要測試 / 驗證

- 完成最終符合性測試、證據缺口關閉與 CE 上市前查核。
- 重要 / 關鍵產品依規定辦理 NB 評定；一般產品不一定需要第三方驗證。

交付 | 技術檔案 | DoC / CE | 維護與評定紀錄

名詞對照

法規與治理

CRA 歐盟網路韌性法 | Cyber Resilience Act

PSIRT 產品資安事件應變團隊 | Product Security Incident Response Team

ARCI 負責、當責、諮詢、知會 | Responsible, Accountable, Consulted, Informed

供應鏈證據

SBOM 軟體物料清單 | Software Bill of Materials

VEX 漏洞可利用性交換 | Vulnerability Exploitability eXchange

SLA 服務水準協議 | Service Level Agreement

SOP 標準作業程序 | Standard Operating Procedure

產品與漏洞

CVE 常見漏洞與揭露 | Common Vulnerabilities and Exposures

HMI 人機介面 | Human-Machine Interface

DoC 符合性聲明 | Declaration of Conformity

符合性評定

CE 歐洲合格標誌 | Conformité Européenne

NB 公告機構 | Notified Body

IEC 國際電工委員會 | International Electrotechnical Commission

CNC 控制器廠商 | CRA 公開準備度呈兩極

2026.08.06更新



判讀：西門子、三菱已明確對外連結 CRA；其餘多為既有漏洞管理，或尚缺產品層公開證據。

控制器廠商	公開狀態	官方已公開措施	工具機廠採購 / 整合重點
	明確 CRA	SINUMERIK ONE 新 NCU 依 CRA 強化資安；CRA 納入產品生命週期、風險與資訊分享	索取型號別符合性時程、支援期、SBOM / VEX 與通報 SLA
	明確 CRA	CRA 納入開發 / 營運 / 支援 / IEC 62443-4-1；PSIRT + CNA、簽章韌體、角色權限、監控與免費安全更新	確認 CNC 型號 CRA 相容 / CE 時程、更新簽章與支援期
	能力對應	PSIRT、ISO/IEC 29147 揭露流程、公開安全公告與產品安全指南	尚未查得 CRA 專屬方案；要求路線圖、SBOM / VEX、通報與更新承諾
	能力對應	Delta PSIRT 五階段漏洞處理、CVSS 與公告；具 CNA、IEC 62443-4-1 / 元件監控能力	尚未查得 CNC 專屬方案；釐清型號範圍、支援期、修補與 EOL 政策
	未查得	已公開 TNC7 / StateMonitor 聯網能力；本次未查得官方 CRA 專屬措施	要求 CRA 聲明、PSIRT / 漏洞窗口、SBOM / VEX、簽章更新與支援期
	未查得	已取得 ISO 27001:2022，公開企業 ISMS、事件應變與軟體下載；未見產品層 CRA 證據	要求產品 PSIRT、安全開發、漏洞公告、生命週期更新與 CE 計畫

官方來源：六廠商官方 CRA / 產品資安 / 資安政策頁；查詢日 2026-08-03。完整連結見備註。

能力對應 ≠ 已符合 CRA

CRA 輔導單位與聯絡方式



台灣在地窗口 | 2026.09



重要：在台可做差距分析、測試或既有標準驗證，不等於已取得 CRA Notified Body 資格；法定資格請以歐盟 NANDO 最新名單為準。

輔導單位	定位	可協助內容	聯絡窗口	聯絡方式
數產署 CRA 服務團	政府計畫	顧問、軟體安全檢測、文件證據檢核	中華軟協余小姐	menghsin.yu@tissa.org.tw
工研院產業學院	法人培訓	IEC 62443、智慧製造與產品資安課程	課程窗口	03-591-2994
工研院資通所	法人研究	產品 / 工業資安研發、測試技術與輔導鏈結	資通所窗口	itri.org.tw 資通所
國家資安院	法人研究	CRA 法規解析、產業準備與治理指引	官方聯絡頁	nics.nat.gov.tw
PMC 精密機械中心	產業法人	工具機需求盤點、技術整合與輔導轉介	產業服務窗口	pmc.org.tw
ISA 臺灣分會	協會培訓	IEC 62443-4-1 / 4-2、ISASecure 課程	官方聯絡頁	isa.org.tw
SGS 台灣	國際 TIC	CRA / IEC 62443 差距分析與測試規劃	顏志仲 經理	02-22993279 # 1306 Kelvin.yen@sgs.com
TÜV NORD 北德台灣	國際 TIC	CRA 適用性、Gap、IEC 62443 導入	台灣辦公室	taiwan@tuv-nord.com
Bureau Veritas 必維	國際 TIC	CRA Gap、漏洞管理、標準映射與培訓	Joseph Chan	Joseph.Chan@bureauveritas.com
UL Solutions Taiwan	國際 TIC	CRA 範圍判定、培訓、流程框架	台灣客服	02-7737-3168
商檢中心 (ETC)	產業法人	適用性 / Gap、PSIRT、SBOM、技術文件	資通部 陳先生	03-3280026 (ext.559) hsien@etc.org.tw

CRA 測試 / 驗證單位與聯絡方式



測試 / 驗證

台灣在地窗口 | 2026.07



本表列的是在台可提供產品資安測試、既有標準驗證或 CRA 評定準備的機構；是否具 CRA 公告機構資格，仍須依產品分類至 NANDO 確認。

測試 / 驗證單位	可提供服務	聯絡窗口	聯絡方式
SGS 台灣	產品資安測試；IEC 62443、EN 18031、ETSI EN 303 645	顏志仲 經理	02-22993279 # 1306 Kelvin.yen@sgs.com
Intertek 全國公證	Annex I / CE 文件；IEC 62443、EN 18031 測試	台灣 CRA 窗口	02-6602-2888 #729 website.tw@intertek.com
Bureau Veritas 必維	CRA Gap / 漏洞處理；產品資安測試與驗證準備	Joseph Chan	02-2570-7655 Joseph.Chan@bureauveritas.com
TÜV NORD 北德台灣	CRA 評估；IEC 62443 測試 / 驗證準備	Claire Huang Director	02-2378-0578 clhuang@tuv-nord.com
DEKRA 德凱台灣	IEC 62443、產品資安評估、弱點測試	官方聯絡頁	dekra.com.tw Contact
TÜV Rheinland 台灣	CRA Readiness Check、產品合規與評定路徑	台灣辦公室	02-2172-7000 tuv.com/taiwan
UL Solutions Taiwan	工業資安評估、IEC 62443 與 CRA 合規準備	台灣客服	02-7737-3168 taiwan.ul.com

來源：各機構台灣 / 全球官方 CRA 與資安服務頁；聯絡資訊查詢日 2026-07-30。

RED NB / ISO 17025 ≠ CRA NB