工業控制 Testbed 與資安攻防研究

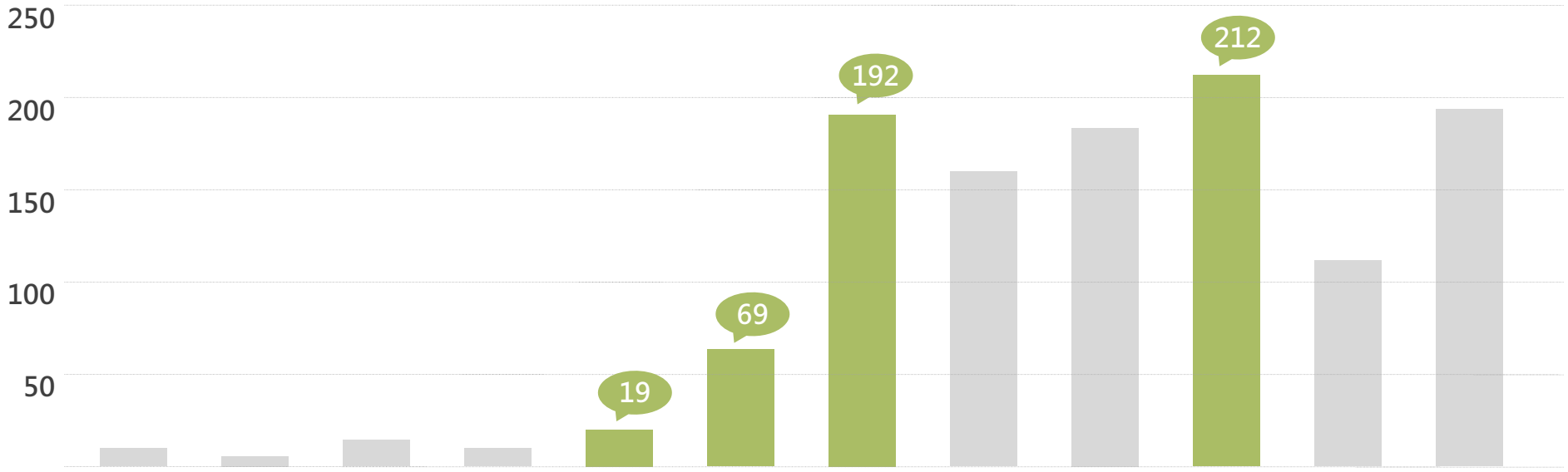
黃瓊瑩

安碁資訊技術副總

工業控制系統真的安全嗎

工控系統重大威脅入侵事件頻傳

ICS 安全漏洞數量逐年增加



TOTAL 1,180

資料來源：ICS-CERT

自 2010 Stuxnet 病毒攻擊伊朗核電廠以來，遭揭露之安全漏洞數量倍增，顯見駭客對 OT 之興趣提升

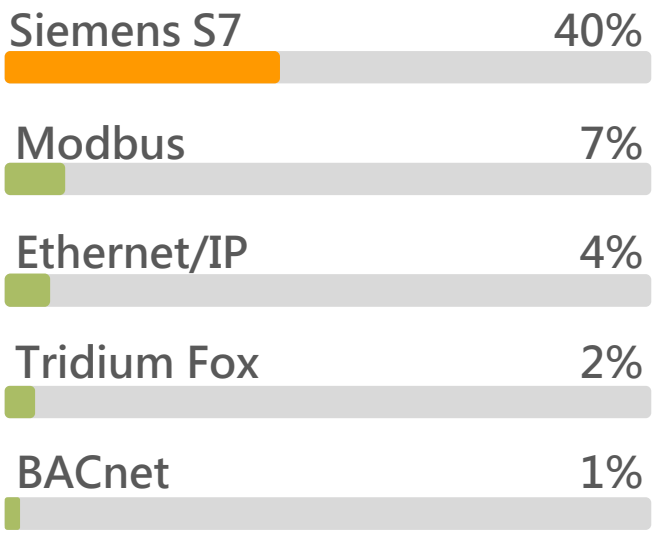
台灣的工業控制系統現況

安全嗎

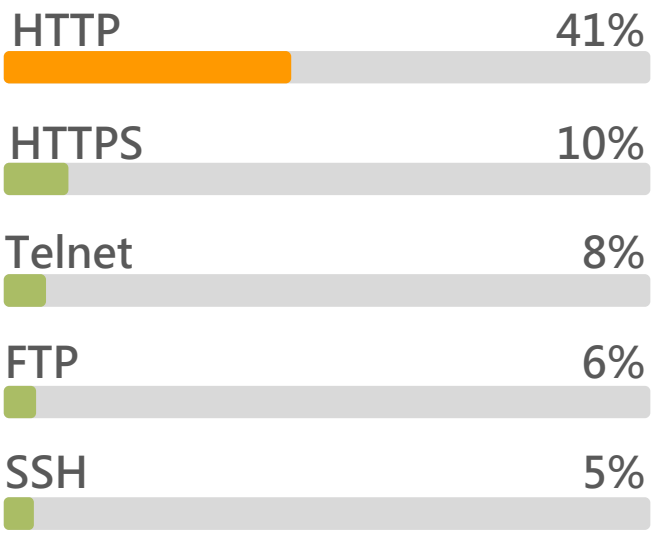
10,546 個

台灣工控設備暴露於網際網路

採用之工控通訊協議

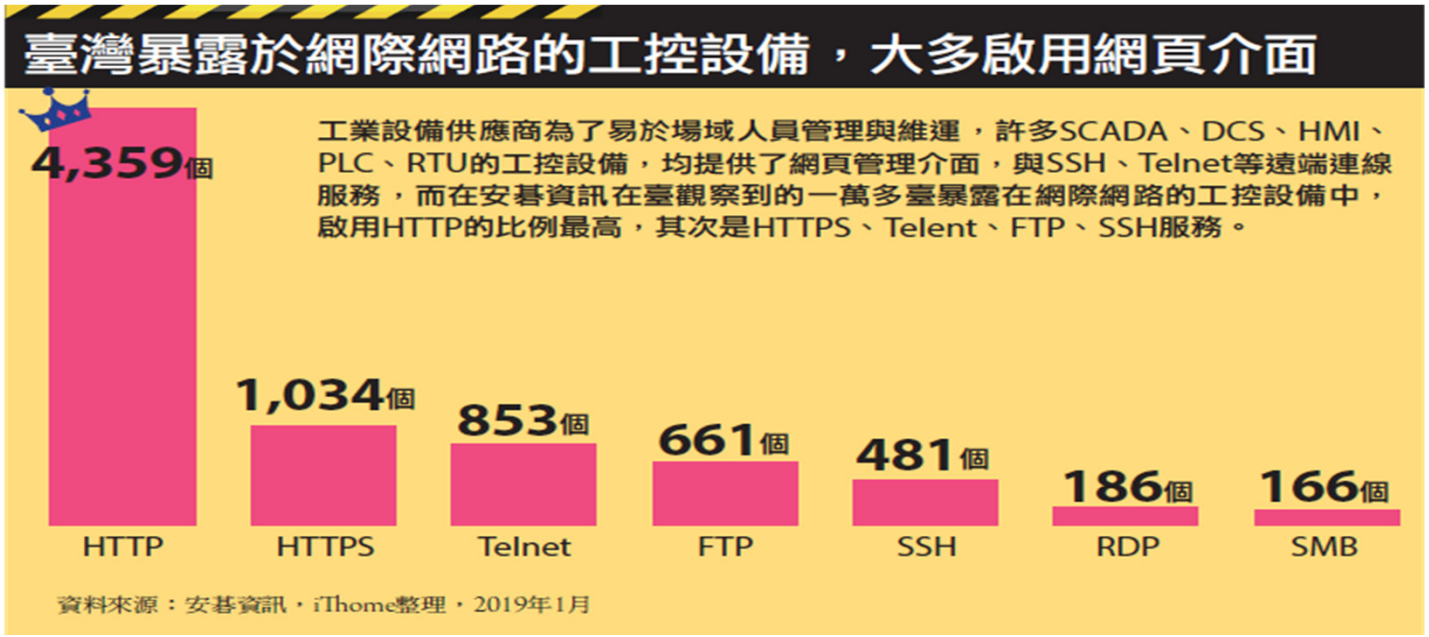


啟用之服務

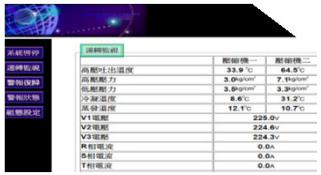


ITHome 2019 資安趨勢報導

- 【2019資安十大趨勢3】ICS系統漏洞激增，暴露在外的數量眾多，ITHome報導，2019-01-08

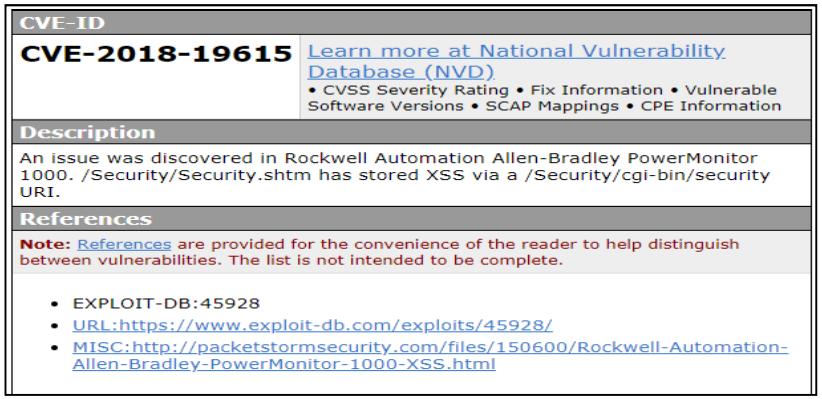


台灣暴露之工控設備產業別



台灣各產業均採用之工控設備漏洞挖掘

CVE ID	Vul. Type	Vender of Product / Affected Product	CVSS v3.0 Score	Published by
CVE-2018-19615	Stored Cross Site Scripting (XSS)	Rockwell Automation Allen-Bradley / PowerMonitor - 1000	6.1 MEDIUM	ICS-CERT W-ISAC ExploitDB CNNVD
CVE-2018-19616	Incorrect Access Control	Rockwell Automation Allen-Bradley / PowerMonitor - 1000	9.8 CRITICAL	ICS-CERT W-ISAC ExploitDB CNNVD



CVE-ID

CVE-2018-19615 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

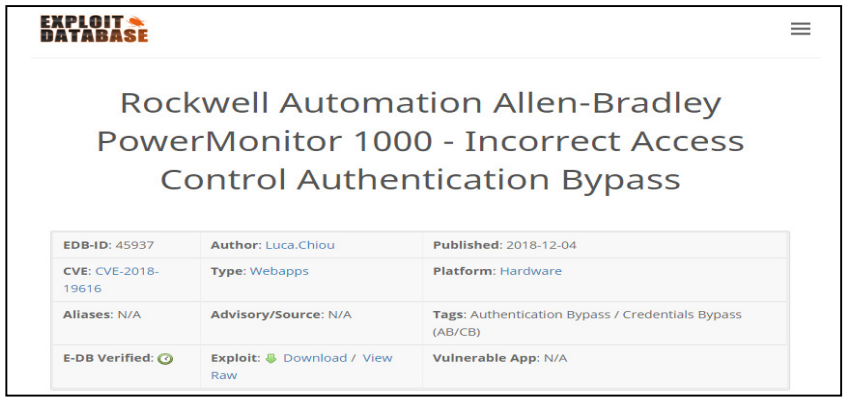
Description

An issue was discovered in Rockwell Automation Allen-Bradley PowerMonitor 1000. /Security/Security.shtm has stored XSS via a /Security/cgi-bin/security URI.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:45928
- URL:https://www.exploit-db.com/exploits/45928/
- MISC:http://packetstormsecurity.com/files/150600/Rockwell-Automation-Allen-Bradley-PowerMonitor-1000-XSS.html



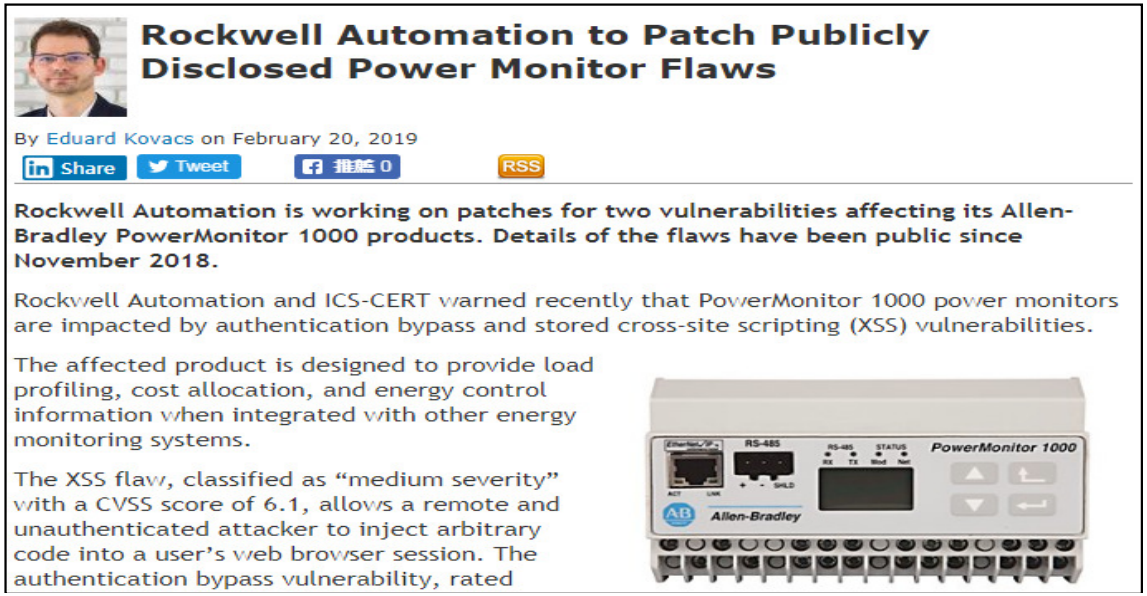
EXPLOIT DATABASE

Rockwell Automation Allen-Bradley PowerMonitor 1000 - Incorrect Access Control Authentication Bypass

EDB-ID: 45937	**Author:** Luca.Chiou	**Published:** 2018-12-04
CVE: CVE-2018-19616	**Type:** Webapps	**Platform:** Hardware
Aliases: N/A	**Advisory/Source:** N/A	**Tags:** Authentication Bypass / Credentials Bypass (AB/CB)
E-DB Verified: ✓	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

ICS-CERT 及 Rockwell 認證

- ICS-CERT 已為該漏洞發布漏洞編號 ICSA-19-050-04，該漏洞 CVSS v3 評分高達 9.8 分（最高10分）
- Rockwell Automation 已公開承認此漏洞
- 該漏洞影響層面涵蓋全球能源領域，國外已針對此漏洞大篇幅報導



Rockwell Automation to Patch Publicly Disclosed Power Monitor Flaws

By Eduard Kovacs on February 20, 2019

Share Tweet 推薦 0 RSS

Rockwell Automation is working on patches for two vulnerabilities affecting its Allen-Bradley PowerMonitor 1000 products. Details of the flaws have been public since November 2018.

Rockwell Automation and ICS-CERT warned recently that PowerMonitor 1000 power monitors are impacted by authentication bypass and stored cross-site scripting (XSS) vulnerabilities.

The affected product is designed to provide load profiling, cost allocation, and energy control information when integrated with other energy monitoring systems.

The XSS flaw, classified as "medium severity" with a CVSS score of 6.1, allows a remote and unauthenticated attacker to inject arbitrary code into a user's web browser session. The authentication bypass vulnerability, rated

台灣工控環境存在大量威脅 OT 研究亦非常困難

- IT v.s. OT
  - OT 具有可用性至上之特性
    導致 IT 之安全控制措施無法適用於 OT
  - OT 與 IT 連接，若缺乏有效隔離，則增加入侵風險

- OT 研究困難
  - 設備不易取得、且十分昂貴
  - 工控資安資料較 IT 少
  - 一般研究人員難以取得設備研究

安碁建置之
工業控制 Testbed

ICS Testbed - 以交通運輸為情境

安碁資訊股份有限公司
Acer Cyber Security Inc.

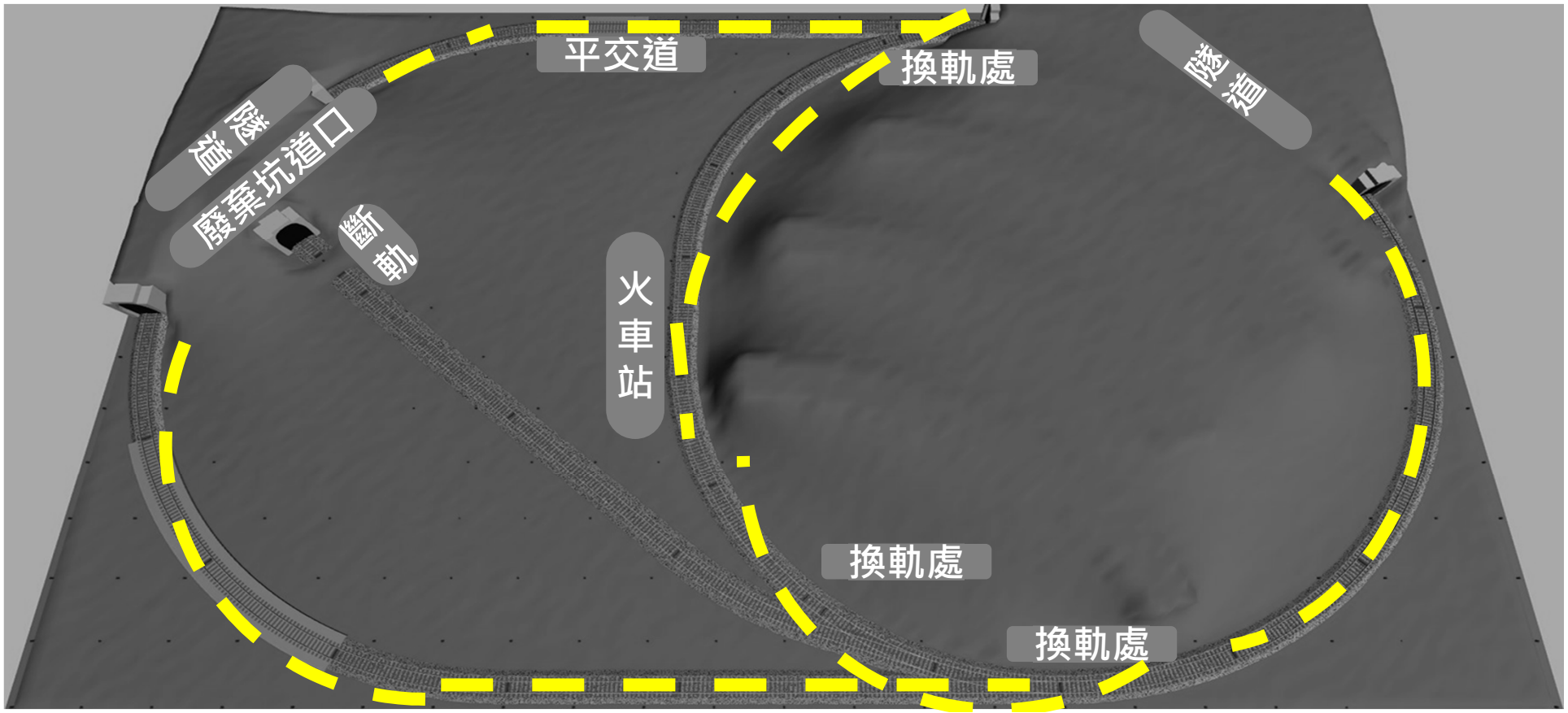
ICS Testbed - 以交通運輸為情境

Testbed 模型說明

Testbed 模型說明 - Sensor

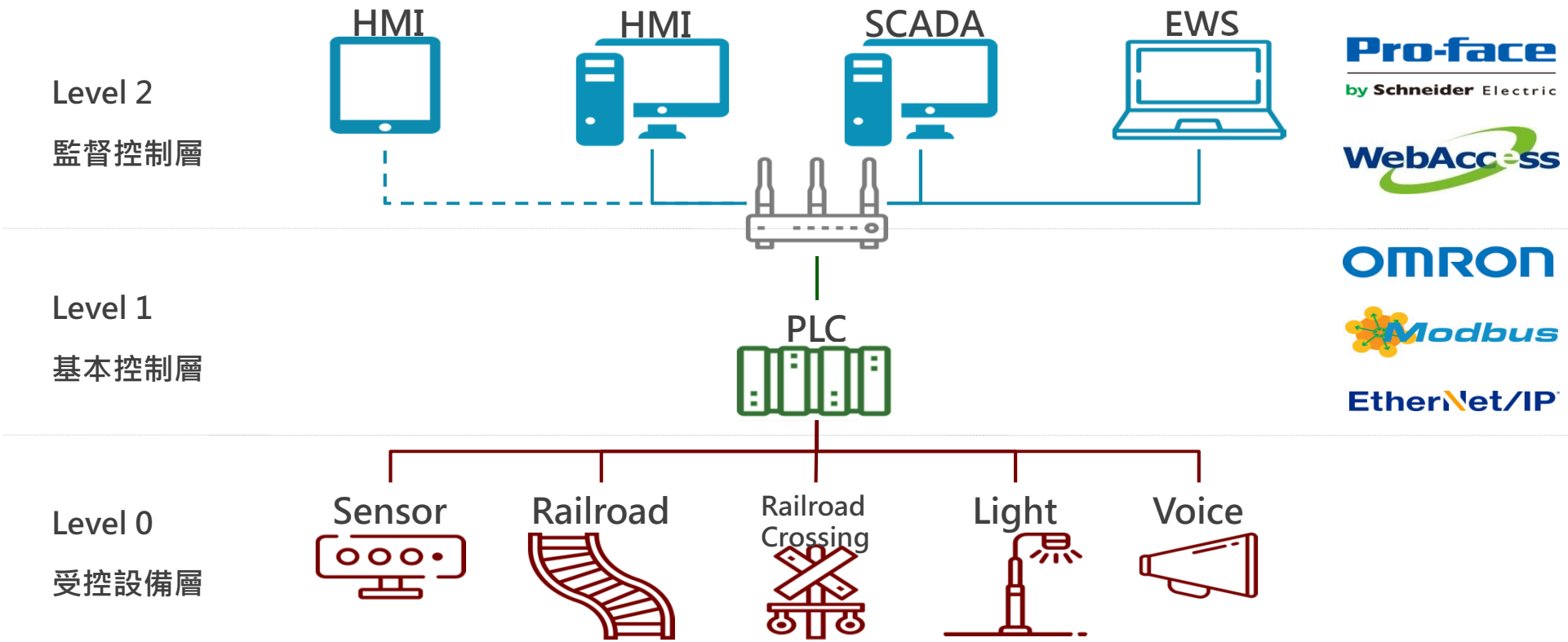
Testbed 模型說明 - 聲音及燈光

正常運行模式



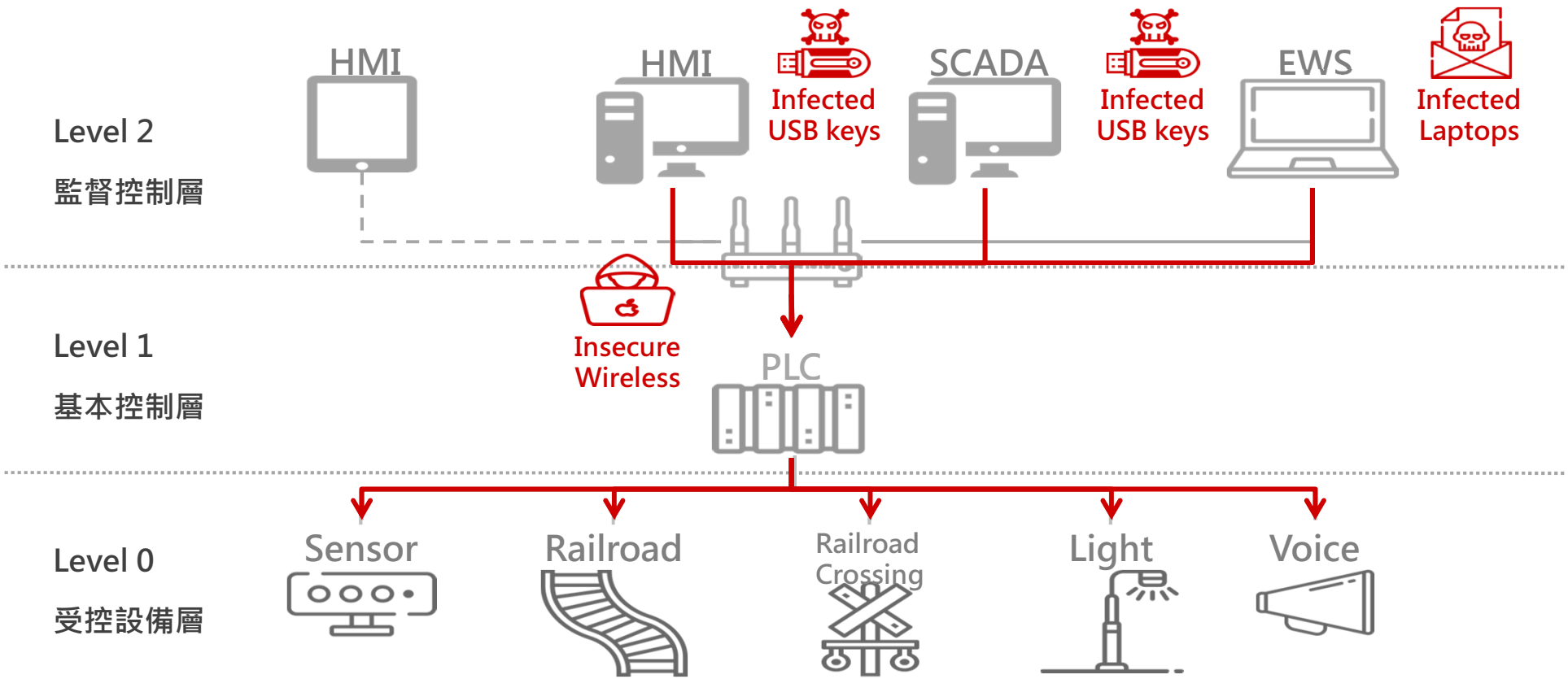
於工業控制 Testbed 模擬
駭客攻擊工業控制網路之途徑

ICS Testbed 實體隔離系統架構



Icons made by Freepik www.flaticon.com is licensed by CC 3.0 BY

入侵至 OT 實體隔離環境途徑



Icons made by Freepik www.flaticon.com is licensed by CC 3.0 BY

駭客進入 OT 網路後之攻擊手法

- 利用已知之 ICS 設備漏洞，或 Zero-Day 漏洞發動攻擊
- 嘗試取得 SCADA、HMI、PLC 之操作權限
- 最終改變受控設備之物理狀態

利用 ICS 設備及系統之漏洞

- 協定之固有設計瑕疵：缺乏加密、缺乏認證及缺乏授權
- 中間人攻擊（MitM）
- 封包側錄及解析
- 封包重放及竄改
- 最終改變受控設備之物理狀態

利用工控通訊協定固有之瑕疵

- 許多廠牌 ICS 設備之 SSH、Telnet 服務預設開啟，且密碼為硬編碼（Hard Code）
- 利用此些管理服務之不安全設置，嘗試取得 ICS 設備控制權
- 最終改變受控設備之物理狀態

利用工控設備啟用之 SSH/Telnet 等服務

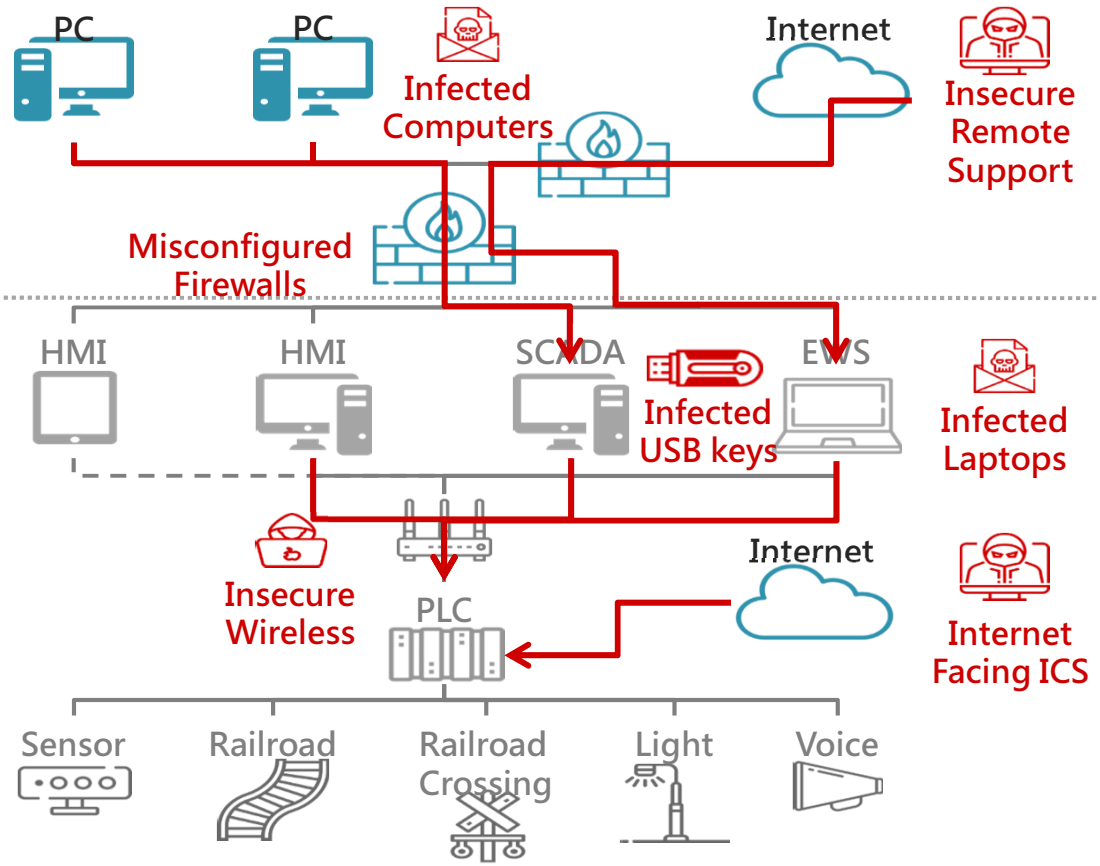
與 IT/Internet 連接後，入侵途徑

IT 網路

Level 4~5

OT 網路

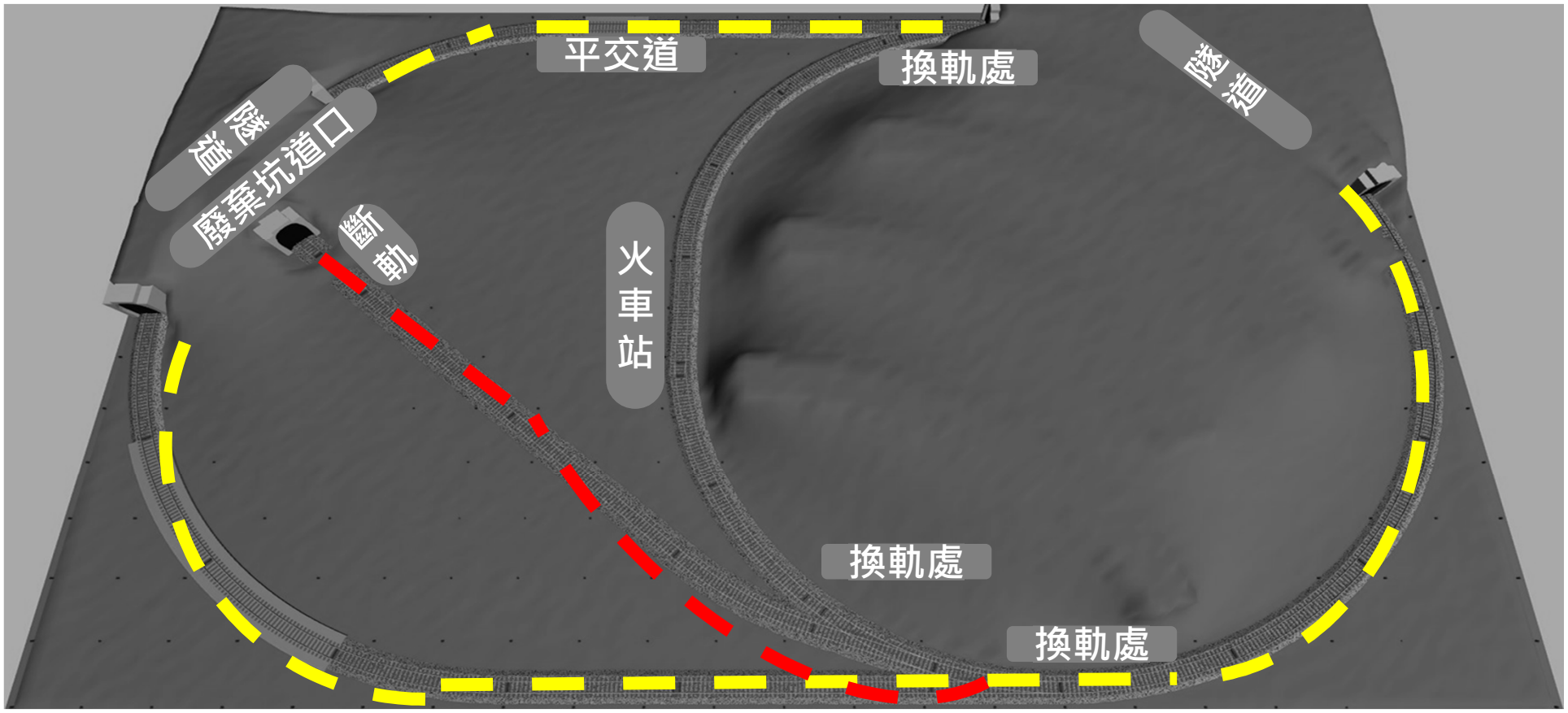
Level 0~3



Icons made by Freepik www.flaticon.com is licensed by CC 3.0 BY

工業控制 Testbed
攻擊入侵手法展示

攻擊者嘗試改變場域物理狀態



安碁工業控制網路攻防實務課程

臺灣資安大會 CYBERSEC 2019 MAR 19-21 TAIPEI PRESENTED BY iThome EN

安碁資訊股份有限公司 Acer Cyber Security Inc.

工業控制網路攻防實務（初階）

03/19 15:30-17:30 TICC 雅軒 (4樓)

教室：TICC 雅軒 (4樓)

Speaker
安碁資訊股份有限公司資深專案工程師 邱鈺雯

Speaker
安碁資訊股份有限公司資深專案工程師 黃文治

課程簡介：

工業控制系統資訊安全漏洞遭揭露之數量近年來大幅上升，工業控制環境、甚至是國家關鍵基礎設施入侵威脅事件頻傳，顯見駭客對於工業控制環境的興趣提升。然而，與IT環境相比，工業控制環境多採用專有之協議、專有之設備（如：PLC、RTU），對於資安研究人員而言，進入門檻相對較高。透過此次課程，學員不僅可以快速獲取工業控制系統資訊安全之基礎知識，更可以學習如何滲透至工業控制網路，並解析工業控制系統協議封包、工業控制系統協議攻擊等。

課程目標

- 了解工業控制系統元件（component）
- 了解廣泛應用之工業控制系統協議封包解析方式
- 了解工業控制系統協議攻擊之手法、工具

課程綱要：

- 工業控制系統概述
- 工業控制系統協議封包解析實作
- 工業控制系統服務辨識
- 工業控制系統協議攻擊實作：Modbus、Ethernet/IP、Siemens S7

進階課程持續開課

THE BEST IS YET TO COME