
5G Field Test and Information Security
「 5G場域測試及資訊安全」
財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Agenda

1 | **5G通訊重要價值及面臨之資安挑戰**

2 | 物聯網場域資安防護評估指引
指引架構

3 | 評估流程
威脅建模、漏洞檢測、滲透測試、衝擊分析

5G通訊技術最重要之價值在垂直場域

Smart Factory

Smart Traffic

Airport

Shopping Mall

Healthcare

Smart Grid

駭客攻擊無孔不入，攻擊事件層出不窮

項目	事件名稱
1	烏克蘭能源勘探生產公司Burisma Holdings遭駭客入侵網路
2	美國天然氣運營商遭受網路攻擊勒索事件
3	德國葡萄牙電力集團(EDP)遭勒索巨額錢款
4	以色列供水部門工控設施受到駭客攻擊
5	澳大利亞航運及物流公司四個月內接連兩次遭受網路攻擊
6	台灣兩大煉油廠遭駭客勒索
7	本田公司受到工業型勒索軟體攻擊
8	Sodinokibi勒索軟體攻擊巴西電力公司Light S.A.
9	印度新冠疫苗製造廠遭受攻擊導致數據洩露
10	巴西全球第三大飛機製造商遭勒索攻擊並導致數據洩露
11	SolarWinds事件波及美國核武器庫

駭客類型與目標：

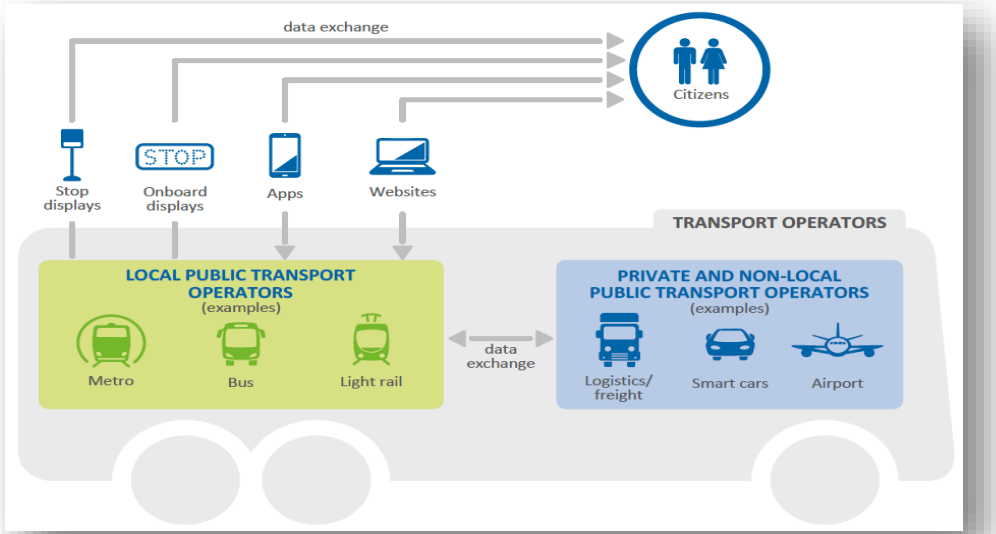
係為一群技術頂尖的團體組成(可謂是數位世界的黑幫)，挑選特定企業之動機就是破壞影響運作及勒索。為達到此目的在入侵階段必須繞過企業資安防護重重關卡，進而取得具有價值的資料或破壞用以勒索，**通常透過一段時間縝密的滲透和隱藏**。

衝擊影響概要：

1.客戶合約、個資等遭竊取外流，可能衍生賠償。
2.攜手跨境不同公司的研發設計心血遭竊取外流，可能衍生違約賠償問題。
3.相關產線可能受影響。
4.登上媒體頭條，企業品牌、連帶相關產品形象重創。

5G垂直場域應用資安威脅與挑戰: IT + OT + CT整合

應用場景需求



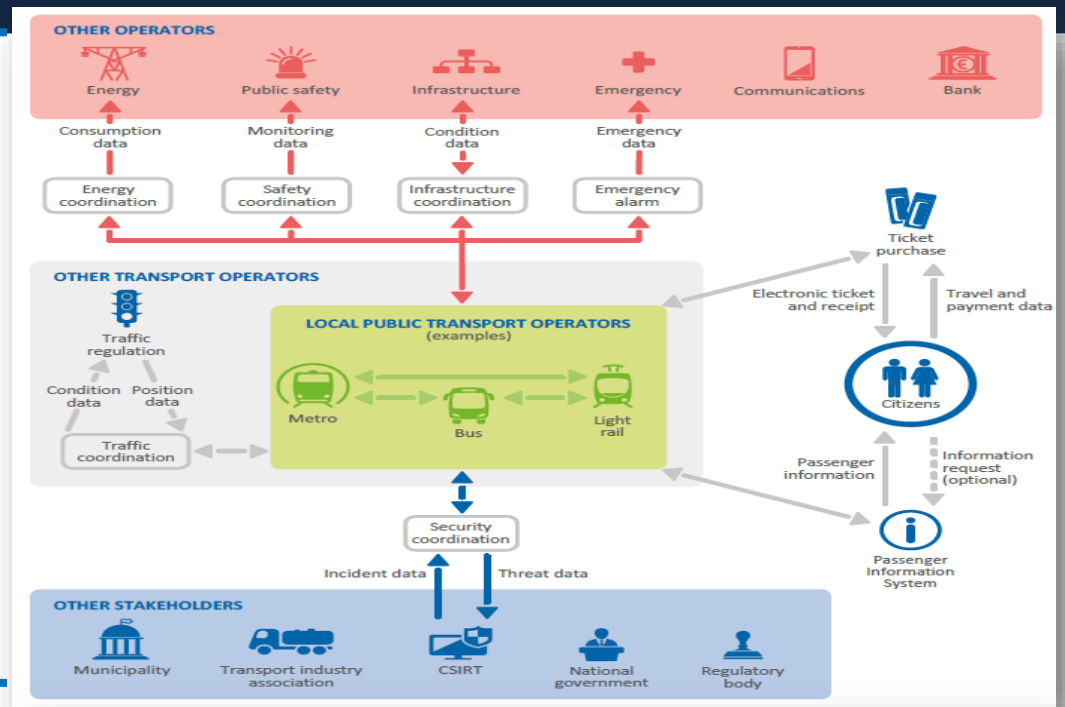
混合通訊協定與技術:5G, IEEE 802.11, TCP/IP, Modbus IP, CAN Bus, MQTT等

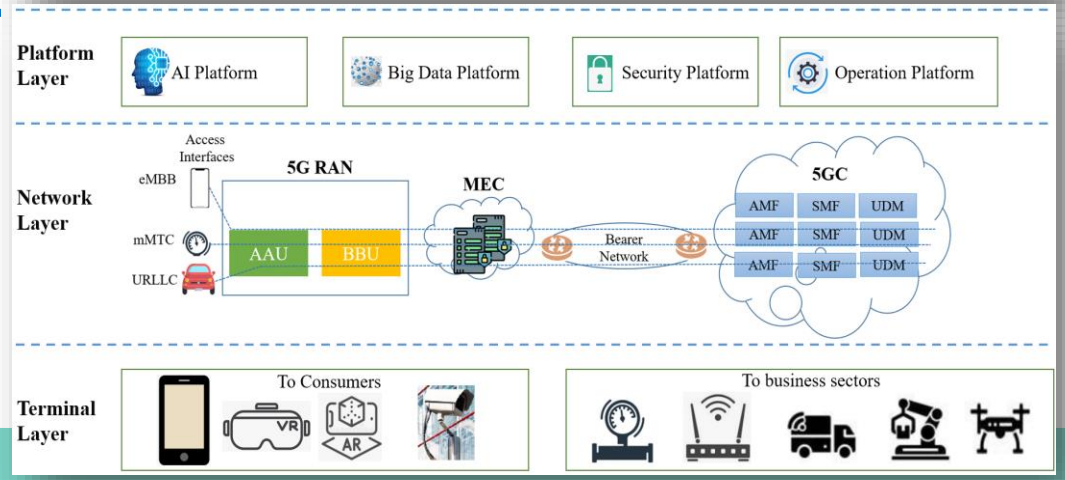
機電系統 | SCADA | 號誌系統 | 監控系統

大數據分析系統

營運資料 | 量測資料 | 維修資料 | IOT感測資料

應用場景與其他系統的介接和整合 5G通訊網路架構





參考來源與部份摘錄整理: ENISA和Study on security and privacy in 5G-enabled applications

5G垂直場域應用資安威脅與挑戰: IT + OT + CT整合

終端聯網設備安全

實體安全　　通訊傳輸安全
作業系統安全　雲端介面安全
應用程式安全　身分驗證安全

雲端服務平台安全

資料儲存安全

金鑰管理
資料加解密技術
資料的備份/資料遺失防護
資料刪除的安全性/資料隱私

雲端作業系統與虛擬化安全

Docker技術的安全性
虛擬機隔離機制安全
設定配置的安全
Hypervisor安全機制

應用安全

資料內容的安全性機制
網頁與網站安全
軟體與系統更新機制

巨量資料安全

資料儲存安全

關聯性資料庫的安全
NoSQL資料庫的安全
異動記錄檔的安全

分散式運算框架的安全性

Spark平台的安全
Hadoop平台的安全

資料的隱私權與保護

隱私洩漏安全防範
加密演算法
傳輸安全

5G網路安全

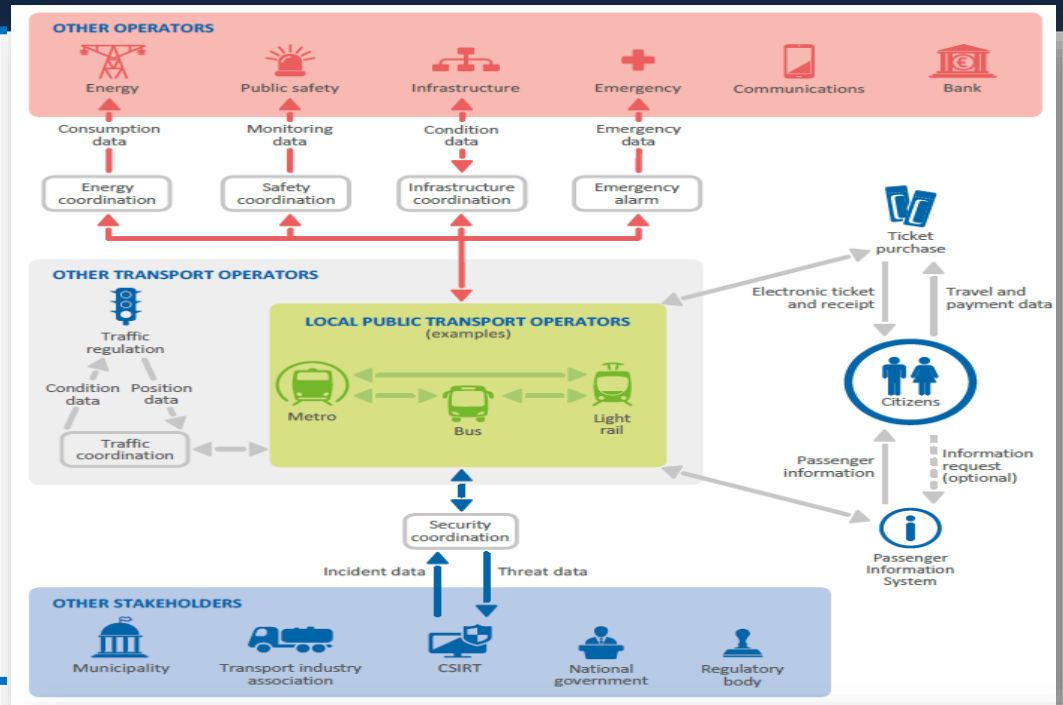
SDN安全　**NFV安全**

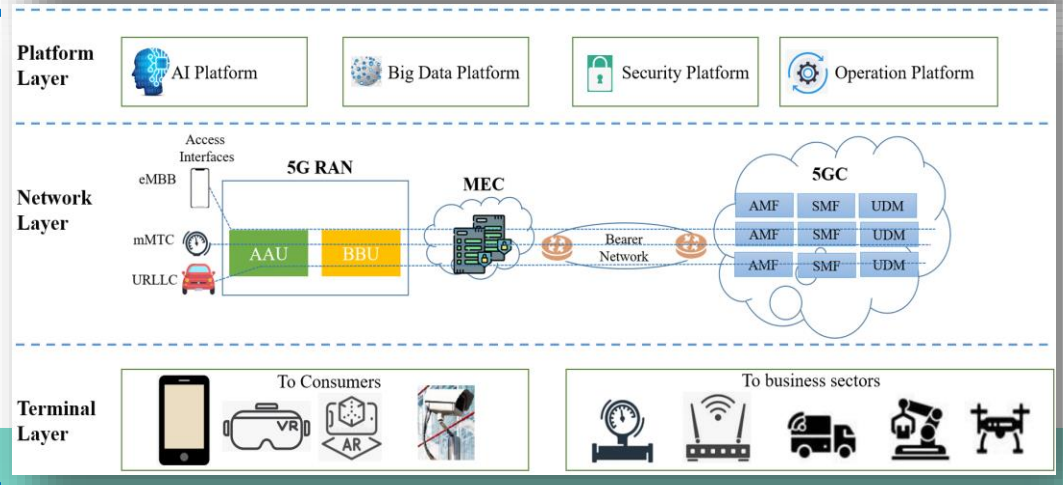
網路切片(Network Slicing)安全

網路部署風險　**MEC安全**

RAN和5GC安全

應用場景與其他系統的介接和整合　5G通訊網路架構





參考來源與部份摘錄整理: ENISA和Study on security and privacy in 5G-enabled applications

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Agenda

1 | 5G通訊重要價值及面臨之資安挑戰

2 | 物聯網場域資安防護評估指引

指引架構

3 | 評估流程

威脅建模、漏洞檢測、滲透測試、衝擊分析

物聯網場域資安防護評估指引

國家發展委員會
NATIONAL DEVELOPMENT COUNCIL

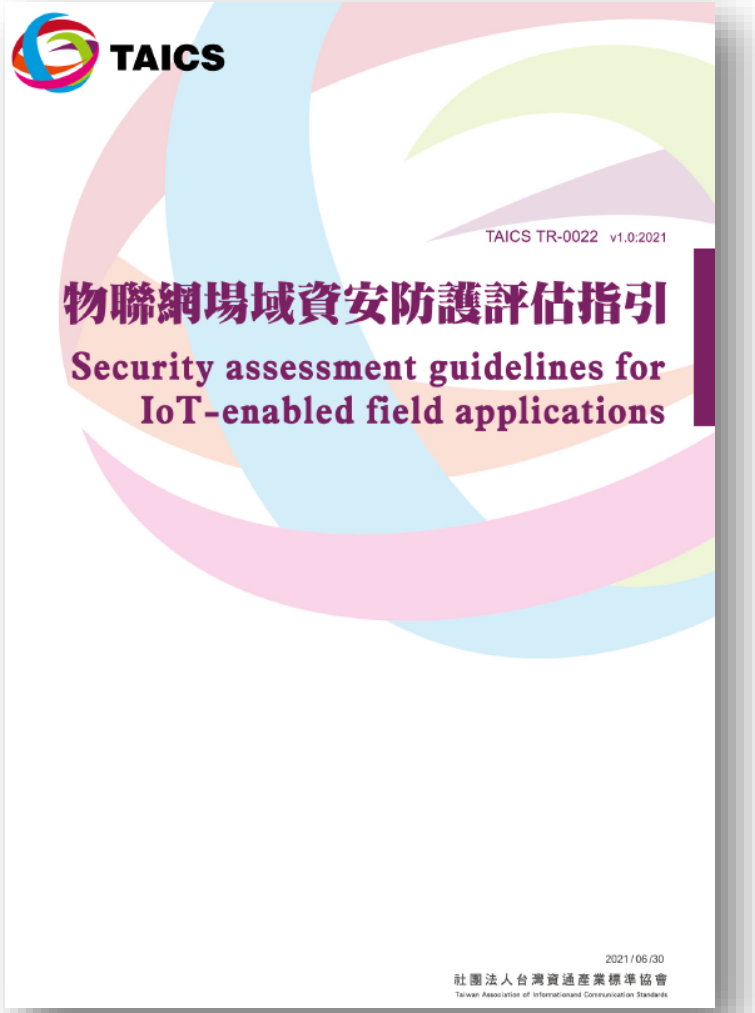
107年

亞洲·矽谷計畫
強化物聯網資安防護

協助國內企業提升其物聯網系統資安防護能力，因應物聯網新興智慧應用面臨的資安風險。

研析並調合國際規範

透過研析國際間物聯網資安評估指引及規範，比對並調和，制定「物聯網場域資安防護評估指引」(TAICS TR-0022)，作為國內物聯網場域資安遵循準則，降低使用各種新興服務所涉及的隱私及資安疑慮，強化場域安全。



物聯網場域資安防護評估指引

物聯網場域資安防護評估指引
Security assessment guidelines for IoT-Enabled field applications

(第1章) 適用範圍

(第2章) 引用標準

(第3章) 用語及定義

(第4章) 資安防護評估

評估流程

威脅建模 Threat Modeling
第 5 章

- 從巨觀的角度進行以架構為基礎的攻擊面分析，進而評估整個場域的應用程式、設備或流程中可能遭受攻擊的弱點
- 透過威脅建模，得知受測系統場域的各項設備軟硬體資訊及功能運作流程等潛在威脅

漏洞檢測 Vulnerability Testing
第 6 章

- 檢測物聯網系統軟硬體是否存在重大漏洞或弱點，以提供後續滲透測試之依據
- 設備漏洞檢測包含應用服務層的資訊系統、網路傳輸層的網通設備及感知控制層的物聯網終端設備等三種

滲透測試 Penetration Testing
第 7 章

- 根據威脅建模及漏洞檢測對應後制定滲透測試情境
- 滲透測試主要的目的在於透過檢測手段評估威脅建模的各種威脅在各種檢出的漏洞下，確認實現該項威脅的可能性

衝擊分析 Impact Analysis
第 8 章

- 依據滲透測試結果，以DREAD及OCTAVE Allegro兩種影響評估分析模型並依據不同垂直應用，評估影響層面(包含技術、生命安全健康、財物損失等)

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Agenda

1 | 5G通訊重要價值及面臨之資安挑戰

2 | 物聯網場域資安防護評估指引
指引架構

3 | **評估流程**
威脅建模、漏洞檢測、滲透測試、衝擊分析

威脅建模(Threat Modeling, TM)

step 1

場域
資產設備盤點

5.1.1實體資產
5.1.2資訊資產

step 2

建立場域架構圖

為瞭解系統整體運作程序，並提供後續解析場域潛在的攻擊面向(Attack Surface)及潛在資安威脅。架構圖必須包含系統功能及所採用的通訊協定和技術。

step 3

解析運作程序

主要在於追蹤其運作時，各個進入點的資料流並記錄經過系統內哪些設備，識別出攻擊者最有可能的攻擊目標

step 4

識別並分析威脅

- 透過 STRIDE 威脅模型依照不同安全屬性進行各種威脅識別並進行分析。
- 物聯網場域 STRIDE常見威脅模型身分冒用、資料竄改、否認性、資訊洩漏、阻斷服務、權限提升

step 5

記錄威脅

完成識別所有可能威脅後，記錄至少包含STRIDE威脅類型、威脅模型、威脅目標、可能的攻擊技術與情境、潛在的衝擊。

威脅建模

物聯網場域 STRIDE 威脅模型分析說明

威脅類型	威脅情境	安全屬性
身分冒用 **Spoofing Identity**	• TM 01：檢視5G物聯網系統各種設備身分被冒用的可能性及攻擊者利用此威脅取得設備間信任而進行攻擊的情境 • TM 02：檢視設備間建立通訊管道的認證（Authentication）協定是否可能被冒用 • TM 03：檢視設定設備身分及帳密的程序是否有適當的安全管控，以防止非法設備接取至5G物聯網系統或洩漏帳密的可能性	認證
資料竄改 **Tampering with Data**	• TM 04：檢視資料在5G物聯網系統傳送途徑，確認竊取敏感性資料可能發生的節點，這些節點可能是資料收集點、處理點、傳送點或儲存點。 • TM 05：檢視資料完整性及組態保護機制，確保發生資料被竄改時能有效處理 • TM 06：即使資料已經被安全地傳輸（如SSL/TLS），也須檢視是否存在中間人（Man-in-the middle）攻擊的可能性	完整性 (I)
否認性 **Repudiation**	• TM 07：檢視5G物聯網系統提供或產生資料的節點，可能是各種感知設備。確保資料是可以追溯到確實是合法感知設備所產生且沒經過修改 • TM 08：檢視5G物聯網是否存在攻擊者可以注入一個產生偽資料之節點的可能性，這些偽資料上傳後可能導致5G物聯網系統非正常運作 • TM 09：確保攻擊者不會誤用5G物聯網系統功能，例如關閉可能違法使用的情境	不可否認性
資訊洩漏 **Information Disclosure**	• TM 10：檢視5G物聯網系統資料傳送路徑，包含後端處理系統，確保處理敏感性資料的設備有識別管控及適當的資料加密機制 • TM 11：確保5G物聯網系統資料儲存節點內的資料有加密（Data-at-Rest）管控 • TM 12：檢視5G物聯網系統內有價值設備被竊取的風險並考慮金鑰歸零（Key Zeroization） • TM 13：系統網路資訊洩漏，如通訊埠開啟狀態、使用的通訊協定、使用的服務種類。 • TM 14：資訊損害包含機敏性資料外洩，私密通訊遭未經授權第三方攔截取得，如Email、電話、即時通訊等。	機密性 (C)
阻斷服務 **Denial of service, DoS**	• TM 15：針對5G物聯網系統的每個應用目標進行檢視是否有確保持續運作的規劃 • TM 16：檢視每個5G物聯網節點的設計容量是否能有效承受DoS攻擊 • TM 17：檢查5G物聯網系統資料結構、變數及API，以防止漏洞存在導致攻擊者利用偽節點占滿合法節點的傳輸容量	可用性 (A)
權限提升 **Elevation of Privilege**	• TM 18：檢視5G物聯網系統每個設備的管理能力，是否有區分管理者與一般使用者的權限 • TM 19：檢視帳號認證（Authentication）機制是否存在漏洞 • TM 20：設備軟韌體存在漏洞或使用弱密碼遭攻擊者利用	授權

威脅建模

威脅紀錄表參考範例

威脅編號	**Threat 01**
STRIDE威脅類型	權限提高（Elevation of Privilege）
威脅模型	TM 18：檢視5G物聯網系統每個設備的管理能力，是否有區分管理者與一般使用者的權限
威脅目標	利用系統存在的漏洞或弱點取得智慧應用場域後端管理系統管理者權限
可能的攻擊技術	① 暴力破解帳號密碼 ② 網頁介面注入攻擊 ③ 利用漏洞讓一般用戶登入取得管理者權限
潛在的衝擊情境	① 入侵管理系統修改計費系統 ② 入侵管理系統中斷系統運作 ③ 入侵管理系統取得客戶資訊

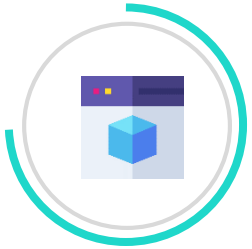
漏洞檢測(Vulnerability Testing, VT)

8項安全政策 **46**安全控制項目

- 確認物聯網場域可能存在的威脅後，利用8項安全政策及46個安全控制項目進行查核，並檢測場域軟硬體是否存在重大漏洞或弱點，做為滲透測試之依據。
- 漏洞檢測程序含「安全控制項目」查核及「設備漏洞/弱點檢測」。安全等級L1~L3係為確保物聯網場域可達到一定安全之要求。檢測內容包括設備韌體檔案安全測試、軟/韌體更新機制測試、惡意程式測試、弱點掃描、模糊測試(選用)、資料傳輸加密檢測及動態分析(選用)等。

初始化安全及隱私設定

系統收集/處理/儲存可識別使用者的相關資料應遵守個資規定、物聯網場域所有的系統預設值初始化設定可被改變等。(L1:2/L2:5/L3:7)



安全軟體及韌體更新機制

軟韌體應具備更新機制、設備軟韌體更新檔具加密機制，更新前驗證正確性及完整性、確保設備軟韌體更新完後保持原有的全部設定等。 (L1, L2:4/L3:6)

通行碼及加密機制

通行碼管理策略、使用加密演算法以保護資料與資訊的機密性及完整性、採用國際認可之加密演算法並關閉不安全的協定等。 (L1:2/L2/L3:5)

軟體及功能安全

與安控相關的服務應提供手動操作的替代方式、提供文件給使用者，讓其知道相關風險、允許使用者啟用非預設以外之功能等。 (L1:1/L2:2/L3:5)

授權機制

以最小許可權原則(Principle of least privilege，POLP)為考量、應確保設備敏感性資料之存放、交換應有保護機制，避免在非授權情況下被輕易存取等。 (L1~L3:2)

鑑別機制

機敏資訊服務存取或改變應通過身分驗證，日誌與錯誤訊息內的敏感性資料應鑑別存取，避免關鍵除錯資訊或通行碼外洩等 (L1:2/L2:3/L3:5)

安全的通訊方式

設備通訊傳輸須能抵抗重送與中間人攻擊、遠端存取連接應加密鑑別機制、通訊連接須使用國際公認標準安全的協定，並防止降等攻擊等。 (L1:5/L2~L3:6)

程序與文件要求

雲端、網頁、系統等弱點掃描不得有已知的重大風險及高風險漏洞、紀錄所有使用之協定、紀錄系統所使用之服務、提供產品使用手冊 (L1:4/L2:7/L3:10)

漏洞檢測

安全控制項目(僅列出L1項目)

安全政策	L1 安全控制項目基準
初始化安全及隱私設定 (2)	① SC03 系統收集/處理/儲存可識別使用者的相關資料應可供使用者審閱，且具有同意/不同意之選項。 ② SC06 確保物聯網場域所有的系統預設值(如通行碼、憑證、加密金鑰)都應於初始化設定時被改變。
安全軟體及韌體更新機制 (4)	① SC08 軟韌體應具備更新機制，且必須使用可用的網路或無線介面來支援軟韌體更新。 ② SC09 應預設開啟軟韌體自動更新，或更新提醒機制。 ③ SC10 應確保設備軟韌體更新檔具加密機制，並於更新前驗證正確性及完整性檢查。 ④ SC11 應確保設備軟韌體更新完後應保持原有的全部設定，若無法完成軟韌體更新程序，軟韌體應可還原至前一版本或提供更新過程失敗訊息。若已成功完成軟韌體更新，則禁止還原回較舊版本。
通行碼及加密機制 (2)	① SC14 應執行通行碼管理策略，具備8碼以上長度，且包含大小寫字母、特殊符號、數字。 ② SC15 應確保適當且有效率的使用加密演算法以保護資料與資訊在儲存或傳送過程的機密性、真實性及完整性。應選擇適當的標準，採用國際認可之加密演算法並關閉不安全的協定。
軟體及功能安全 (1)	① SC21 與安控相關的服務應提供手動操作的替代方式。 例如由門鎖執行的服務，此類系統需要提供可能因惡意軟體，電源不足等方式造成的安控問題，故應提供一種手動操作的替代方式。例如：電子門鎖，應該提供實體鑰匙用於鎖定和解鎖的手動方法。
授權機制 (2)	① SC24 應提供文件呈現確保設備之預設授權僅給予一般所需的功能操作即可，以最小許可權原則(Principle of least privilege，POLP)為考量，包含設備所開啟的通訊埠。 ② SC25 應確保設備敏感性資料之存放、交換應有保護機制，避免在非授權情況下被輕易存取。
鑑別機制 (2)	① SC27 任何機敏資訊的(由製造商提供清單)服務存取或改變前應先通過身分驗證才可做相對應的操作存取或改變。 ② SC30 日誌與錯誤訊息內的敏感性資料，應在鑑別的基礎上才可存取，避免關鍵除錯資訊或通行碼等資訊外洩。
安全的通訊方式 (5)	① SC31 設備通訊傳輸必須能抵抗重送與中間人攻擊。 ② SC32 設備若有Wi-Fi連線，須支援預設為業界可接受安全設定，且不會遭受降階攻擊。例如：WPA2機制降為WEP。 ③ SC33 遠端存取連接應實施加密鑑別機制。 ④ SC34 安全協定應防止降等攻擊(downgrade attack)。 ⑤ SC35 通訊連接必須使用使用國際公認標準安全的協定，確保通訊傳輸的安全。
程序與文件要求 (4)	① SC39 應針對雲端環境、網頁、系統等進行弱點掃描並整理相關報告，不得存有已知的重大風險及高風險漏洞，或除有其它緩解措施。 ② SC41 應提供文件，紀錄系統所使用之協定，系統所使用到的任何協定都可能遭受攻擊，故必須紀錄所有使用之協定。 ③ SC42應提供文件、紀錄系統所使用之服務，啟用服務的理由是重要的，可用於了解系統的安全狀態，並確保採取足夠的安全措施來保護這些介面 ④ SC43 應提供產品安裝、使用手冊。

漏洞檢測

漏洞檢測

項次	說明
設備韌體檔案安全測試	① VT01 使用韌體拆解與分析功能工具對未加密韌體進行檔案拆解，驗證韌體是否存在高風險弱點。 ② VT02 驗證未加密韌體更新檔是否會洩露敏感性資料。
軟/韌體更新機制測試	① VT03 確認設備更新軟/韌體機制，及軟/韌體更新失敗是否可還原至前一版本或提供更新過程失敗訊息。若已成功完成軟/韌體更新，則是否禁止還原回較舊版本。
惡意程式測試	① VT04 使用通過資安測試機構(AV-Comparatives)認可之防毒軟體掃描，確認拆解後韌體檔案中是否存在已知惡意程式。
模糊測試(選用)	① VT08 使用模糊測試工具，進行通訊協定的異常輸入或非預期輸入測試，評估設備是否存在軟體缺陷或資安弱點，該測試項目依送測單位自行決定是否測試。
資料傳輸加密檢測	① VT09 使用安全通道檢測工具或側錄網路封包檢測是否採用安全傳輸通道。
動態分析 (選用)	① VT10 使用動態分析測試工具分析設備連網狀態的網路封包，檢視評估有無傳輸資料至可疑網站或 IP 位址，該測試項目依送測單位自行決定是否測試。

漏洞檢測

弱點掃描

項次	說明
弱點掃描	① VT05 使用具系統漏洞與設定評估、網路服務埠與網站弱點掃描功能工具，對設備進行弱點掃描，評估是否存已知 CVE 漏洞，且應不可存有 CVSS 為重大風險、高風險等級公開漏洞、網頁部分則應不可存有 Injection、Cross-Site Scripting(XSS)及緩衝區溢位(Buffer Overflow)等常見之資安攻擊風險，Level 3 應無任何已知公開漏洞。 ② VT06 使用網路服務埠掃描工具，確認設備是否存在預期以外的服務埠。 ③ VT07 針對原始碼進行靜態分析，評估是否存有安全風險。



- 本指引採用 NIST NVD(National Vulnerability Database)之通用漏洞評分系統，用於評估資產設備漏洞。
- CVSS 得分基於一系列維度上的測量結果，這些測量維度被稱為量度(Metrics)。漏洞的最終得分最大為 10，最小為 0。得分 7~10 的漏洞通常被認為比較嚴重，得分在 4~6.9 之間的為中級漏洞，0~3.9 的則是低級漏洞。
- 本評分依CVSS v3為主，如無CVSS v3 評分則以該漏洞當下CVSS版評分(如CVSS v2)或最新CVSS版評分為主。

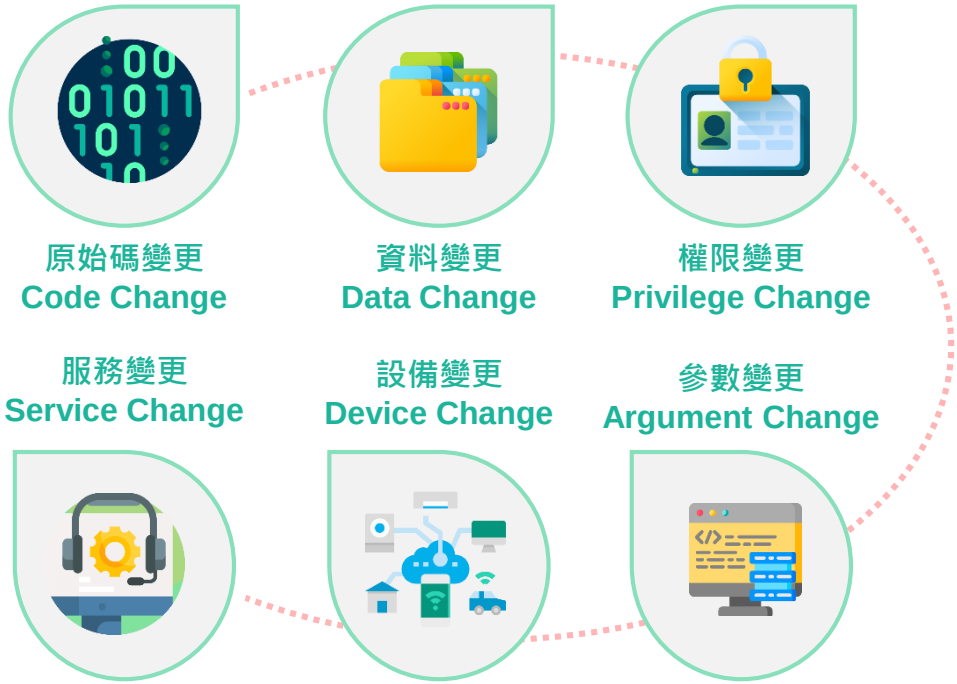
圖片來源 https://nvd.nist.gov/

漏洞嚴重性評定量表

項次	說明
0.0	無
0.1 - 3.9	低
4.0 - 6.9	中
7.0 - 8.9	高
9.0 - 10.0	嚴重

滲透測試(Penetration Testing, PT)

- 場域滲透測試與傳統資訊領域針對單一系統不同，著重於廣度並找出重大危害弱點為目標。
- 針對已經發現之威脅途徑與或各項漏洞與弱點，評估其對於使用者、場域、服務商之衝擊影響。滲透測試結果應含以下項目：
  - ① **不可被輕易利用之漏洞**
  - ② **不可被提升權限之漏洞**
  - ③ **不可被阻斷式服務攻擊之漏洞**
  - ④ **不可被繞過鑑別及授權之漏洞**
  - ⑤ **軟/韌體及通訊不可被降級之漏洞**
  - ⑥ **不可規避任何安全控制之漏洞**
  - ⑦ **不可獲得任敏感性資料之漏洞**
- 針對場域應用層、網路層、感測設備層滲透測試的衝擊種類包括原始碼、參數、資料、權限、服務、設備等變更，其滲透情境共有15種類型，詳閱物聯網場域資安防護評估指引。



滲透測試

滲透測試情境列表

項次	說明
應用層 (6)	① IS01作業系統、應用程式、韌體及硬體的變更而造成資訊安全威脅。[Code Change] ② IS02指令參數、作業系統參數、軟體及硬體的改變而造成惡意活動。[Argument Change] ③ IS03實驗數據、研究成果、組織或個人識別資料、圖片及研究成果等資料外洩，甚至資料遭竄改。[Data Change] ④ IS04系統權限變更，造成受害設備淪為殭屍電腦，可隨時按照攻擊者的命令與控制(C&C)進行非預期操作行為。[Privilege Change] ⑤ IS05服務異常或中斷，在物聯網場域環境中，無法提供正常服務的狀態。[Service Change] ⑥ IS06硬體裝置毀損，物聯網場域架構中之硬體裝置遭受直接或間接實體損壞，導致硬體裝置無法正常運作。[Device Change]
網路層 (4)	① IS07閘道器上的作業系統、應用程式、韌體及硬體的改變而造成資訊安全威脅。[Code Change] ② IS08利用封包截取竄改，造成機敏資料外洩或遭偽冒。[Data Change] ③ IS09系統權限改變，可開啟對外非預期網路傳輸服務(Tunnel)，可隨時按照攻擊者的命令與控制(C&C)進行非預期操作行為。[Privilege Change] ④ IS10在物聯網場域環境中，網路連線服務異常或中斷，造成服務被更改或無法提供正常服務的狀態。[Service Change]
感測設備層 (5)	① IS11感測設備上的應用程式、韌體及硬體遭到竄改而造成資訊安全威脅。[Code Change] ② IS12遠端維運感測設備之指令參數與管理應用程式參數遭竄改。[Argument Change] ③ IS13感測裝置上的資料，包括溫度、空氣汙染等物聯網裝置上之資料遭竊取。[Data Change] ④ IS14感測設備最高權限遭到變更， 造成淪為殭屍設備進而發動分散式阻斷服務攻擊(Distributed Denial-of-Service , DDoS)或報到中繼站等。[Privilege Change] ⑤ IS15感測設備裝置毀損、實體位置異動造成服務異常或中斷，在物聯網場域環境中，無法提供正常服務與運作的狀態。[Device Change]

衝擊分析(Impact Analysis, IA)

- 依據滲透測試結果進行衝擊分析，採用 DREAD及 OCTAVE Allegro 兩種不同面向之風險評估模型進行衝擊分析。分析結果可提供相關利益關係人制定資安應變計畫參考之依據。

DREAD威脅模型評估及風險值給分參考

評估風險係數的演算法模型，對這5個維度針對每個威脅進行等級評估。5個維度的平均值即為該威脅風險值，風險值越大，表示威脅風險越高

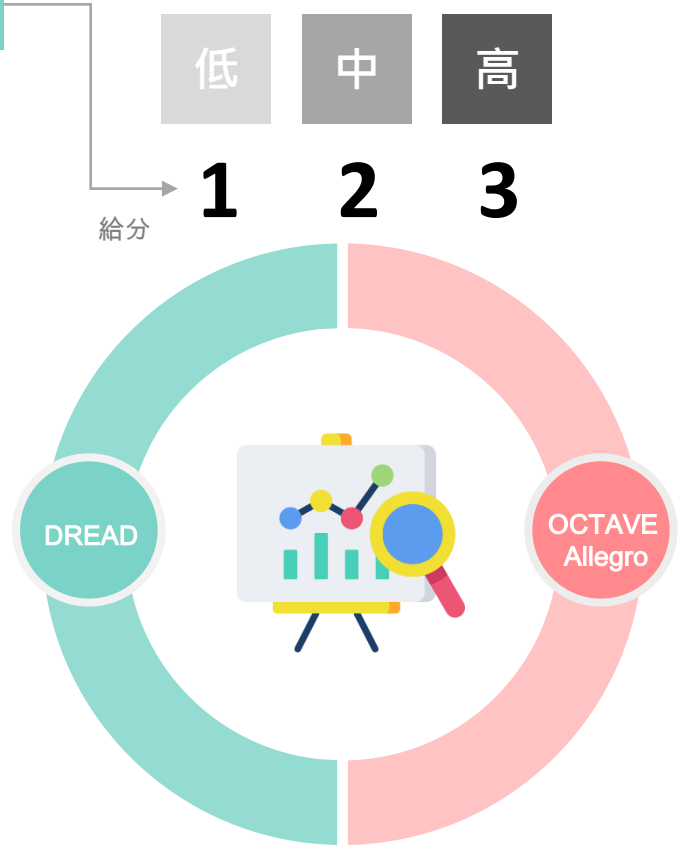
D **Damage Potential 潛在破壞性**
如果這個"漏洞風險被攻擊者利用"進行攻擊，會對企業和組織造成多少破壞

R **Reproducibility 重現難度**
要重現這個漏洞攻擊的難度有多大

E **Exploitability 可利用性**
要發動這個攻擊需要哪些條件

A **Affected Users 受影響用戶**
有多少用戶會遭受到這個風險漏洞的影響

D **Discoverability 發現難度**
對於攻擊者來說，要發現這個漏洞的難度有多大



OCTAVE Allegro影響程度評估準則

偏重於威脅發生造成使用者各種層面的影響評估。各維度的影響程度區分低(Low)、中(Moderate)、高(High)三級。

Reputation and Customer Confidence 聲譽及客戶信心
非商業用戶商譽受影響，商譽回復費用為0或低於或高於1萬美金；商業用戶回復費用為0或低於或高於10萬美金，且流失率低於 5 %或5-10%或10%上者

Financial Loss 財物損失
非商業用戶增加的年維運費用及一次性財務損失；商業用戶的年營收損失

Productivity 生產力
商業用戶增加人力成本低於5萬美金、介於5~10萬美金或高於10萬美金

Life Safety and Health 生命安全與健康
對於使用者生命、健康及安全性等影響程度

Fine and Legal Penalty 罰金與法律懲罰
罰金、無法律訴訟或訴訟損失及是否須接受政府部分或其他調查單位查詢等影響

標章等級及核發要求

- L1：針對應用層、網路層及感測設備層所包含設備之一般性安全功能的資安要求和測試評估。
- L2：包含L1所需評估和測試要求外，另有供應商設備軟體安全設計和風險評估其他補充要求。
- L3：包括L1和L2評估和測試要求以及供應商安全管理作為的其他補充要求。並透過供應商的內部安全控制作為和實踐規劃來評估設備的持續性安全能力，以支持應用層、網路層及感測設備層所包含設備之安全的生命週期。

	標章樣式	核發要求
L1	System-level IoT Security Evaluation	① 安全控制項目須符合L1基準安全等級 ② DREAD風險評估判定為不存在高風險 ③ OCTAVE風險評估判定為不存在高度影響
L2	System-level IoT Security Evaluation	① 安全控制項目須符合L2基準安全等級 ② DREAD風險評估判定為不存在中風險 ③ OCTAVE風險評估判定為不存在高度影響
L3	System-level IoT Security Evaluation	① 安全控制項目須符合L3基準安全等級 ② DREAD風險評估判定為不存在中風險 ③ OCTAVE風險評估判定為不存在高度影響

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

THANK YOU

資安組 王慶豐
pippen.wang@ttc.org.tw