護國神山保衛戰 –
從 SECS/GEM 標準來看晶片製造安全

Yenting Lee, Sr. Threat Researcher
PSIRT and Threat Research, TXOne Networks Inc.
April 15, 2025 @CYBERSEC 2025

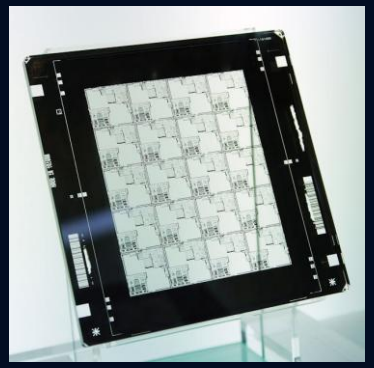
Outline

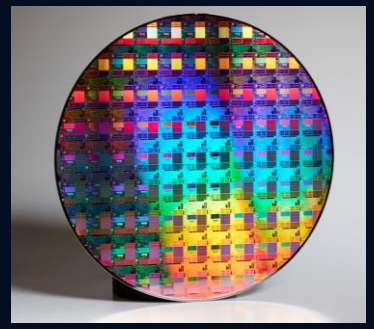
- 半導體產業鏈與製造環境
- 用於晶圓廠通訊的 SECS/GEM 標準
- 如同工控環境存在的資安隱憂
- 對於晶圓製造環境與設備供應商可能的防護策略

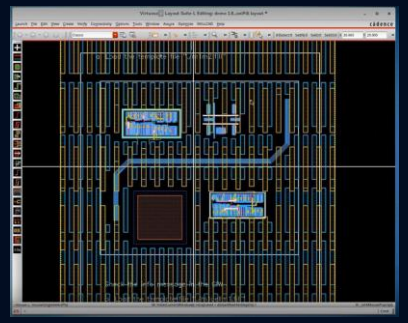
https://www.cw.com.tw/article/5119487

半導體製造過程

Equipment







Mask

晶片製造

Foundry

晶片封裝

Assembly

EDA tool

(電子設計自動化)

IC 設計

Design house

Wafer Material

Packaging Material

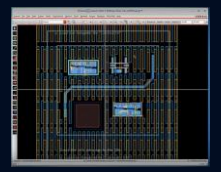
Keep the Operation Running

產業鏈關係緊密、高度專業化

txOne networks

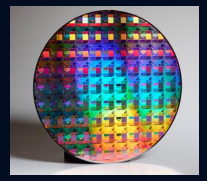
半導體 OT 環境

IC 設計



晶片製造

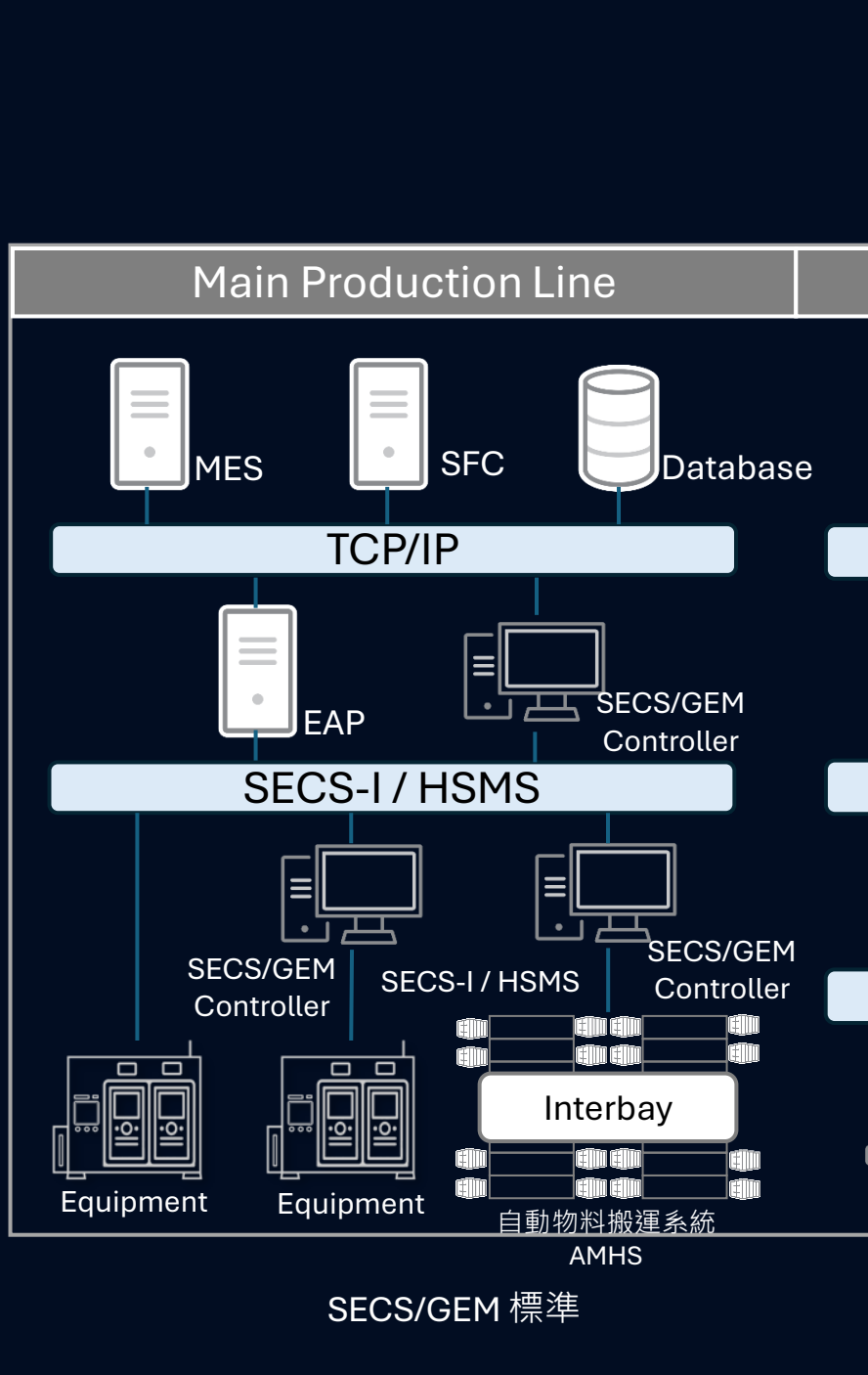
Foundry



晶片封裝

Assembly

消費者



SECS/GEM 標準

一般 OT 環境的脆弱性

第三方工程師或整合商攜帶自己的設備

內部威脅

老舊系統

許多作業系統或設備已終止支援

網路未適當地隔離

網路扁平

更新限制

設備保持運行，難以實現更新流程

晶圓廠自動化需求

- 提高製造效率與良率
- 晶圓尺寸越來越大
- 降低人員操作失誤風險
- 適應不同製造商的設備
- SECS/GEM 標準

自動物料搬運系統 (AMHS)

SECS/GEM 標準相關者

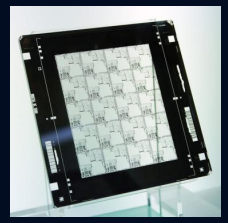
Lithography

CMP

Ashing

Inspection

Mask



Support SECS/GEM

Wafer Process

Slicing and Polishing

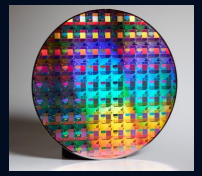
Oxidation/ Diffusion/ Deposition

Photolithography

Etching

Inspection

Foundry



晶片製造

晶片封裝

Die Attach

Wire Bonding

Encapsulation

Testing

Assembly

Package Bonder

Wire Bonder

Test

Cz Pulling

Growth

Wafer Material

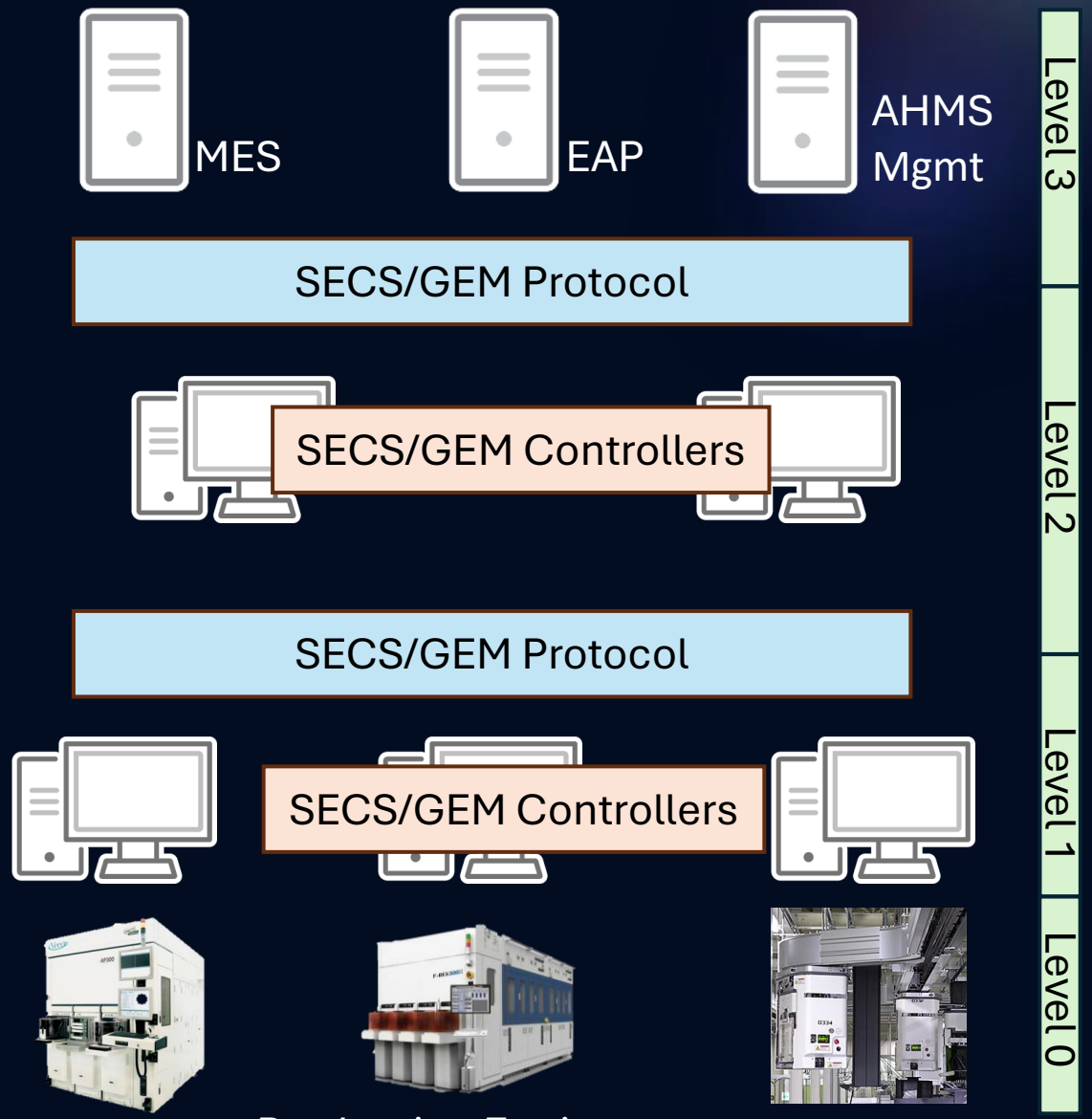
Packaging Material

Keep the Operation Running

1. https://ecmlabsolutions.com/products/czochralski-crystal-growth/
2. https://www.ebara.com.sg/index.php?route=product/product&product_id=117
3. https://www.esi-semi.com/e3511-asher
4. https://www.cncbul.com/urun/kla-tencor-surfscan-sp1-tbi-unpatterned-wafer-defect-inspection-systems-year-2001/
5. https://veeco.com/products/ap200-300-lithography-systems/
6. https://www.yamaha-robotics.com/en/products/process/fpb-1ws_neoforce
7. https://skti.com.tw/product_d.php?lang=tw&tb=1&id=15
8. https://www.tel.com/product/precio.html

晶圓廠自動化

- SECS/GEM 影響整個晶圓廠
- 晶圓製程採用逐層堆疊的方式在晶圓上製作電路
  - 只要流程被打斷，就必須從頭開始
- 高度專業化的設備和技術
  - 影響全球晶圓產量和生產週期



晶圓廠自動化

- SECS/GEM 影響整個晶圓廠

疊的方

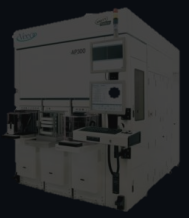
必須從

高度客製化的設備和技術

Semiconductor量和生產週期

Solar Power

PCB



MES

EAP

AHMS Mgmt

SECS/GEM Protocol

SECS

SECS

SECS/GEM Cont s

Production Equipment

Level 3

Level 2

Level 1

Level 0

SECS/GEM 概述
(SEMI Equipment Communication Standard/Generic Equipment Model)

SEMI E30 (GEM)

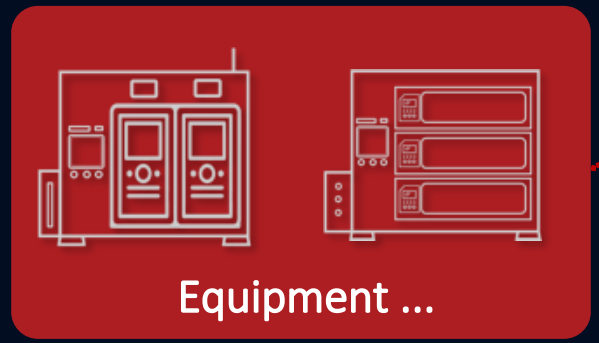
SEMI E5 (SECS-II)

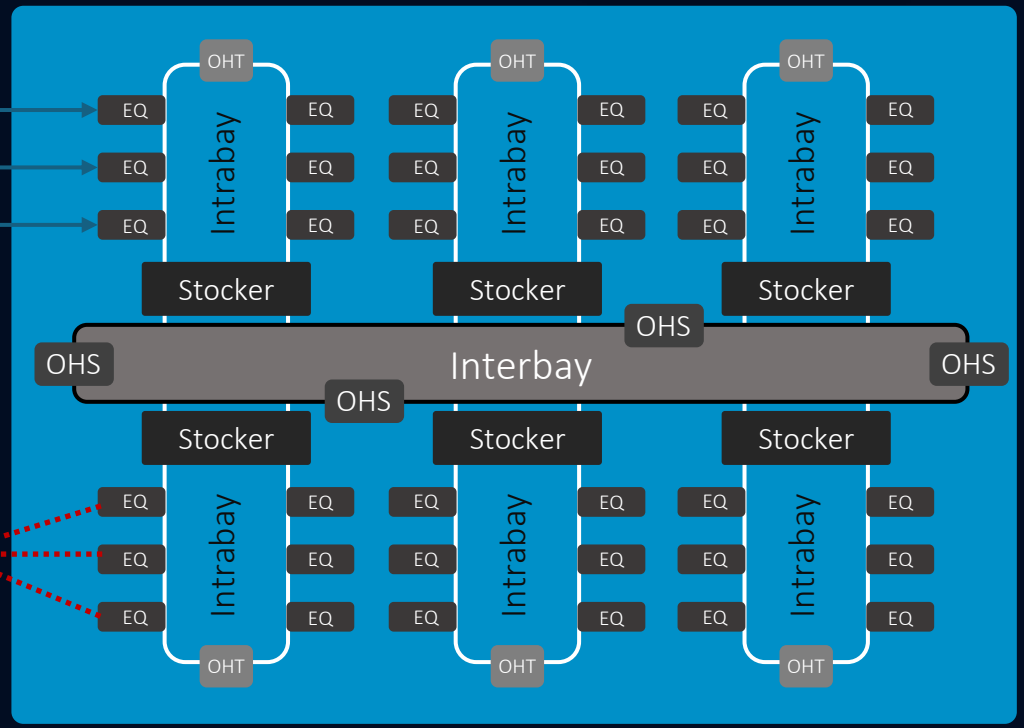
SEMI E37 (HSMS)

...

SECS/GEM

設備控制





自動物料搬運系統 (AMHS)

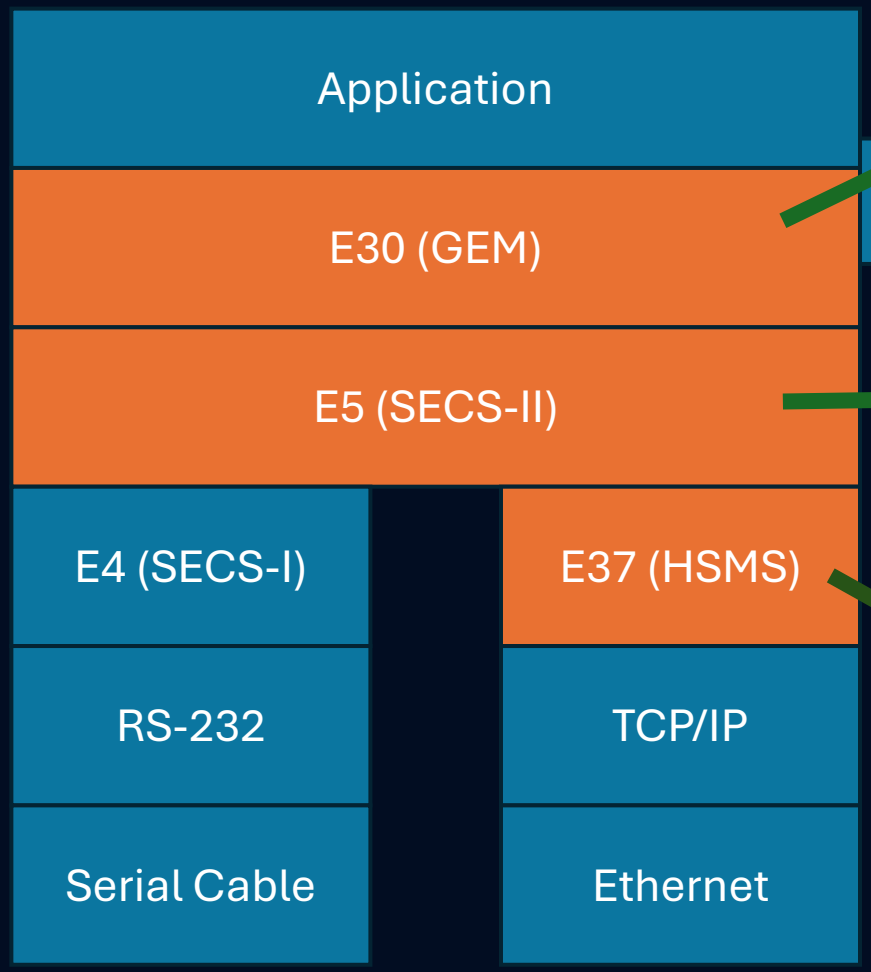
txOne networks

SECS/GEM 關係

設備的行為與狀態

訊息的格式與內容

收發訊息的通訊協定



E87, E40, E39, E90

Host Request Status Data ...

訊息的格式

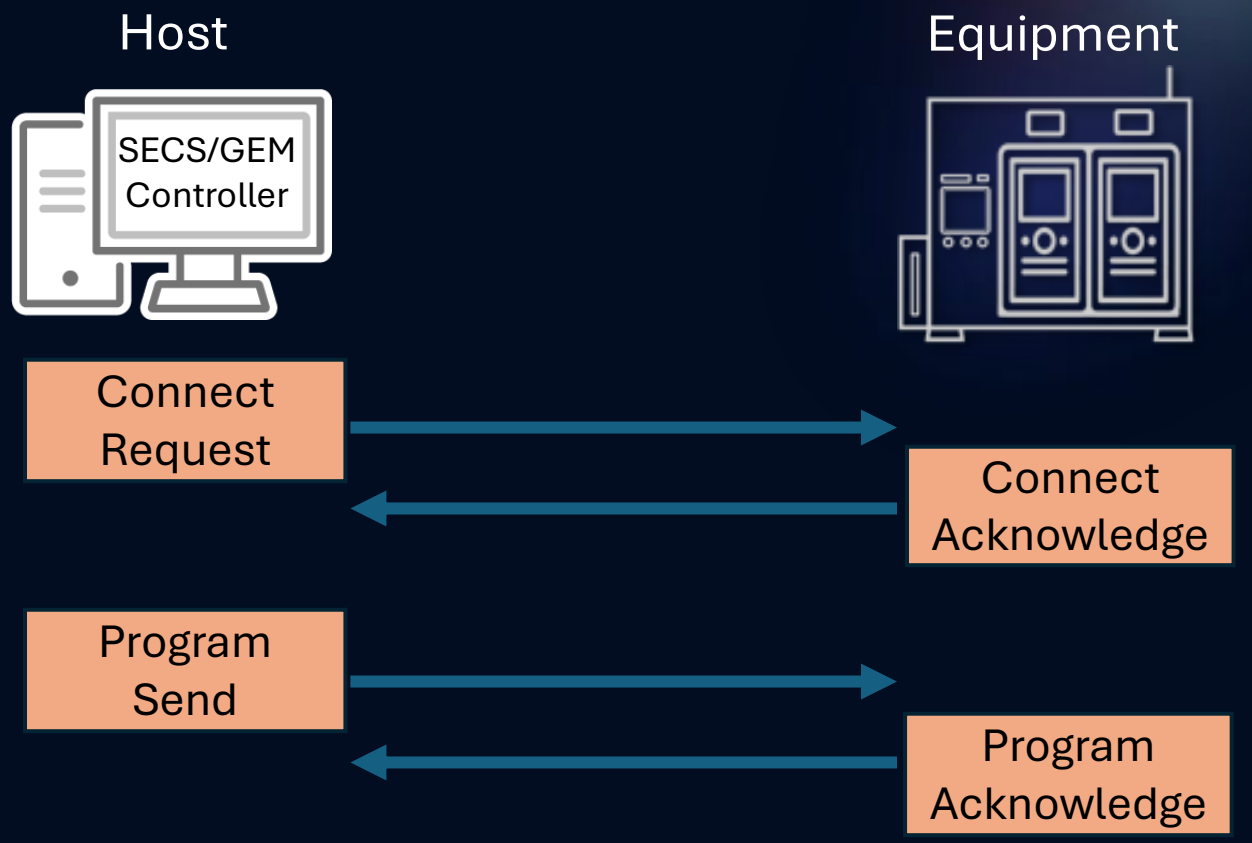
```
s1f1_1: S1F1 W
<L
  <L
    <Boolean 0x01 0x00>
    <F4 0.5567>
    <L
      <F8 0.9>
    >
  >
  <B 0x00 0x05 0x06 0x09 0xff>
>.
```

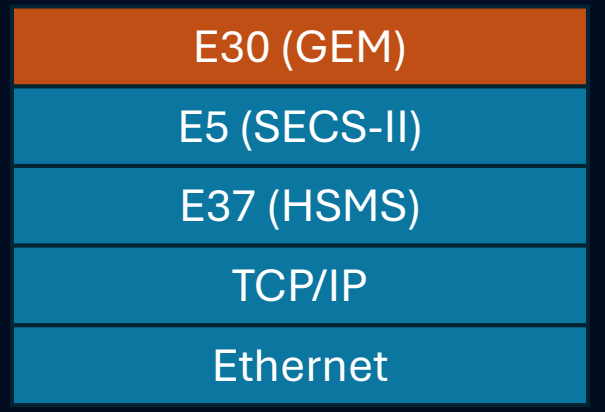
```
> Frame 10235: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: VMware_fc:b2:96 (00:0c:29:fc:b2:96), Dst: VMware_de:e6:
> Internet Protocol Version 4, Src: 192.168.59.161, Dst: 192.168.59.153
> Transmission Control Protocol, Src Port: 50174, Dst Port: 5000, Seq: 385,
v High-speed SECS Message Service Protocol
    Packet length: 10
  > Header (Separate.req)
```


txOne networks

GEM
(Generic Equipment Model)

- 定義設備包含哪些功能以及在不同狀態下應發送哪些訊息
  - Establish Communications
  - Control
  - Process Program Management
  - Status Data Collection
  - Material Movement
  - Alarm Management
  - …





SECS-II

(SEMI Equipment Communication Standard-II)

- 定義了主機與設備之間收發訊息的格式以及涵義

- 使用 SxFy 標識：
  - Stream (行為分類)
    - Equipment Status
    - Equipment Control and Diagnostics
    - System Errors
    - …
  - Function (具體的內容)
    - Establish Communications Request
    - Host Command Send
    - Unrecognized Device ID
    - …


```
S1F13:'S1F13' W
      <L
          <A "WET.01">
          <A "REV.01">
      >.

S1F14:'S1F14'
     <L
          <B 0x00>
          <L
              <A "WET.01">
              <A "REV.01">
          >
      > .
```

E30 (GEM)

E5 (SECS-II)

E37 (HSMS)

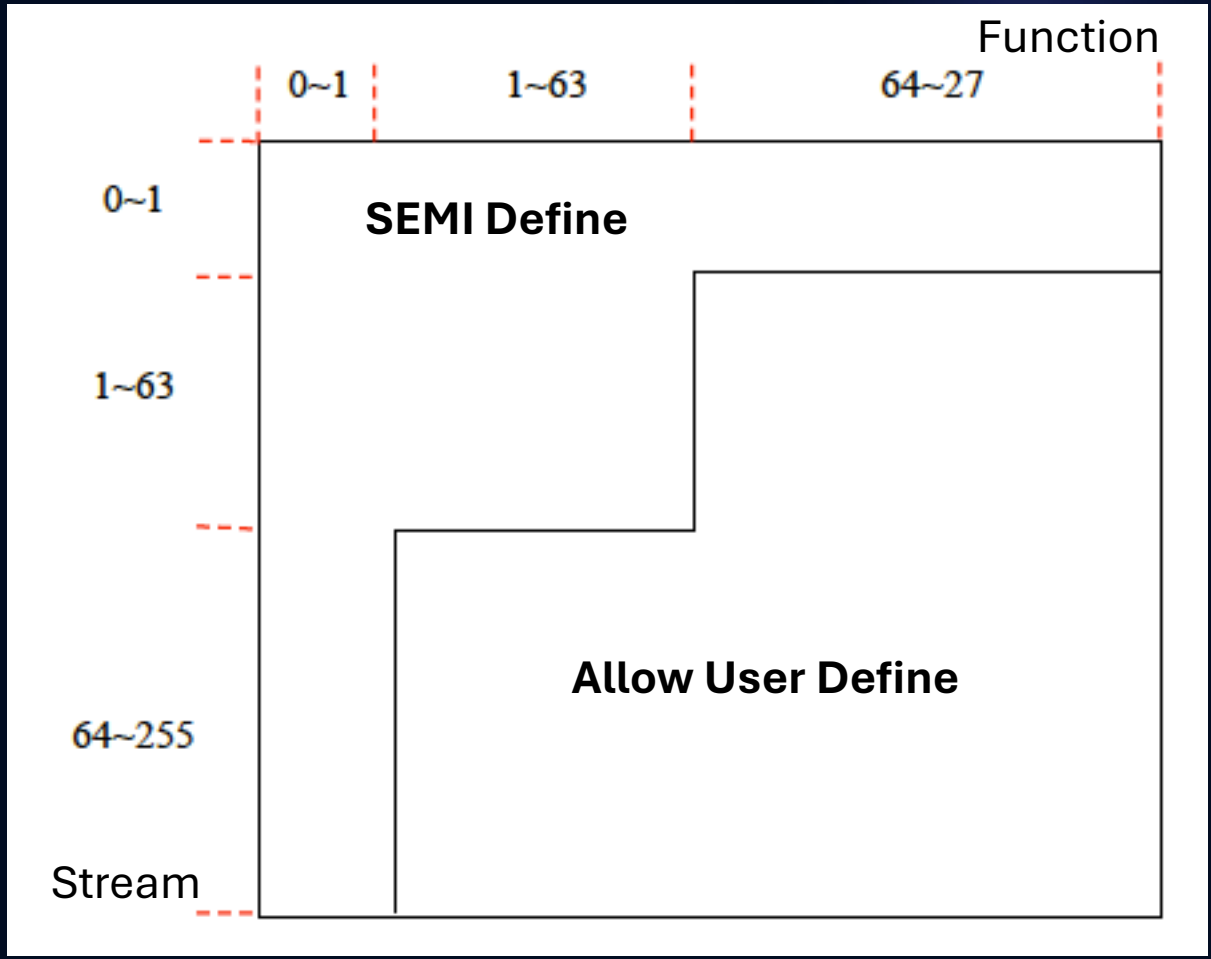
TCP/IP

Ethernet

SECS-II Stream/Function 標識

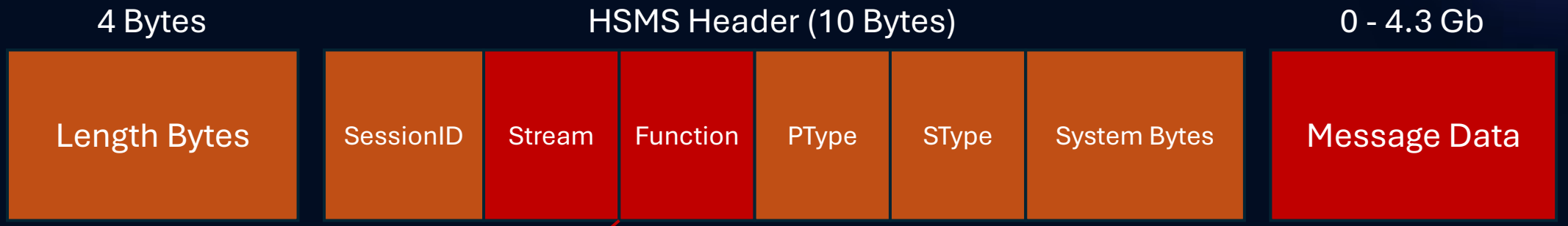
- Stream 1 - Equipment Status
  - F1 – Are You There Request
  - F3 – Selected Equipment Status Request
  - F13 – Establish Communications Request
  - F15 – Request Offline
  - F17 – Request Online
  - …
- Stream 2 – Equipment Control and Diagnostics
  - F15 – New Equipment Constant Send
  - F21 – Remote Command Send
  - F41 – Host Command Send
  - …
- Stream 9 – System Errors
  - Unrecognized Device ID
  - Unrecognized Stream
  - Unrecognized Function
  - …

User Definable
Streams 1-63, Functions 64-255
Streams 64-127, Functions 1-255

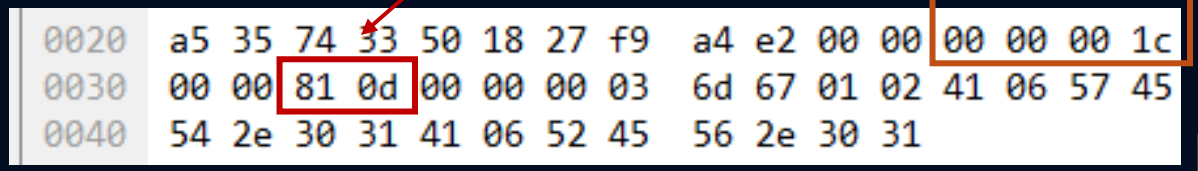


HSMS
(High Speed Message Service)

- 基於 TCP/IP 協定的訊息交換流程



Host



Equipment

S1F13

Connect Request

Connect Acknowledge

S1F14

E30 (GEM)

E5 (SECS-II)

E37 (HSMS)

TCP/IP

Ethernet

HSMS Message

- Data Message：資料訊息 (SxFx)
- Linktest.req / Linktest.rsp：通訊狀態確認訊息
- Select.req / Select.rsp：建立 HSMS session 訊息
  - 設備須在 selected 狀態下，才能收發資料訊息
- Deselect.req / Deselect.rsp：終止 session 訊息
- Separate.req：單方面通訊終止訊息
- Reject.req：收到無效訊息時發送

ARP Spoofing to Inhibit Response Function

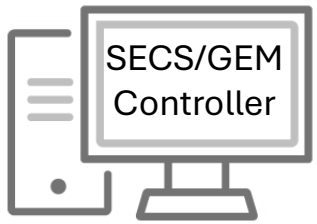
Active/Host **Host**

```
13:59:17.554: Send Linktest.req.
13:59:17.569: Receive Linktest.rsp.
13:59:29.085: Send S1F3(13369886).
S1F3 W
<L[1]
  <U2[1] 1>
>
.
14:00:14.085: T3 Timeout(13369886).
14:00:14.085: Receive Linktest.req.
14:00:14.085: Send Linktest.rsp.
14:00:17.554: Send Linktest.req.
14:00:17.554: Receive Linktest.rsp.
```

Normal data message

```
14:01:30.569: Send S1F3(13369889).
S1F3 W
<L[1]
  <U2[1] 1>
>
.
```

```
14:02:17.554: Send Linktest.req.
Remote Server Disconnected!
HSMS Communication Disconnected!
SECS Emulator v1.5  2001/09/05
HSMS Communication Started!
Remote Server Disconnected!
HSMS Communication Disconnected!
```

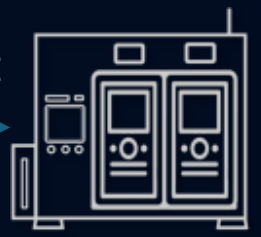


Host

Normal data message

MITM attack

Separate request



Equipment

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 5000

No.	Time	Source	Destination	Protocol	Length	Info
10143	10000.979038	192.168.59.153	192.168.59.161	TCP	54	5000 → 50174 [ACK] Seq=155
10176	10045.928323	192.168.59.153	192.168.59.161	HSMS	68	HSMS Message Linktest.req
10177	10045.937704	192.168.59.161	192.168.59.153	HSMS	68	HSMS Message Linktest.rsp
10178	10045.992242	192.168.59.153	192.168.59.161	TCP	54	5000 → 50174 [ACK] Seq=169
10180	10049.397444	192.168.59.161	192.168.59.153	HSMS	68	HSMS Message Linktest.req
10181	10049.401018	192.168.59.153	192.168.59.161	HSMS	68	HSMS Message Linktest.rsp
10182	10049.477825	192.168.59.161	192.168.59.153	TCP	60	50174 → 5000 [ACK] Seq=357
10219	10105.916877	192.168.59.153	192.168.59.161	HSMS	68	HSMS Message Linktest.req
10220	10105.933638	192.168.59.161	192.168.59.153	HSMS	68	HSMS Message Linktest.rsp
10221	10105.979522	192.168.59.153	192.168.59.161	TCP	54	5000 → 50174 [ACK] Seq=197
10224	10109.381705	192.168.59.161	192.168.59.153	HSMS	68	
10225	10109.385216	192.168.59.153	192.168.59.161	HSMS	68	
10226	10109.461477	192.168.59.161	192.168.59.153	TCP	60	50174 → 5000 [ACK] Seq=385
10235	10122.413452	192.168.59.161	192.168.59.153	HSMS	74	HSMS Message Separate.req
10236	10122.463922	192.168.59.153	192.168.59.161	TCP	54	5000 → 50174 [ACK] Seq=211

Separate.req

```
> Frame 10235: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
> Ethernet II, Src: VMware_fc:b2:96 (00:0c:29:fc:b2:96), Dst: VMware_de:e6:fc
> Internet Protocol Version 4, Src: 192.168.59.161, Dst: 192.168.59.153
> Transmission Control Protocol, Src Port: 50174, Dst Port: 5000, Seq: 385, A
v High-speed SECS Message Service Protocol
    Packet length: 10
  > Header (Separate.req)
```

```
0000  00 0c 29 de e6 fd 00 0
0010  00 3c 94 73 40 00 80 0
0020  3b 99 c3 fe 13 88 b4 0
0030  04 01 ce 31 00 00 00 00  00 0a ff ff 00 00 00 09   ···1···· ········
0040  00 cc 02 21 01 01 a9 02  00 01                     ···!···· ··
```

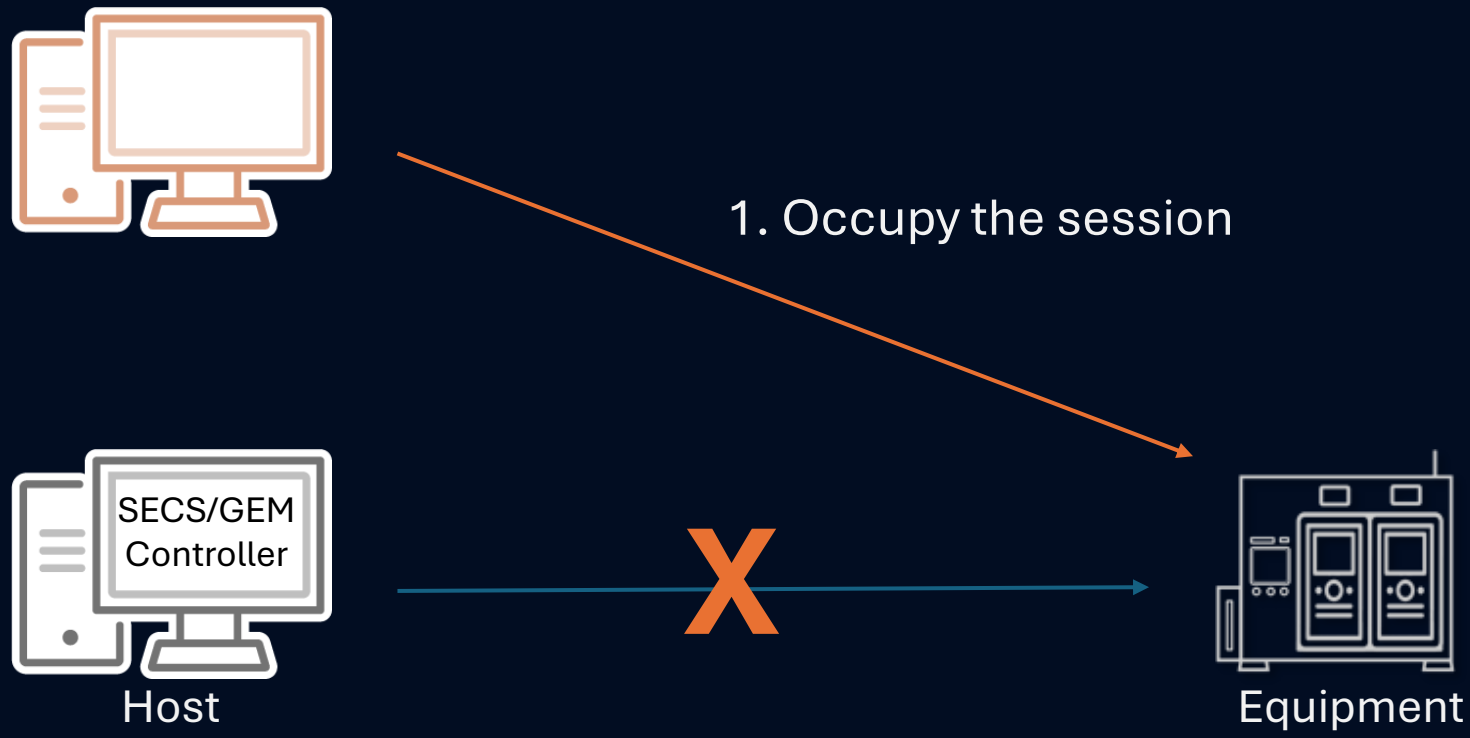
Passive/Equipment **Equipment**

```
13:59:14.086: Send Linktest.req.
13:59:14.086: Receive Linktest.rsp.
13:59:17.555: Receive Linktest.req.
13:59:17.555: Send Linktest.rsp.
13:59:29.086: Receive S1F3(13369886).
S1F3 W
<L[1]
  <U2[1] 1>
>
.
14:00:14.082: Send Linktest.req.
14:00:14.091: Receive Linktest.rsp.
14:00:17.551: Receive Linktest.req.
14:00:17.555: Send Linktest.rsp.
14:01:14.070: Send Linktest.req.
14:01:14.086: Receive Linktest.rsp.
14:01:17.524: Receive Linktest.req.
14:01:17.524: Send Linktest.rsp.
14:01:35.570: T8 Timeout.
14:02:22.570: T8 Timeout.
Remote Client Disconnected!
14:02:27.586: T8 Timeout.
```

HSMS

- 基於 TCP/IP 通訊協定
- 不需認證也未進行加密

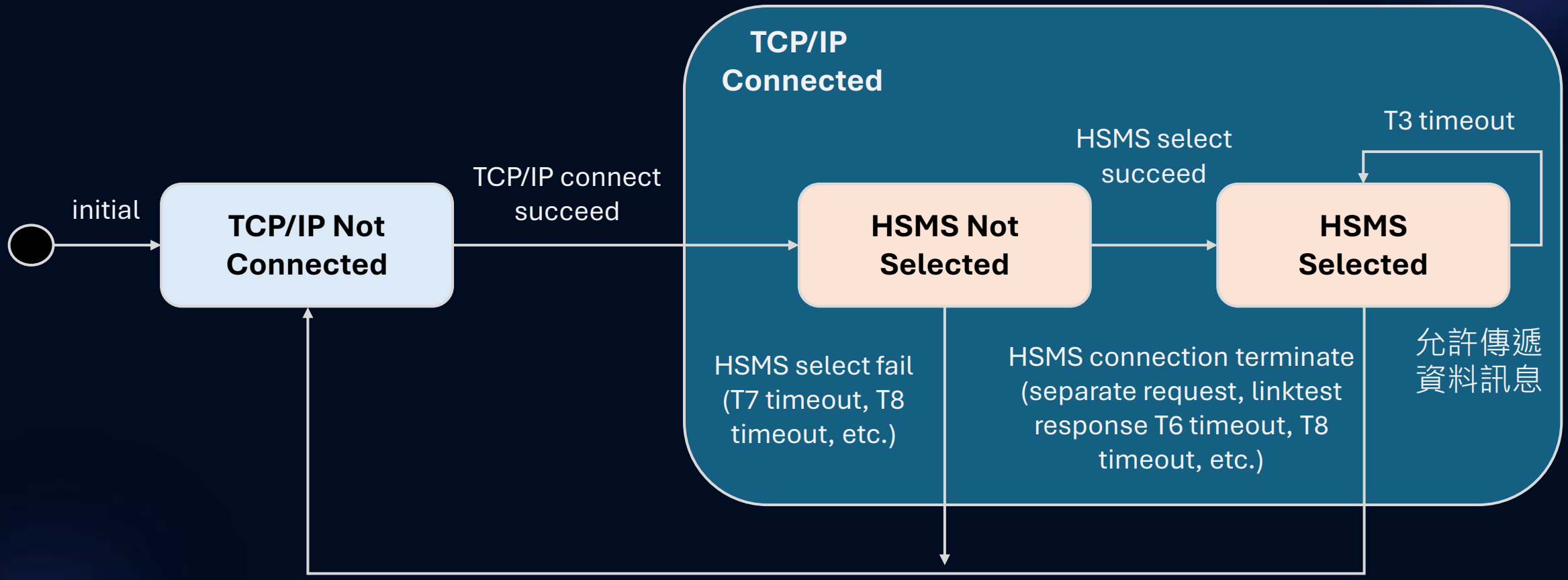
ARP Spoofing to Inhibit Response Function



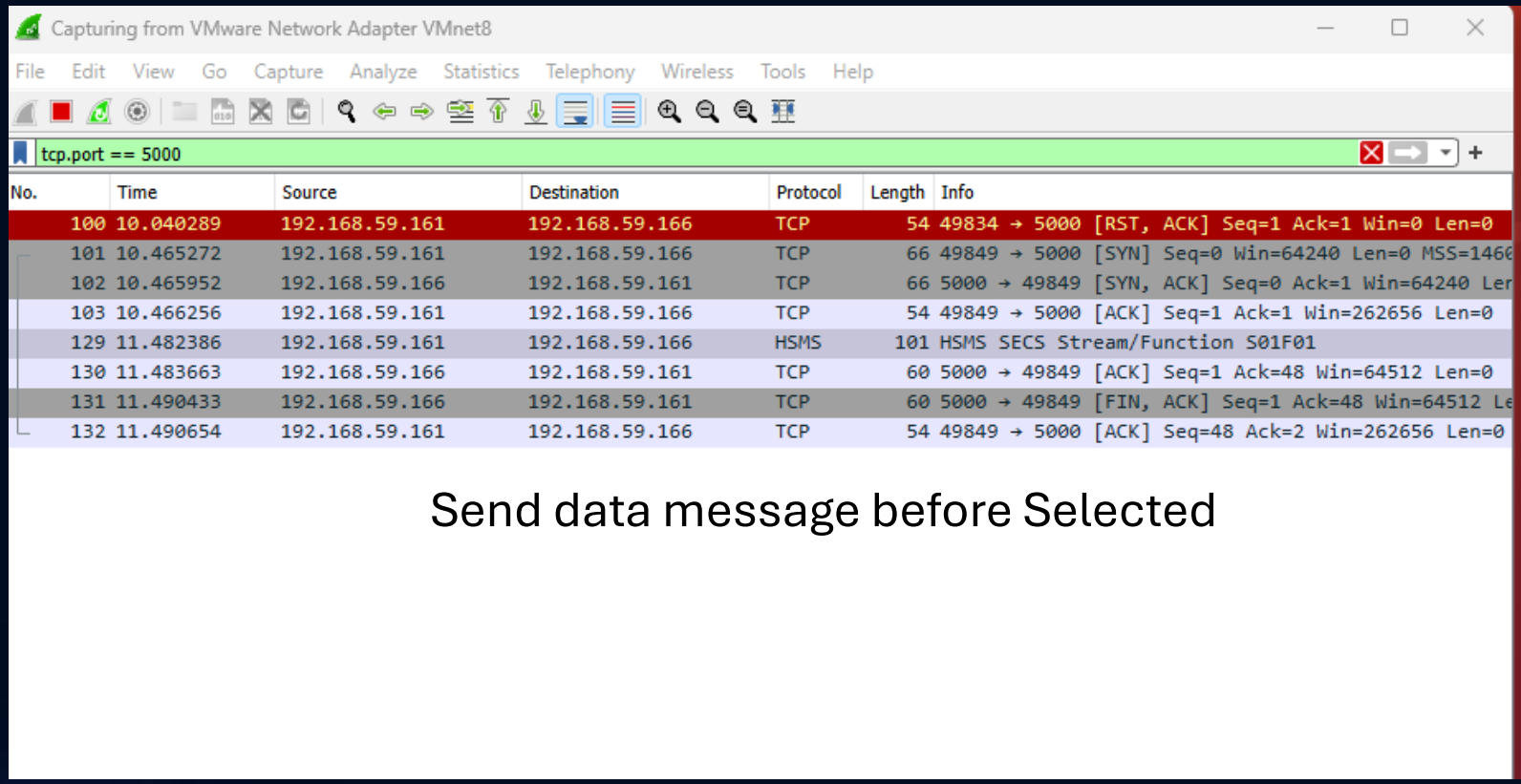
2. Since production network lack visibility. It's difficult to detect the issue

SINGLE SELECTED-SESSION MODE (HSMS-SS)
單一 session 的模式

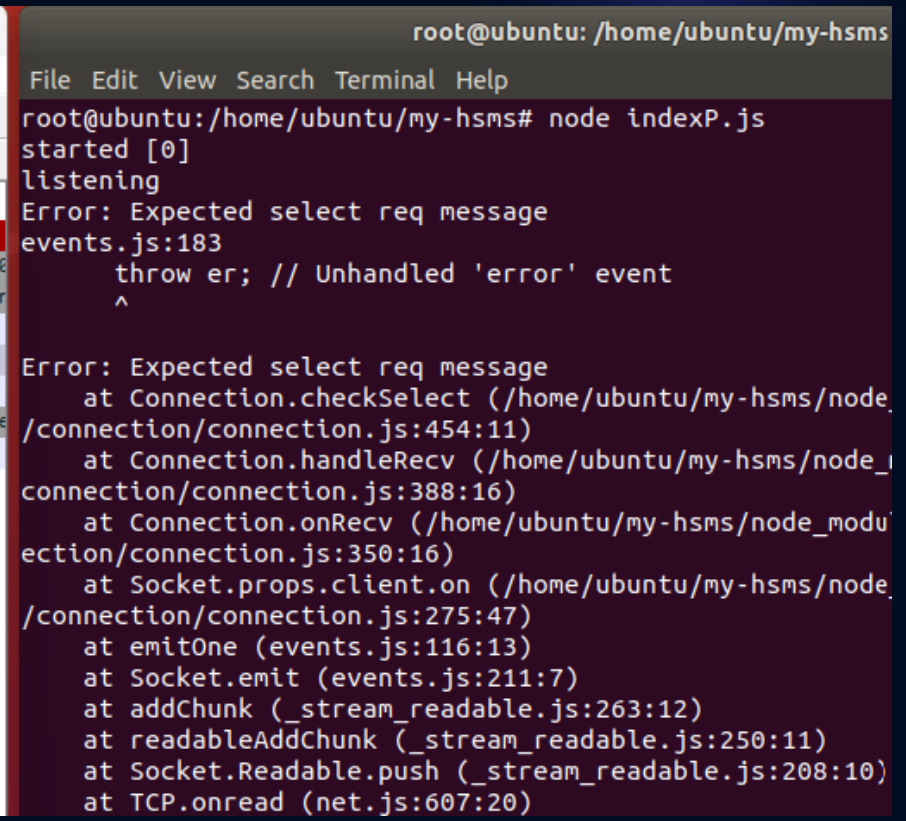
HSMS 狀態機


TCP/IP
Connected
initial
TCP/IP Not
Connected
TCP/IP connect
succeed
HSMS Not
Selected
HSMS select
succeed
HSMS
Selected
T3 timeout
HSMS select fail
(T7 timeout, T8
timeout, etc.)
HSMS connection terminate
(separate request, linktest
response T6 timeout, T8
timeout, etc.)
允許傳遞
資料訊息

未適當實作例外處理 – Unexpected request



Send data message before Selected



半導體製造環境如同 OT 環境存在難以避免的資安隱憂

Description	Potential risks
基於 TCP/IP 的 HSMS 通訊協定並無資訊安全考量	不需認證、通訊未加密
部分 HSMS 通訊協定設計僅允許 Single session	占用 session 來延遲設備復原時間
採用四種狀態來描述 TCP/IP 和 Select 的當前情況，只有在正確的狀態下才能執行特定的操作	當缺乏正確的異常處理時，會導致程式崩潰
在 SECS II 規範中，使用者可自行定義 Stream 與 Function	製造商可能設計高風險的功能
...	...

網路未適當地隔離

網路扁平

更新限制

設備保持運行，難以實現更新流程

對於晶圓製造環境與設備供應商的防護策略

txOne networks

https://www.cw.com.tw/article/5119487

對於晶圓製造環境

- SEMI- 半導體製造環境的網路安全參考架構 (Oct 2023)
  - Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment

採用防護設備

- Tool Configurations – 防火牆/路由器進行安全配置
- Prevent, Detect and Response – 使用 SIEM 等提升網路安全可視性
- Vulnerability/Threat Assessment and Patch Management – 資產盤點，以有效識別漏洞

落實資安管理

- Move-in/Move-Out/Transfer – 搬入前確保最新的更新、病毒掃描
- Tool Network and Application Integration - 工廠設備與系統整合安全
- Local & Remote Accesses – 管理遠端存取，避免未經授權的訪問
- Secure data exchange – 資料的輸出或輸入，需要嚴格控制
- User Awareness Training – 針對不同角色進行定制化的安全意識培訓
- Security Key Performance Indicators – 定義與監控安全關鍵指標

從設計上強化安全

- Secure by Design – 應用 SEMI E187，保障設備在設計階段滿足基本網路安全要求
  - → 適用於半導體設備供應商

Keep the Operation Running

https://www.semi.org/zh/Cybersecurity_Reference_Architecture_for_Semiconductor_Manufacturing_Environment

txOne networks

對於設備供應商

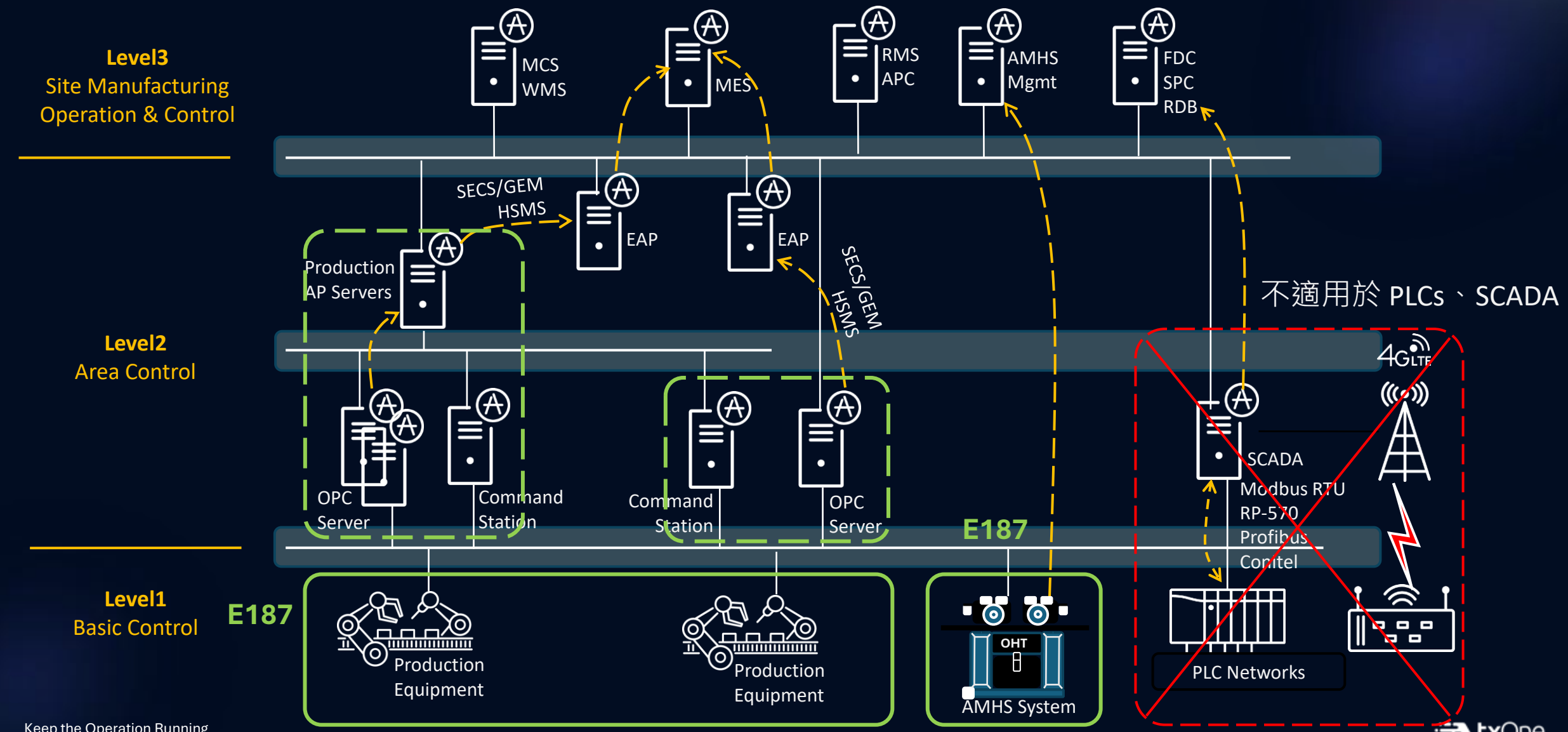
- SEMI E187
  - 適用於為半導體製造廠提供設備或服務的實體，如設備供應商和系統整合商
  - 定義半導體設備基本的網路安全要求，透過設計來保護半導體製造設備安全
  - 共 12 項要求

- 歐盟資安韌性法 (Cyber Resilient Act)
  - 適用於歐盟範圍內的數位產品
  - 要求數位產品設計、開發及整個生命周期內符合網路安全
  - 具強制力，2027/12/11 生效
  - 對於網路安全與漏洞處理，共 22 項要求

Scope of SEMI E187

- 半導體生產設備
- 自動化物料搬運系統 (AMHS)

(安裝有 Windows 或 Linux 作業系統)



txOne networks

E187 - Specification for Cybersecurity of FAB Equipment

Operating System

- Supported OS
- Doc of Security patch update

不得使用過時的作業系統

Network Security

- Secure transmission Protocol
- Doc of Network configuration

網頁服務、檔案傳輸等，
須支援安全的傳輸協定

Endpoint Protection

- Vulnerability Mitigation
- Malware Scanning
- Anti-Malware Protection
- Security Hardening
- Authentication Mechanism
- Authorization Solutions

設備出貨前須進行漏洞、惡意程式掃描，並
提供安全強化與認證等設置

Security Monitoring

- Security Event Log
  ① Included OS and Application
- Log type
  ① Access Control
  ② Configuration Changes
  ③ System Error

設備須提供安全日誌功能

歐盟資安韌性法 (Cyber Resilient Act)

- 網路安全要求
  - 須正式的風險管理與評估流程
  - 不可以存在已知漏洞
  - 預設為安全配置
  - 能夠進行安全性更新
  - 須有機制防止未經授權的訪問
  - 保護資料的機密性
  - 保護資料的完整性
  - 資料最小化原則
  - 保護產品可用性
  - 不應影響其他設備或網路服務
  - 減少外部接口
  - 採用緩解措施來減少安全事的影響
  - 記錄並提供安全訊息
  - 提供永久刪除資料與設定功能
- 漏洞處理要求
  - 須建立產品 SBOM
  - 須立即修復漏洞並提供安全性更新
  - 定期對產品進行安全性測試與審查
  - 須公開已修復的漏洞訊息
  - 制訂與執行漏洞揭露政策
  - 須採取措施取得產品及其第三方元件潛在的漏洞
  - 提供安全地分發產品更新的機制
  - 確保安全性更新可用時，立即發布更新，

Takeaway

- 半導體廠如同工控環境存在難以避免的資安隱憂
  - SECS/GEM 標準設計時，未以資安作為優先考量
  - 自動化工廠設備與系統的整合
  - 設備移入、移出的管理風險

- 對於晶圓製造環境
  - 落實半導體製造環境的網路安全參考架構
  - Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment
    - 採用防護設備
    - 落實資安管理
    - 從設計上強化安全

- 對於設備供應商
  - 遵循 SEMI E187
  - 參考 Cyber Resilient Act 的基本網路安全要求


txOne
networks