

以 SEMI E187 為基礎之
半導體設備資安查核規範

Semiconductor Equipment Cybersecurity
Validation Criteria based on SEMI E187

中華民國 115 年 3 月 10 日

摘 要

以 SEMI E187 為基礎之半導體設備資安查核規範（本查核規範）係為依據 SEMI E187 半導體設備資安標準所揭示之設備資安要求，建立一致且可操作之設備資安查核（Validation）之技術準則。本查核規範說明查核流程、查核項目及符合性判斷原則，作為半導體設備資安符合性評估之依據。

本查核規範以「設備型號（Equipment Model）」作為查核基本單位，並納入設備型號一致性與出場品管相關查核，以合理確保查核結果對同型號設備之代表性。

本查核規範設計係支援符合 ISO/IEC 17025 之檢測實驗室執行設備資安技術查核，並作為符合 ISO/IEC 17065 之驗證機構進行驗證決策之技術依據，採取風險基礎（Risk-based）與漸進式導入原則，以兼顧制度可行性與設備資安基本要求。

Abstract

The Semiconductor Equipment Cybersecurity Validation Criteria based on SEMI E187 (the Validation Criteria) is established, based on the cybersecurity requirements set forth in the SEMI E187 - Specification for Cybersecurity of Fab Equipment, to develop a consistent and operational set of technical validation criteria for semiconductor equipment cybersecurity.

The Validation Criteria adopts the equipment model as the fundamental unit of validation and incorporates validation activities related to equipment model consistency and production release controls, in order to reasonably ensure the representativeness of validation results across equipment of the same model.

The design of this document supports cybersecurity technical validation performed by testing laboratories accredited to ISO/IEC 17025 and serves as a technical basis for conformity assessment and certification decisions made by certification bodies accredited to ISO/IEC 17065. A risk-based and phased implementation approach is adopted to balance practical feasibility and baseline cybersecurity assurance for semiconductor equipment.

目 錄

1	概述.....	1
2	待查核設備與查核原則.....	4
3	查核前置條件與責任界定.....	6
4	設備型號一致性與出場品管相關查核.....	8
5	查核(Validation)項目 ^{[1][2][3][4]}	10
6	參考資料.....	19

制定與修訂紀錄

制定/修訂日期	修改內容摘要	修改後版本別
2026. 3. 10	初版公布	1. 0

1 概述

隨著工業 4.0 與智慧製造之發展，自動化、資料分析及人工智慧等技術廣泛應用於製造環境，使各類操作技術（Operational Technology，OT）系統逐步連接至網路。此一趨勢在提升生產效率與營運彈性的同時，亦使製造設備與製造環境面臨日益嚴峻之網路安全威脅。包括供應鏈設備、外部人員或維運作業所引入之風險，均可能成為攻擊媒介，對既有設備與網路造成重大影響。上述因素顯著提升半導體製造設備及其營運環境之網路安全風險，晶圓廠因此有必要採用具結構性之設備與網路安全標準，以降低惡意軟體與內部威脅所帶來之影響[2]。

SEMI E187 半導體設備資安標準[1]（下稱 SEMI E187 標準）為半導體晶圓廠設備（Fab Equipment）之網路安全建立基礎性規範，旨在透過設備設計與支援機制，從源頭確保設備之安全性，並於設備營運與維護過程中提供必要之安全保護。鑑於半導體設備已成為製造環境中關鍵之連網節點，其資安狀態將直接影響產線穩定性、營運持續性及供應鏈安全，因此有必要建立具一致性與可操作性之技術查核機制，以客觀且可重複之方式評估設備之資安符合性。

SEMI E187 標準係專為半導體晶圓廠設備情境所制定之標準，明確界定設備層級之資安設計與支援要求，與產業實務具高度對應性。爰以 SEMI E187 標準作為本查核規範之主要技術依據，建立「以 SEMI E187 為基礎之半導體設備資安查核規範」（下稱本查核規範），作為設備資安查核及後續認驗證作業之技術準則。

本查核規範並不排除申請者依其營運需求採用其他國際資安框架或控制措施；惟於本制度架構下，設備資安符合性之技術評估，係以 SEMI E187 標準所揭示之設備層級要求為主要判定依據。

本查核規範依據 SEMI E187 標準所揭示之設備層級要求，聚焦於半導體製造設備之四項基礎資安要求，包括作業系統支援、網路安全、端點保護及安全監控，作為設備資安符合性判定之技術範疇。

1.1 目的與制度設計原則

- 1.1.1 本查核規範係依據 SEMI E187 標準所揭示之設備層級資安要求，建立半導體設備資安查核（Validation）之技術準則與作業依據，明確規範查核流程、查核項目及符合性判斷原則。
- 1.1.2 本查核規範作為符合 ISO/IEC 17025 之檢測實驗室執行半導體設備資安技術查核之技術規範，並提供符合 ISO/IEC 17065 之驗證機構進行驗證決策之技術參考。查核執行前之相關作業（例如查核申請、文件提交、查核計畫及查核範圍確認等），非屬本查核規範之範疇，應由檢測實驗室及／或驗證機構，依其適用之 ISO/IEC 17025 或 ISO/IEC 17065 要求，自行建立並執行。
- 1.1.3 本查核規範之設計，係基於在半導體設備資安認證制度推動初期，採取風險基礎（Risk-based）與漸進式導入之設計原則，以兼顧制度可行性與設備資安之基本要求，並保留未來依 SEMI E187 標準演進與制度成熟度提升，調整查核要求與深度之彈性。

1.2 適用範圍

- 1.2.1 本查核規範適用於依 SEMI E187 標準進行之設備資安查核作業，其主要查核標的為半導體晶圓廠設備（Fab Equipment）。
- 1.2.2 本查核規範係以 SEMI E187 標準所揭示之設備資安原則為基礎，建立具可重複性、可比對性及可擴充性的設備層級資安查核機制，並得延伸適用於具備相似資安風險特性之智慧製造或工業設備。
- 1.2.3 本查核規範可作為查核人員訓練及執行設備資安查核之依據，並得隨資安技術發展及制度需求適時修訂

1.3 名詞定義

- 1.3.1 待查核設備（Audited Equipment）：詳 2.1 說明。
- 1.3.2 設備型號（Equipment Model）：詳 2.2 說明。
- 1.3.3 申請者：指申請本查核、提供查核文件並接受查核之單位。通常指對待查核設備具設計或出場設定控制權之設備製造商、代理商

或其授權單位。

1.3.4不適用（Not Applicable，N/A）：用於查核結果之紀錄，指待查核設備因其設計、架構或功能特性，致無法適用本查核規範中特定查核項目之情形。查核人員於判定為不適用時，應於查核紀錄或查核報告中說明其判定理由。

1.3.5查核基準日：指檢測實驗室實際進行設備查核之日期，並應於查核報告中明確記載。

1.3.6佐證資料：指用以支持查核結果之文件、紀錄、測試結果、系統畫面、訪談紀錄或其他可合理證明設備資安狀態之資料。如需以電腦螢幕畫面截圖作為佐證資料，則應截圖全螢幕，並包含系統時間。

1.3.7緩解措施：指待查核設備本身所具備，且可透過設備設定、組態或操作方式加以啟用、調整或限制之技術性或架構性控制措施。其目的，在於降低已知資安風險，或補強設備於特定資安要求下之防護能力，以支持設備資安符合性之判定。不包含以設備外部之組織管理控制、作業程序、人工操作機制，或環境性防護措施，取代設備本身應具備之資安功能或控制機制。

1.3.8本查核規範中所稱「合理」、「資安技術水準」及相關判斷：指依查核基準日當時，普遍被產業及資安專業社群接受之技術水準，由查核人員依據文件證據、實際設備狀態及其專業判斷，綜合評估後所作之判定。查核人員於進行前述判斷時，應避免將查核要求延伸為組織管理系統稽核或設備設計審查，並應於查核紀錄或查核報告中說明其判斷理由。

1.4 查核原則與判斷基準

1.4.1依本查核規範進行查核時，如遇風險管控或資安設計採用緩解措施是否符合之判斷爭議時，查核人員於符合查核基準日之資安技術水準前提下，綜合考量該等措施是否可為待查核設備提供合理的網路安全性，作為符合與否之判斷依據。

2 待查核設備與查核原則

2.1 待查核設備之界定與適用原則

- 2.1.1 本查核規範所適用之待查核設備，係指於製造或工業營運環境中使用，具備作業系統（Operating System），且可透過有線或無線方式進行網路連線之設備，其功能包含但不限於運算、控制、監控或通訊等用途。
- 2.1.2 前述設備包含但不限於半導體晶圓廠製程設備、自動化物料搬運系統，以及其他智慧製造設備或廠務相關設備。
- 2.1.3 不具備作業系統，或無任何網路連線能力之設備（例如僅具單一功能之純感測器、被動式元件或僅具硬體邏輯控制之裝置），不屬於本查核規範之適用範圍。
- 2.1.4 本查核規範原則上適用於安裝有具備使用者管理、系統服務管理及軟體更新機制之作業系統（例如 Microsoft Windows、Linux 或其他具相似系統架構之作業系統）之設備；其資安查核係以設備之作業系統、系統軟體及相關資安功能為主要查核對象。
- 2.1.5 前項所述原則性適用對象之外，若設備採用之作業系統僅具部分前述機制，查核人員應依設備實際架構與功能，判斷其是否具備與本查核規範所列資安要求相對應之功能；如無法對應，得於相關查核項目中紀錄為【不適用】，並於查核紀錄或查核報告中加以說明。
- 2.1.6 本節之界定係用以說明本查核規範之適用對象，並不取代後續各項查核條文中對具體查核內容與符合性判定之要求。

2.2 設備型號為基礎之查核原則

- 2.2.1 本查核規範係以「設備型號（Equipment Model）」作為資安查核之基本單位。
- 2.2.2 所稱「設備型號」，係指由同一申請者所設計或生產，且於硬體架

構、作業系統版本、系統軟體、資安功能設計及預設安全組態上具有一致性之設備系列。

2.2.3 若設備型號之資安功能、系統架構及安全控制設計未發生變動，原則上該次申請所取得之查核結果，得一體適用於該型號之設備。

3 查核前置條件與責任界定

3.1 注意事項

- 3.1.1 開始查核前，查核人員應確認已依本查核規範之要求，瞭解查核流程、查核項目及符合性判定原則，以確保查核作業之一致性與可重複性。
- 3.1.2 於對待查核設備進行目視或現場檢視時，查核人員應確認設備處於可進行資安查核之合理狀態；本查核不包含設備功能、製程能力或生產效能之驗證。
- 3.1.3 本查核規範中以 Note 標示之內容，係屬建議事項或對查核作業之補充說明，供查核人員於判斷符合性時參考，並非獨立之查核要求。

3.2 查核文件準備清單

- 3.2.1 查核前，申請者宜依「查核文件準備清單」提供相關文件，以利查核人員進行事前審閱與查核規劃，加速查核作業之進行。
- 3.2.2 如部分文件於查核前尚未備妥，查核人員得視實際情形，於查核紀錄中說明其影響範圍，並於查核過程或查核報告中加以記載。
- 3.2.3 查核文件準備清單

項目	文件名稱	必要性 ●必須提供 ○如果需要再提供	相關查核條款
1	設備編碼規則	●	4.2
2	設備出場品管作業相關文件	●	4.3
3	設備規格文件	●	5.1、5.3
4	作業系統供應商或其授權維運來源提供之延伸支援或長期支援（Long-term Support，LTS）證明文件	○	5.1
5	設備進行安全性更新的程序或流程說明文件	●	5.2
6	設備操作手冊	●	5.3
7	設備的安全指南或使用者的文件	●	5.4、5.6、5.7、5.8、5.9、5.10、5.11、5.12
8	設備弱點掃描報告	●	5.5
9	弱點管理機制說明文件	●	5.5

10	惡意軟體掃描(Malware Scan)報告	●	5.6
11	惡意軟體掃描管理機制說明文件	●	5.6
12	API 相關技術文件	○	5.10、5.11
13	設備 LOG 紀錄檔(作業系統與應用程式)	●	5.12

4 設備型號一致性與出場品管相關查核

本章係因應 SEMI E187 認驗證制度以「設備型號」為驗證基礎之設計，針對設備出場時與資安功能相關之一致性控管機制進行查核，以合理確保查核結果可適用於同一設備型號後續出廠之設備。

4.1 設備適用性確認

4.1.1 詢問申請者或檢視本次查核申請文件，確認本次待查核設備是否適用設備型號一體驗證。

Note1：適用設備型號一體驗證之常見情形包括（但不限於）：待查核設備非為單一客製化設備，或待查核設備係以型號方式進行重複生產者。

如是，即完成本項查核紀錄為【符合】；若否，則紀錄【不適用】。
並同步紀錄查核項目 4.2 與 4.3 為【不適用】。

4.1.2 記錄以下內容之一：

- a. 符合
- b. 不適用

4.2 設備型號

4.2.1 詢問申請者或檢視設備編碼規則文件，確認申請者內部是否就設備型號已有文件化的設備編碼規則，並能明確定義該設備型號之適用範圍。

若是，則續查 4.2.2；若否，則紀錄為【不符合】。

4.2.2 設備型號如有主型號與次（附屬）型號之區分，則確認其何層級型號之變動，不致影響設備的資安相關功能，並以該層級型號為本次查核範圍之設備型號紀錄。

Note1：設備的資安相關功能，包括但不限於：硬體架構、作業系統類型與版本、系統軟體／應用程式、預設安全組態等。

若是，即完成本項查核紀錄為【符合】，並同步紀錄本次查核之設備型號；若否，則紀錄為【不符合】。

4.2.3 記錄以下內容之一：

- a. 符合
- b. 不符合

4.3 出場品管作業

4.3.1 查核申請者就設備出場所執行之品管作業相關文件，確認設備於出場時，其與資安相關之設定具有一致性控管機制。出場品管作業相關文件內容，至少應包含或能合理說明下列事項：

- a. 與本查核相關之資安功能（如帳號管理、網路設定、系統強化、日誌功能等）是否為出場檢查項目；
- b. 當出場設備之資安功能設定與設計規格不符時之處理方式。

Note1：本項查核之目的，係確認申請者是否具備合理的出場一致性控管機制，不要求申請者建立或符合 ISO 9001 等品質管理系統。

若是，則續查 4.3.2；若否，則紀錄為【不符合】。

4.3.2 依據 4.3.1 所提供之文件，查核人員應透過文件審查、訪談或其他合理方式，確認申請者就設備之出場品管作業，是否足以合理確保後續出廠之同型號設備，其與資安相關之系統設定與功能，與本次待查核設備具有一致性。

Note2：本條所稱之「文件審查、訪談或其他合理方式」，係指在不構成品質管理系統稽核之前提下，查核人員得採用之合理佐證方式。其方式包括（但不限於）：

- 比對設備之出廠預設設定或系統強化基準設定與實際待查核設備之設定一致性；
- 交叉檢視設備規格文件、操作手冊、安全指南及出場檢查清單等文件內容之一致性；
- 檢視與資安相關之系統軟體、作業系統或設定版本控管及變更紀錄。如採此方式，應確認資安功能變更是否需經內部核准？以及是否有變更紀錄（Change Log）；
- 抽樣檢視申請者其他出場設備與資安相關之出場設定確認紀錄或檢查紀錄；
- 透過具結構性之技術訪談方式，確認出場品管作業與文件內容之一致性。

Note3：查核重點在於是否具備「合理確保一致性之機制」，而非要求申請者保證完全一致或不存在任何偏差。

Note4：本項查核不要求查核人員進行實際生產線稽核或現場查廠；惟查核人員基於專業判斷認為有必要時，仍得要求進行現場確認。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

4.3.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5 查核(Validation)項目^{[1][2][3][4]}

本章所列各項查核要求，係依據 SEMI E187 標準及其相關參考文件所揭示之設備資安原則，並參酌實務檢核工具與指引加以具體化與操作化說明。

5.1 [E187.00-RQ-00001-00] (條款 7.2 對作業系統的支持)

5.1.1 詢問申請者或檢視設備規格文件，確認待查核設備所使用之作業系統及其版本，並判斷該作業系統是否屬於具備使用者管理、系統服務管理及軟體更新機制之作業系統。

若是，則續查 5.1.2；若否，則依 2.1.5 原則，於本項查核紀錄為【不適用】，並於查核紀錄或查核報告中加以說明。

5.1.2 實際檢查待查核設備狀態，確認其作業系統類型與版本，是否與申請者說明或相關設計文件標示一致。

若是，則續查 5.1.3；若否，即完成本項查核紀錄為【不符合】。

5.1.3 依據 5.1.2 所確認之作業系統版本資訊，比對作業系統供應商或相關維運來源所提供之支援資訊，確認該作業系統版本之終止支援日期，是否距離查核基準日超過 12 個月。

若是，即完成本項查核紀錄為【符合】；若否，則續查 5.1.4。

5.1.4 如該作業系統版本之終止支援日期距離查核基準日少於 12 個月，應確認申請者是否具備延伸支援、長期支援 (Long-term Support, LTS) 或等效之維運證明文件，並應請申請者提出相應之作業系統升級、汰換或修補計畫。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.1.5 記錄以下內容之一：

- a. 符合
- b. 不符合
- c. 不適用

5.2 [E187.00-RQ-00002-00] (條款 7.2 對作業系統的支持)

5.2.1 查核人員應檢視申請者所建立之設備安全性更新相關程序或流程說明文件，以確認該等文件是否說明在設備上執行作業系統安全性更新之步驟與注意事項。

Note1：更新程序或流程說明文件中，「注意事項」可包含對下列項目的評估要求與檢查方法：

- 軟體相容性：確認安全性更新後，應用程式與驅動程式仍能在新版本下正常執行。

- 軟體相依性：避免更新導致底層套件或共用元件版本不符，造成系統功能失效。
- 性能影響：確保更新後系統反應時間、CPU 與 Memory 使用率…等系統效能影響，符合申請者就待查核設備所設定之基準門檻。
- 套用補修程式或安全性更新副作用：辨識更新後可能潛在副作用，例如服務中斷、憑證過期、通訊協定變更或登錄機碼變動…等，並說明可能的解決方法。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.2.2 記錄以下內容之一：

- a. 符合
- b. 不符合

5.3 [E187.00-RQ-00003-00] (條款 8.2 網路傳輸安全)

5.3.1 詢問申請者並檢視待查核設備的操作手冊、設備規格文件等資料，查核待查核設備是否具備聯網功能，例如 Web 服務、檔案傳輸或終端服務的能力。

若是，則續查 5.3.2；若否，即完成本項查核紀錄為【不適用】。

5.3.2 查核待查核設備若使用 HTTPS、SFTP、SSH 等安全協議，是否正常支援運作。

Note1: 查核時可使用封包監聽工具 (eavesdropping tool)，例如 Wireshark，在系統執行正常作業期間，擷取部分通訊封包以確認其加密與傳輸行為是否符合安全要求。

Note2: 傳輸協議、加密標準與雜湊演算法是否符合查核時的資安技術水準，查核人員於有判斷需求時，得參考 NIST SP 800-52 或其他等效之國際資安技術指引。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.3.3 記錄以下內容之一：

- a. 符合
- b. 不符合
- c. 不適用

5.4 [E187.00-RQ-00004-00] (條款 8.3 網路設定管理)

5.4.1 檢查待查核設備的安全指南或使用文件，並查核文件中是否描述設備的網路組態配置，內容應包括下列事項：

- a. 明確標示待查核設備之對外連接介面，包含所用通訊協定 (protocols) 與連接埠 (ports)，以及與工廠網路連線之使用案例 (Use Case) 的設備網路架構圖；
- b. 用於更改網路組態配置 (若支援) 的維護說明。

若是，續查 5.4.2；若否，則紀錄為【不符合】；若依據 5.3 查核結

果，確認設備不具備聯網功能，即完成本項查核紀錄為【不適用】

5.4.2 透過查核確認下列事項：

- a. 操作待查核設備的人員，能否透過設備介面（Equipment Interface），檢視並存取 5.4.1 文件中所述的網路設定，且設備實際設定與 5.4.1 文件描述相符；
- b. 如有查核時發現預設設定有不符合查核時的資安技術水準情形，應予修改。

Note1：本項所稱「不符合查核時之資安技術水準」，係指設備於出廠預設設定中，仍啟用未使用、已知不安全或缺乏必要防護機制之通訊服務或通訊埠者，例如未關閉明顯不建議於出廠預設啟用之服務（如 FTP、Telnet、未加密之 HTTP 等）。本項判定不包含設備進入晶圓廠場域後，由使用單位依其網路架構或營運需求所進行之後續設定。

- c. 修改後，再次透過設備介面檢視並查核前項設定變更結果，已正確反應於最終組態配置中。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.4.3 記錄以下內容之一：

- a. 符合
- b. 不符合
- c. 不適用

5.5 [E187.00-RQ-00005-00] (條款 9.2 弱點緩解)

5.5.1 查核人員應確認待查核設備已執行弱點掃描，並檢視弱點掃描報告，是否包含下列事項：

- a. 已執行弱點掃描，並顯示掃描結果，以及通過標準；

Note1：弱點掃描執行方式，得採下列方式之一：

- 由申請者自行執行(提供弱點掃描報告予檢測實驗室)；
- 由檢測實驗室執行；
- 由申請者於檢測實驗室監督下執行。

Note2：針對 *Note1* 第一點所述情境，檢測實驗室應記錄未由檢測實驗室執行或未由申請者於檢測實驗室監督下執行之原因。

Note3：針對 *Note1* 第三點所述情境，檢測實驗室應確認並紀錄掃描工具、掃描設定與掃描範圍，並留存相關監督紀錄作為查核佐證資料。

- b. 掃描工具名稱及版本；

Note4：查核人員應確認弱點掃描工具之版本及其所使用之弱點資料庫，於執行掃描時已完成最近一次可取得之更新，或其更新狀態足以合理反映查核基準日當時已知之主要資安弱點；如非即時更新，申請者應能說明其更新頻率與合理性。

Note5：查核人員於評估弱點掃描工具之適用性時，得參考第三方專業社群或研究機構（如 OWASP、Gartner 等）所公布之工具資訊，作為判斷該掃描工具功能完整性與成熟度之輔助依據。

c. 掃描覆蓋範圍、掃描設定和掃描日期。

Note6：掃描範圍應包含當次待查核設備之設備全部，得經由 5.4.1 所取得文件進行確認。

Note7：弱點掃描之執行日期，應早於或等於查核基準日，且其所使用之弱點資料庫更新狀態，應符合前述 Note4 所述之更新合理性要求。

若是，則續查 5.5.2；若否，則紀錄為【不符合】；依據 5.3 查核結果，確認設備不具備連網功能，即完成本項查核紀錄為【不適用】。

5.5.2 查核是否為所有弱點建立嚴重性分級機制；且所有最嚴重等級弱點，均已修復或執行緩解措施。

Note8：弱點分級可參考常見之弱點評分或分級方法（如 CVSS 等），或依弱點掃描工具所採用之分級規則進行判斷。若採用之分級方法或其版本非屬目前普遍使用之作法，查核人員應檢視其分級邏輯與評估依據，以確認其於查核基準日當時具備合理性與一致性。

Note9：如採用緩解措施，查核人員應確認緩解措施經申請者內部權責人員簽核確認，並符合查核時的資安技術水準。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.5.3 記錄以下內容之一：

- a. 符合
- b. 不符合
- c. 不適用

5.6 [E187.00-RQ-00006-00] (條款 9.3 惡意軟體掃描)

5.6.1 查核人員應確認待查核設備已執行惡意軟體掃描 (Malware Scan)，並檢視惡意軟體掃描報告，是否包含下列事項：

- a. 已執行惡意軟體掃描，並顯示掃描結果及其判定依據，例如：是否偵測到惡意軟體、偵測結果之處置狀態，以及申請者用以判斷設備是否符合資安要求之標準或原則；

Note1：惡意軟體掃描之執行方式，得採下列方式之一：

- 由申請者自行執行(提供惡意軟體掃描報告予檢測實驗室)；
- 由檢測實驗室執行；
- 由申請者於檢測實驗室監督下執行。

Note2：針對 Note1 第一點所述情境，檢測實驗室應記錄未由檢測實驗室執行或未由申請者於檢測實驗室監督下執行之原因。

Note3：針對 Note1 第三點所述情境，檢測實驗室應確認並紀錄掃描工具、掃描設定與掃描

範圍，並留存相關監督紀錄作為查核佐證資料。

b. 掃描工具名稱及版本；

Note4: 查核人員應確認惡意軟體掃描工具之版本，以及其所使用之病毒碼或惡意程式資料庫，於執行掃描時已完成最近一次可取得之更新，或其更新狀態足以合理反映查核基準日當時已知之主要惡意軟體威脅；如非即時更新，申請者應能說明其更新頻率與合理性。

Note5: 查核人員於評估惡意軟體掃描工具之適用性時，得依據設備所使用之作業系統，參考第三方測試或評測機構（如 AV-Comparatives、AV-Test.Org 等）所公布之資訊，作為判斷該掃描工具防護能力與成熟度之輔助依據。

c. 掃描覆蓋範圍、掃描設定和掃描日期。

Note6: 掃描範圍應包含當次待查核設備之設備全部，可經由 5.4.1 所取得文件進行確認。

Note7: 惡意軟體掃描之執行日期，應早於或等於查核基準日，且其所使用之病毒碼或惡意程式資料庫更新狀態，應符合前述 *Note4* 所述之更新合理性要求。

若是，續查 5.6.2；若否，則紀錄為【不符合】。

5.6.2 查核申請者是否已分析掃描結果，且所有問題均已修復或執行緩解措施。

Note8: 如採用緩解措施，查核人員應確認緩解措施經申請者內部權責人員簽核確認，並符合查核時的資安技術水準。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.6.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5.7 [E187.00-RQ-00007-00] (條款 9.4 反惡意軟體保護)

5.7.1 檢查設備的安全指南或使用者文件，並查核其中是否描述相容的反惡意軟體解決方案，包括預設設定和建議設定。

Note1: 反惡意軟體解決方案，包括(但不限於)防毒軟體或應用程式允許清單 (Application Allow List) 控制機制。

若是，續查 5.7.2；若否，則紀錄為【不符合】。

5.7.2 透過查核確認，根據安全指南或使用者文件中的預設設定和建議設定操作，指定的相容反惡意軟體解決方案是否與設備正常運作。

Note2: 如設備採用防毒軟體作為反惡意軟體解決方案，該防毒軟體與設備中所用應用程式有已知誤判（例如無毒判斷為有毒）情形，或特定應用程式或資料夾掃描後可能引起系統運作問題者，申請者應於安全指南或使用者文件予以明文標示。

Note3: 查核人員於評估設備所採用之反惡意軟體保護解決方案時，得依據設備所使用之作業系統，參考第三方測試或評測機構，如 AV-Comparatives、AV-Test.Org 等，所公布之資

訊，作為判斷該解決方案防護能力與成熟度之輔助依據。

Note4：如申請者所採用之反惡意軟體保護解決方案未列於前述第三方評測資訊中，申請者得視實際情形，提供其他可合理說明其防護效能與適用性之資料（例如效能評估報告、測試報告或相關技術文件），供查核人員於整體判斷時參考。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.7.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5.8 [E187.00-RQ-00008-00] (條款 9.4 反惡意軟體保護)

5.8.1 檢查設備的安全指南或使用者的文件，並查核其中是否包含設備系統強化（System Hardening）說明或預設狀態清單，且其中需描述安裝、操作和維護設備時，應遵守的強化指南、說明、安全配置選項和建議設定。

Note1：申請者提供之設備系統強化說明，內容至少應包含下表「強化領域」所列事項：

強化領域	預期內容
輸入/輸出介面管理	描述 I/O 埠口的控制措施（例如在不需時停用 USB 埠口）
作業系統服務與工具	識別並停用未使用的作業系統服務、工具或背景程序
最低要求功能配置	描述設備功能所需的作業系統服務
實施指南	說明如何在不中斷設備運作的情況下應用強化措施

Note2：申請者可參考已被廣泛認可的安全框架，例如 CIS Benchmarks（網際網路安全中心基準）、SCAP Frameworks（安全內容自動化協定）等，建立適用於設備的系統強化基準設定（Baseline Secure Configuration）。

若是，續查 5.8.2；若否，則紀錄為【不符合】。

5.8.2 透過查核確認，設備的預設狀態，是否與前述設備系統強化說明或預設狀態清單一致。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.8.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5.9 [E187.00-RQ-00009-00] (條款 9.5 存取控制機制)

5.9.1 檢查待查核設備的安全指南或使用者的文件，查核其中是否包含設備中的所有可存取介面（包含作業系統及設備層級介面）及其所對應

的裝置列表。

若是，續查 5.9.2；若否，則紀錄為【不符合】。

5.9.2 依據 5.9.1 查核結果，實際檢視待查核設備，查核下列事項：

- a. 設備是否可以在所有可存取介面（作業系統或設備）上，識別（Identify）和認證（Authenticate）所有用戶，且不得存在未經申請者說明，或無法對應其技術文件之帳號、群組或權限設定。

Note1：申請者識別和認證可能是基於角色的或基於群組的（Role-Based or Group-Based），例如於部分設備介面中，允許多名使用者共用相同之身份識別。

Note2：本項所稱帳號、群組或權限，包含使用者帳號及系統內建帳號。對於作業系統或設備正常運作所需之系統帳號、服務帳號或內建角色，申請者得以技術文件或合理說明方式揭露其用途與權限範圍，無須於使用者操作文件中逐一系列示。

Note3：設備的實體可存取介面，例如 USB 接口，應有實體保護措施，以避免未授權存取。

- b. 未執行登入識別前，所有可存取介面（作業系統或設備）上的操作功能均須保持不可操作狀態。
- c. 至少應查核管理員帳號與一般使用者帳號分離（Separated），並使用不同的登入憑證（Login Credentials）。
- d. 如有訪客（guest）帳號或任何未經驗證的帳號（non-authenticated accounts）應予預設停用（disabled）。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.9.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5.10 [E187.00-RQ-00010-00] (條款 9.5 存取控制機制)

5.10.1 檢查待查核設備的安全指南或使用者文件，並查核其中是否說明帳號管理設定（Account Management Configuration），並至少應支援權責分離（Segregation of duties）與最小特權（Least privilege）原則。

Note1：可作為權責分離與最小特權原則之實作或說明方式者，包含但不限於：設備設定具不同權限層級之角色帳號、不同角色帳號之權限範圍具差異性、管理員或具高度權限之帳號僅配置於必要之角色，以及角色或帳號之設定具備可識別性等。

Note2：其他帳號管理設定可能的內容包括（但不限於）：強化指南、設定說明、安全配置選項和建議設定等。

若是，續查 5.10.2；若否，則紀錄為【不符合】。

5.10.2 查核待查核設備是否支援應用程式介面（Application

Programming Interface，API）或將裝置（Devices）視為使用者。若是，則查核待查核設備能強制對 API 和裝置進行使用者授權管理，以紀錄相關作業歷程。

Note3：如待查核設備具備應用程式介面（API）功能，查核人員應檢視申請者所提供之相關技術文件（例如 API 規格說明、通訊方式、存取控制或授權機制說明），以確認其設計符合本項要求。

若是，續查 5.10.3；若不支援，則於查核文件中應予紀錄；若否，則紀錄為【不符合】。

5.10.3 依據 5.10.1 與 5.10.2 查核結果，實際檢查設備，確認設備實際狀態是否與設備的安全指南或使用者文件描述相符。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.10.4 記錄以下內容之一：

- a. 符合
- b. 不符合

5.11 [E187.00-RQ-00011-00] (條款 10.2 日誌要求)

5.11.1 檢查待查核設備的安全指南或使用者文件，並查核待查核設備是否支援產生與安全相關的事件記錄的功能，並提供事件紀錄存取方式；同時系統和安全事件日誌應至少可以記錄並保存 1 個月。

Note1：事件紀錄存取方式可透過手動機制、應用程式介面（API）或傳送到集中式系統等。

Note2：若依據 5.10.2 查核結果，若設備支援應用程式介面（API）或將裝置（Devices）視為使用者，則應查核 API 或裝置行為亦有依據本項要求支援留存與輸出事件紀錄。

Note3：如待查核設備具備應用程式介面（API）功能，查核人員應檢視申請者所提供之相關技術文件（例如 API 規格說明、通訊方式、存取控制或授權機制說明），以確認其設計符合本項要求。

若是，續查 5.11.2；若否，則紀錄為【不符合】。

5.11.2 依據 5.11.1 查核結果，實際檢查設備，確認待查核設備實際狀態是否與其安全指南或使用者文件描述相符。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.11.3 記錄以下內容之一：

- a. 符合
- b. 不符合

5.12 [E187.00-RQ-00012-00] (條款 10.2 日誌要求)

5.12.1 檢查待查核設備的安全指南或使用者文件，並查核下列事項：

- a. 設備是否支援產生與下列類別相關的安全事件記錄的功能，包括存取控制（Access Control）、配置變更（Configuration Changes）及系統錯誤（System Errors）。
- b. 前述事件類別之事件日誌，是否包括足以識別事件之基本資訊，例如事件類型、事件描述、相關使用者帳戶及時間戳記等。

若是，續查 5.12.2；若否，則紀錄為【不符合】。

5.12.2 檢查待查核設備實際產出的範例日誌，查核是否確實能產生每個事件類別的記錄，且紀錄內容與設備的安全指南或使用者文件描述相符。

若是，即完成本項查核紀錄為【符合】；若否，則紀錄為【不符合】。

5.12.3 記錄以下內容之一：

- a. 符合
- b. 不符合

6 參考資料

1. SEMI E187-0122 SPECIFICATION FOR CYBERSECURITY OF FAB EQUIPMENT, January 2022.
2. SEMI E187 Reference Practice, Version 2.0, October 2022.
3. SEMI E187 CHECK LIST, 20230531.
4. SEMI E187 COMPLIANCE GUIDANCE, Semiconductor manufacturing cybersecurity consortium (SMCC), 20250707.