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

《工控資安異常行為技術研發》

建議書徵求文件

財團法人資訊工業策進會

中華民國　110 年 3 月

110年度合作研究計畫建議書徵求文件

一、 簡介

近年來國內工控之資安事件層出不窮，例如2018年Wanncry病毒散播至台積電內網，造成損失逾52億，而去年工控資安攻擊事件更是延伸到關鍵基礎設施，像是中油和台塑在2020年就遭受到勒索病毒ColdLock攻擊，緊接著半導體封測大廠力成也遇到類似的攻擊事件，甚至2020年的下半年度，工控電腦大廠研華和鴻海墨西哥廠也都傳出遭受駭客攻擊的消息，所以針對工控資安的防護解決方案已到了刻不容緩的地步。

正因為工業控制系統缺乏資安考量，許多生產設備原本在獨立的系統與隔離的環境操作，在設計建置之初，缺乏資安防護、身份驗證和基本加密等防護功能，導致近幾年各項工控設備聯網之後，產生大量的網路漏洞，讓駭客有機可乘。甚至是在2017年，第一個針對SIS (Safety Instrumented System)攻擊的Trisis惡意程式，把攻擊目標轉向了施耐德電氣的Triconex安全儀表系統(SIS)控制器。

為了強化工控(OT, Operational Technology)資安，本合作計畫（以下簡稱本計畫），將從以攻為守的角度，先就常見的工控關鍵裝置開發攻擊測試案例，如例DCS(Distributed Control System)或是PLC (Programmable Logic Controller)，而攻擊的測項，則以據MITRE ATT&CK公司彙整定義的攻擊手法發展。MITRE ATT&CK for ICS (https://collaborate.mitre.org/attackics/index.php/Main_Page) 中已定義了11個策略(Tactics)和81個技術 (Techniques)，如下圖所示：

圖1 MITRE ATT&CK for ICS

因此，本計畫預期針對Trisis惡意程式研析，以了解工控惡意程式的攻擊手法，並針對Mitre所定義的攻擊技術先行分析，並根據Trisis惡意程式的Cyber Kill Chain，實作出其中20條關鍵的攻擊手法，並針對這20條攻擊滲測案例，研發對應的AI防禦偵測方法。

二、 計畫目標

本計畫目標完成兩項工作目標，1）工控攻擊測試案例；2）工控資安異常行為偵測技術，以下細部說明：

1）工控攻擊測試案例：

預計針對Mitre Att&ck for ICS 探討工控資安的攻擊手法，並從81個攻擊技術(Techniques)中，實作出20個關鍵的攻擊腳本，並將這些攻擊腳本實際在測試平台上演練，而演練成果紀錄下來存成PCAP紀錄檔，以利後續驗證異常行為偵測技術。

2）工控資安異常行為偵測：

預計針對上述20個關鍵的攻擊腳本，提供工控網路異常行為偵測技術，可以利用Autokeras或AutoML等自動化機器學習工具，自動分析工控異常行為。

三、 計畫範圍

本計畫預期產出兩個項目，工控攻擊測試案例20條和工控資安異常行為偵測技術一式，針對工控攻擊測試案例，主要需要模擬Trisis惡意程式，並以MITRE定義的攻擊手法實作出攻擊手法，不限使用何種語言實作；針對工控資安異常行為偵測技術，可分析工控專屬協定，並提供工控網路AI異常偵測技術，但不限定用特定AI技術偵測工控異常資安行為。

四、 預期成果

本計畫會有期中測試案例報告一份和期末偵測技術驗證報告一份報告各一份(含教育訓練)，並且預期投稿國內外知名研討會或期刊論文一篇。

本研究計畫案之工作項目如下表：

表 1 工作項目查核點時間表

項次	工作項目	工作內容&交付項目	查核時間點
1	工控攻擊測試案例	• 以Mitre定義之工控攻擊測試案例20條以上，包含測試案例腳本原始碼一份 • 測試案例報告一份	110/6/30
2	工控資安異常行為偵測技術一式	• 偵測項次1之攻擊測試案例之偵測程式一份 • 偵測技術驗證報告一份	110/11/30
3	投稿國內外知名研討會或期刊論文一篇	• 投稿國內外知名研討會或期刊論文一篇	110/11/30

※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

本計畫預計將結合學界在理論面以及本會在資安弱點測試平台建置的實務面經驗，透過雙方相互合作討論的方式來進行，本計畫亦需提供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. 完成相關文獻蒐集等先前技術整理。
2. 完成工控攻擊測試案例程式編寫。
3. 完成工控資安異常行為偵測技術，並完成系統功能測試。
4. 完成結案報告，驗證分析系統的正確性、成果品質以及教育訓練分享。

六、 計畫期程及預估計畫總經費

計畫執行區間： 110 年 01 月 01 日 至 110 年 11 月 30 日

總經費：70萬元整(含稅)

七、 驗收標準(含教育訓練)

1、 期中、期末報告:分別預計於 110 年 6 月 30 日前與 110 年 11 月 30 日前完成期中與期末報告:

- 期中報告的內容包含: 工控攻擊測試案例報告。
- 期末報告的內容包含: 工控資安異常行為偵測技術的研究成果、相關的功能驗證報告以及雛形展示。

2、 雛形系統:期末完成工控資安異常行為偵測技術模組，包含執行檔、程式原始碼及檢測功能驗證。

- 智慧工廠實際資料存取案例分析針對至少一個測試平台進行探討。

3、 提供教育訓練:針對計畫成果移交、系統運作機制及操作說明等提供教育訓練。

4、 進度討論會議:每月召開一次進度研討會議。

5、 投稿國內外知名研討會或期刊論文一篇。

八、 技術能力需求

1、 資料分析與人工智慧相關背景:須瞭解網路系統運作原理，熟悉巨量資料分析技術，並具備機器學習等各項人工智慧相關技術模組開發經驗，能掌控本計畫研發所需核心技術。

2、 相關計畫參與經驗:熟悉深度學習運作原理，了解轉移學習運作原理，並具相關領域研究論文發表及計畫執行經驗。

3、 其他:如熟悉 C/C++、Python、一般深度學習架構如 Keras/TensroFlow/PyTorch 等框架的運作與程式撰寫。