科技部工程技術研究發展司
「發展智慧製造及半導體先進製程資安實測場域專案計畫」
徵求說明

壹、計畫背景說明

智慧製造的範疇相當廣泛，從單機智慧化、產線智慧化、到整廠智慧化，各有其重要的關鍵技術。單機透過機邊電腦(Edge computing)可達到單機智慧化(智慧機械)、製程數據收集以及與雲端資料庫連結等目的，在整線製程方面則可透過 Gateway 電腦(Fog computing)連結不同機台來進行高效率與稼動率之協作，而整廠通常是透過雲端伺服器來達成，其主要的任務與智慧排程、工廠管理、預防保養與數據分析(智慧製程)等有關。從單機自我學習之智慧化，到數個機台(含機械手臂)之智慧合作互動與決策，最後到包含許多功能不同機台之複雜大型系統(整廠)，其間各製造與自動化單元的之智慧合作互動與決策，如此才能形成完整之智慧製造系統，實現無人機械(單機智慧化)、無人生產線(整線智慧化)與無人工廠(整廠智慧化)。然而，當增加設備與網路之間的連接，則可能會產生許多隱私與安全風險。

在物聯網(Internet of Things, IoT)、大數據(Big Data)與人工智慧(Artificial Intelligence, AI)等技術的潮流下，各國政府在智慧製造、智慧工廠、工業 4.0 等產業積極推動政策，促進智慧化轉型升級，使得工控設備連網需求逐年遞增，同時也將面臨網路威脅，而如何有效管理並加以防範為國人關注的議題。

此外，近年來勒索病毒日趨猖獗，越來越多駭客組織注意工控系統是脆弱的，製造業的資安事件頻出不窮，其攻擊手法大多為使用勒索病毒，在 2020 年後更是針對關鍵基礎設施進行更多的攻擊，如飛機零組件供應商 Asco 公司遭勒索軟體攻擊、南非約翰尼斯堡電力公司 City Power 遭勒索軟體感染等攻擊事件，2019 年至 2021 年國際資安攻擊事件統計如表 1 所示。除國外勒索事件，近年國內重大資安事件如表 2 所示，2020 年 5 月爆發兩家石化公司遭到勒索病毒攻擊、2018 年台積電產線資安事件，造成 52 億元的經濟損失、2019 年卡巴斯基發現駭客透過華碩的更新伺服器，為電腦安裝後門，

造成眾多用戶受害。然而，隨著資訊科技(IT)快速發展，使得 OT 場域逐漸失去實體隔離的特性，工業控制系統與 IT 環境介接或是直接連上網際網路，都為工業工控環境帶來極大的風險，一旦工控設備遭駭客控制，後果不堪設想。在智慧製造導入資安技術的研究當中，國內趨勢科技分析在 IT (Information Technology)、OT (Operational Technology)、IP (Intellectual property)系統整合下，對於資安問題必須有新的思維。近年來大大小小的資安事件頻傳，都證明關鍵基礎設施在生產的當下其安全系統也非常重要，任意中斷服務容易造成生產線停工，進而影響公司營運。

表 1 近年 ICS 國際攻擊重大事件統計

日期	事件描述
2021 年 2 月	美國淨水廠系統遭駭，攻擊者意圖加入大量氫氧化鈉汙染水質
2020 年 7 月	南非約翰尼斯堡電力公司 City Power 遭勒索軟體感染 ，造成家庭與企業用戶停電長達 12 小時
2019 年 6 月	飛機零組件供應商 Asco 公司遭勒索軟體攻擊，造成四個國家的工廠停產
2019 年 3 月	鋁業大廠 Norsk Hydro 遭 LockerGoga 攻擊，部分自動化生產線關閉
2019 年 3 月	委內瑞拉電網(古里水電站)工業控制系統遭受駭客攻擊導致全國大停電
2019 年 2 月	日本光學製造商 HOYA 泰國工廠遭到網路攻擊，部分生產線因此癱瘓

表 2 近年國內重大資安事件

日期	事件描述
2021 年 4 月	廣達遭勒索軟體攻擊，許多客戶的設計圖因此外洩，駭客團體 REvil 要求廣達支付 5000 萬美元
2020 年 7 月	GPS 及穿戴式裝置大廠 Garmin（臺灣國際航電）遭勒索軟體攻擊，多項應用程式與服務停擺
2020 年 6 月	PCB 大廠欣興部分系統遭病毒感染，導致生產受影響
2020 年 5 月	半導體封測廠力成湖口廠區遭勒索軟體攻擊，造成生產作業發生短暫停工
2020 年 5 月	中油、台塑等兩大石化公司受到勒索軟體攻擊
2018 年 8 月	台積電產線中毒，造成 52 億元的經濟損失

由上述可知，安全轉型扮演著至關重要的關鍵。在全球數位轉型趨勢下，企業應同時對資訊 IT (Information Technology)、整體產業自動化營運 OT (Operational Technology)與相關個資保護之資安防護進行整體性規劃。製造業數位轉型升級需要的是根據 ISO27001 設計管理制度，然而 ISO 27001 缺少實作的指導方針(guideline)與實作細節，將可透過 IEC 62443 進行 OT 端工

控補強。(備註： IEC 62443 由 ANSI (美國國家標準學會)/ISA (美國國際標準管理局)提出，被 ISO/IEC 採納；所以該標準會以不同的名字出現，包括：ANSI/ISA-99，ISA-99，ISA 62443，ISO/IEC 62443，ISO 62443，IEC 62443)。

貳、計畫目標

一、由智慧製造領域/半導體製程領域及資安領域學者共同合作，以縱深防護策略發展資安技術，涵蓋邊界層、內部層、應用層、實體層、主機層、資料層等智慧製造場域各防護層，且研發之技術必須在智慧製造場域/半導體製程場域進行實測驗證。

二、藉由弱點掃描、滲透測試、資安檢測、攻防演練等，持續精進資安防護技術。

三、開設工控資安培訓課程，培養種子師資及博碩士班學生等工控資安科研人才。

四、藉由智慧製造資安實測場域/半導體製程資安實測場域之建置經驗、培育之工控資安人才，協助合作企業之智慧製造場域/半導體製程場域提升資安防護能量。

參、計畫內容與重點研究項目

一、本專案計畫以資安應用導向為主要目標，需符合圖 1 所列項目主題且以「智慧製造場域」及「半導體製程場域」之實測為發展主軸，並進行資安軟硬體技術、資安應用導向技術開發。此外，若有符合智慧製造的資安議題，但未羅列於圖 1 之 12 項範圍中，計畫團隊提出申請且經審查後符合本專案計畫精神者，亦可納入推動。其研究主題列舉如表 3 所示。

圖 1 智慧製造技術前瞻研發 vs. 資訊安全議題

表 3 資安研究主題列舉

項目	研究主題列舉
感測層 工業物聯網架構與應(IIoT)、 工業控制系統(ICS)安全	● 符合IEC62443規範之感測層主題 ● 安全程式來源偵測與佈建研究 ● 針對需要人機協作(HMI)的環境，將資安落實到韌體層次 ● Embedded/IIOT/ICS(工業控制系統)逆向工程研究 ● 研究保護update/patchEmbedded/IIOT/ICS系統 ● Embedded/IIOT/ICS(工業控制系統)入侵偵測系統研究 ● 相容於Embedded/IIOT/ICS(工業控制系統)通訊標準之訊息來源驗證研究 ● 工業物聯網網路架構安全技術研究 ● 匿名網路攻擊溯源與防範 ● 惡意行為偵測與分類技術等研究
網通層(資料傳輸層) 機邊電腦與邊緣計算	● 符合IEC62443規範之網通層主題 ● 實施自動化軟體風險分析 ● 建立偵測精密製造設備漏洞或惡意邏輯的機制 ● 建立工業設備與開發環境的軟體隔離與權限劃分機制 ● 保護數據分析和邊緣運算技術，包含：機邊電腦，傳輸程式，資料閘道器和等研究 ● 設計安全的新系統，並提供有效的選項來保護和操作

	大量正在使用的舊系統等研究
應用層 雲端資料與行動HMI資安防護	● 符合IEC62443規範之應用層主題 ● 製造執行系統資料庫防護 ● 採取和非OT環境軟體(如行動應用程式、網站應用程式、雲端環境等等)相同等級的程式設計安全與防禦措施 ● 智慧製造環境當中建立完整的資料與軟體「信任鏈」 ● 惡意程式與雲端攻擊偵測 ● 大數據及智慧製造等自動化攻防技術等研究

二、計畫時程及預計達成目標

本專案計畫時程為 3 年(110-112 年)，每年度預計達成之目標概述如下。計畫團隊將每年進行考評，考評不通過者將予以退場。

(一)第一階段(Phase I)

本階段係針對學界團隊於智慧製造/半導體製程資安實測場域內之聯網機邊電腦與控制器等設備進行資安攻防演練。主要工作包含：

1.透過攻防劇本設計，完成智慧製造/半導體製程資安實測場域用攻防演練實驗環境建置。

2.智慧製造場域/半導體製程場域資安技術導入，藉以整合 IT 與 OT。

3.計畫執行團隊須參加計畫辦公室所舉辦之資安攻防演練公測。

4.實測場域導入 IEC 62443 工業控制系統資訊安全標準規範，並進行 IEC 62443 工控資安人才培育。

(二)第二階段(Phase II)

持續精進資安技術，並導入智慧製造/半導體製程實測場域，透過智慧製造/半導體製程實測場域環境與雲端資安攻防平台(Cyber Defense Exercise, CDX)結合，做為虛實整合攻防平台，同時進行設備端資安防護實測與弱點掃描，主要工作包含：

1.智慧製造資安實測場域進行實體維運及資安測試。

2.在半導體製程資安實測場域部分，計畫執行團隊需掌握、並依循國際半導體產業協會(SEMI)之相關規範，同時依據 OT 層安全漏洞進行研究評估(如 SEMI 6506A 所訂定之 OT 資安規範)。

3.開設工業控制系統資訊安全標準驗證認證之培訓課程。

4.智慧製造場域通過 IEC 62443 工業控制系統資訊安全標準規範驗證。

(三)第三階段(phase III)

持續精進資安技術，智慧製造/半導體製程資安實測場域在面臨到攻擊時，可自主因應並主動提出示警資訊。主要工作包含：

1.建置虛擬化、智慧化資安攻防演練環境(平台)，協助計畫團隊工控資安技術能量。

2.建立驗證規範(例如訂定指引或白皮書)，協助國內製造業建立資安防護能量。進一步與國外驗證單位(如 TÜV)界接，協助國內業者取得 IEC 62443 工業控制系統資訊安全標準認證。

3.由種子教師開設 IEC 62443 工控資安相關課程，提升學界及業界對於工控資安之瞭解，進而提升資安防護能量。

4.計畫團隊參加資安技術成果發表會，加速將學界之資安研發成果推廣至產業應用，並促進產學研人才合作交流。

肆、計畫申請與審查

一、計畫申請

(一)申請機構及計畫主持人資格須符合「科技部補助專題研究計畫作業要點」規定之資格。

(二)計畫主持人以申請一件本專案計畫為限。

(三)申請案必須為單一整合型計畫，請將總計畫及各子計畫(至少 3 項(含)子計畫)之執行內容及經費需求等整合成一份計畫書，並由總計畫主持人之服務機關提出申請。

(四)主持人按本部規定列入執行本部專題研究計畫計算件數，共同主持人不列入執行本部專題研究計畫計算件數。

(五)本專案計畫必須跨領域合作，主持人需具備智慧製造或半導體製程技術背景專長，共同主持人需具備資安技術專長。

(六)計畫團隊必須具備實測場域，並於計畫書中載明場域之設施及規格(詳如

附件 1)供審查。

(七)計畫書中須詳述擬研發之目標技術，其國內現況與國際比較，包含下列項目：

1.目標技術之臺灣發展現況、國際發展現況、與國際標竿技術規格之比較。

2.藉由 IEC 62443 等相關規範進行弱點掃描、資安檢測，以瞭解目前場域中資安防護能量不足之處。

3.藉由本項整合型計畫之投入，目標技術、資安防護能量預期可提升程度(分年及 3 年全程)，與國際標竿之比較(需有明確規格與數據)。

(八)計畫書須明確說明每季技術里程、查核點及評量指標、最終效益，以做為審查委員查核之依據。

(九)本專案計畫以強化產學合作、落實產業應用為目標，故計畫內容必須以產業技術需求(demand pull)為導向，必須以產業技術需求(demand pull)為導向，針對智慧製造及半導體製程之資安技術缺口進行研發。此外，學界研究團隊必須邀請國內業界參與共同執行計畫，並於 110 年度計畫提案時，一併檢附合作企業參與計畫意願書及合作內容說明(詳如附件 2)，合作企業參與之方式可以為提供實測場域、提供研究設備、提供研發人力、投入配合款…等。

(十)若計畫相關內容有獲得本部、其他部會、法人、業界經費補助，請於計畫書中敘明本計畫申請案與本部、其他部會、法人、業界經費補助執行內容間之差異與互補。

(十一)本項專案計畫每年度申請總經費以不超過新臺幣 600 萬元為原則(專案計畫推動辦公室之申請經費不受此限)。基於資源有限，本專案計畫以不補助購置大型硬體設施或軟體為原則，請強化學界現有設施及平台之共用與協調支援，以使有限資源發揮最大效益。此外，鼓勵業界及校方投入資源，與本部共同推動本項專案計畫。

(十二)本專案計畫為分年核定之 3 年期(110-112 年)計畫，每年進行考評，考評通過者始核給下一年度計畫。本部除了淘汰執行成效不佳之計畫團隊

外，並得整併計畫團隊與調整計畫成員、調整計畫執行內容。

1.第一年計畫執行期間為 110 年 11 月 1 日至 111 年 5 月 31 日。

2.後續二年(111-112 年)計畫之執行期間為當年度 6 月 1 日至翌年 5 月 31 日。

(十三)申請書表格請採用本部一般專題研究計畫之計畫書格式。線上申請時，請選擇「專題類-隨到隨審計畫」，計畫類別請選擇「一般策略專案計畫」，計畫歸屬請選擇「工程司」。研究型別請選擇「整合型計畫」，學門代碼請選擇「E9865 物聯網應用場域資安強化推動計畫」。

(十四)有關本專案計畫相關問題，請洽詢科技部工程司杜青駿副研究員，電話：(02)27377527，電子郵件信箱：cctu@most.gov.tw，國研院儀科中心林郁洧組長，電話：(03)5779911 分機 642，電子郵件信箱：james722@narlabs.org.tw。有關線上申請系統操作問題，請洽本部資訊系統服務專線，電話：(02)27377590、27377591、27377592，電子郵件信箱：misservice@most.gov.tw。

二、計畫審查

(一)審查作業包括初審及複審，如有必要，將安排計畫主持人、共同主持人或合作企業出席審查會議，或由本部至申請機構實地訪查。

(二)除本部「補助專題研究計畫作業要點」所列審查重點，以及工程司「專題研究計畫審查意見表」所列審查項目之外，本專案計畫審查重點包含：

1.對國際發展現況、國內產業發展現況與技術缺口之掌握，擬開發之目標技術是否確為業界所需，技術里程、查核點及評量指標、分年執行內容及階段性里程碑(milestone)、最終效益、落實於產業應用之作法、對國內產業之具體助益等是否明確。

2.國內外標竿技術規格之掌握與比較，研發成果超越標竿技術規格之可行性。

(三)本專案計畫無申覆機制。

三、其餘未盡事宜，應依本部補助專題研究計畫經費處理原則、專題研究計畫補助合約書與執行同意書及其他有關規定辦理。

伍、計畫考核

一、依本部「補助專題研究計畫作業要點」，於期中各年計畫執行期滿前 2 個月至本部網站線上繳交進度報告，全程計畫執行期滿後 3 個月內至本部網站線上繳交研究成果報告及辦理經費結報。

二、每季或不定期(依本部通知)繳交執行進度或績效指標達成情形等資料，供本部檢視執行情形。

三、為加強跨計畫團隊間之互相觀摩，並藉由同儕間之激勵而提升研發成效，將由各計畫團隊輪流主辦成果觀摩會，各計畫團隊均須出席。

四、計畫執行團隊須出席本部舉辦之成果展或技術媒合會等，以加速計畫成果推廣至產業應用，以及出席本部於測試場域舉辦之實測考評，並由本部邀請之審查委員檢視各計畫團隊之執行成果。

五、本部邀請審查委員進行書面審查及現場訪視之審查結果，成果展或技術媒合會、實測考評、資安攻防演練之審查結果，將一併做為是否核給下一年度計畫之參考。此外，本部得依據審查結果，調整計畫內容及經費(含刪除計畫共同主持人、刪減經費等)、提前終止計畫，俾確保所研發之技術可落實於產業或社會民生應用。

附件 1、場域設備資產盤點表

序號	設備類型	廠牌	型號	控制器型號或作業系統版本	通訊介面	備註
1	(填寫參考範例)振動感測器模組	NI	NI cDAQ-9189	NA	Ethernet	連線到機邊電腦 B
2	(填寫參考範例)交換器	Cisco	Catalyst 2960	NA	Ethernet	接收與轉發數據
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

附件 2：合作企業參與計畫意願書

合作企業參與計畫意願書

本企業（名稱：＿＿＿＿＿＿＿＿）參與科技部「發展智慧製造及半導體先進製程資安實測場域專案計畫」（計畫名稱：＿＿＿＿＿＿＿＿，主持人＿＿＿＿），同意並遵守下列合作事項：

一、 ...（提供研究經費、軟硬體設備項目及數量、研究人力如工程師人數及參與方式等等）

二、 ...（提供實務場域供測試驗證等等）

三、 ...（技術移轉費用等等）

四、 ...（配合舉辦公開成果發表會等技術推廣活動等等）

五、 ...（啟動後續產學合作經費與時程等等）

本企業所提供之本計畫申請書內容及各項資料，皆與本企業現況與事實相符。本企業於本計畫所提出之內容未曾向其他政府機關（構）申請補助，且絕無侵害他人專利權、著作權、商標權或營業秘密等相關智慧財產權，如有不實情事，本企業願負一切責任。特此申明，以茲為憑。

此致

科技部

合作企業負責人：＿＿＿＿＿＿（簽章）

合作企業印鑑：

中華民國　　年　　月　　日