經濟部 110 年度
《人工智慧導向資安共創技術計畫》
合作研究計畫

《工控資安合規驗證自動化先導研究》

建議書徵求文件

財團法人資訊工業策進會

中華民國 110 年 03 月 22 日

110年度合作研究計畫建議書徵求文件

一、 簡介

工業控制系統（ICS）之資安問題日益嚴峻，然而國內多數擁有工控系統的製造業者缺乏對廠辦整體的全盤檢視能力，對此可透過已研析建立的自檢表來實現全面初步檢視；製造業者在確認可能缺弱處後，進一步需要短期或長期的監控分析，對此則有已開發的網路流量側錄軟體可供偵測、預警，但在實施偵測佈建前需先掌握廠區基本環境，在環境允許下方可實施，因而有基本調查程序。

針對工控資安檢視到防護，雖已有對應的自檢表、布建前環境調查表、布建後的長短期偵測分析，最後提供資安分析報告，但各程序各自分立，缺乏自動化串連機制，難以快速複製、擴展工控資安防護。為強化資安防護，需在廠區依據規範導入工控資安，並對其進行驗證，然現階段的導入與驗證，仍高度倚賴人力介入，若無法將程序自動化(Process Automation)，將放慢防護擴展速度，影響整體安全。因此需進行導入及驗證程序之自動化先導研究。並依此開發一套線上資訊系統，以便加速防護程序，包含工控資安導入前全盤檢視、防護導入前環境調查、防護導入後長短期偵測分析，以及最終檢測報告。

二、 計畫目標

本計畫目標為開發一套線上資訊系統(包含工控資安導入前全盤檢視、防護導入前環境調查、防護導入後長短期偵測分析，以及最終檢測報告)，藉由導入程序自動化技術與工具，加速上述四階段防護程序之執行與管理，產出之系統預計導入至少 10 家製造業者並完成概念性驗證，並針對產出結果，針對製造業進行問題分析及建議報告。

三、 計畫範圍

本計畫預期工作項目包括：

1. 資訊系統整體設計如下：

(1) 整體系統管理需包含：使用者操作介面設計、會員之權限設定、線上報名、系統功能安全性檢測、源碼掃描等說明。並符合開源原則以及提供具體明確可正確執行之 API 規範等相關功能。

(2) 工控資安防護自動化程序系統，須具備以下功能模組/元件：

(a)製造業者工控資安檢視基準模組：根據合乎美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）制定的資安框架 1.1 版（Cybersecurity Framework version 1.1, CSF v1.1），客製化成為製造業者資安檢核基準，並可加總計算整體防護分數，以及繪製、呈現可比較之雷達圖。

(b)製造業者工控資安快篩評估模組：為確認製造業者適合參與工控資安快篩，應針對場域完成「應用系統」、「網段設計」、「資安防護設備」分析，協助製造業者針對自行場域進行自評(如選擇項目、測試範圍等相關資訊)，並提供相關快篩場域佈署教學操作手冊(如 IT/OT 佈署所需設備與如何安裝等相關資訊)。

(c)產線網路封包流量側錄資料上傳模組：可讓製造業者上傳其錄製之封包檔案，需有加密機制的功能，並可單一檔案上傳或指定資料夾批次上傳。

(d)工控資安檢測報告模組：針對檢測問題設計開單與追蹤機制，並可收容、彙整各檢測資訊，自動產生工控資安檢測報告，並可分頁檢視、列印檢視，以及提供給會員檢視功能。

以上 4 個模組功能需達到自動化服務串連機制。

2. 概念性驗證

透過辦理先導 POC 工作坊等方式，針對上述工控資安防護自動化程序系統，導入至少 10 家製造商進行概念性驗證，導入對象、方式以及驗收規範，需與主計畫團隊溝通同意方可進行。最後針對導入之 10 家製造業者，完成驗證分析書面報告；我方視需要召開工作會議，承接單位需派員出席，提出報告驗收。

四、 預期成果

1. 110年6月底前完成工控資安防護自動化程序系統(雛型)，110年10月底前完成工控資安防護自動化程序系統(正式版)，系統需包含4項模組：工控資安廠辦整體資安檢視調查模組、工控資安防護布建前環境評估調查模組、產線網路封包流量側錄資料上傳模組、工控資安檢測報告模組，並於正式版產出相關文件(使用者操作手冊、測試報告書)。
2. 110 年 11 月前完成至少 10 家製造商進行概念性驗證，並產出 1 份場域實證導入成果分析報告。
3. 12 月初舉辦 1 場聯合成果發表會。

※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

本計畫運用業界的研發能量與領域知識，配合主計畫「人工智慧導向資安共創技術計畫」提供我國製造業者工控系統資安相關防護，進行如「三、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. 建置工控資安防護自動化程序系統，包含 4 項模組，完成對系統之原碼安全檢測作業。
2. 召募至少 20 家國內製造商，透過工作坊蒐集資安需求，並促成至少 10 家業者導入所建置之工控資安防護自動化程序系統，進行概念性驗證。
3. 針對上述同意導入業者之驗證結果，以書面方式提出場域實證導入成果分析報告及提出建議，我方視需要召開工作會議，承接單位需派員出席，提出報告驗收。

六、 計畫期程及預估計畫總經費

計畫執行區間： 110 年 04 月 15 日 至 110 年 12 月 15 日

總經費：700,000元(含稅)

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	工控資安防護自動化程序系統(雛型)	1.包含 4 項模組(雛型)檢視模組、環境調查模組、側錄檢測模組、檢測報告模組 2.原始程式碼、安裝檔 3.設計檔	1 式	電子檔	110 年 6 月 30 日
2	5 家製造業場域實證	完成場域實證結果紀錄	1 式	電子檔	110 年 8 月 30 日
3	5 家製造業場域實證	完成場域實證結果紀錄	1 式	電子檔	110 年 10 月 29 日
4	相關手冊	1.使用者操作手冊 2.測試報告書 (1) 功能測試報告 (2) 第三方安全性檢測報告	1 式	電子檔	110 年 10 月 29 日
5	工控資安防護自動化程序系統(正式版)	包含 4 項模組(正式版)檢視模組、環境調查模組、側錄檢測模組、檢測報告模組	1 式	電子檔	110 年 10 月 29 日
6	至少 10 家製造商驗證結果分析報告	報告內容含： ● 檢測結果 ● 檢測分析 ● 效益 ● 建議	1 式	電子檔	110 年 11 月 30 日
7	成果發表會	舉辦 1 場聯合成果發表會	1 場	電子檔	110 年 12 月 10 日

八、 技術能力需求

本計畫執行人員須具備資訊領域相關基礎知識背景包含：

1. 具有商務流程管理軟體之開發經驗。
2. 具有製造業客戶服務經驗。