經濟部 109 年度
《人工智慧導向資安共創技術計畫》
合作研究計畫

《資安應用場域規劃與導入實證》

建議書徵求文件

財團法人資訊工業策進會

中華民國　109 年　　月

109年度合作研究計畫建議書徵求文件

一、 簡介

工業控制系統（Industry Control System, ICS）負責控制工廠自動化設備、油水電運輸等社會關鍵基礎設施。過往工控系統採封閉運作，近年來因應網際網路、智慧製造興起而逐漸連網，因而資安威脅隱憂增加。

然過往至今我國工控系統佈建運作鮮少考慮資安防護，此不利於我國持續對外輸出工業控制設備、工具機設備，亦不利現行接單代工生產業務與未來提升至智慧製造等發展。

因此需要制訂系統層級資安防護評估程序，以驗證工控場域在實施資安防護後是否符合國際資安規範。此資安防護評估程序有兩項主目的，一為評估國人自行開發工控資安防護方案之有效性，另一為透過國際合規驗證提升國內工控設備產業競爭力。

有關評估程序與場域驗證，其主要內容包含工控場域威脅建模技術與國際合規驗證技術，前者亦包含確認工控系統架構、定義威脅建模範圍、建議威脅建模方法、找出已知及潛在威脅情境；後者則包含人員管理、解決方案堅實性、網路安全、帳戶安全、安全資訊及事件管理、補丁管理、備份與復原機制。

二、 計畫目標

本合作研究計畫目標包括：

1. 國際工控資安標準研究
2. 工控場域威脅模型基準建議
3. 工控場域測試與驗證

三、 計畫範圍

本計畫預期工作項目包括:

1. 研究資安防護規範並訂立指引

   1.1 針對實證場域，針對所需的國際連網產品與系統網路安全測試規範進行研究與整理，如 UL 2900，並至少包含連網產品軟體資安標準之一般需求(Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1)、工業控制系統特定需求(Particular Requirements for Industrial Control Systems, UL 2900-2-2)、協助緩解物聯網資安風險(Helps Mitigate IoT Cybersecurity Risk, UL 2900-2-3)等，以及美國工控系統防護指引標準 NIST 800-82。

   1.2研究物聯網相關資安評估框架，如全球移動通信系統協會(Groupe Speciale Mobile Association, GSMA)之物聯網防護評估評量，包含服務生態系統(Service Ecosystems)、端點生態系統(Endpoint Ecosystems)、網路營運商(Network Operators)等，設計資安評估之必要規範。

1.3研究 ISA/ IEC 62443，並至少包含 IEC 62443 2-4、3-2 及 3-3 實證所需的系統整合檢測項目，發展智慧製造所需的必要檢測項目。

1.4制定工業控制系統資安防護評估指引，至少包含威脅建模、漏洞檢測、滲透測試與影響分析。並挑選兩項智慧製造物聯網設備，發展智慧製造物聯網設備資安白皮書，提供產業參考使用。

2. 建立工控系統資安解決方案系統層級資安防護評估技術

2.1發展風險評量塑模與防護技術，符合工控系統參考模型，定義協作領域(Domains)、運作層級(Levels)與生命週期(Lifecycle)三個維度威脅模型，以及符合國際規範之檢測規範，如 ISA/IEC 62443，並至少包含工控服務提供者之防護程序需求(IEC 62443 2-4)、區域(zone)與導管(conduit)防護層級需求(IEC 62443 3-2)、系統防護需求與防護層級(IEC 62443 3-3)實證所需的系統整合檢測項目，發展智慧製造所需的必要檢測項目。

2.2發展國際合規驗證技術。以符合 IEC 62443-2-4 要求之服務供應商為例，至少應具備資安解決方案能力(僅列出部分)如人員管理、解決方案堅實性、網路安全、帳戶安全、安全資訊及事件管理、補丁管理、備份與復原機制等。

3. 執行驗證工作及系統層級工控資安防護驗證規範

3.1找出本委託工作指定之場域之資安威脅(例如 OWASP IoT Top 10 資安風險、國際其他同類型場域可能的資安漏洞)。

3.2針對導入之資安解決方案進行國際合規驗證，建立工控系統系統層級資安防護評估。成效評估為實施前後場域或設備符合國際工控系統資安規範的合規程度比較。

四、 預期成果(明確說明合作研究成果之產出)

1. 國際工控資安標準研究報告。
2. 工控場域威脅模型基準建議報告。
3. 場域測試驗證報告。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、 執行方式(包括計畫時程、計畫分工方式)

本合作研究計畫運用業界的研發能量與領域智識，配合主計畫「人工智慧導向資安共創技術計畫」提供測試驗證、技術評量、接軌產業與國際共通標準等，進行如「計畫範圍」所定義分析與開發。

預計將結合業界之研發能量與領域實務面經驗，回饋給主計畫技術研發方向，透過雙方相互合作討論的方式來進行。本合作研究計畫亦需提供相關系統之教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 參酌現況與未來展望訂立工業控制資訊安全之基準建議。
2. 依據通用的工業控制系統架構圖建構風險模型之方法並列出已知威脅、潛在威脅之清單。
3. 於現場場域進行測試並依據驗證項完成報告。
4. 完成成效評估實驗及對應結案報告，驗證本主計畫產出系統的有效性、效率成果品質，以及相關配合施作分享。

六、 計畫期程及預估計畫總經費

計畫執行區間： 109 年 03 月 15 日 至 109 年 12 月 15 日

總經費：5,000,000元

七、 驗收標準(含教育訓練)

項次	交付項目	交付內容	數量	交付型態	交付期限
1	國際工控資安標準研究報告	在工控資安之規範現況與應納入基準分析建議： ● IEC /ISA 62443 ● NIST SP 800-82 ● UL 2900	1 式	電子檔	109 年 5 月 15 日
2	工控場域威脅模型基準	報告內容含： ● 通用的工控系統架構圖 ● 風險建模方法 ● 工控領域威脅建模 ● 已知風險威脅、潛在威脅情境清單	1 式	電子檔	109 年 6 月 15 日
3	工控場域物聯網資安防護評估指引	內容應包含： ● 物聯網裝置驗證 ● 物聯網公開金鑰基礎建設防護方法 ● 防護物聯網網路 ● 物聯網資料傳輸加密 ● 物聯網硬體防護 ● 物聯網應用程式介面防護方法 ● 物聯網資安防護分析 ● 避開峰期啟動物聯網裝置 ● 最新物聯網資安防護威脅與事故	1 式	電子檔	109 年 8 月 15 日
4	場域解決方案符合國際工控系統資安規範合規程度檢測報告	報告內容含： ● 測試驗證規格項與列表 ● 測試驗證結果報告 ● 建議與相關附件	1 式	電子檔	109 年 11 月 15 日

項次	交付項目	交付內容	數量	交付型態	交付期限
5	期末報告	包含交付項目 1 至 4	1 式	電子檔	109 年 11 月 30 日

八、 技術能力需求(請詳述所需要之技術能力或專長)

本計畫執行人員須具備資訊領域相關基礎知識背景外，尚須對工控設備資安之風險威脅、滲透測試手法、以及相關檢測方法、工具有專業執行能力。

附件1：契約書格式
1-1：計畫書格式
1-2：經費動支報表
1-3：成果報告撰寫須知
1-4：報告格式
1-5：論文格式
1-6：保密聲明書
1-7：委託匯款同意書