

FORTINET®

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展

能源產業於資安議題的覺醒

鄭炎富 Yenfu Cheng

Yatec 能源暨監控事業處 處長



YATEC

安華機電工程股份有限公司
YATEC Engineering Corporation

工控系統應用之 Cyber Security 經驗分享

處長:鄭炎富

8/3/2022

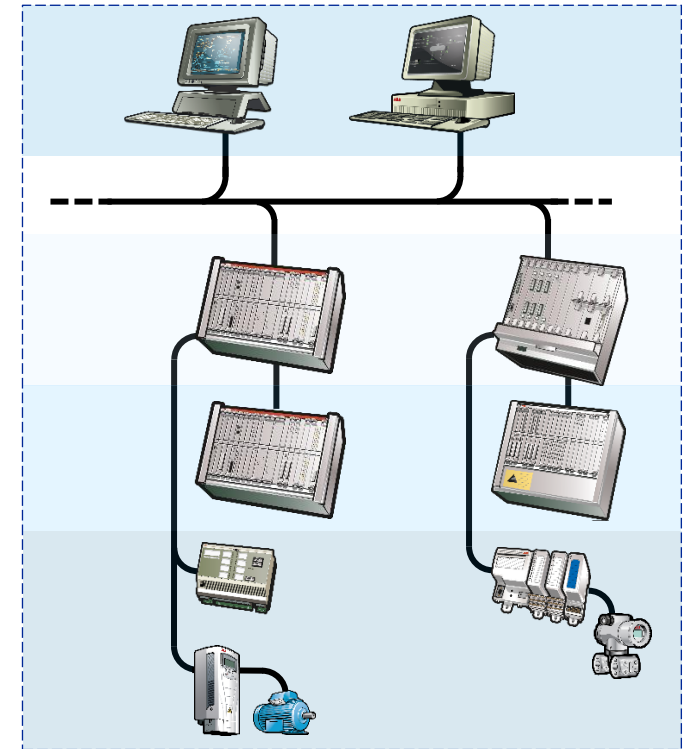
Agenda

- 那些年OT與Cyber Security的愛恨情史
- 迷惘與困境
- 致勝的關鍵
- 需要盟軍的戰爭

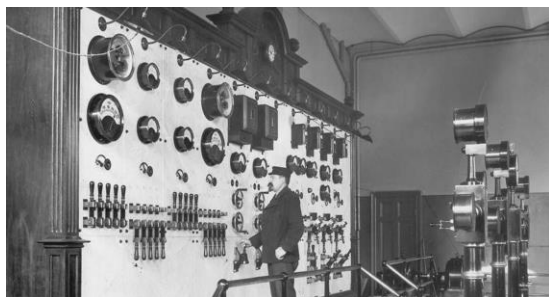


那些年OT與Cyber Security的愛恨情史

- 從封閉走出來
 - 控制系統廠商自行開發的作業系統與應用平台
 - 專用鍵盤、滑鼠甚至螢幕
 - 磁帶機
 - 最快6秒一筆的歷史紀錄
 -
- 開放系統的呼聲(open system)
 - Unix(1990) or Windows(2000-)
 - 乙太網的衝擊
 - 建置成本的挑戰
 - IT技術與便利性的誘惑



那些年OT與Cyber Security的愛恨情史



- Classic/Pneumatic Control system



- Central Control or DCS control System.
- Unix/VMS/QNIX or proprietary human interface
- Limited interface to external access
- Security: Hard Key & Password protection

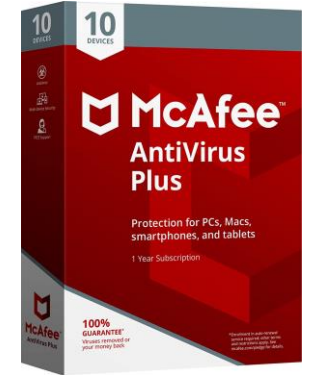
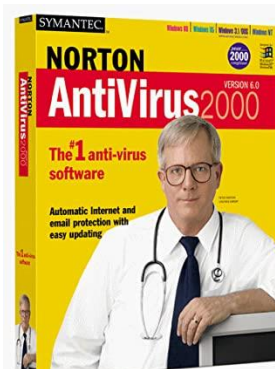
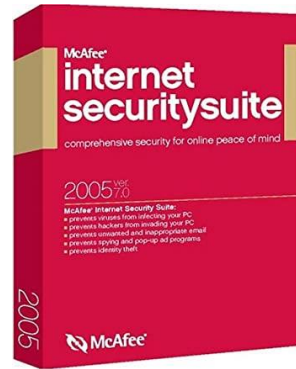
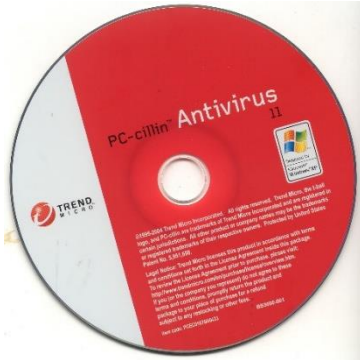


- Windows base w/ PC technology
- More and more convenient interface
- More Vulnerable and need bug fixing
- Security: Password protection
- Isolated environment to protect external intruder.



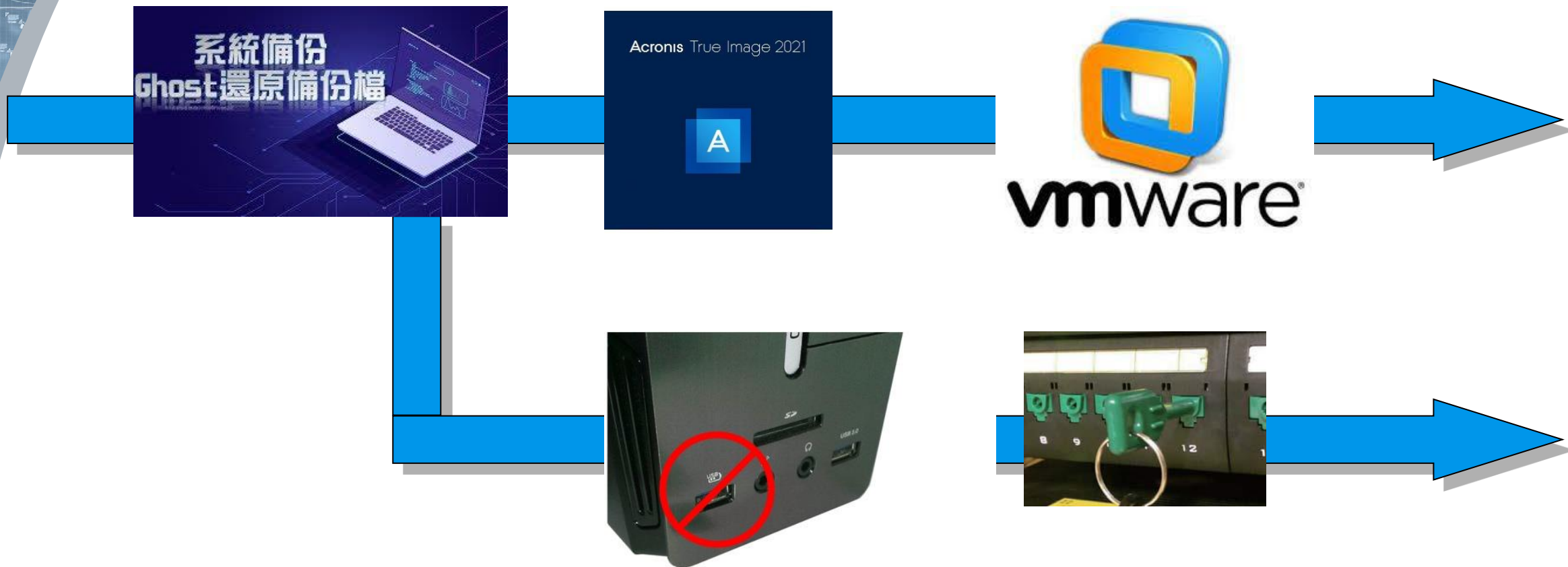
- Digitalization
- Industrial 4.0
- AI / IoT era
- Interconnection is inevitable
- Cyber Security and system hardening require long-term strategy

那些年靠防毒軟體...但

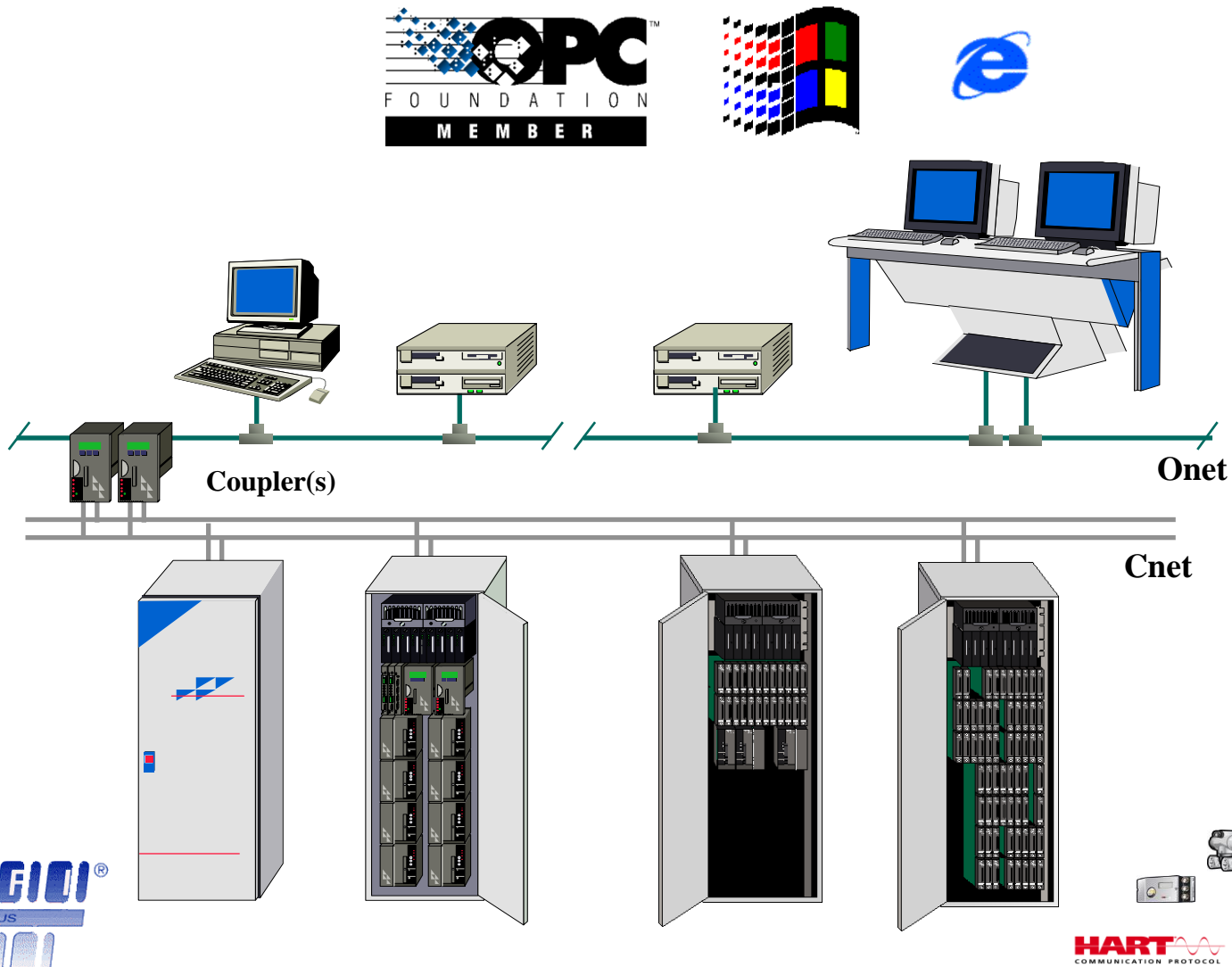


1. 不敢裝 掃毒掃不完
2. Debugging 時優先移除防毒
3. 病毒和防毒軟體會不會... ..系出同源
4. 又沒有上那些“網站”，應該不會.....

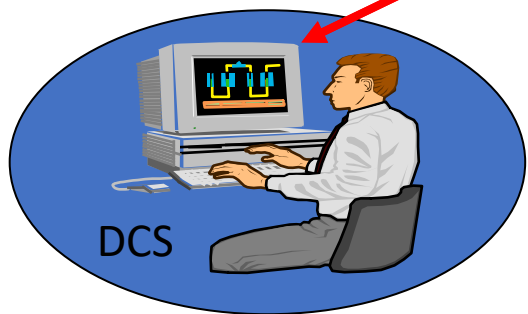
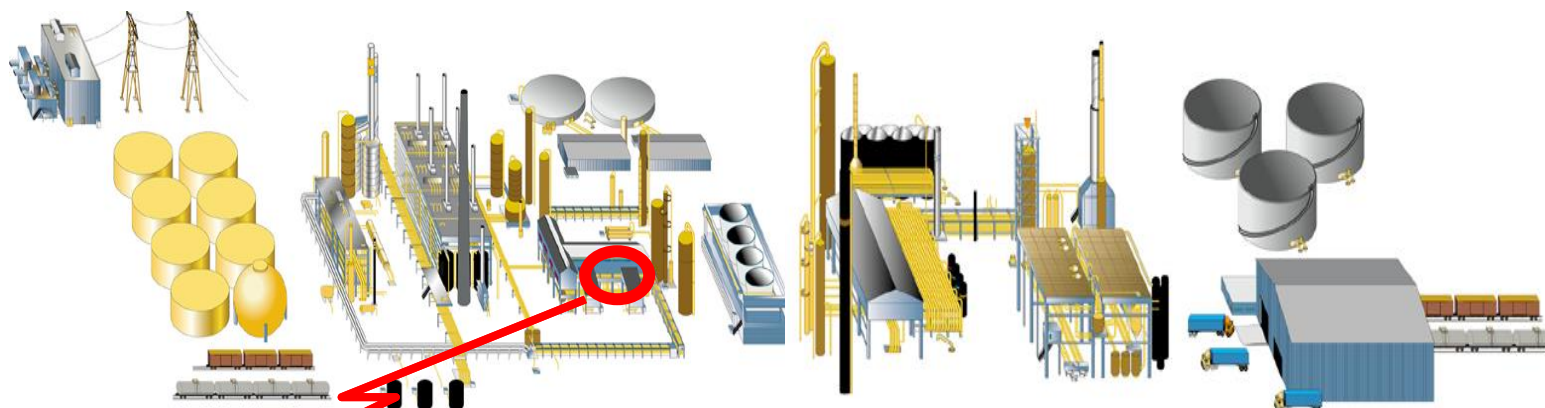
既然防毒不可靠...還得有還魂術



話說..控制室內是與世隔絕的世界

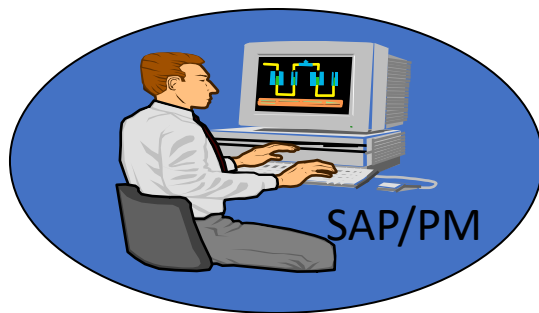


由儉入奢易....

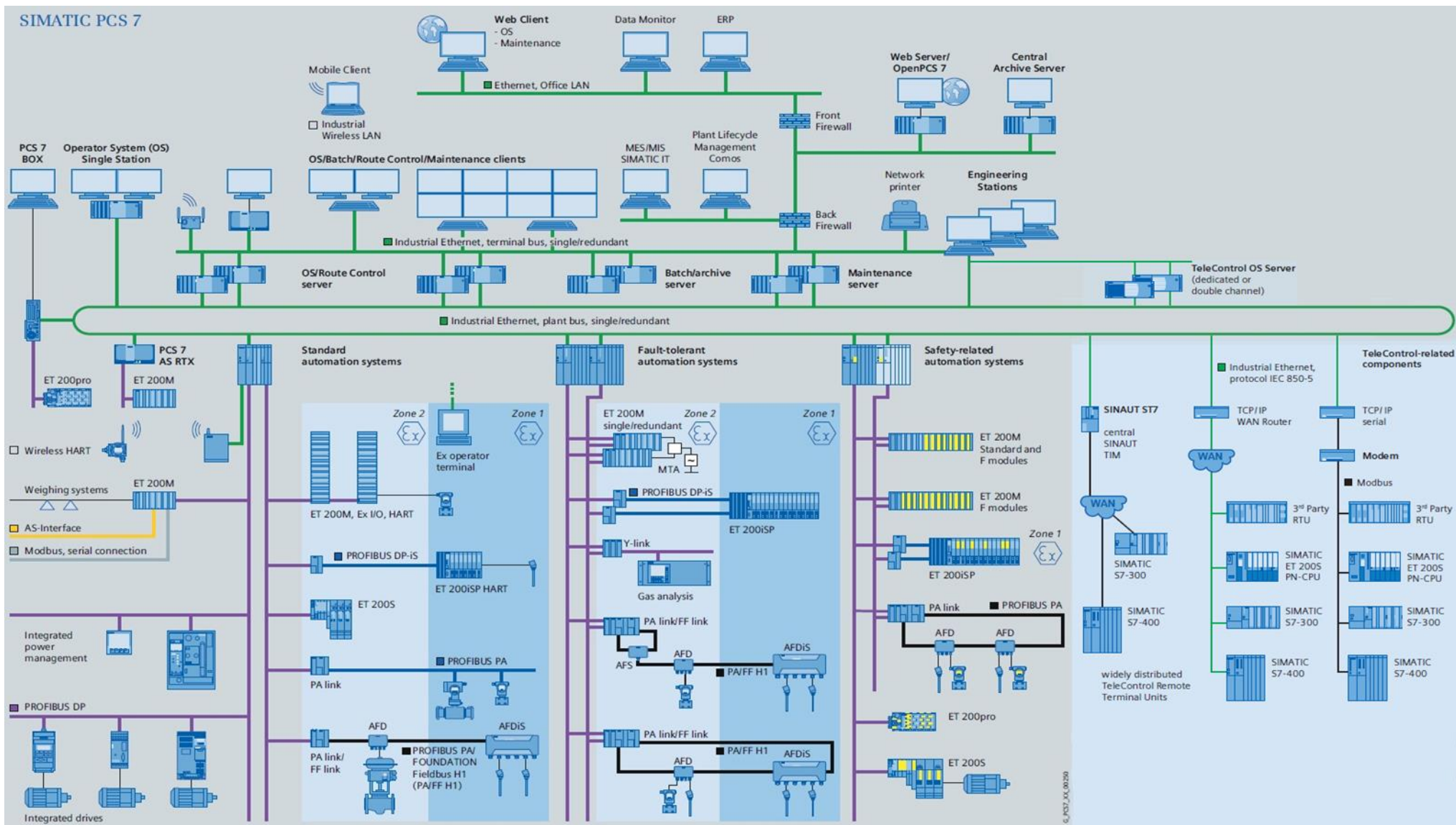


控制系統的便利..... > 工業 4.0

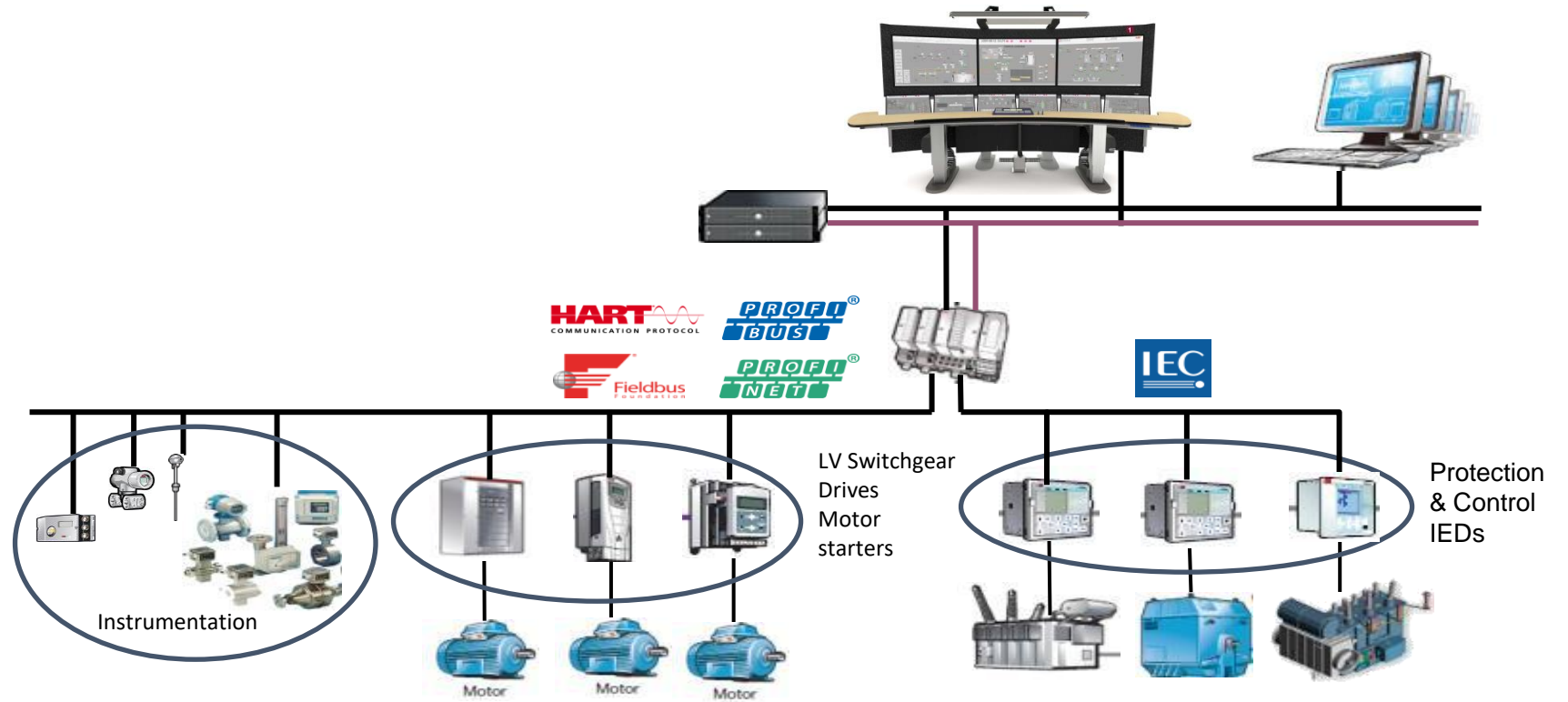
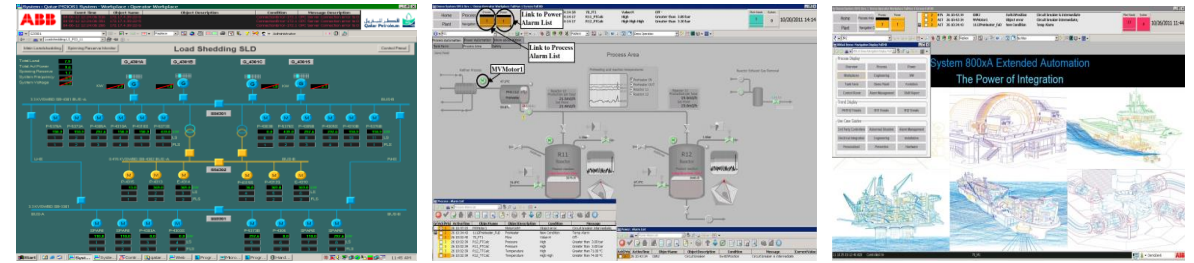
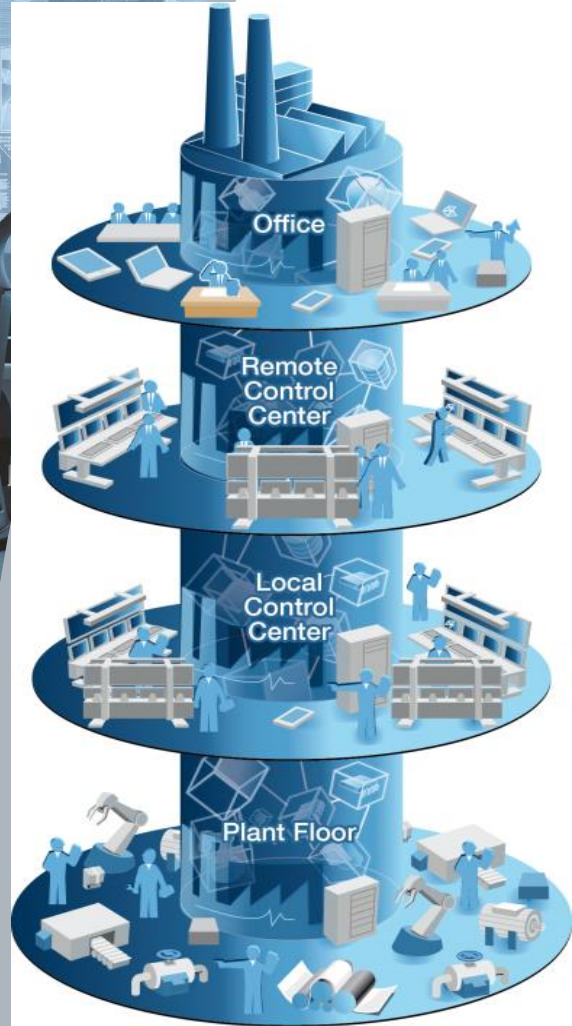
自動化與更多的資料處理是一條不歸路



這樣的系統如何封閉?

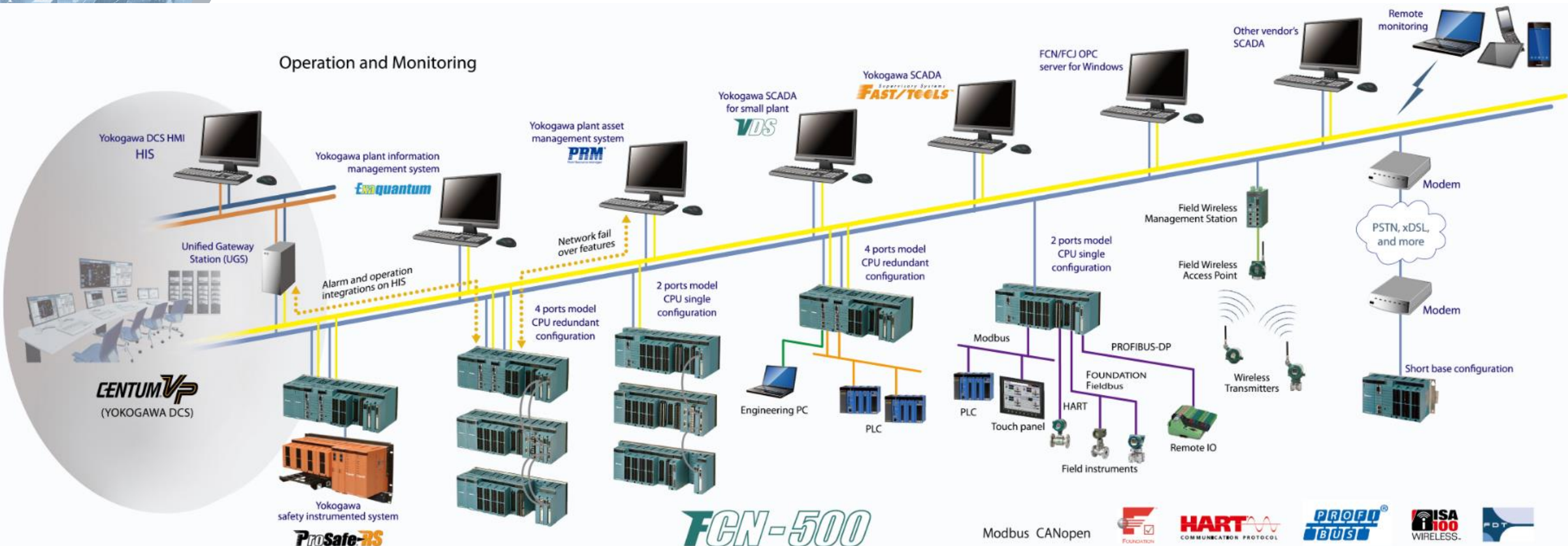


這樣的系統如何封閉?



這樣的系統如何封閉?

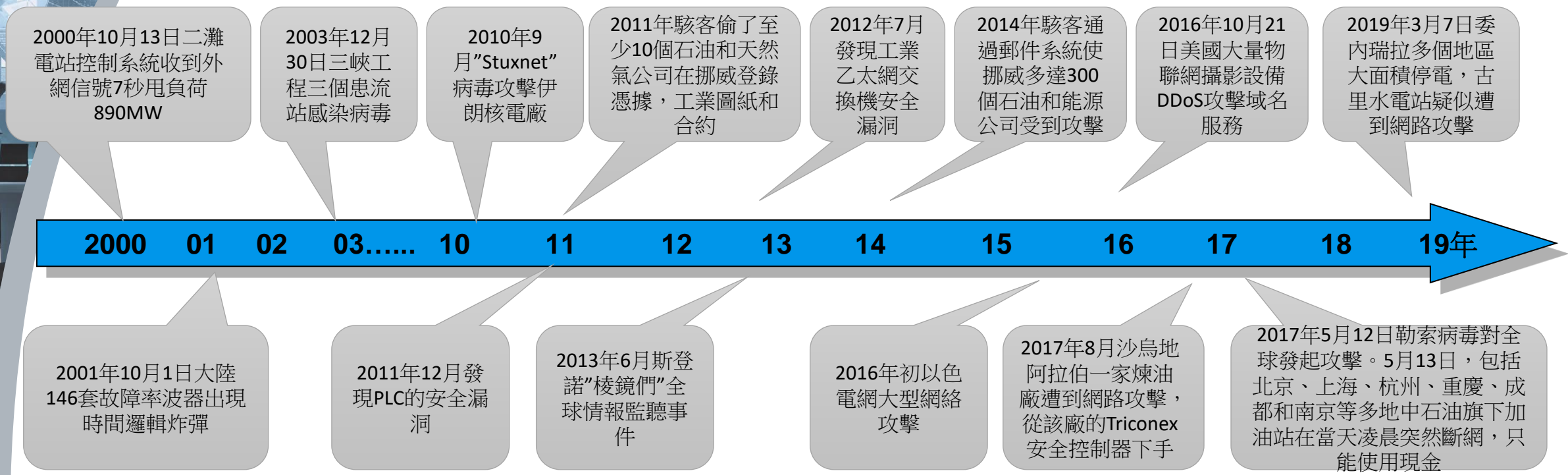
Operation and Monitoring



迷惘與困境

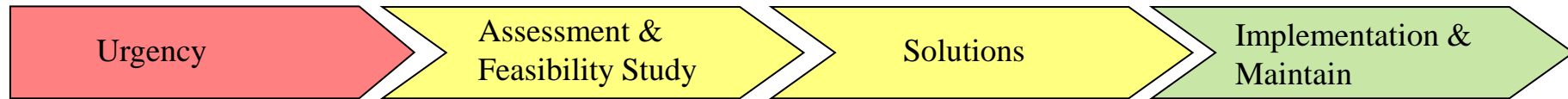
- 安全與生產是基本要求，就算是失去所有...
 - 網路可以封閉，可以中斷，可以與世隔離。
- IT系統被攻擊時啟動防護措施，OT卻必須維持系統運作
 - 安全運轉重於一切。
 - 如何兼顧安全運轉與資安？
- 24/7運轉，就是24/7運轉，只有在工廠停機檢修時才能進行維護工作。
 - 系統越龐大，檢修的機會就越低，同時歲修的機會極低。
 - 誰能做出保證？(代價往往比想像還高昂)
- IT人才在OT世界中...是個寶，卻看不到未來；當系統與技術越來越複雜，OT人看IT的視線就越來越模糊....
- 危機到來.....

Some Accidents In History ... 不到黃河不掉淚



致勝的關鍵

- 由上而下重視資安。
- 從別人的慘痛教訓中學習，不要遲疑，快速行動。
- 對的方法比便宜的方法更便宜。



CLP龍鼓灘發電廠Cyber Security案例

Background introduction

- 龍鼓灘發電廠擁有八台(8) 350MW 複循環機組， ABB 為DCS 供應商，另外GE提供汽機及燃機的控制系統，CLP透過PI (Plant information system) 收集整廠運轉資訊，成為ERP的一部份。
- 有鑒於網路攻擊事件日益頻繁，中電集團高層非常重視，特別是香港對於用電穩定之要求極高，故由董事會直接要求執行資安管理措施，並在2016底完成佈署。其中聘請外部顧問Digital Bond (CLP's cyber security consultant)進行現有系統狀況稽核，並給出建議，在很短的時間下，由ABB建置完成Cyber Security管理架構，同時由ABB及GE分別對自家系統進行升級及必要之補強，以符合Cyber Security要求，全案於2016年底如期完成，並於2017/1交付使用。



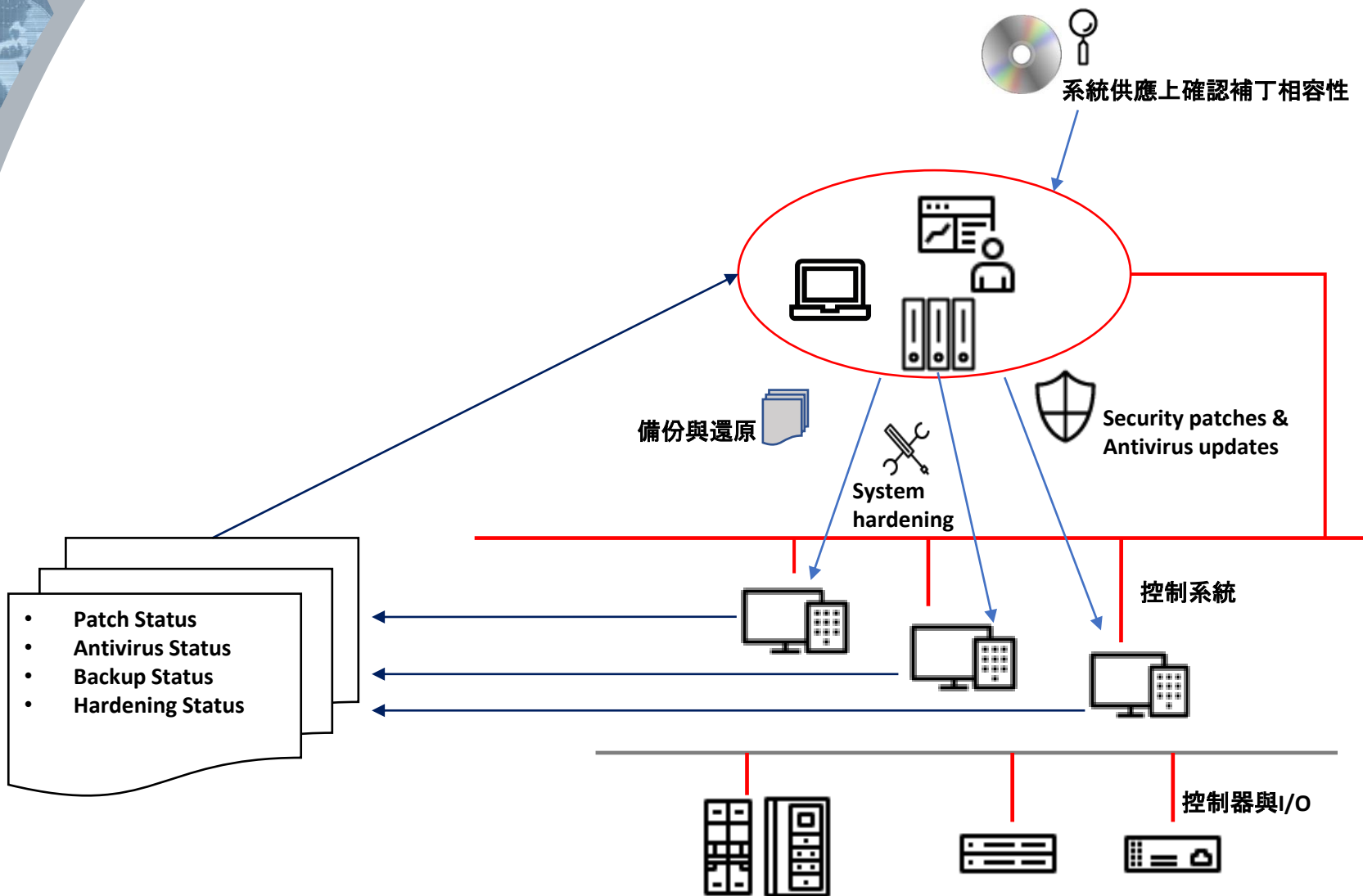
Security Assessment

TABLE OF CONTENTS

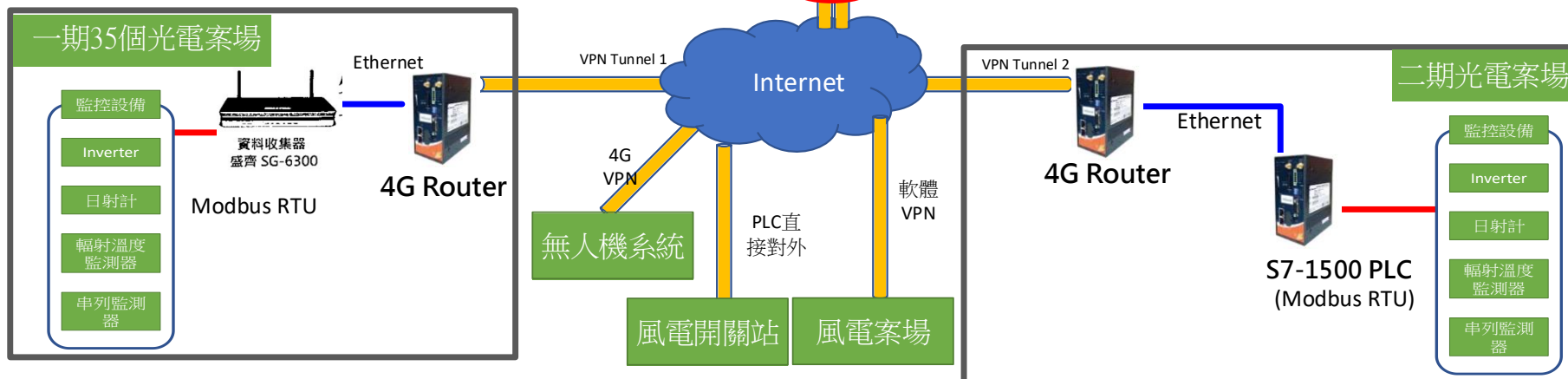
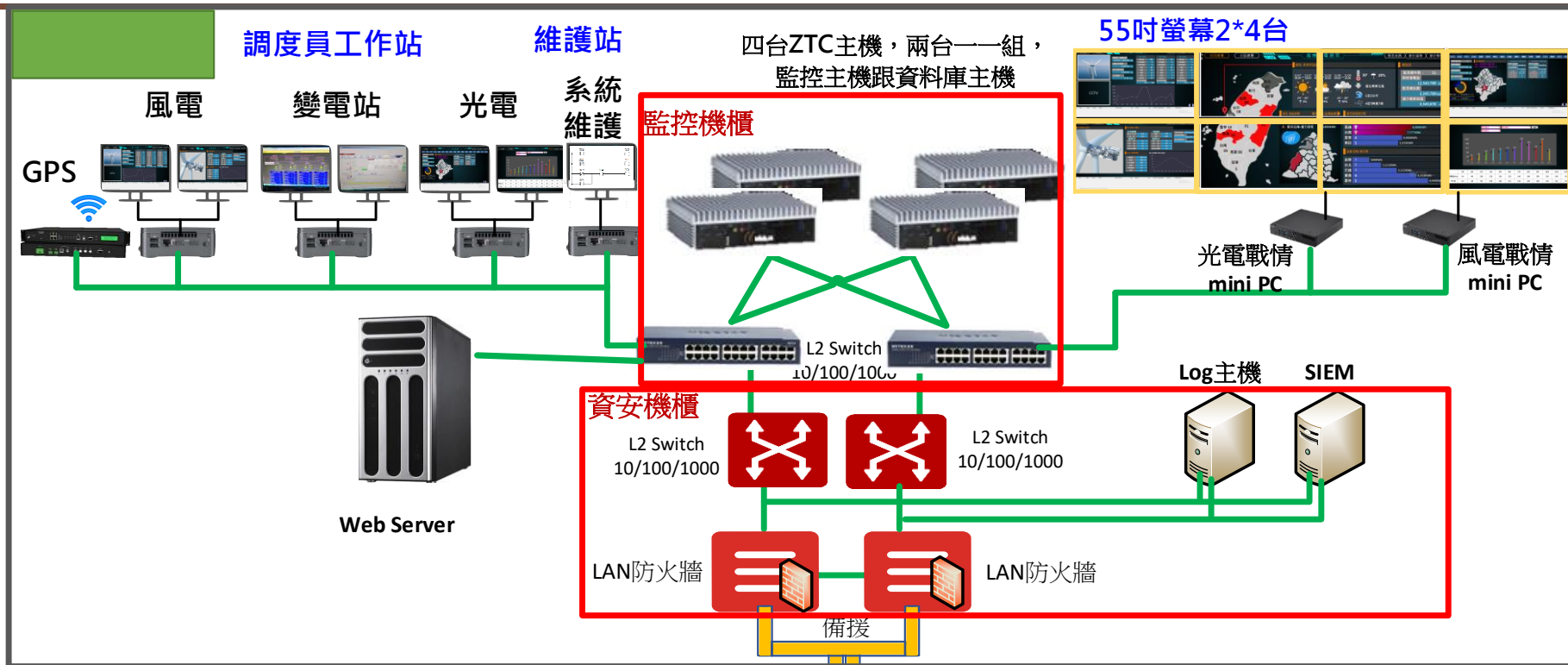


| | | |
|-----------|---|-----------|
| 1. | EXECUTIVE SUMMARY | 2 |
| 1 | INTRODUCTION..... | 4 |
| 2 | SECURITY ARCHITECTURE | 5 |
| 2.1 | PI SERVER / HISTORICAL DATA EXPORT..... | 5 |
| 2.2 | ACTIVE DIRECTORY | 7 |
| 2.3 | McAFEE MANAGEMENT / ePOLICY ORCHESTRATOR..... | 8 |
| 2.4 | SECURITY PATCH MANAGEMENT | 9 |
| 2.5 | NETWORK MONITORING | 10 |
| 2.6 | FDSI – GE MARK VI E TO FOXBORO CONNECTION | 10 |
| 3 | SECURITY ANALYSIS AND PHASE II TESTS..... | 12 |
| 3.1 | PURPOSE AND SCOPE..... | 4 |
| 3.2 | AUDIENCE | 4 |
| 3.3 | USE OF ENGLISH | 4 |
| 3.4 | NOTES FOR CONTRACTOR | 5 |
| 3.5 | 1 CYBER SECURITY CONTROLS | 7 |
| 3.6 | 1.1 OPERATION SUSTAINABILITY REQUIREMENTS..... | 7 |
| 3.7 | 1.2 OT CYBER SECURITY PROTECTION & DETECTION REQUIREMENTS | 8 |
| 3.8 | 1.3 CYBER SECURITY VERIFICATION..... | 16 |
| 3.9 | 1.4 OT SECURITY DOCUMENTATION REQUIREMENTS | 17 |
| | 1.5 IT SECURITY PROTECTION & DETECTION REQUIREMENTS..... | 19 |

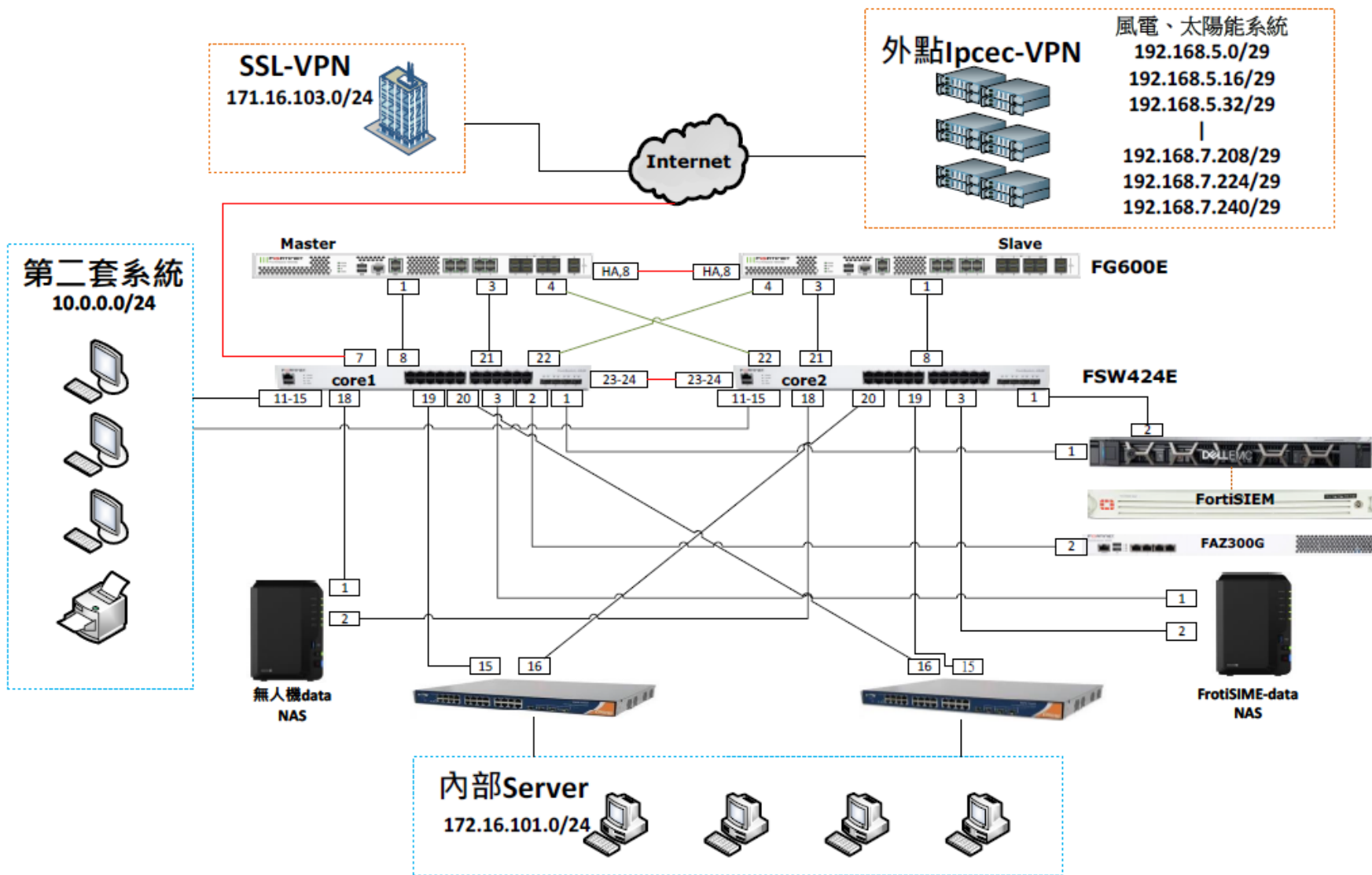
甚麼是對的策略?



新能源監控中心應用實例

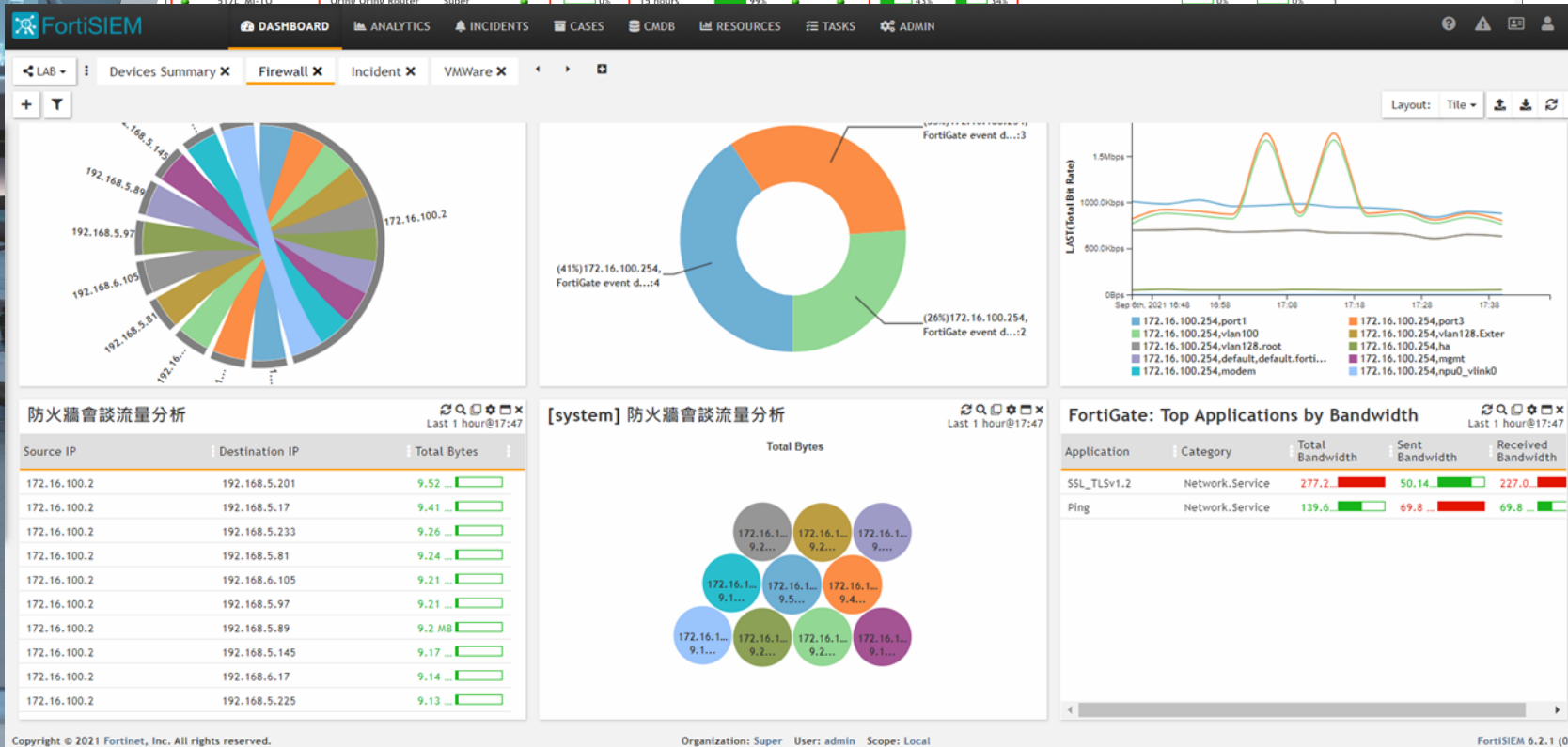


FortiSIEM/FortiGate/Fortianalyzer



| Maint | Device | Type | Organization | Avail Status | Packet Loss | Uptime | Uptime % | Perf Status | Sec Status | CPU Util | Mem Util | Disk Util | Free Disk | Recv Util | Sent Util | EPS | Avail Incidents | Perf Incidents | Sec Incidents |
|-------|-----------------|--------------------|--------------|--------------|-------------|------------|----------|-------------|------------|----------|----------|-----------|-----------|-----------|-----------|-----|-----------------|----------------|---------------|
| ● | 535L_CHAO-HUI_4 | Oring Oring Router | Super | ● | 0% | 6 hours | 99% | ● | ● | 44% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 535L_CHAO-HUI_3 | Oring Oring Router | Super | ● | 0% | 9 hours | 100% | ● | ● | 43% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 535L_CHAO-HUI_2 | Oring Oring Router | Super | ● | 0% | 16 minutes | 99% | ● | ● | 44% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 535L_CHAO-HUI_1 | Oring Oring Router | Super | ● | 100% | | | ● | ● | | | | | | | | ● | ● | ● |
| ● | 522A_LUNG-CHING | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 43% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 567L_CHUN-YI | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 44% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 518C_YUNG-AN | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 44% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 518E_LU-CHU | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 43% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 518D_YUNG-AN | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 44% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |
| ● | 517I_MU-TO | Oring Oring Router | Super | ● | 0% | 15 hours | 99% | ● | ● | 43% | 34% | 0% | 0% | 0% | 0% | 1 | ● | ● | ● |

- 簡易辨識ORing設備名稱、CPU、Memory。
- 使用PING偵測封包遺失來判斷設備狀態。
- 可監控防火牆各項事件產生報表分析。
- 監控內部網段流量以及sslvpn連線狀況。



需要盟軍的戰爭

- 認清敵人是強大的、專業的、不會手軟的...
- 專業的戰爭關係，傳統火砲效果有限。
- 不只是一場戰爭，資安的戰爭已是日常。
- OT需要更專業與強大的支援來打贏”每一場“戰爭...
- 支援是：
 - 盟友 (FORTINET, Control system supplier, ...)
 - 優良先進(順手)的武器裝備
 - 情資分享
 -



敬請指教



安華機電工程股份有限公司

YATEC Engineering Corporation

115 台北市南港區三重路19-8號2F

TEL : 02-26551333

FAX : 02-26551555

<http://www.yatec.com.tw>

FORTINET®

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展