台灣電力公司

太陽光電系統資安風險評估機制之建立與應用

台電綜研所 資通室
林呈鴻

2022年11月11日

TPRI

報告大綱

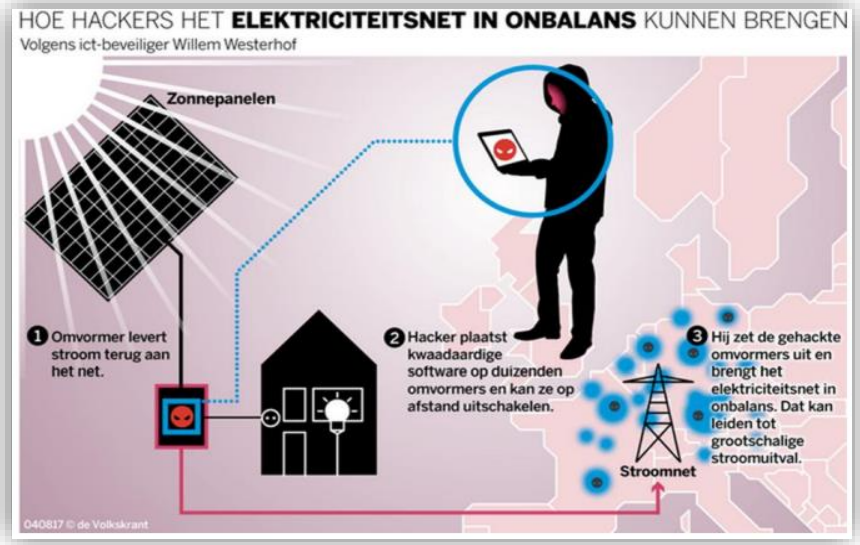

壹 太陽光電系統資安議題
貳 PV資安相關國際標準規範
參 PV案場資安風險評估
肆 太陽光電變流器資安檢測
伍 結論與建議

壹

太陽光電系統資安議題

太陽光電系統資安議題(1/2)

Mr Westerhof described the vulnerabilities at a security conference in the Netherlands

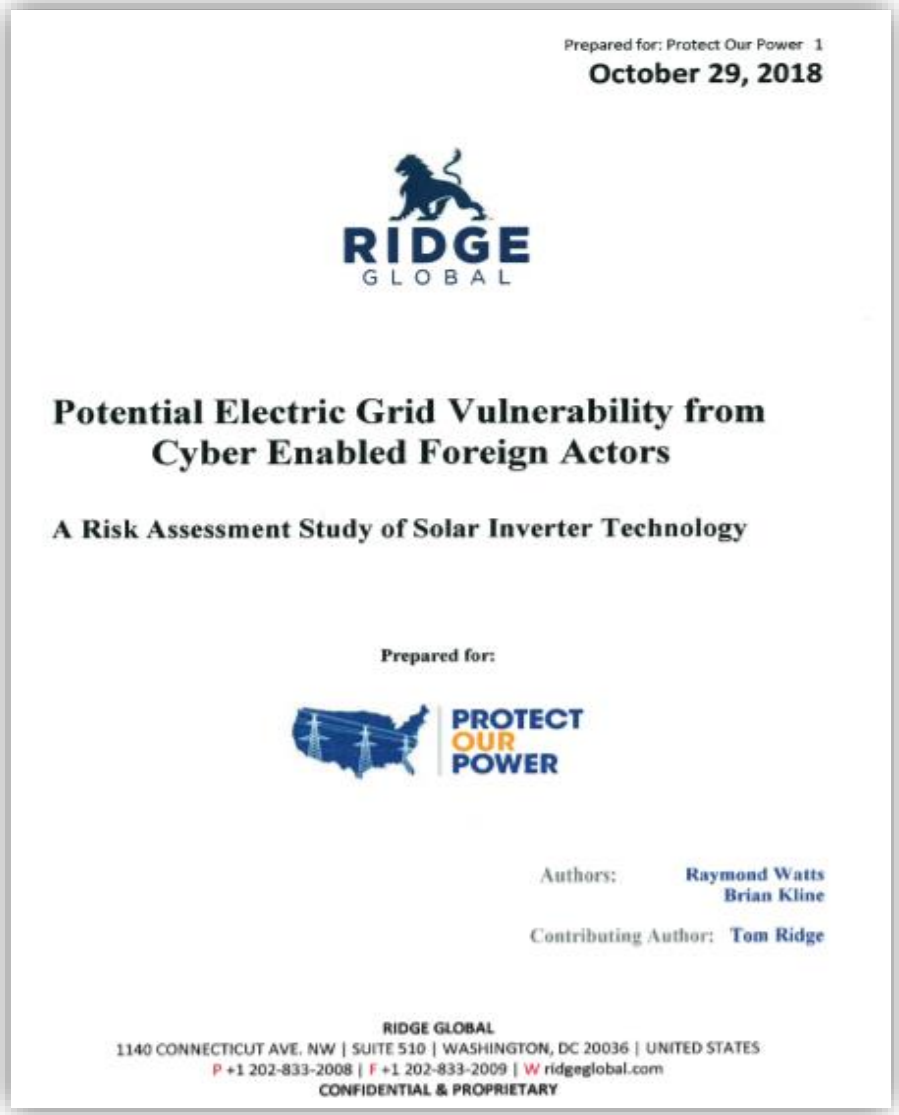


荷魯斯情境(Horus Scenario)

- 2017/8/4荷蘭資安研究人員 Willem Westerhof 公布一項研究成果，指出他在知名的德國太陽能設備供應商SMA Solar的產品上發現21個安全漏洞，將允許駭客危害太陽能電廠的正常運作。
- Westerhof 所發現的漏洞主要位於SMA太陽能面板上的智慧變流器（inverter），用途是將太陽能面板所產生的直流電轉換成交流電。
- 下列則是較為嚴重 CVE，CVSS等級為 HIGH：
  - CVE-2017-9858：以特製封包 SQL Injection，可偵測出設備的登人帳號。
  - CVE-2017-9857：資料傳輸易受中間人攻擊。
  - CVE-2017-9851：應用程式會因接收無意義資料而崩潰。

Source: https://www.bbc.com/news/technology-40861976

太陽光電系統資安議題(2/2)



Prepared for: Protect Our Power 1

October 29, 2018

RIDGE GLOBAL

Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors

A Risk Assessment Study of Solar Inverter Technology

Prepared for:

PROTECT OUR POWER

Authors: Raymond Watts, Brian Kline

Contributing Author: Tom Ridge

RIDGE GLOBAL
1140 CONNECTICUT AVE. NW | SUITE 510 | WASHINGTON, DC 20036 | UNITED STATES
P +1 202-833-2008 | F +1 202-833-2009 | W ridgeglobal.com
CONFIDENTIAL & PROPRIETARY

太陽光電變流器主要安全挑戰

① 目前美國境內的太陽光電變流器皆在**美國境外或是外資公司生產**，例如全球最大的太陽光電變流器製造商是HUAWEI。

② 目前**尚未有一個廠商擁有通用標準**來確保太陽光電變流器之完整性。

③ 太陽光電變流器**線上的管理監控系統**越來越多，容易導致駭客有更多的切入點和利用系統漏洞來控制太陽光電變流器。

④ 若由**帶有惡意的廠商製造**，可以透過製造過程中，將惡意軟體植入於太陽光電變流器的作業系統或韌體中，或是透過修改硬體元件使其可被允許遠端存取。

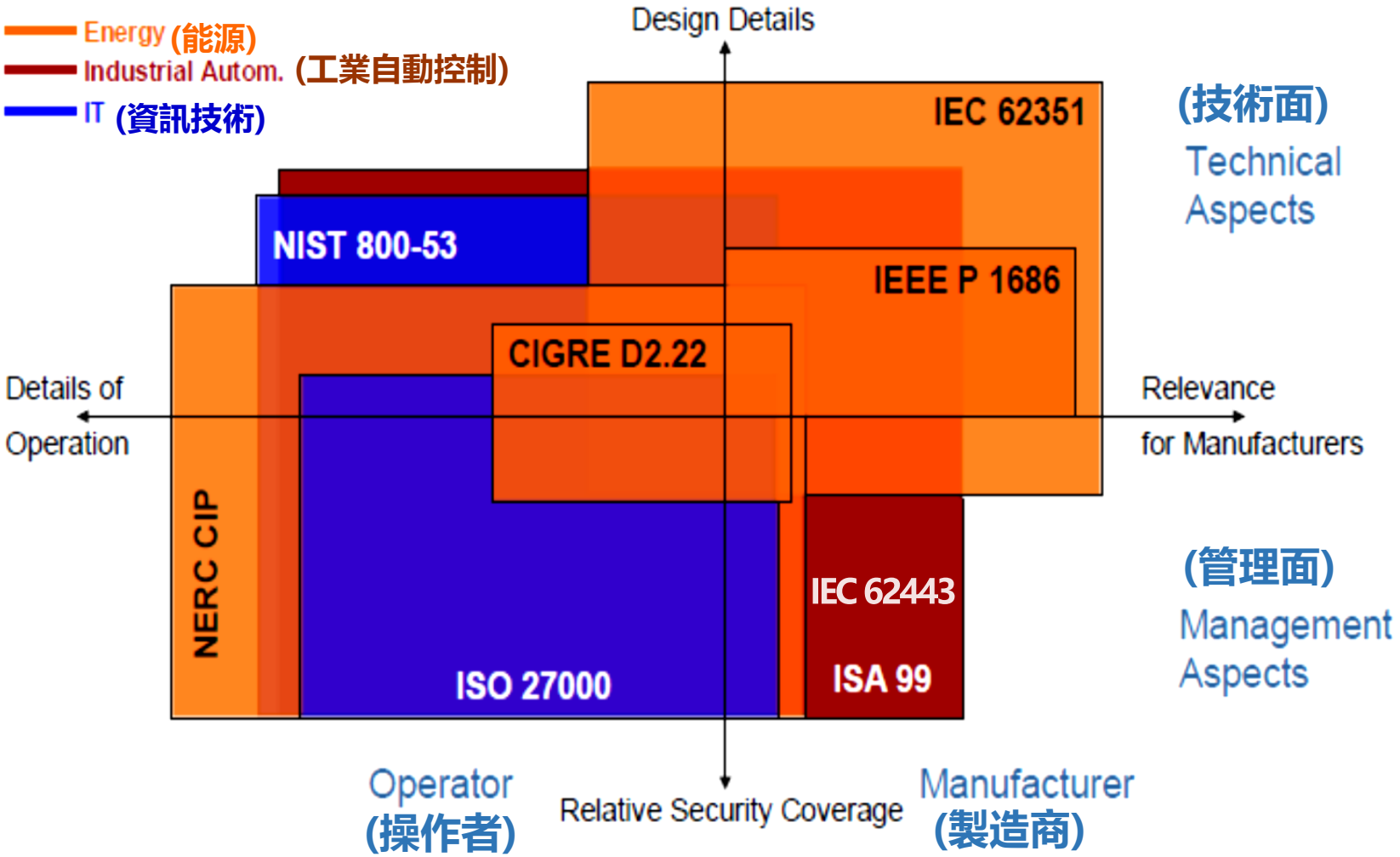
Source: RIDGE GLOBAL

貳

PV資安相關國際標準規範

與PV資安相關之國際標準

- IEC 62351
  電力系統安全
- NERC-CIP
  能源系統操作安全
- ISA99, IEC 62443, NIST SP800-82, NIST SP800-53
  工控系統安全
- ISO 27000, NIST 800-53 IT 環境
  資訊安全

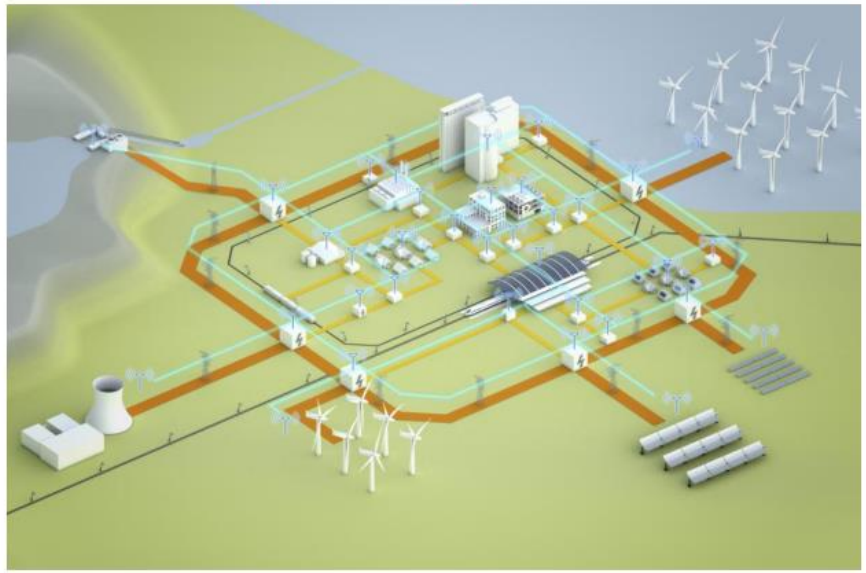


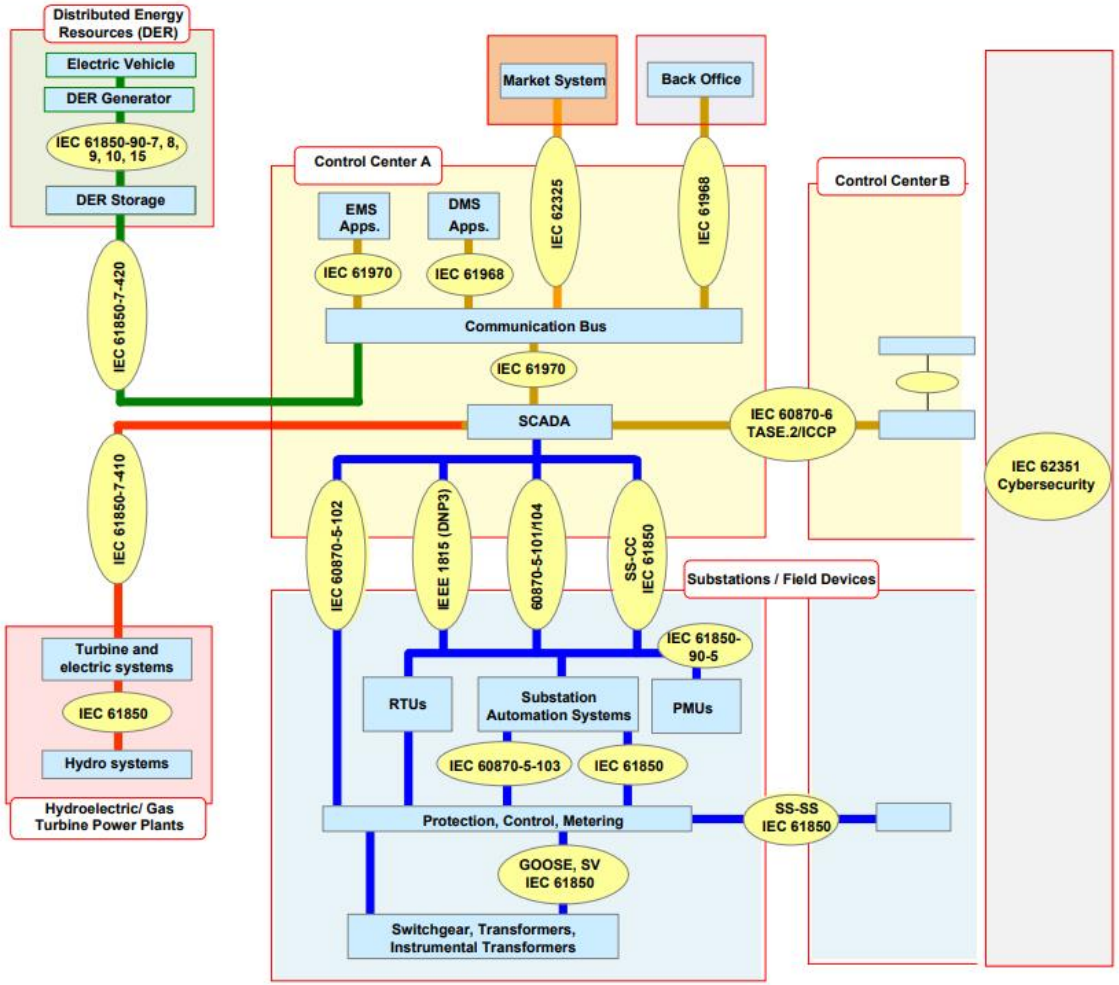
Source: IEC 62351-10

IEC 62351 電力系統資安標準(1/3)

Core communication standards for Digital Grids
IEC TC57 reference architecture with domain-specific cyber security

- **IEC 61970 / 61968** Common Information Model (CIM)
- **IEC 62325** Market Communication using CIM
- **IEC 61850** Substation, Distribution, DER Automation
- **IEC 60870** Telecontrol Protocols (serial/TCP)
- **IEC 62351** Security for Power Systems

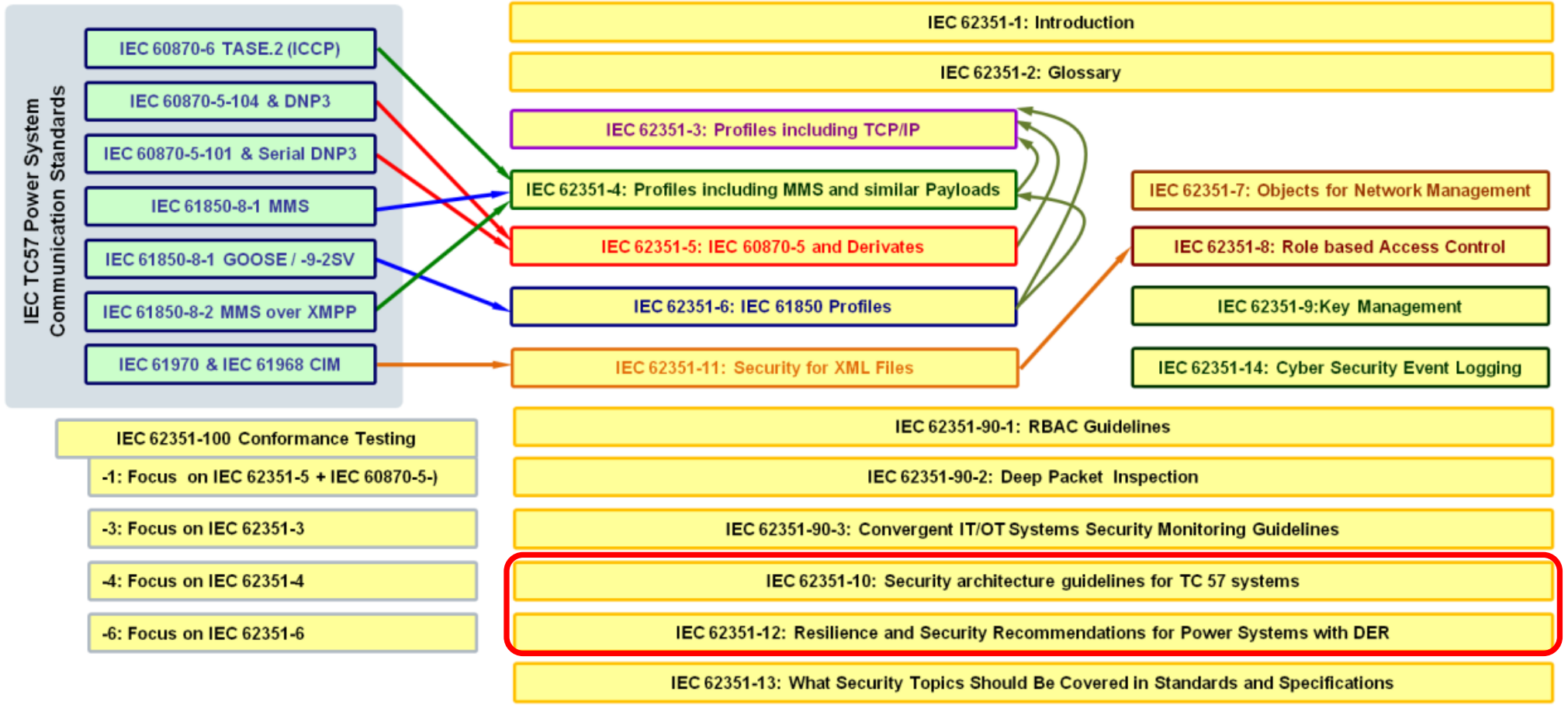




Source: IEC TC57

IEC 62351 電力系統資安標準(2/3)

Cyber security in Digital Grids
IEC 62351 provides technical security measures and guidelines



Source: IEC 62351

IEC 62351 電力系統資安標準(3/3)

風險評估概念

- **資產識別** 何種資產須被保護
- **威脅分析** 何種攻擊須被考量
- **風險估計** 何種潛在損害
- **對策研擬** 技術性/組織性

全面的資安架構，包括**資安管理系統**(建議定期審查)期間應用於目標系統產品定義階段。

風險評估實務

- **發現** 蒐集系統資訊
- **弱點分析** 弱點掃描
- **攻擊驗證** 利用已識別的弱點
- **建議** 可行資安對策

檢測可利用的弱點和透過駭客攻擊潛在的資安弱點。提供當前系統**建置/操作**階段安全性狀態(定期重複)。

共同目標：提高資安等級和對IT相關攻擊的抵抗力

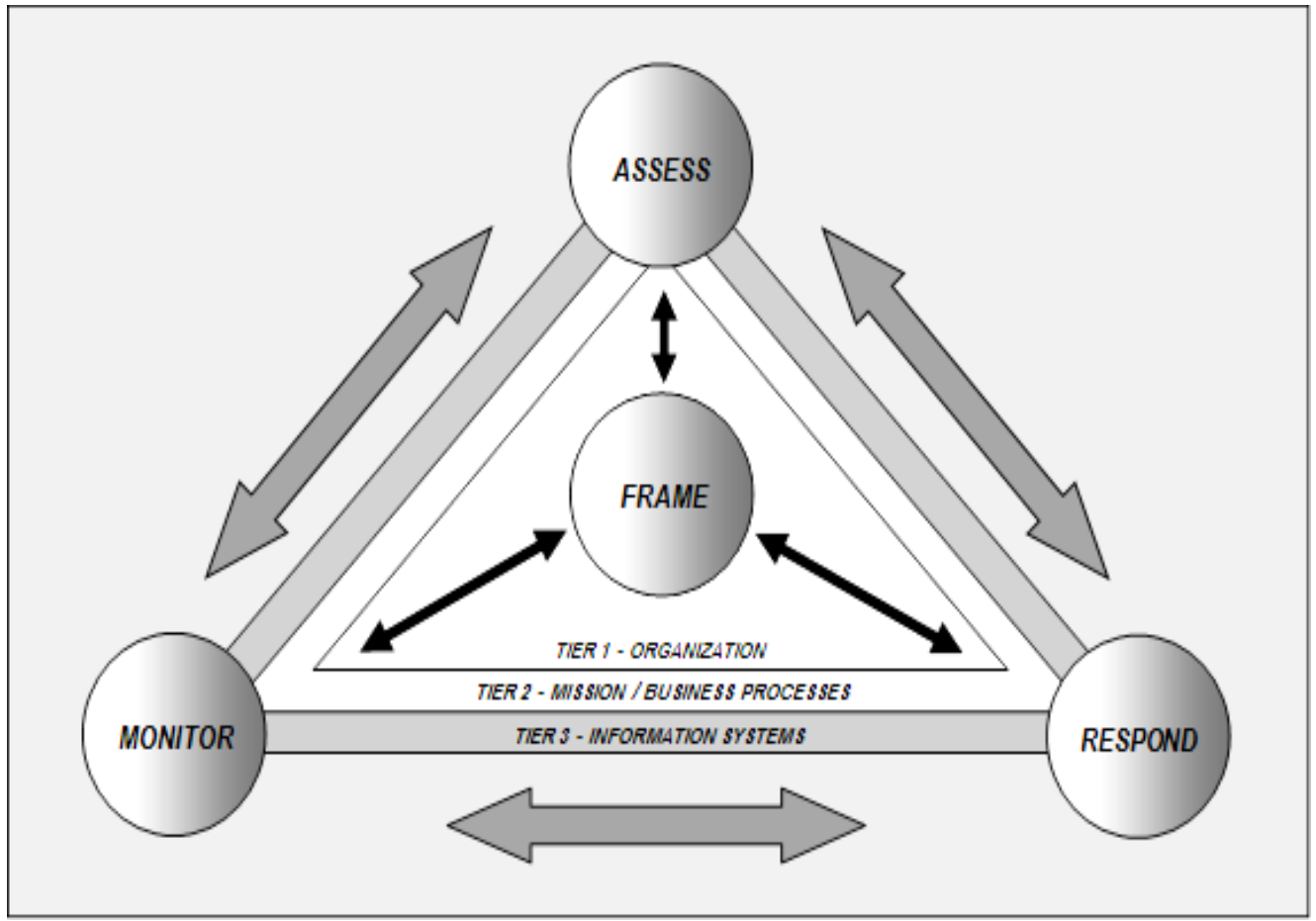
Source: IEC 62351-10

IEC 62443 工控系統資安標準

IACS：Industrial Automation and Control Systems

Source: IEC 62443

NIST SP 800-82 工控系統安全指引



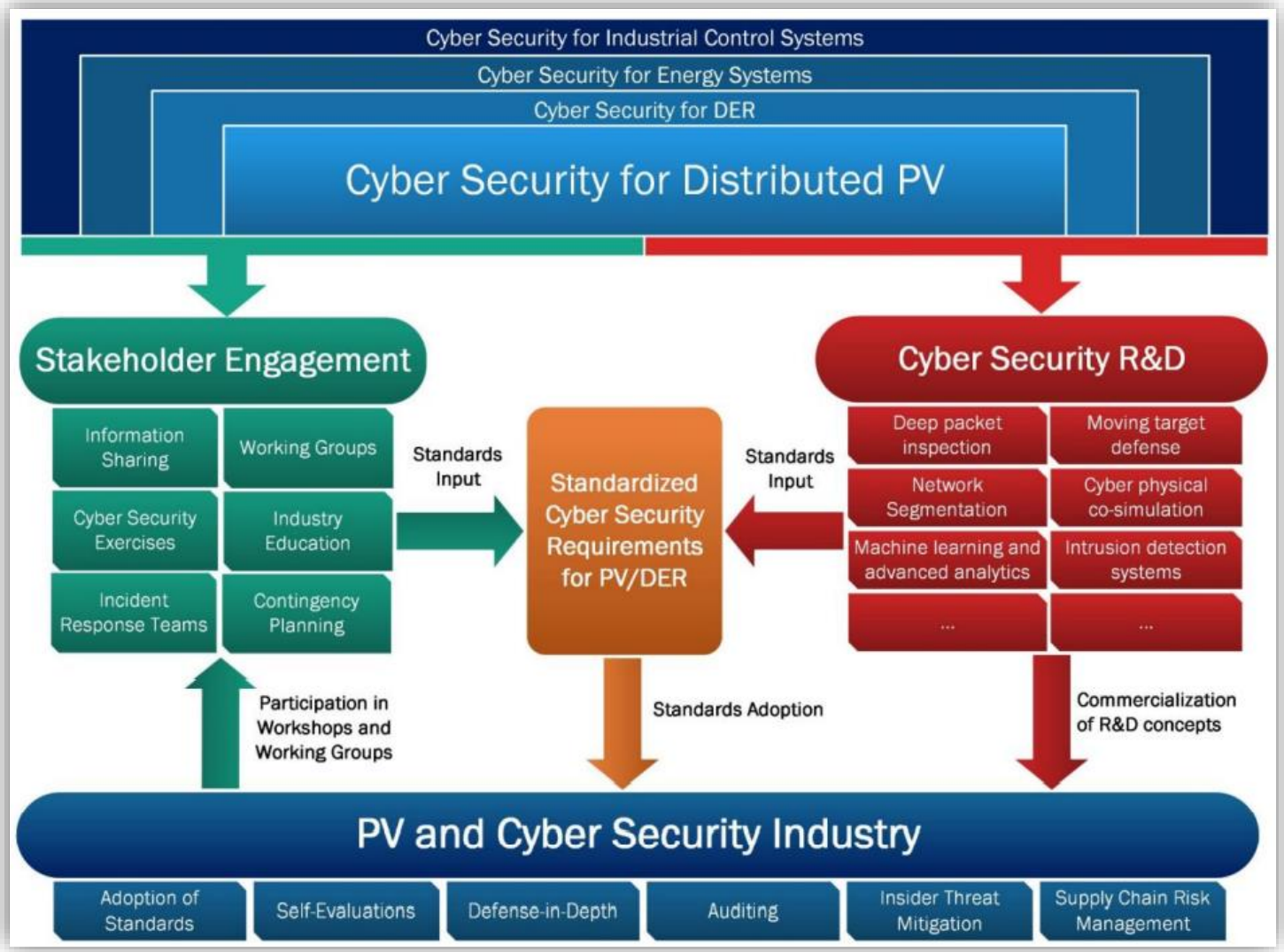
- **NIST SP 800-82 目的為提供工控系統(ICS)安全的指導方針，包含提供 ICS 的概觀和典型系統系統拓撲、識別典型威脅和對這些系統脆弱性提供建議的安全對策以降低相關的風險。**
- **風險管理過程使用三層方法來處理：**
  1. **組織層面的風險**
  2. **任務/業務流程層面**
  3. **資訊系統層面 (IT和ICS)**
- **風險管理過程由四個部分組成：**
  1. **框架 (Frame)**
  2. **評估 (Assess)**
  3. **反應 (Respond)**
  4. **監控 (Monitor)**

Source: NIST SP 800-82 R2

叁

PV 案場資安風險評估

太陽光電系統建立資安標準流程



- 許多再生能源資安相關研究報告，均有將 IEC 62443 工控資安標準納入考量。
- 美國 Sandia 國家實驗室的PV系統資安報告將PV系統視為工控系統的一部分。
- PV系統建立資安標準流程可參考 IEC 62443 標準制定。

Source：Jay Johnson, "Roadmap for Photovoltaic Cyber Security", Dec. 2017.

太陽光電系統資安風險評估機制建立與試行

Phase1

工作項目1

資安國際能源系統相關威脅案例研究

- 國際能源系統
- 太陽光電系統
- 工業控制系統

工作項目2

國際工業控制系統資安風險評估方法

- IEC 62443
- NIST SP 800-82 Rev.2
- United States DOE

Phase2

工作項目3

資安工具導入與引進

- 威脅建模
- 弱點掃描
- 模糊測試

工作項目4

太陽光電案場系統環境現場佈署與分析評估

- 環境勘查與分析評估
- 評估範圍與設備清單
- 差異評估

Phase3

工作項目5

- 威脅建模與弱點識別
- 漏洞檢測
- 滲透測試
- 影響分析

Phase4

工作項目6

建立資安風險評估機制

試行資安風險評估機制

主要研究成果

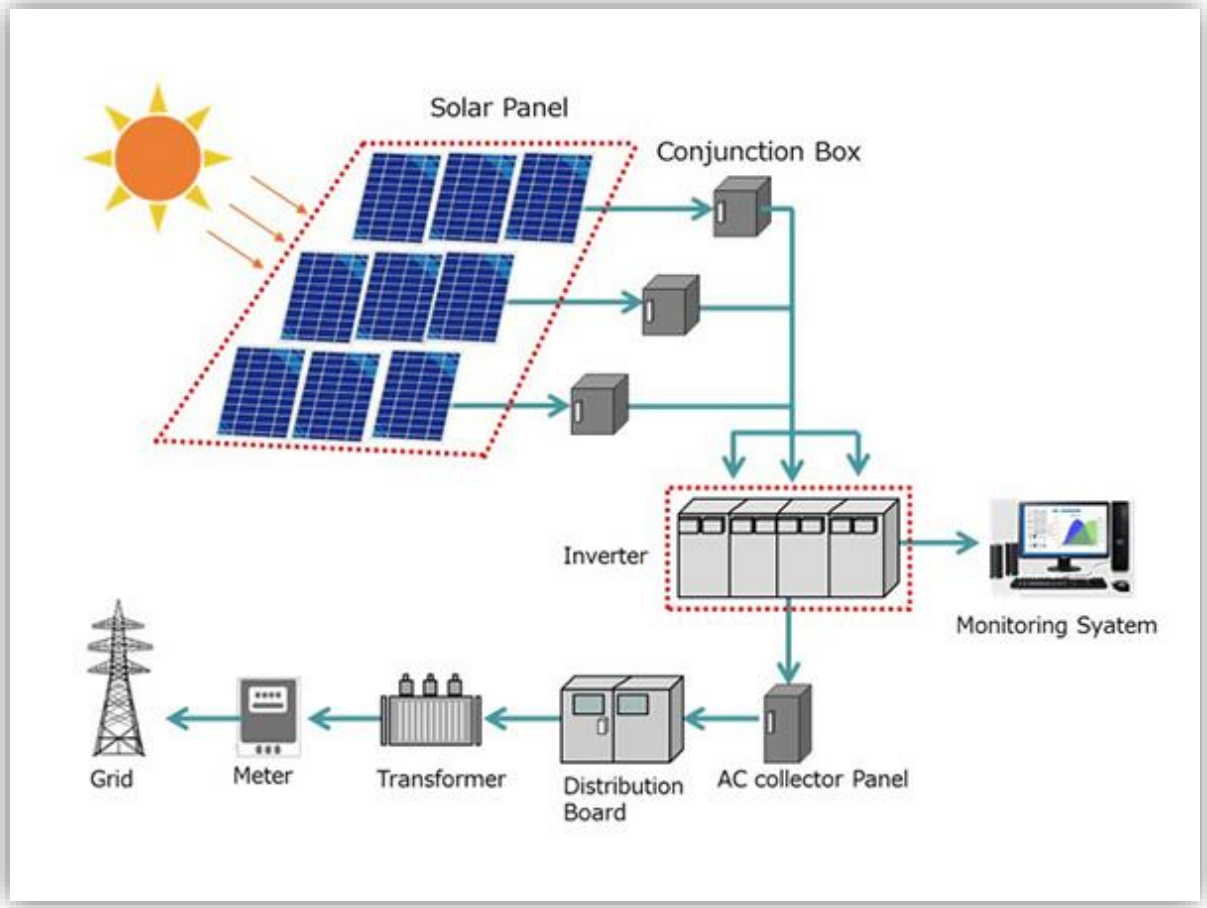
- 產製研究與測試報告
- 協助建立一套太陽光電系統資安風險評估機制
- 建立一套入侵偵測資安監控平台

工作項目7

教育訓練

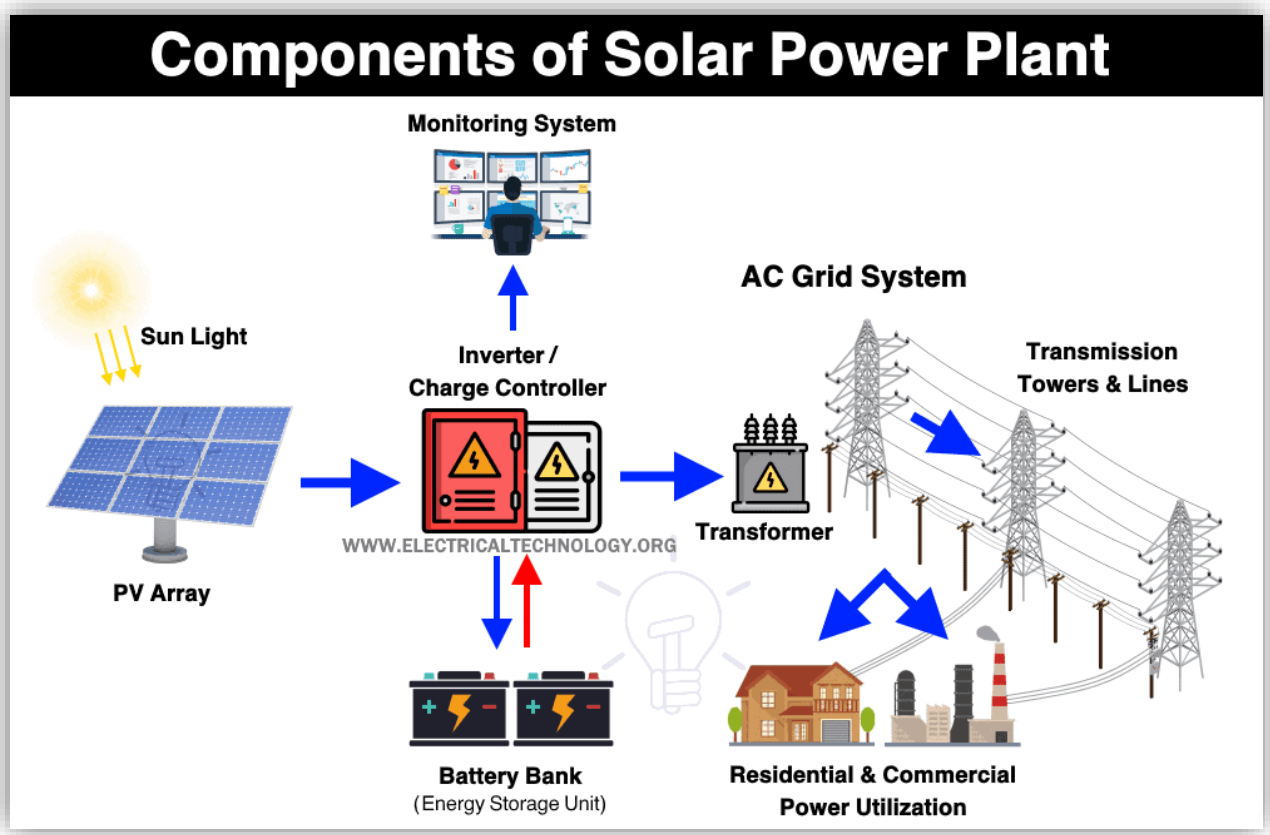
太陽光電案場環境勘查與分析評估

評估確定太陽光電案場整體系統邊界範圍與設備清單



太陽光電系統初始資安風險評估案例

匡列太陽光電案場關鍵設備



評估設備資安等級

PV 案場組件	CIA 資安等級		
	機密性	完整性	可用性
Inverter	低	中	高
PLC	低	低	高
CANopen Box	低	低	低
Metering Box	高	高	高
Monitoring 系統	低	低	高
PV Array	低	低	低

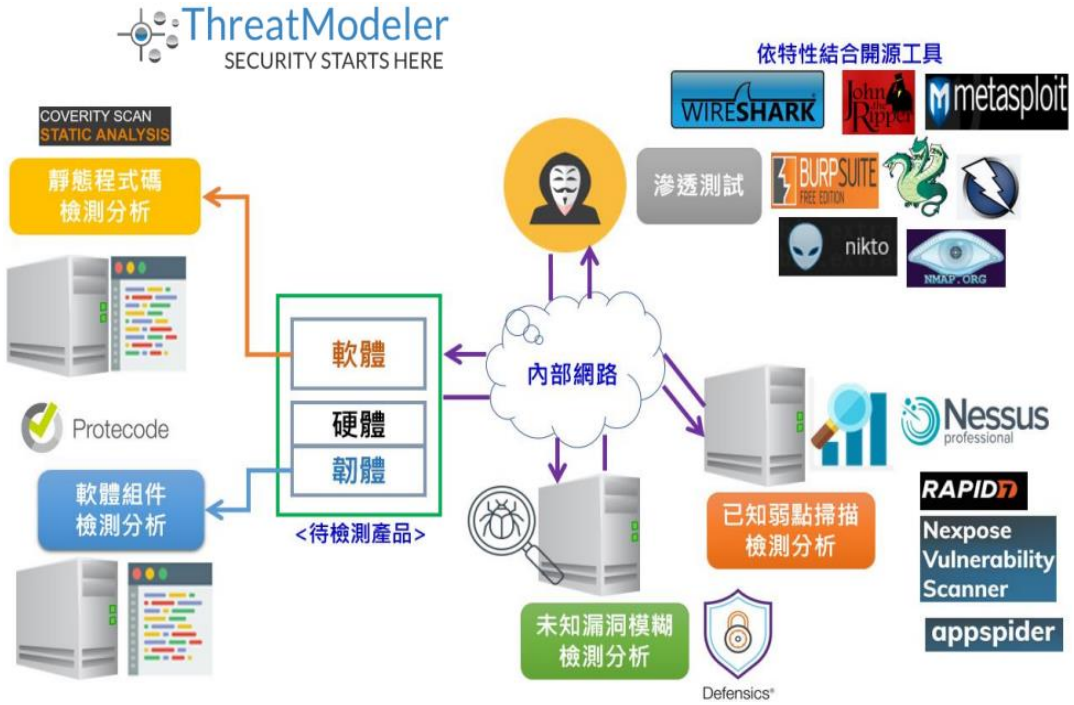
STRIDE 威脅建模與弱點識別

威脅類型	分析說明
身分冒用 Spoofing Identity	1. 檢視此案場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。 2. 檢視設備間建立通訊管道的認證(Authentication)協定是否可能被冒用。 3. 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物聯網系統或洩漏帳密的可能性。
資料竄改 Tampering with Data	1. 檢視資料在此案場系統傳送途徑，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。 2. 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。 3. 如果資料已經被安全地傳輸，也須檢視是否存在中間人(Man-in-the middle)攻擊的可能性。
否認性 Repudiation	1. 檢視此案場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。 2. 檢視此案場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此案場系統非正常運作。 3. 確保攻擊者不會誤用此案場系統功能，例如關閉可能違法使用的情境。
資訊洩漏 Information Disclosure	1. 檢視此案場系統資料傳送路徑，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。 2. 確保此案場系統資料儲存節點內的資料有加密(Data-at-rest)管控。 3. 檢視此案場系統內有價值設備被竊取的風險。
阻斷服務 Denial of service, DoS	1. 針對此案場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。 2. 檢視每個此案場節點的設計容量是否能有效承受DoS攻擊。 3. 檢查此案場系統資料結構、變數及API，以防止漏洞存在導致攻擊者利用偽節點佔滿合法節點的傳輸容量。
特權提升 Elevation of privilege	1. 檢視此案場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。 2. 檢視帳號認證(Authentication)機制是否存在漏洞。

漏洞檢測

利用資安檢測工具和技術人員的測試評估，釐清關鍵資產目前的弱點漏洞，及是否可能被利用成為攻擊的進入點。

1. 確認整體網段的範圍?
2. 確認不同網段之間是否有從實體上或軟體層面上隔開?
3. 確認關鍵資產之軟韌體、作業系統版本等資訊
4. 確認網域內未知主機與連接埠
5. 網域內漏洞掃描和漏洞分析
6. 網頁應用程式弱點檢測與掃描
7. 遠端連線服務，包含SSH、TELNET、RDP等常見遠端連線服務之弱點測試
8. 設定管理、使用者認證、功能測試評估安全設計瑕疵、輸入驗證
9. WPS機制測試評估
10. 機櫃感測鎖Zigbee安全測試評估



太陽光電系統資安風險評估機制試行

- **完成風險評估報告與改善建議**
- **完成建立一套太陽光電系統資安風險評估標準作業程序**

入侵方式	建議事項
實體攻擊	• 加強場區人員進出、資訊設備管控 • 建立、執行資訊系統資安風險評估機制
網路攻擊 (包含:軟體、伺服器、協定、應用程式等)	• 重要節點設置偵測裝置 • 較高風險漏洞，後續建議視場域運作情況進行更新作業 • 定期在場域利用工具執行弱點評估作業，檢視資產和環境現況是否有被更動? 例如：非必要的服務Port • 持續掌握資產設備新弱點漏洞，以利風險追蹤與管控
社交工程	• 門口守衛基本對訪客之盤查和紀錄能力 • 廠商到場任何系統的更新或安裝等作業，需有人員到場陪同及記錄執行作業。嚴防廠商利用工具蒐集到一些場域內的資訊，並將資訊攜帶出去。

- 作業程序
  - 人力資源管理作業程序
  - 資訊存取控制作業程序
  - 資訊資產管理作業程序
  - 資通安全風險評鑑與管理作業程序
  - 實體安全管理作業程序
  - 網路安全管理作業程序
- 作業要點
  - 中央控制室作業要點
  - 資通設備暨媒體管理作業要點
  - 網路安全管理作業要點
  - 網路連接設備建置與管理作業要點
- 表單、紀錄
  - 異動工單
  - SSID清單
  - 人員進出管制表
  - 系統與設備使用者權限列表
  - 場域網路通訊服務清

肆

太陽光電變流器資安檢測

IEC 62443 安全保障認證方案(1/2)

一、設備

嵌入式裝置安全保障(EDSA)
(Embedded Device Securyity Assurance)

- 確認產品可抵抗網路攻擊的強健度，並確認產品未存在已知的資安漏洞
- 主要安全規範：
  - ✓ IEC 62443-4-1
  - ✓ IEC 62443-4-2

二、系統

系統安全保障(SSA)
(System Security Assurance)

- 確認工業控制系統或子系統可抵抗網路攻擊的強健度，且未存在已知的資安漏洞
- 主要安全規範：
  - ✓ IEC 62443-3-3
  - ✓ IEC 62443-4-1
  - ✓ IEC 62443-4-2

三、供應商

開發生命周期安全保障(SDLA)
(Security Development Lifecycle Assurance)

- 確認供應商對產品開發環境、生產程序及生命周期的安全設計
- 主要安全規範：
  - ✓ IEC 62443-4-1

Source： ISASecure®

IEC 62443 安全保障認證方案(2/2)

資安檢測項目，採用 ISCI 認可應用於 IEC 62443 標準驗證的資安檢測工具

Source： ISASecure®

標檢局變流器及監視單元資安檢測技術規範

- 經濟部標檢局於109年12月30日公布「太陽光電變流器及監視單元資安檢測技術規範」，提供相關業者作為產品開發符合資安規範依據，該規範所定的方法與要求，目的在確認太陽光電變流器及監視單元具有基礎資安防護能力，包含(1)實體安全(2)系統安全(3)通訊安全(4)身份鑑別等四個資安構面，以確保產品資訊安全。
- 標檢局將前述資安檢測規範納入VPC檢驗範圍。

安全構面	安全要求分項(僅列出部分)	安全等級			參考標準
		1級	2級	3級	62443-4-2
實體安全	實體防護	V	V	V	CR 3.11
	安全啟動			V	CR 3.14
系統安全	已知弱點偵測(VIT)	V	V	V	EDSA SSA-420
	網頁管理介面安全測試		V	V	EDSA SSA-420
	惡意程式防護			V	CR 3.2
通訊安全	網路裝置資訊探詢功能測試		V	V	CR 3.1
	通訊強健度測試(CRT)	V	V	V	EDSA 401~406
身份鑑別	人員用戶識別與鑑別	V	V	V	CR 1.1
	軟(韌)體更新機制		V	V	CR 1.2
	裝置之識別與鑑別			V	CR 1.2
	通行碼強度(長度基礎)	V	V	V	CR 1.7
	預設通行碼變更機制		V	V	CR 1.5

Source： 經濟部標檢局

VPC：自願性產品驗證(Voluntary Product Certification)，有標示 VPC 標誌的產品，其品質及安全性符合標檢局「自願性產品驗證實施辦法」及相關標準規範之規定。

伍

結論與建議

結論與建議

1 建立綠能資安場域

建立台電公司國內第一個大型綠能資安代表性場域，並可以此成果擴散至其他場域。

2 資安風險評估機制

透過本計畫檢視太陽光電廠場域及關鍵工控系統組成可能的資安威脅現況、控制措施與實施建議，並經由實際案場試行後建立一套可行的資安風險評估機制。

3 確保場域可持續穩定的運作

此資安風險評估機制將有效評估太陽光電廠場域是否存在重大資安威脅，進而依據評估結果提供改善建議。未來可做為太陽光電案場併網要求條件之一，降低資安事件所造成的全國供電不穩定性之風險。

報告完畢
敬請指教