符合 IT 與 OT 資安規範之半導體製程具可擴充性微隔離場域之資安系統架構設計

Information Security System Architecture Design of the Micro-isolation Field with the Expandable of the Semiconductor Manufacturing Processes Obeying the IT and OT Information Security Standards

蔡佳勳、蔡坤諭、陳興忠、莊旻儒、李建霖

Jia-Syun Cai, Kuen-Yu Tsai, Hsing-Chung Chen, Min-Ju Chuang, Chien-Lin Lee

資訊科技 (information technology, IT) 著重於計算機與網路通用面向，它不同於運營科技 (operational technology, OT) 著重於工業控制系統 (industrial control system, ICS) 的操作和程序控制面向。一旦 OT 設備連上網路後，OT 場域將面臨和 IT 相同之資訊安全問題，因此需要具有 IT-OT 整體考量之網路安全功能，以確保半導體關鍵製程與環境參數資料的安全性與正確性。本文簡介並探討一個研究中的 IT-OT 微隔離場域資安防護架構，微隔離場域內使用攜帶式防毒工具與入侵防禦系統進行惡意軟體掃描與網路存取管控，防止攻擊者存取場域內的關鍵製程參數。未來並將導入相關國際資安標準 (如 IEC 62443、SEMI E187) 之規範，協助半導體產業之製程場域提升資安防護能量。

Information technology (IT) focuses on the general aspects of computers and networks. It is different from operational technology (OT), which focuses on the operation and program control aspects of the industrial control system (ICS). Once OT equipment is connected to the Internet, the OT field will face the same information security issues as IT. Therefore, it is necessary to have a network security function with the overall consideration of both IT and OT to ensure the safety and accuracy of the semiconductor key process and environmental parameter data. This article briefly introduces an ongoing research on an IT-OT micro-isolation field cybersecurity protection framework that uses portable antivirus tools and intrusion prevention systems for malware scanning and network access control to prevent attackers from accessing critical process parameters in the field. The related international information security standards (such as IEC 62443 and SEMI E187) will be incorporated to facilitate information security protection in the semiconductor manufacturing facilities.

一、前言

工業控制系統 (industrial control systems, ICS) 是一種基於工業控制域 (industrial control domain) 中特殊協定且不同於基於 TCP/ IP 通用協定下傳統的商業域 (commerce domain) 所使用的資訊系統。ICS 的主要用途是管理重要的基礎設施，例如石油和瓦斯設施、核能電廠、智慧電網、自來水和廢物水處理以及機場或捷運中央監控系統等資訊設備。ICS 有許多獨特的功能特性，包括提供即時監控和非常高需求的可用性、可預測性、可靠性，以及分散式智慧計算。其中，許多先進的計算，通信和網際網路科技被結合到 ICS，使得能涵蓋並滿足更多的用戶要求，例如結合到外部世界開放系統的 ICS，使得工業控制系統支援具有移動性、資料分析以及可擴展性的裝置進行遠端監控。但是，對 ICS 而言，這些支援開放性系統的功能卻暴露了關鍵基礎設施的幾個 ICS 的重大安全問題[1]。簡而言之，IT 著重於計算機與網路通用面向，它不同於 OT 著重於 ICS 的操作和程序控制面向[2]。

隨著先進工業的發展，許多廠房設備已將 IT-OT 整合在一起。藉由無線通訊連線，可為 OT 提供更好的系統監控及遠端控制設備的能力。當資料採集與監控系統 (supervisory control and data acquisition, SCADA) 連上網際網路時，OT 將面臨與 IT 相同的惡意軟體、身分管理、存取控制等安全問題。兩者間的差異在於 OT 系統中的漏洞，可能會導致關鍵的基礎設備遭受到被破壞的風險[3]。Fortinet 公司於 2018 年的報告指出，將近 90% 有連線 OT 基礎架構的企業組織，其監控和資料擷取與工業控制系統 (SCADA/ICS) 架構，都曾遭遇安全漏洞，其中超過一半的漏洞發生在過去 12 個月內。安全問題包括病毒 (77%)，內部 (73%) 或外部 (70%) 駭客，敏感或機密資料外洩 (72%)，以及缺乏設備驗證 (67%)[4, 5]。目前已有許多措施可採取，以確保系統的可靠性與安全性，包括：使用防毒軟體與應用程式白名單保護 PC 資產、建立系統修補政策以保持軟體在最新狀態、將連網設備建置在防火牆後進行隔離、遠端存取時需透過虛擬私人網路 (virtual private network, VPN) 進行連線、導入多因子驗證技術等[6]。

目前工業自動化和控制系統 (IACS) 的網路安全 (工業控制資訊安全) 標準主流是 IEC 62443，該標準是由國際自動化協會 (International Society of Automation, ISA) 提出並由美國國家標準協會 (American National Standards Institute, ANSI) 公開頒布，而後被國際電工委員會 (International Electrotechnical Commission, IEC) 組織採納。而 IECEE 是 IEC 系統給電機工程學設備及零件的符合性評鑑方案，並且是一個基於 IEC 國際標準的多邊認證系統。IEC 62443 標準技術規範的群體範圍[7-13] 包括 IACS 的所有用戶 (包括機構) 組織的運營、維護、工程、公司元件、與控制有關或受其影響的製造商、供應商、政府組織系統網路安全、控制系統從業人員及安全從業人員。

雖然半導體的生產設備場域的工業控制資訊安全標準仍以 IEC 62443 為重要標準。但是近二、三十年以來，由於半導體的生產設備的兩項資安上的重大問題：第一個問題是多數製程設備所使用的作業系統相當老舊，原廠已經停止支援，例如：Windows XP 以及 Windows 2000 等作業系統；第二個問題則是防駭客攻擊、防毒軟體和白名單等資安防護機制與半導體機台設備之間的相容性問題，使得半導體業者部署這些產品之後，可能面臨嚴重影響廠房運作的現象[14]。半導體代工大廠台積電 (TSMC) 於 2018 年遭遇大規模資安攻擊事件[15]，也讓資訊安全成為全球高科技產業不可忽視的重要議題。透過國際半導體產業協會 (SEMI) 的標準推動平台，工研院 (ITRI) 與台積電於 2018 年 9 月著手成立晶圓廠暨

設備資安工作小組 (Fab & Equipment Information Security Task Force)，並於 2021 年 12 月正式在 SEMICON Taiwan 2021 國際半導體展上發佈 SEMI 首個半導體晶圓設備資安標準 (SEMI E187-Specification for Cybersecurity of Fab Equipment)，於 2022 年 1 月正式上架，成為全球業界推動半導體資安標準的先驅[16]。SEMI E187 著重於四大類晶圓廠設備的最低安全需求，包含：作業系統支援、網絡安全、端點防護和安全監控，適用於安裝 Microsoft Windows® 或 Linux® 作業系統的半導體晶圓廠設備的計算裝置，但不適用於可程式化邏輯控制器 (Programmable Logic Controllers，PLC) 和 SCADA[17]。於同年 3 月，SEMI 推出半導體資安標準 SEMI E188 (SEMI E188-Specification for Malware Free Equipment)，說明在半導體製造廠內的製造設備於生命週期中，從設備交付、安裝和支援活動中，所需要的資訊安全措施。適用於設備供應商、設備用戶、硬體和軟體組件供應商，以及任何計算設備 (例如：電腦、控制器、PLC) 等[18]。SEMI E187 與 SEMI E188 的設計目的主要都是防止設備的漏洞與威脅，SEMI E187 要求設備供應商應確保設備在整個生命周期的每個階段具有必要的安全能力。與其相比，SEMI E188 要求設備供商應確保設備在整個資產生命週期中遵循設備的無惡意軟體程序，以減輕惡意軟體的傳播[19]。

二、具可擴充性之半導體 IT-OT 微場域建置

近幾年來，異質整合及先進封裝已經是半導體業界熱門的技術議題。透過異質整合及先進封裝的技術，可將不同製程的小晶片模組整合在一起，確保設計擁有最大的彈性。異質分散式製造網不僅可有效利用既有製程資源、節省重複投資，也具備連結可擴充性與製造彈性，尤其在國際疫情與區域不穩定影響產業供應鏈韌性趨勢下，對於半導體產業創造新價值與穩定產能更是相當重要的技術。然而相對於傳統單一封閉型廠房，異質分散式製造網將面臨嶄新且嚴峻的資訊安全以及設備、廠務管理挑戰。

本文作者代表之團隊自 110 年 6 月迄今參與科技部 (現國科會)「發展智慧製造及半導體先進製程資安實測場域」專案計畫，研究主題為「符合 IT 與 OT 資安規範之半導體製程具可擴充性與聯防性設計的虛實整合場域之資安自主檢測機制研究」，探討可擴充性微場域的 IT-OT 系統設計法則與建置實務，以有效增強異質分散式半導體製造網的強韌性。

本研究規劃建置之可擴充性半導體製程 IT-OT 微場域與跨微場域聯防戰情與備援中心，其地理位置圖如圖 1 所示，共分為下列五大場域：

I. 臺灣大學竹北校區半導體資安場域研究實驗室 (主場域，微隔離場域 A：研發 (research & development, RD) 及資訊整合中心總部 (headquarter, HQ)、製程資料高效能運算 (high performance computing, HPC) 伺服器；微隔離場域 B：半導體製程場域 (蝕刻、微機電製程、微影檢測、晶粒測試))。
II. 亞洲大學半導體製程參數設計模擬實驗室 (副場域 1，微隔離場域 C：晶片設計、虛擬製程場域)。
III. 國研院台灣儀器科技研究中心奈米鍍膜實驗室 (副場域 2，微隔離場域 D：鍍膜場域)。
IV. 臺灣大學離子束實驗室 (副場域 3，微隔離場域 E：微影光罩製程場域)。
V. 亞洲大學智慧系統與網路安全研究室 (資安監控場域，微隔離場域 F：資安可視化及測試微場域、雲端虛實整合攻防平台)。

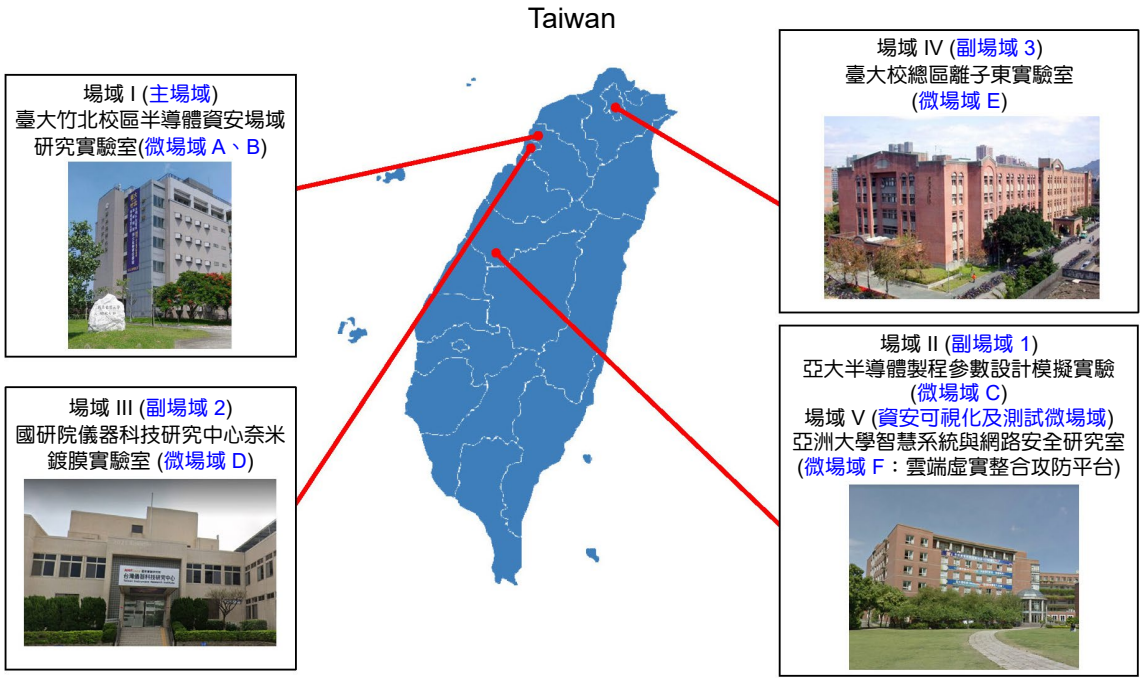


圖 1. 可擴充性半導體製程 IT-OT 微場域與跨微場域聯防戰情與備援中心地理位置圖。

本團隊目前主要集中於主場域微隔離場域 B 之半導體製程場域擴建與副場域 3 之網路與資安設備建置，其場域所提供之製程設備，可供異質整合技術開發使用。

三、半導體 IT-OT 微場域應用與資安挑戰

在次波長等級的微影下，受到非理想光學效應的影響，印在晶圓上的影像與原先設計的不同，這些由非理想光學效應所造成的圖形失真會嚴重影響電路的特性及效能，透過光學鄰近效應修正 (optical proximity correction, OPC) 技術，可經由軟體模擬微影後的圖形，並計算與設計圖案間的誤差，進行光罩圖案修正，讓最後印出的圖形貼近設計者的需求，達到可製造性設計 (design for manufacturability, DFM) 的目的[20, 21]。晶片製作人員將依照修正後的光罩資料、關鍵製程與設備設定參數，在穩定的環境狀態下進行光罩實作。因此半導體製程 IT-OT 微場域需要受到保護的資料主要可分為以下 3 大類：

1. 客戶所設計的光罩電路佈局資料 (含 OPC 前、後)。
2. 關鍵製程參數與主要製程設備設定參數。
3. 製程設備環境參數資訊監控 (例如：無塵室溫、溼度等)。

若未做好資安保護工作，異質光罩設計 (第 1 類) 與關鍵製程參數資料 (第 2 類)，將容易被駭客竊取，導致機密外洩，影響公司的產出及獲利；同時也需避免異質不同公司間資料混淆與 IP 保護。各場域製程設備的溫濕度及狀態資訊 (第 3 類) 也將受到監控，以確保設備皆在穩定的製程環境下運作。不穩定的環境，將增加製程的變異性，影響最終生產出的晶片良率。

半導體製程資料傳輸概念圖如圖 2 所示。亞大半導體製程參數設計模擬實驗室 (副場域 1) 內的兩台 IBM X3850 X6 伺服器採用 CentOS 7 作業系統，每台具備 Intel E7-4800 系列 CPU 與 1 TB 記憶體，將設計出來的異質電路光罩佈局 (第 1 類)，透過臺灣學術網路

(Taiwan Academic Network, TANet) 傳送至臺大碧禎館主場域之 HPC 伺服器。主場域內的 3 台自組 HPC 主機採用 Windows 11 作業系統，每台具備 12 核心的 Intel i7-12700 處理器與 128 GB 記憶體，將副場域 1 設計的光罩電路佈局進行光學鄰近效應模擬與修正。計算完成後，將修正後的異質光罩設計 (第 1 類) 與關鍵製程參數資料 (第 2 類) 同樣透過 TANet 由主場域傳送至臺大離子束實驗室 (副場域 3) 進行光罩製作。副場域 3 內具備一台蔡司 ORION NanoFab 氦離子束顯微鏡，具有 0.5 奈米的高解析度，可進行次 10 奈米結構的高精度加工。在此半導體製程資料傳輸的概念下，所有資料的傳遞必須確保傳輸過程之安全性，增強異質分散式製造網的可行度。此場域架構為一小型分散式半導體製造網之演示，將來可參考或移植本研究之軟硬體資安架構至適當之企業場域進行跨業界的擴充場域結合。

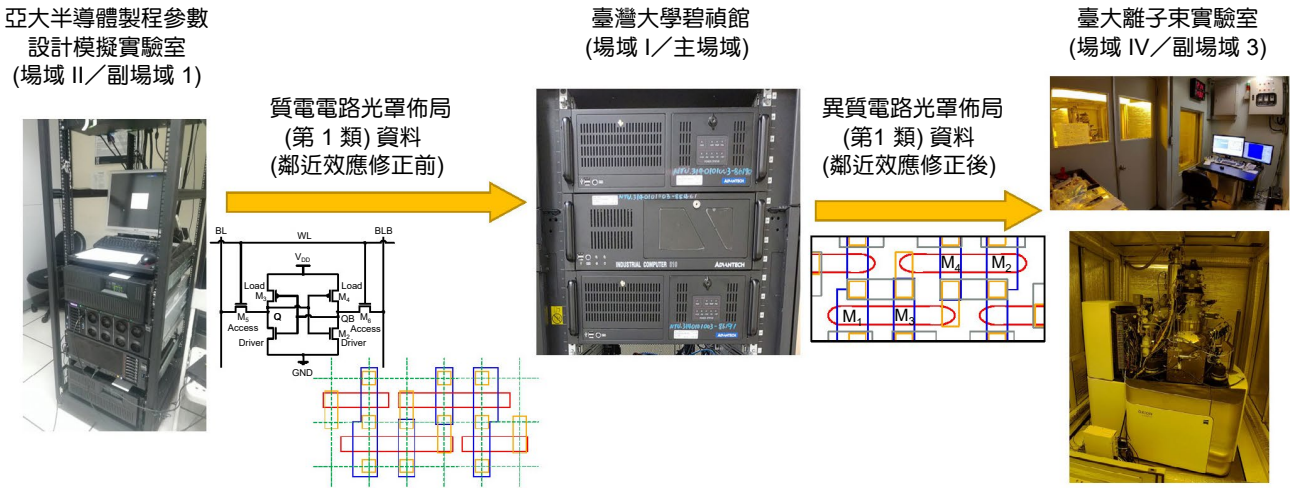


圖 2. 跨場域之製程資料傳輸概念圖。

四、資安防護技術與架構

本文作者代表之團隊依照前述之半導體微場域應用需求，規劃主場域之資安微隔離場域架構如圖 3 所示。因 OT 場域主機大多未做作業系統更新及未做網段隔離，IT 與 OT 邊界並無有效管控存取，因此規劃裝設 OT 微隔離閘道器及 OT 閘道設備進行網路存取管控，並且根據不同存取封包協定進行白名單設計，使外界攻擊者無法任意存取 (第 1 類、第 2 類資料)，也避免竄改呼叫指令 (第 3 類資料) 造成場域危害事件發生。通過弱點掃描及滲透測試也能夠強化防護能力並在實際的攻防演練中驗證其防護有效性，達成場域隔離要求。

位於主場域之微場域 A，設有 RD 及資訊整合中心 HQ，負責跨場域的製程與監控資料整合。當外部連線進入場域時，會先經過多因子防火牆。該防火牆可識別網路流量中的應用，以進行深度檢測和精細的策略執行，阻止加密以及非加密流量中的惡意軟體，漏洞利用及惡意網站的攻擊，並提供 SSL VPN 遠端存取多因子設定功能，防止未經授權的人員存取 OT 場域內的 HPC 伺服器竊取客戶 (副場域 1) 的光罩佈局設計檔案與關鍵製程參數。設置於 HQ 的主機可接收客戶設計的異質光罩電路佈局，並送至 OT 場域內的 HPC 伺服器進行 OPC 運算。HQ 規劃設置多台監控主機，可彙整各副場域與微隔離場域之關鍵狀態資訊 (包含製程設備、環境系統監控、監視主機畫面)。HQ 與 IT 場域間，設有一台網路交換器用於定義網路上各區域的存取權，以保護業務資料安全。

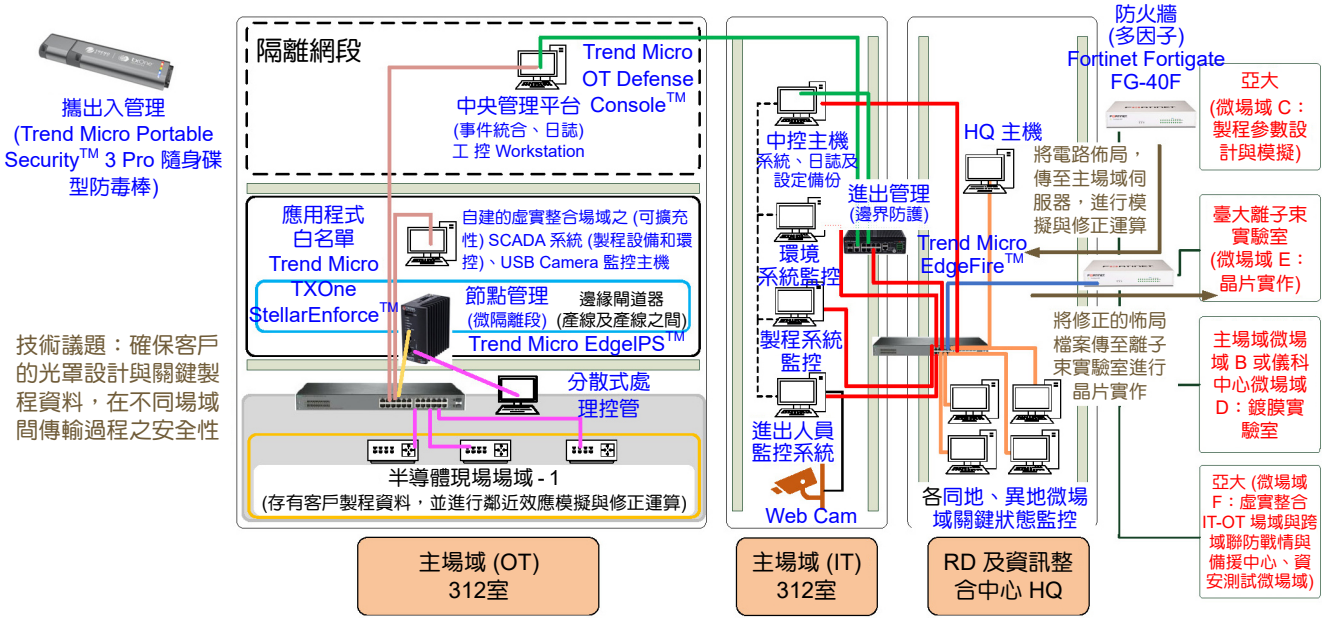


圖 3. IT-OT 微隔離場域網路與資安配置設計 (主場域之微場域 A)。

IT 設有一台趨勢科技 (Trend Micro) 的 EdgeFire 入侵防禦系統，可防止網路攻擊入侵 IT、OT 設備，並提供防火牆進出管制介面，具備流量識別功能，如圖 4 所示。位於 IT 的中控主機，可進行系統、日誌及設定檔之備份。監控主機可進行 OT 製程系統監控、OT 環境系統監控、IT 人員進出與行為監控，確保 HPC 伺服器等製程設備維持在穩定的環境中運行、沒有未經授權的人員進出場域與未經授權的操作。

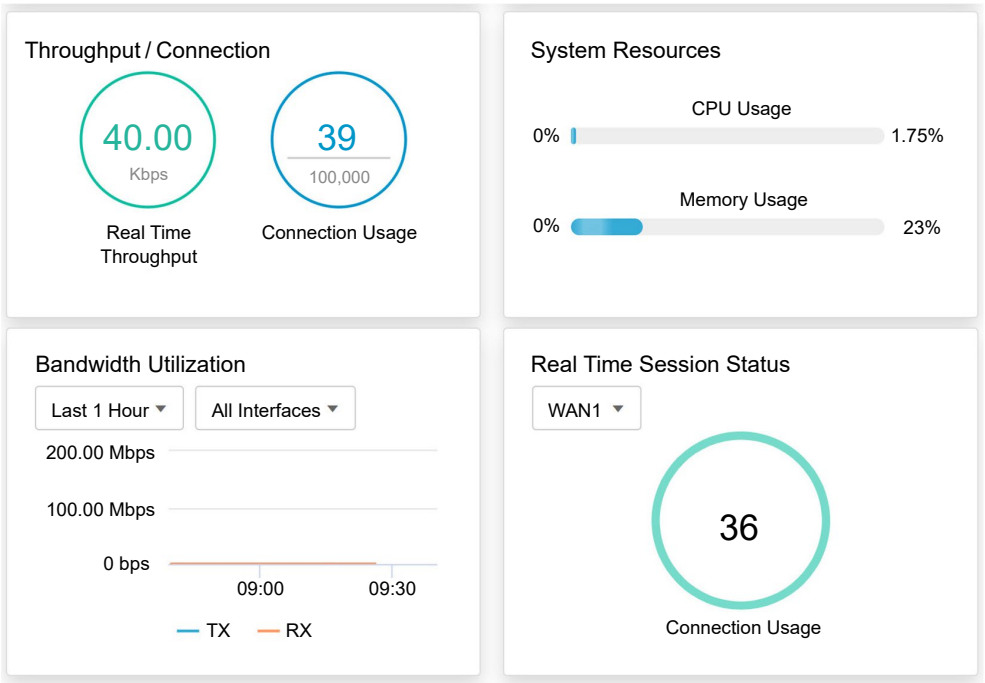
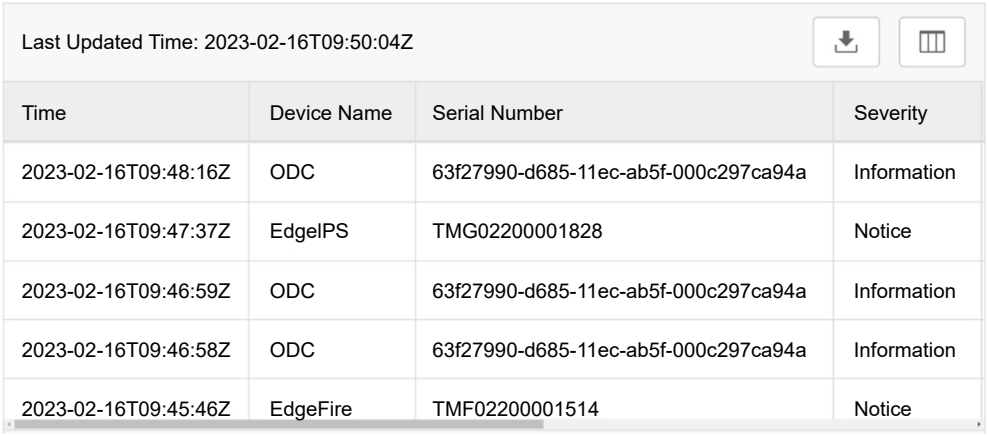


圖 4. EdgeFire 入侵防禦系統儀表板。

OT 設有一台中央管理平台主機，作為 IT 與 OT 間的溝通橋樑，可納管場域內的 EdgeFire 及 EdgeIPS 主機，同時具備事件統合與日誌紀錄的功能，如圖 5 所示。Trend Micro 的 EdgeIPS 主機做為 OT 場域的入侵防禦系統，連接主場域 OT 之 HPC 分散式控管主機，偵測及阻擋網路攻擊 OT 製程設備。Trend Micro 的 Stella MIX 端點白名單軟體，可提供 OT 主機應用程式白名單功能及系統層寫入保護。Trend Micro 的隨身碟型防毒棒 (Portable Security 3 Pro) 可提供攜出入管理，所有攜入至場域內的設備皆需使用防毒棒掃描，可透過網路更新病毒碼，並提供病毒掃描報告，避免惡意程式入侵 OT 場域製程設備影響運作，導致機密外洩。



Last Updated Time: 2023-02-16T09:50:04Z

Time	Device Name	Serial Number	Severity
2023-02-16T09:48:16Z	ODC	63f27990-d685-11ec-ab5f-000c297ca94a	Information
2023-02-16T09:47:37Z	EdgeIPS	TMG02200001828	Notice
2023-02-16T09:46:59Z	ODC	63f27990-d685-11ec-ab5f-000c297ca94a	Information
2023-02-16T09:46:58Z	ODC	63f27990-d685-11ec-ab5f-000c297ca94a	Information
2023-02-16T09:45:46Z	EdgeFire	TMF02200001514	Notice

圖 5. 中央管理平台系統記錄檔檢視。

本文所探討的範圍主要與 SEMI E187 相關，SEMI E187 為 SEMI 首個半導體晶圓設備資安標準，目前內容以規範設備供應商端的資安防護為主。本文作者代表之團隊在 2022 年 3 月已取得 SEMI E187 正式文件，並獲邀參加 SEMI 分別於同年 4 月 29 日與 11 月 30 日舉辦之「SEMI E187 設備資安標準導入與實務研討會」與「SEMI E187 資安驗證方案工作小組啟動會議」。本團隊投入將貢獻於進一步實質半導體晶圓廠內部製程與環境系統之資安增強。透過 2022 年 10 月取得的 SEMI E187 Reference Practice 文件 (草案)，針對主場域微場域 A 之設備進行初步檢視，其檢視成果如下：

1. OT 場域內之 HPC 伺服器機採用 Windows 11 作業系統，仍在維護的生命週期內，符合 SEMI E187 RQ00001：作業系統支援規範。不適用於系統更新的設備，將參考指引建議使用防火牆進行網路隔離。
2. 所有攜入至場域內的設備皆需使用防毒棒掃描確認無病毒及惡意程式，防毒棒可更新病毒碼並提供掃描報告，符合 SEMI E187 RQ00006：惡意程式掃瞄規範。
3. 微場域採用具有多因子驗證之 Fortinet 防火牆，符合 SEMI E187 RQ00009：帳號存取認證規範所高度建議之多因子身分驗證機制，避免未經授權人員存取場域內的關鍵製程設備。
4. 中央管理平台主機可接收 EdgeFire 與 EdgeIPS 傳送之日誌資料，僅有被授權用戶可訪問日誌，符合 SEMI E187 RQ00011：日誌記錄規範。

後續將配合 SEMI 的認證方式，將 SEMI E187 標準導入本文作者代表之團隊提出之 IT-OT 資安微隔離場域架構，進一步推廣及移植至半導體業界場域。

關於 IEC 62443 標準認證的部分，本團隊主要聚焦在提升半導體成熟製程之自動化程度，強化監控管理現有的半導體廠房環境與設備重要參數。目前相關研究正在進行中，未來有明確的成果會再做進一步介紹。

五、資安攻防情境與腳本演練

隨著半導體業界分散式製造網的發展趨勢，不同場域間的資料傳遞，其資安防護及設備管理面臨嚴峻的考驗。若未做好適當的資安保護工作，資料在傳輸過程中容易被有心人士攔截、竊取，導致關鍵製程參數等公司機密外流。任何人員進入場域操作設備時，也必須遵守相關的標準作業流程 (standard operation procedure, SOP)，若未嚴格落實相關程序，也可能造成資安破口，造成關鍵製程設備大量停擺，嚴重影響公司的產出，例如 TSMC 於 2018 年遭遇的大規模資安攻擊事件[15]。本文作者代表之團隊依照半導體業界可能面臨的資安議題，結合實際場域環境及設備，規劃下列 2 套資安攻防情境腳本：

- 情境 1：委託製造客戶設計光罩電路佈局 (副場域 1-微場域 C) → HPC 伺服器進行 OPC 模擬計算 (主場域-微場域 A) → 晶片製造 (副場域 3-微場域 E 之 OT)
  - ＊情境 1 腳本 1：跨場域的資料傳輸過程是否提供安全保護，以確保關鍵製程資料 (第1類、第 2 類) 不被外洩。
- 情境 2：SCADA 圖控系統、製程系統、環境系統廠商進入 OT 場域進行維護作業 (主場域-微場域A)
  - ＊情境 2 腳本 1：OT 現場維運人員操作的裝置存取控制是否有效，避免維運人員未按照 SOP 進行入場全機掃描，導致 OT 設備中毒，造成關鍵製程資料 (第 1 類、第 2 類) 與環境參數 (第 3 類) 遭到竊取或竄改。

由於目前僅主場域之微場域 A 完成資安設備之建置，因此僅先以該微場域進行情境 1 與情境 2 之攻防腳本演練。後續將根據上述之演練成果，加強跨場域的資安攻防情境與演練腳本規劃。

情境 1 之攻防腳本演練流程與結果 (主場域微場域 A)

1. 外部人員為了傳遞資料，誤將帶有病毒的 USB 攜入至 OT 場域，並插入負責執行 OPC 運算的 HPC 伺服器主機 (如圖 6 黃框所示)。

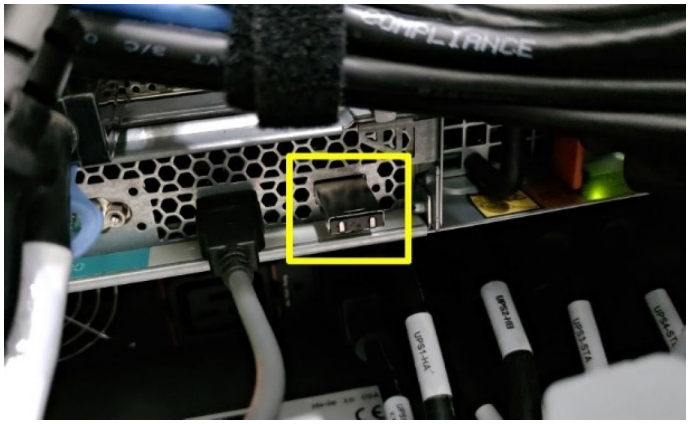


圖 6. 外部人員將 USB 接至 OT 場域設備。

2. HPC 伺服器主機使用 CentOS 7 作業系統，並無安裝防毒軟體，因此使用防毒棒對 USB 進行掃毒作業。
3. 防毒棒發現病毒樣本跳出告警燈號 (如圖 7 所示)及異常訊息 (如圖 8 所示)，並輸出 Excel 格式掃描報告 (如圖 9 所示)。
4. 針對掃描到的病毒威脅進行清除作業，若未即時清除，將導致客戶的光罩電路佈局設計資料 (第 1 類) 遭到竊取。後續規劃進一步透過跨場域聯防戰情與備援中心進行情資分享。

圖 7. 防毒棒跳出告警燈號 (紅色)。

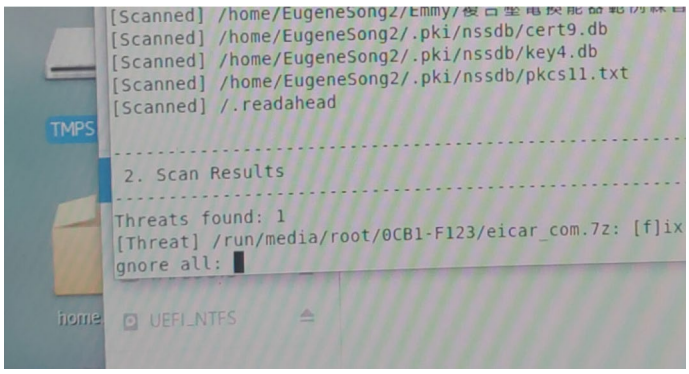


圖 8. 防毒棒發現威脅。

	J	K	L	M	N	O	P
1	MAC Addr	Platform	Scan Resul	Scan Resul	Scanned	Fixed	Infected
2	e4:1f:13:be	Linux 3.10.	Scan comp	Threats fou	236889	0	1
3	e4:1f:13:be	Linux 3.10.	Scan comp	Threats fou	6	0	1
4	A8:5E:45:2	Microsoft \	Scan cance	No threats	0	0	0
5	70:4D:7B:8	Microsoft \	Scan comp	No threats	924262	0	0

圖 9. 防毒棒輸出 Excel 格式掃描報告。

情境 2 之攻防腳本演練流程與結果 (主場域微場域 A)

1. OT 場域 HPC 伺服器執行 OPC 模擬計算時，發生軟硬體異常，隨後 HPC 維護廠商攜帶筆電至 OT 場域，但現場 (IT/OT) 人員為了爭取修復時效，未按照 SOP 使用防毒棒對筆電進行全機掃描，直接使用網路線將筆電連接至 OT 網段。
2. 由於 HPC 維護廠商的筆電已中毒，惡意程式啟動 OT 內網自動掃描。此步驟透過弱點掃描工具 (Nessus scanner) 模擬惡意程式動作，針對 OT 場域 HPC 主機群進行掃描，並從 HPC Host 主機偵測出 Critical 高風險 (CVSS 10.0) 系統漏洞 (NFS 協定漏洞)，如圖 10 所示。
3. 惡意程式發現漏洞後，啟動漏洞利用程序，企圖竊取或竄改關鍵資料 (如關鍵製程與鄰近效應修正參數 (第 2 類))。此步驟透過 Metaexploit 滲透工具模擬惡意程式執行入侵動作，成功以 NFS 協定漏洞掛載 HPC Host 主機家目錄，並可成功存取檔案，如圖 11 所示。
4. 透過 EdgeIPS 可偵測實際攻擊所監測到的流量 (如圖 12 所示)，後續將進一步設置 IPS 連線白名單強化阻擋，避免未經授權的連線存取 OT 場域設備。

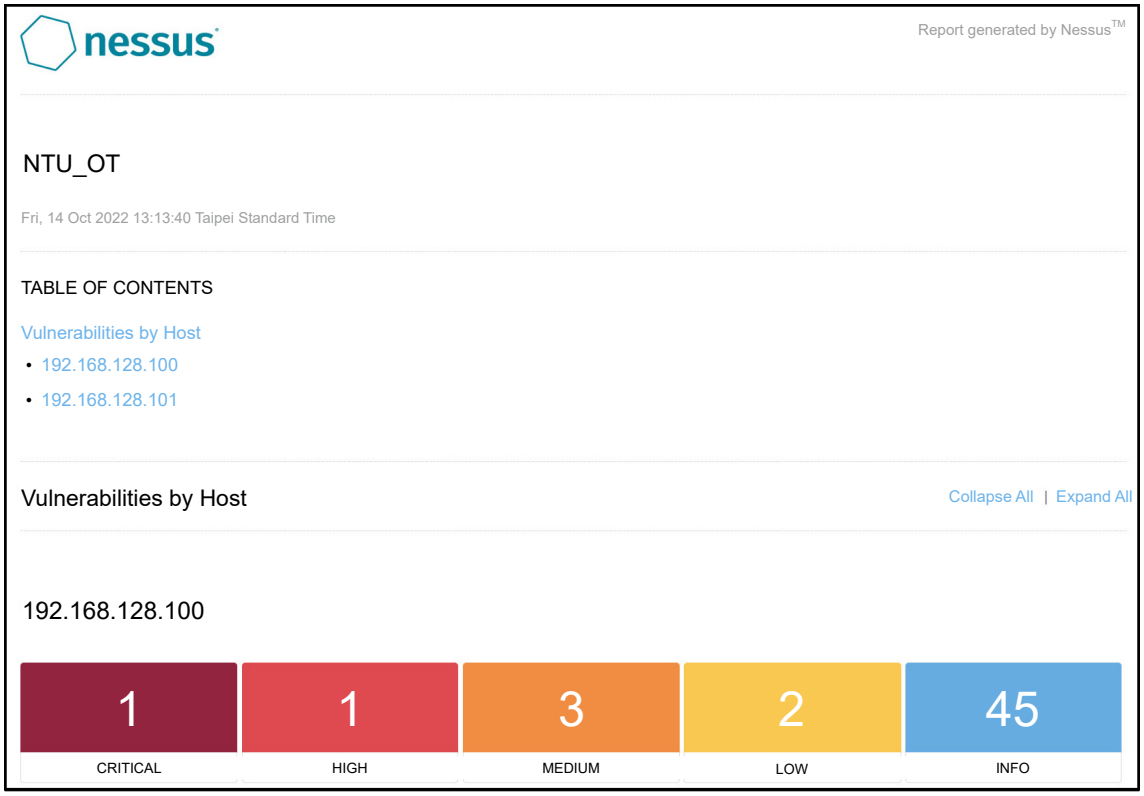


圖 10. OT 段 HPC 伺服器弱點掃描報告。

六、結論

近年來，半導體產業的 OT 場域內的廠房設備與 IT 相互整合已成為產業發展的趨勢，藉由 IT-OT 整合可以提高廠房設備自動化監控的程度，以提升生產效率。但由於成熟製程產線皆已運作多年，許多設備過於老舊，甚至使用已停止維護之作業系統，存在未修補的系統漏洞，容易被有心人士或惡意程式入侵，導致機密外洩或是產線停擺，影響公司的營運與獲利，其資安問題備受考驗。

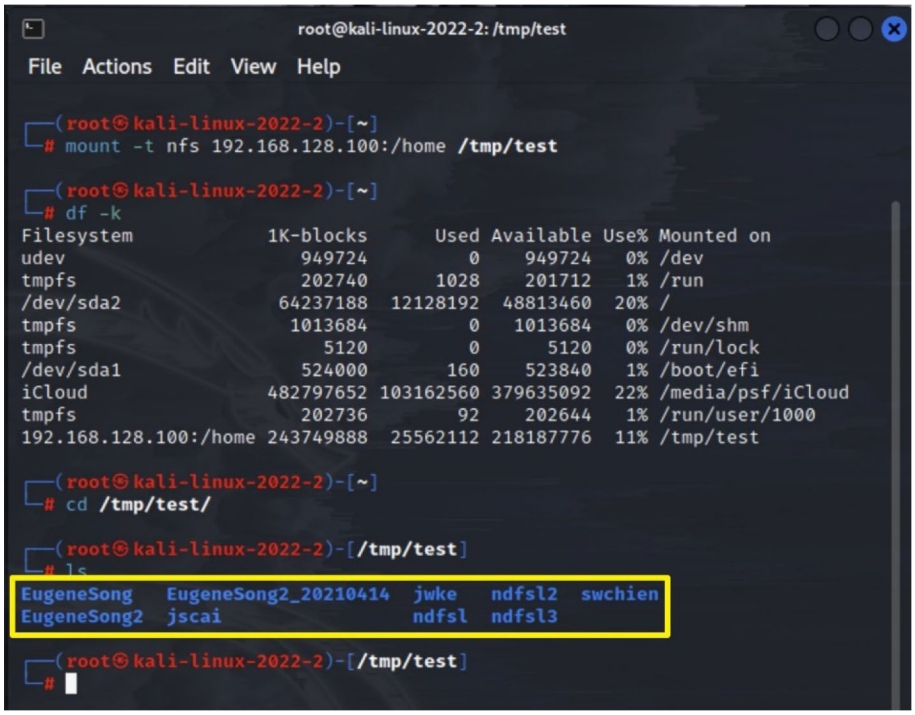


圖 11. 透過滲透工具將 HPC 主機 home 目錄掛載起來。

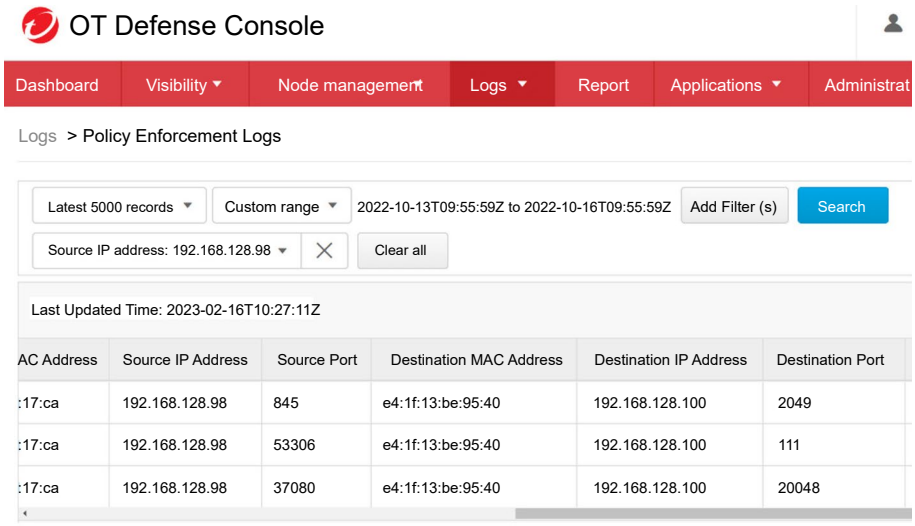


圖 12. EdgeIPS 偵測實際攻擊所監測到的流量。

本文作者代表之團隊提出一個適用於半導體製造領域之 IT-OT 資安微隔離場域架構，並於研究主場域完成資安設備初步建置，進行攻防腳本演練實測，未來將進一步導入國際間通用資安評估標準 (IEC 62443、SEMI E187)，聚焦在半導體成熟製程跨場域資料傳輸之安全性，改善半導體廠房設備自動化監控程度。半導體產業界可透過本研究及早開始評估設備資安相關議題，經由產、學、研間的跨單位合作，大幅縮短技術整合與產業化銜接時程，提高國內半導體製程之工控資安自主化研發能量與國際競爭優勢。並期藉由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，協助半導體業界之製程場域與環境系統提升資安防護能量。

誌謝

此項研究成果由 NSTC 110-2218-E-002-044-、NSTC 111-2218-E-002-037-、NSTC 110-2218-E-468-001-MBK、NSTC 111-2218-E-468-001-MBK 等計畫支持。

參考文獻

1. 陳興忠,劉泰瑋, “工業控制安全的現況與分析”, 台網中心電子報, (2016). Please refer to the website: http://www.myhome.net.tw/2016_12/index.htm
2. 王明德, 廖專崇, “OT 與 IT 全面整合 IIoT 開啟大連結時代”, 新通訊, (2020). Please refer to the website: https://www.2cm.com.tw/2cm/zh-tw/market/A82C62D3C0F54CEEACAEF32612704C92
3. P. K. Garimella, “IT-OT Integration Challenges in Utilities”, *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, Oct 25-27 (2018).
4. John Maddison, “解決 IT 和 OT 融合的挑戰”, FORTINET, (2018). Please refer to the website: https://m.fortinet.com.tw/site/%e8%a7%a3%e6%b1%bait%e5%92%8cot%e8%9e%8d%e5%90%88%e7%9a%84%e6%8c%91%e6%88%b0/
5. FORTINET, “Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks” , Cyentia Cybersecurity Research Library, (Nov. 4, 2018). Please refer to the website: https://library.cyentia.com/report/report_002392.html
6. R. Paes, D. C. Mazur, B. K. Venne and J. Ostrzenski, *IEEE Industry Applications Magazine*, **26** (2), 47 (2020).
7. International Electrotechnical Commission, “IEC TS 62443-1-1:2009-Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models”, IEC，July 09 2009. Please refer to the website: https://webstore.iec.ch/publication/7029.
8. International Electrotechnical Commission, “IEC 62443-2-1:2010-Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program ”, IEC, Nov. 10 2010. Please refer to the website: https://webstore.iec.ch/publication/7030.
9. International Electrotechnical Commission, “IEC 62443-2-4:2015/AMD1:2017-Amendment 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers”, IEC, Aug. 24 2017. Please refer to the website: https://webstore.iec.ch/publication/32227.
10. International Electrotechnical Commission, “IEC TR 62443-3-1:2009-Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems”, IEC, Aug. 30, 2009. Please refer to the website: https://webstore.iec.ch/publication/7031.
11. International Electrotechnical Commission, “IEC 62443-3-2:2020-Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design” , IEC, Jun. 24, 2020. Please refer to the website: https://webstore.iec.ch/publication/30727.
12. International Electrotechnical Commission, “IEC 62443-3-3:2013-Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels”, IEC, Aug. 07, 2013. Please refer to the website: https://webstore.iec.ch/publication/3033.
13. International Electrotechnical Commission, “IEC 62443-4-1:2018-Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements,” IEC, Jan. 15, 2018. Please refer to the website: https://webstore.iec.ch/publication/33615.
14. 周峻佑, “國際半導體展首度談資安, 工作小組揭露推動資安標準現況”, iThome, (2019). Please refer to the website: https://www.ithome.com.tw/news/133168
15. 王宏仁, “【臺灣史上最大資安事件】深度剖析台積產線中毒大當機始末 (上)”, iThome, (2018). Please refer to the website: https://www.ithome.com.tw/news/125098
16. 羅正漢, “全球首個半導體資安標準 SEMI E187 出爐, 台積電與工研院號召臺灣多家半導體與資安業者制定與推動，臺灣制定國際標準新突破”. iThome, (2021). Please refer to the website: https://www.ithome.com.tw/news/148631
17. SEMI, “SEMI E187 - Specification for Cybersecurity of Fab Equipment” , please refer to the website: https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment
18. SEMI, “SEMI E188 - Specification for Malware Free Equipment Integration" , please refer to the website:https://store-us.semi.org/products/e18800-semi-e188-specification-for-malware-free-equipment-integration

19. txOne, “Understanding the SEMI E187 and SEMI E188 Relationships for Protecting Semiconductor Foundries”, please refer to the website: https://www.txone.com/case-studies/understanding-the-semi-e187-and-semi-e188-relationships-for-protecting-semiconductor-foundries/
20. Philip C. W. Ng, Kuen-Yu Tsai, Yen-Min Lee, Fu-Min Wang, Jia-Han Li, Alek C. Chen, *Journal of Micro/Nanolithography, MEMS, and MOEMS*, **10** (1), 013004 (2011).
21. Philip C. W. Ng, Kuen-Yu Tsai, Lawrence S. Melvin III, *Journal of Micro/Nanolithography, MEMS, and MOEMS*, **10** (3), 033010 (2011)

作者簡介

蔡佳勳先生現為國立臺灣大學電子工程學研究所博士生。
Jia-Syun Cai is currently a Ph.D. student in the Graduate Institute of Electronics Engineering at National Taiwan University.

蔡坤諭先生為史丹福大學航太工程與電機工程博士，現為國立臺灣大學電機系副教授。
Kuen-Yu Tsai received his Ph.D. in the Aeronautics & Astronautics Department and Electrical Engineering from Stanford University. He is currently an Associate Professor in the Department of Electrical Engineering at National Taiwan University.

陳興忠先生為國立中正大學電機工程博士，現為亞洲大學資訊工程學系專任特聘教授。
Hsing-Chung Chen received his Ph.D. in the Department of Electrical Engineering from National Chung Cheng University. He is currently a Distinguished Professor in the Department of Computer Science and Information Engineering at Asia University.

莊旻儒先生為逢甲大學資訊工程碩士，現為精誠軟體服務股份有限公司技術處長。
Min-Ju Chuang received his M.S. in the Department of Information Engineering and Computer Science from Feng Chia University. He is currently a Technical Director at Systex Software & Service Corporation.

李建霖先生現為國立臺灣大學電機工程學系博士後研究員。
Chien-Lin Lee received his Ph.D. in the Graduate Institute of Electronics Engineering from National Taiwan University. He is currently a Post-Doctoral Fellow in the Department of Electrical Engineering at National Taiwan University.