IEC 62443-3-3安全等級
在實際應用中的挑戰與解決方案

Leo KT Chang

Kaichen Huang

PROFILE

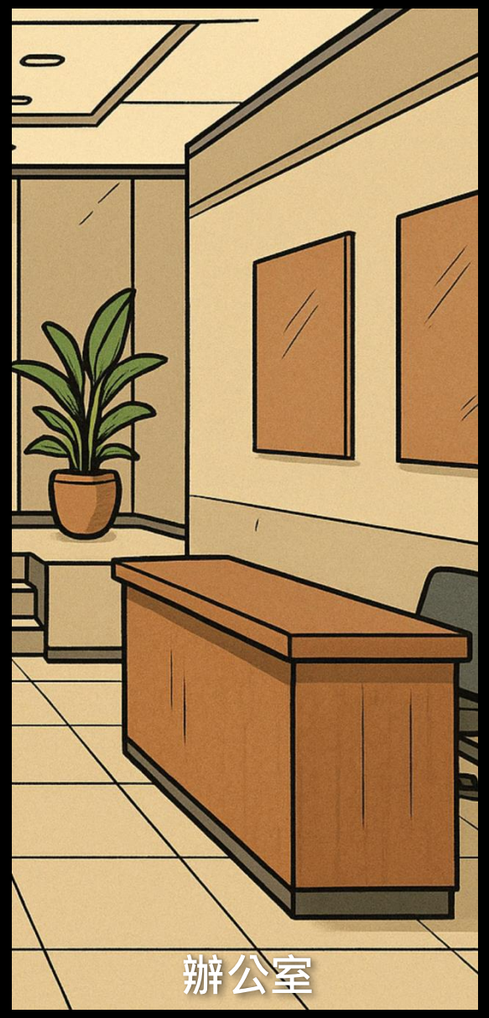
Kaichen Huang
aka Kevin KC Huang

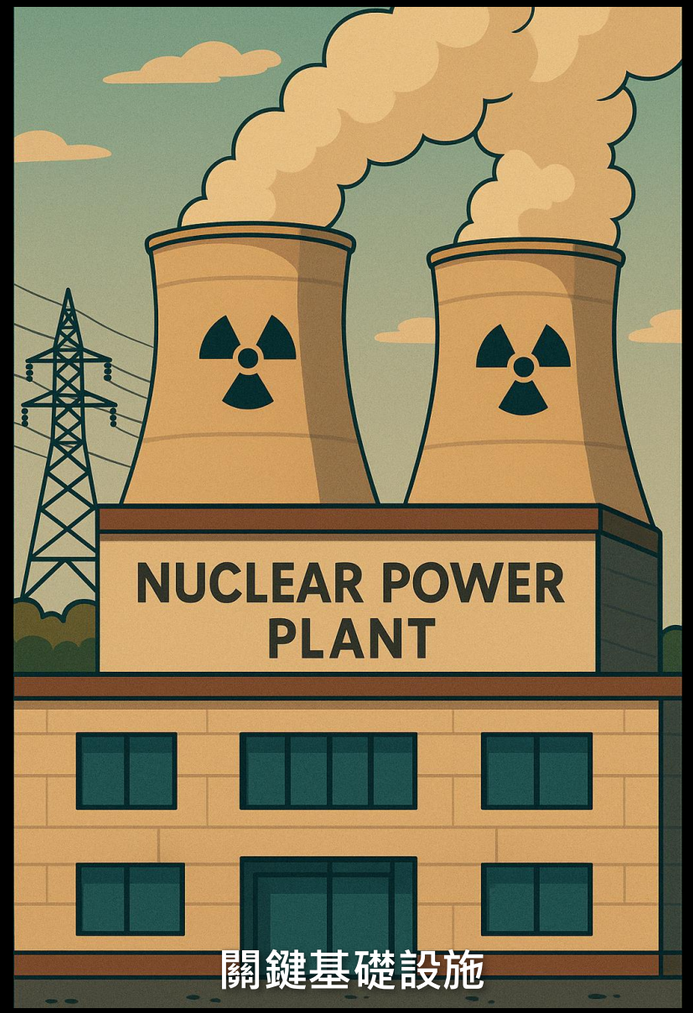
黃凱偵

- **Certification:**
  - ISA/IEC 62443 Expert
  - Certified Information Systems Security Professional (CISSP)

- **Experience:**
  - **工業網路安全路由器 Secure Router 研發**
  - **IEC 61162-460 (Ed.2, 2018) 船籍社 460-Switch / 460-Gateway / 460-Forwarder Type Approval**
  - **IEC 61162-460 (Ed.3, 2024) 船籍社 460-Switch / 460-Gateway / 460-Forwarder Type Approval**
  - **UR E27 (Rev.1, 2023) 船籍社SL2/SP2 Type Approval**
  - **IEC 62443-4-2 SL2 Product Certificate**
  - **RED (EN 18031-1:2024) Product Certificate**
  - **ISA99 JT-62443-3-1**

Impact





Impact低

Impact高

Threat

辦公室

工廠

銀行

關鍵基礎設施

你需要什麼等級的防護？

安全等級	SL-1	SL-2	SL-3	SL-4
防禦目標	意外誤用	簡單故意攻擊	專業目標攻擊	國家級持續性威脅
關鍵措施	基本密碼、權限	身份驗證、角色控制、網絡分隔	集中管理、SIEM、多因素驗證	雙重批准、物理隔離
Cost	$	$$	$$$	$$$$

PROFILE

Leo KT Chang
張凱棠

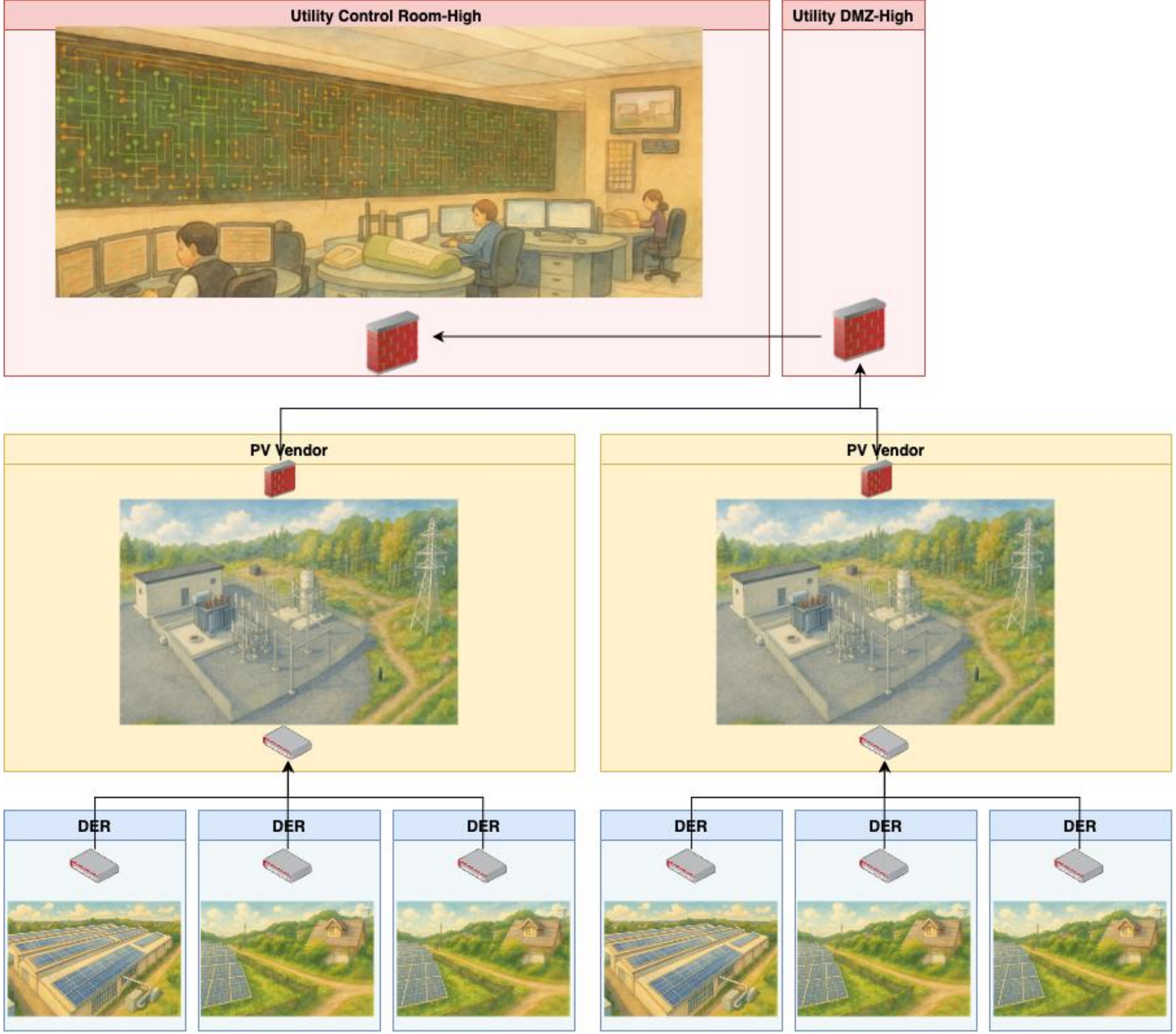
- **Certification:**
  - ISA/IEC 62443 Cybersecurity Expert
  - Certified Information Systems Security Professional (CISSP)
  - Project Management Professional (PMP)
  - PMI Agile Certified Practitioner (PMI-ACP)
  - ISO 27001 LA
  - ISO 27701 LA
  - CEH
- **Experience:**
  - JT-62443-3-2 member
  - ISA 99 WG 16 Incident Management member
  - vPAC Alliance Cybersecurity Spec. Contributor
  - EN 18031-1:2024 – RED compliance

迷思破解

- 安全等級越高越好？
- 如何選擇適當的安全等級？

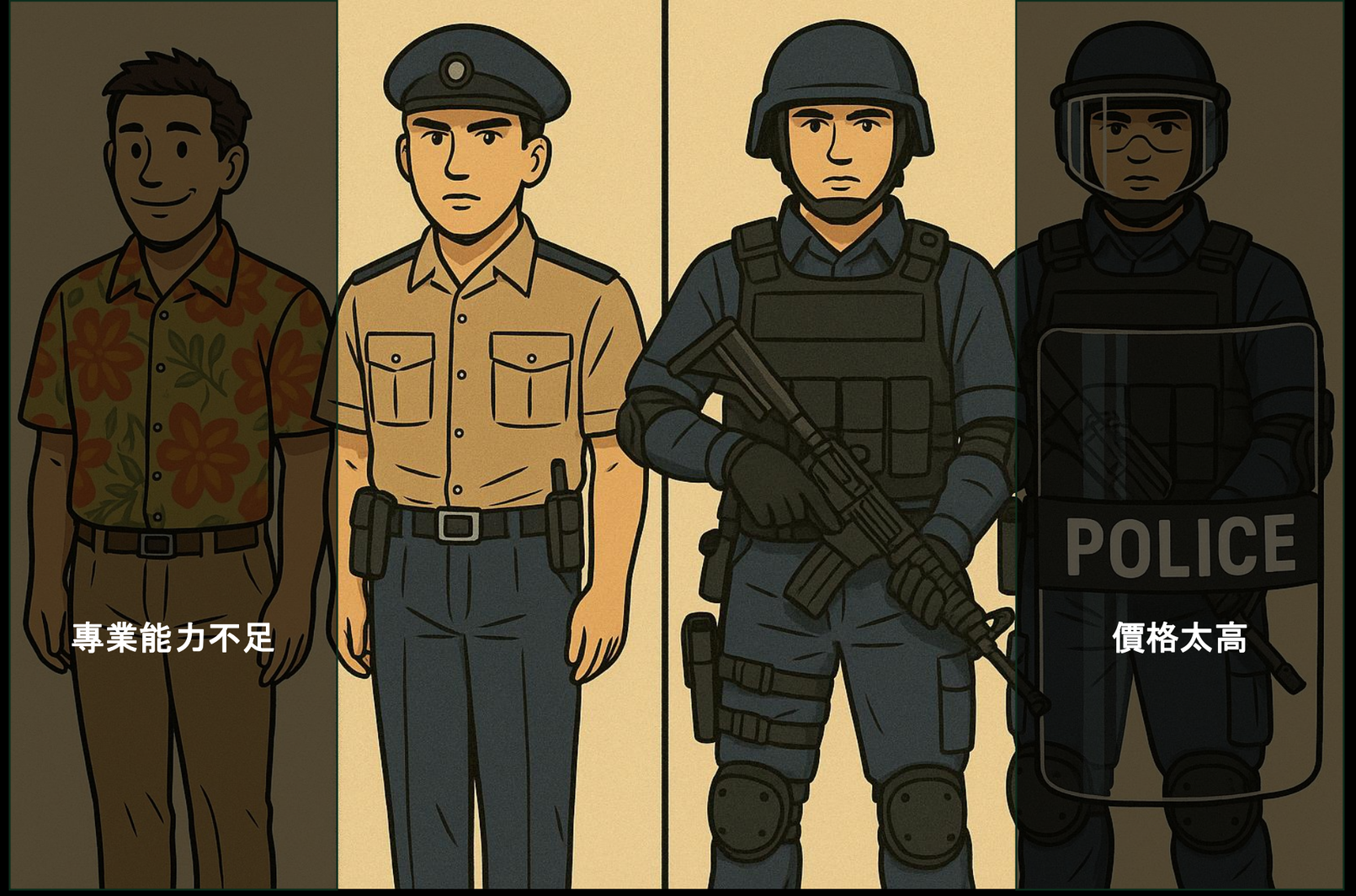
衝擊高

衝擊低



預算多

預算少



安全等級	SL-1	SL-2	SL-3	SL-4
防禦目標	意外誤用	簡單故意攻擊	專業目標攻擊	國家級持續性威脅
關鍵措施	基本密碼、權限	身份驗證、角色控制、網絡分隔	集中管理、SIEM、多因素驗證	雙重批准、物理隔離
Cost	$	$$	$$$	$$$$

存取控制(AAA)

1. 系統具備唯一識別及鑑別使用者（SR 1.1 RE(1)）
2. 最小權限（SR 2.1 RE(1)）

SL-2

SL-3

1. 系統具備唯一識別及鑑別使用者（SR 1.1 RE(1)）
2. 最小權限（SR 2.1 RE(1)）
3. 非信任網路存取需進行多因子身分驗證(MFA)（SR 1.1 RE(2)
   - 遠端維護需進行MFA
4. 集中式帳戶管理（SR 1.3 RE(1)）
   - Active Directory (AD)
   - Radius
   - Tacacs+
5. 人員密碼產生和生命週期限制（SR 1.7 RE(1)）
6. 集中管理稽核追溯能力（SR 2.8 RE(1)）
7. 稽核記錄儲存容量閾值時發出警告（SR 2.9 RE(1)）
8. 不可否認性（SR 2.12）

監控(Detect)

SL-2

1. 保護稽核資訊 （SR 3.9）
2. 持續監控 （SR 6.2）
   - IDS
   - IPS
   - 防毒機制
   - 網路監視機制

SL-3

1. 保護稽核資訊 （SR 3.9）
2. 持續監控 （SR 6.2）
3. 全系統日誌監控(SR 2.8 RE (1))
4. SIEM(SR 3.2 RE (2))
5. 自動通知異常篡改的事件 (SR 3.4 RE (1))

推薦實作流程

1) **確認範圍(SUC):** 網路架構圖, 實體佈線圖
2) **初階風險評估：**
   I. 評估後果：影響發電效率, 單一區域停電 ,影響整個電網。
   II. 法遵需求
3) **區域與通道劃分:**分為安全區域 (zones) 與通道 (conduits)，如現場設備與控制中心分離。
4) **詳細風險評估：**
   i. **資產識別:**列出關鍵組件，例如逆變器、控制伺服器、雲端平台。
   ii. **威脅分析:**識別潛在威脅：網路攻擊 (如DDoS)、物理破壞、內部錯誤。
   iii. **脆弱性檢查:**檢查弱點：未加密通訊、過時軟體、無安全認證。
   iv. **風險評估:**根據威脅機率與影響，計算每個區域的風險。
   v. **安全等級分配:**為每個區域指定目標安全等級 (SL-T)，如SL-2或SL-3。

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Takeaway

1. **安全等級是否越高越好？**

   安全等級並非越高越好。選擇適當的安全等級需要平衡安全性與實用性，考慮具體需求和風險情況。

2. **如何選擇適當的安全等級**

   A. 評估風險：考慮需要保護的資產價值、潛在威脅的嚴重性，以及可能發生的機率。

   B. 了解成本效益：較高的安全等級通常伴隨較高的成本、複雜性和使用不便。

   C. 符合法規要求：某些行業有特定的安全標準需要遵守。

   D. 分層保護：對不同資產採用不同的安全等級，重要資產給予更高的保護。

   E. 定期評估：安全需求會隨時間變化，定期檢視您的安全措施是否仍然適當。

Thank You

For further information, visit www.moxa.com.