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

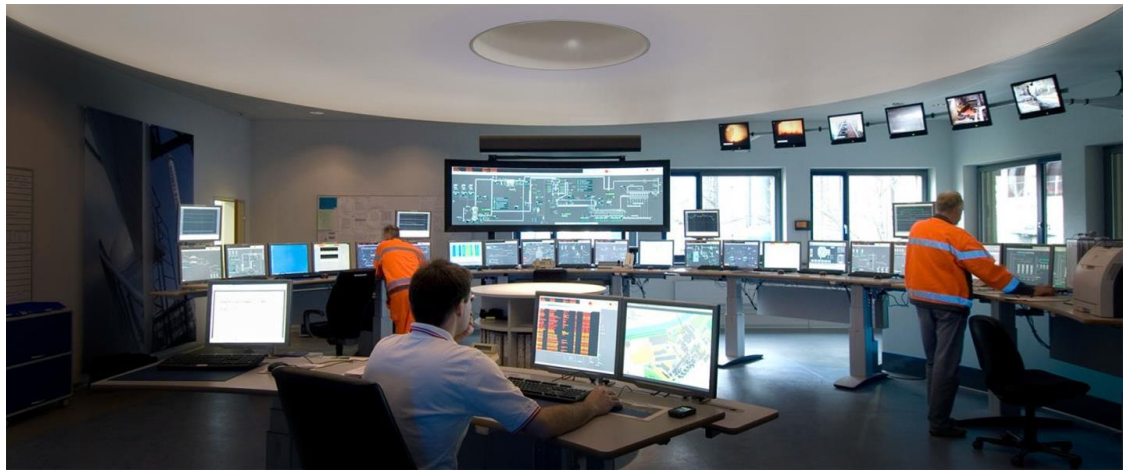
工控系統應用之 Cyber Security經驗分享

處長:鄭炎富

8/3/2022

Agenda

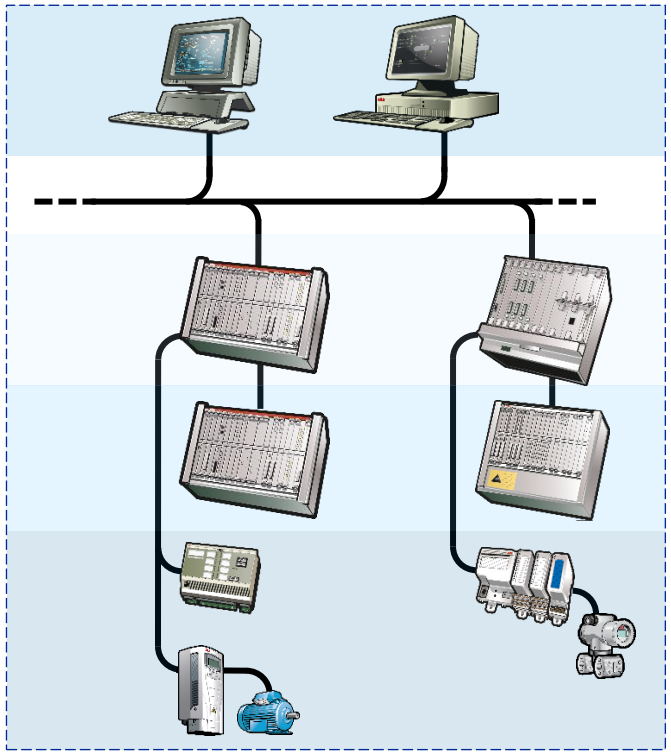
- 那些年OT與Cyber Security的愛恨情史
- 迷惘與困境
- 致勝的關鍵
- 需要盟軍的戰爭



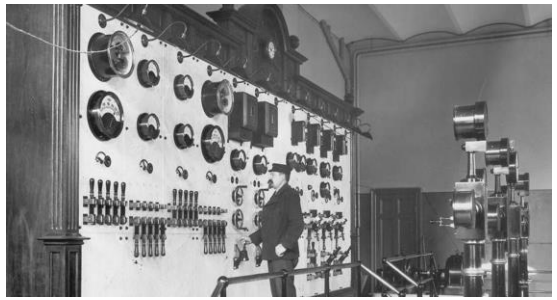
那些年OT與Cyber Security的愛恨情史

- 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



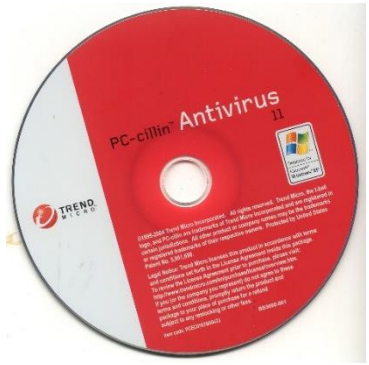
- Classic/Pneumatic Control system

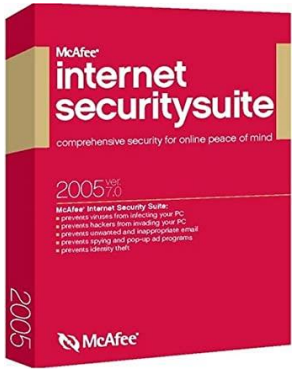
- Central Control or DCS control System.
- Unix/VMS/QNIX or proprietary human interface
- Limited interface to external access
- Security: Hard Key & Password protection

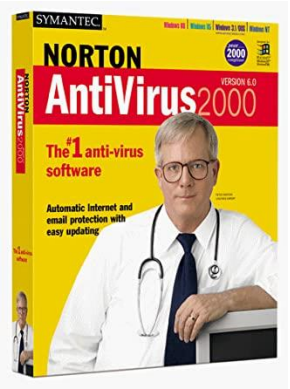
- Windows base w/ PC technology
- More and more convenient interface
- More Vulnerable and need bug fixing
- Security: Password protection
- Isolated environment to protect external intruder.

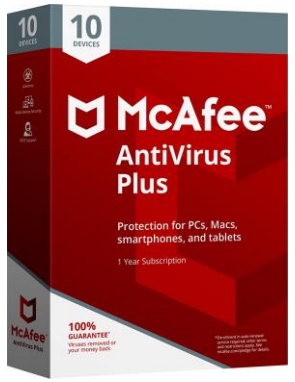
- Digitalization
- Industrial 4.0
- AI / IoT era
- Interconnection is inevitable
- Cyber Security and system hardening require long-term strategy

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.....

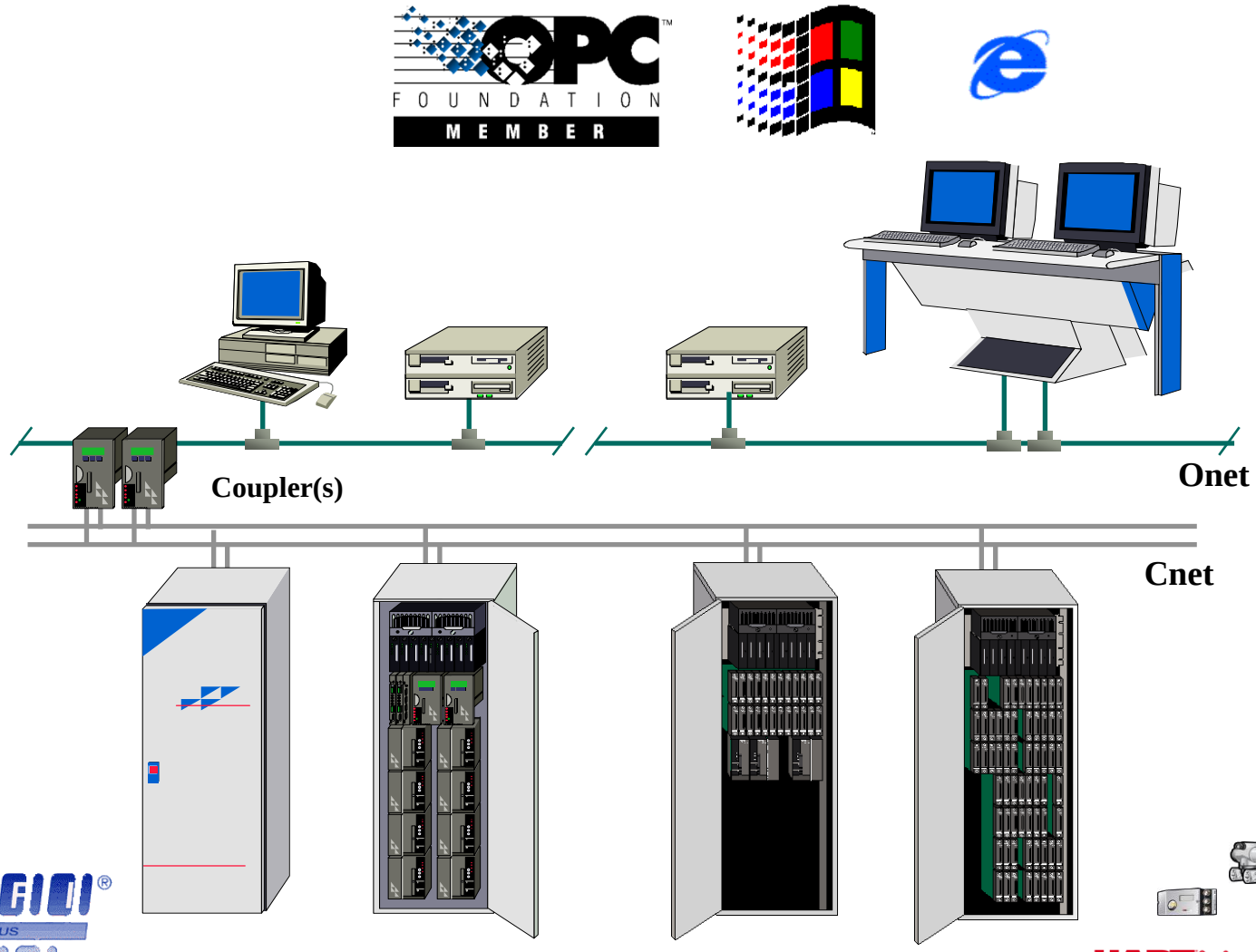
YATEC 安華機電

既然防毒不可靠....還得有還魂術

vmware

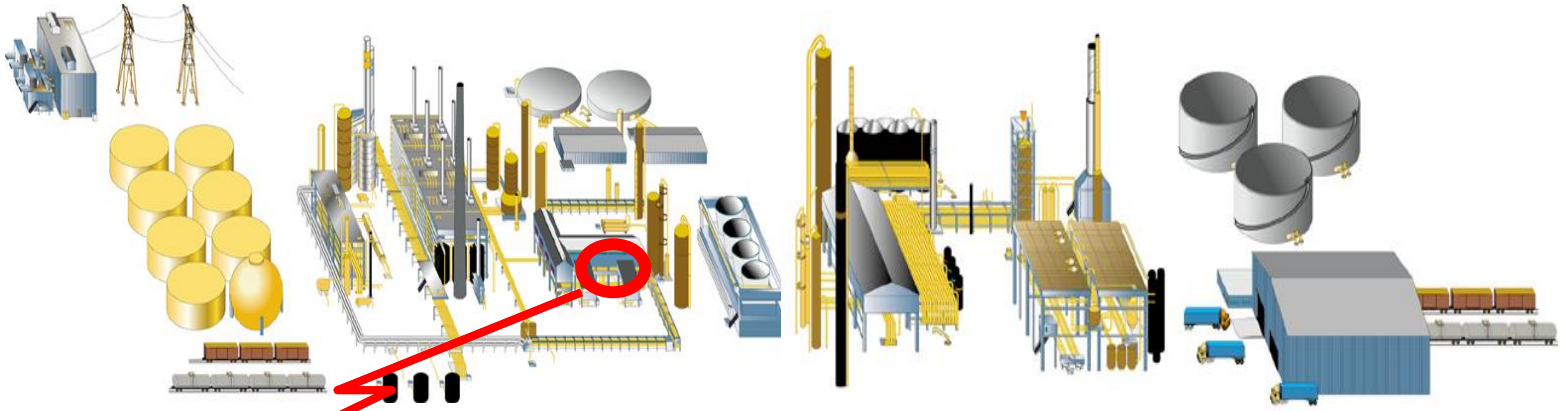
YATEC 安華機電

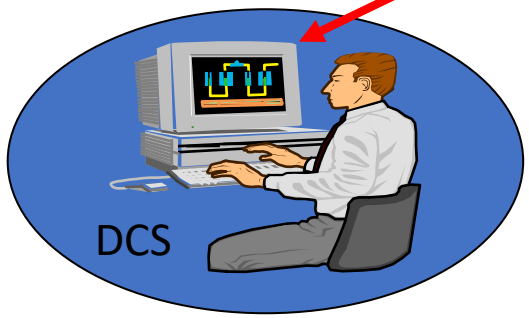
話說..控制室內是與世隔絕的世界



YATEC 安華機電

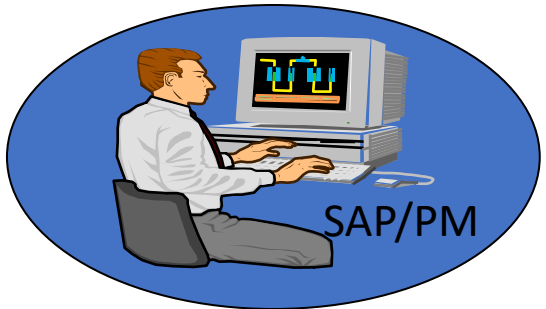
由儉入奢易....





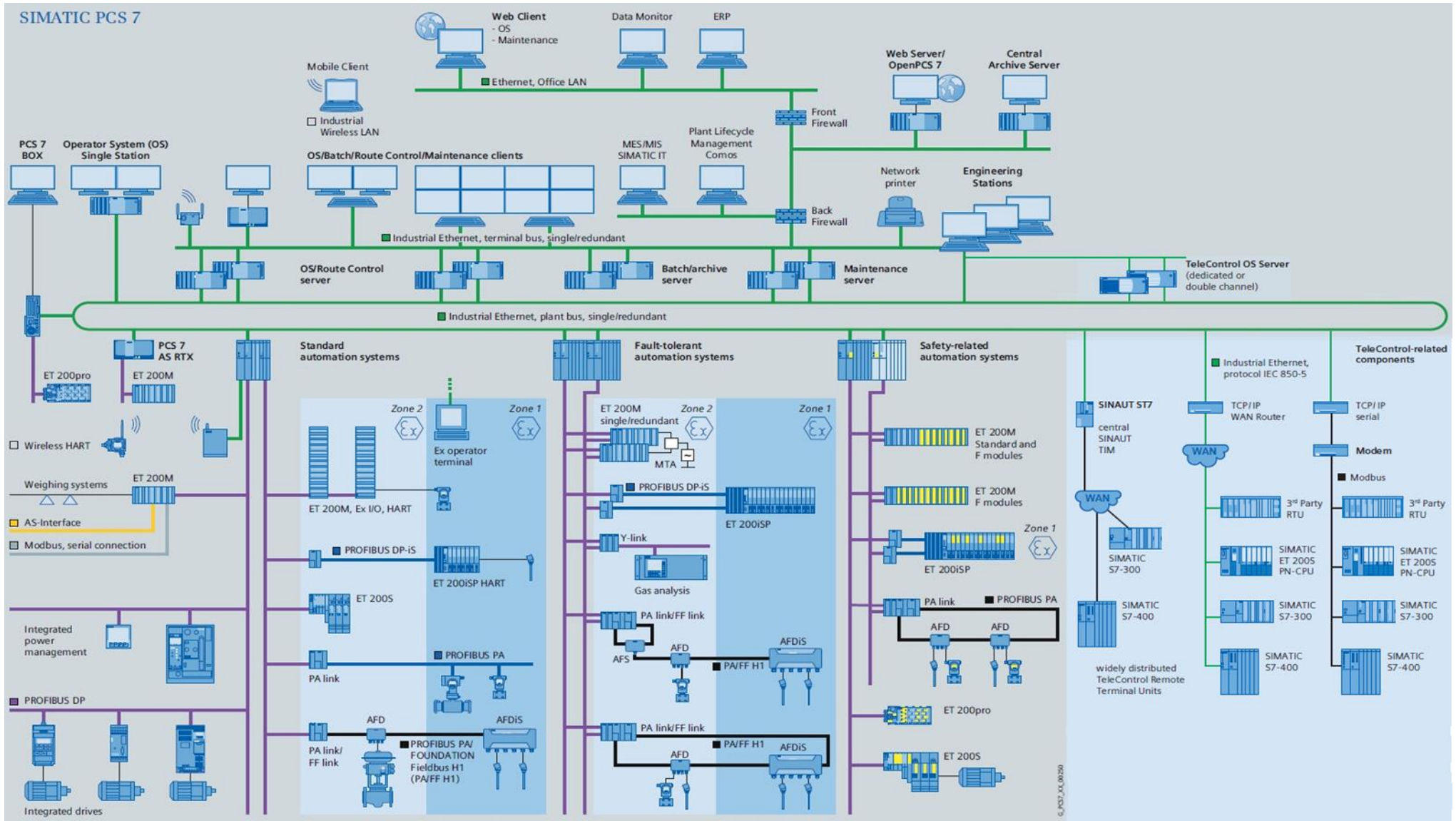
控制系統的便利..... >工業 4.0

自動化與更多的資料處理是一條不歸路



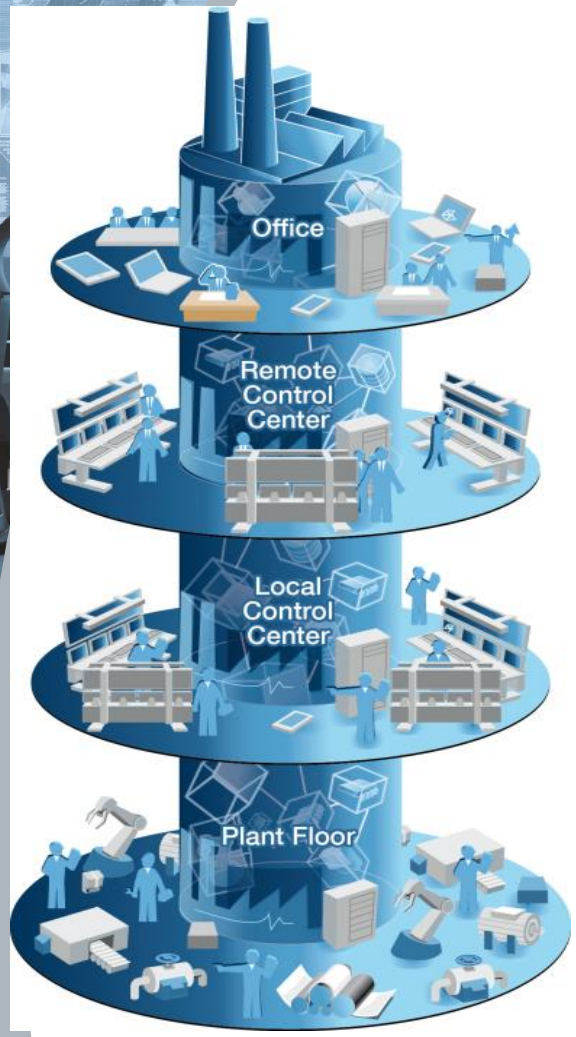
YATEC 安華機電

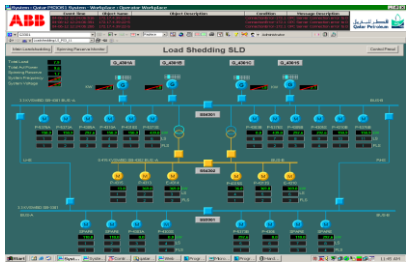
這樣的系統如何封閉?

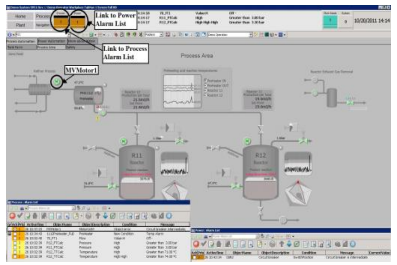


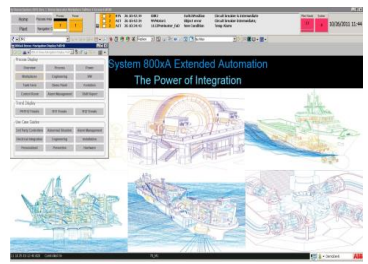
YATEC 安華機電

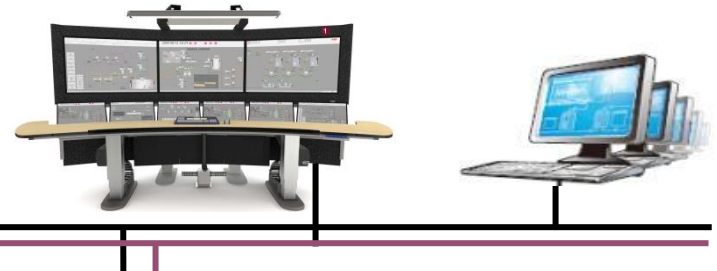
這樣的系統如何封閉?



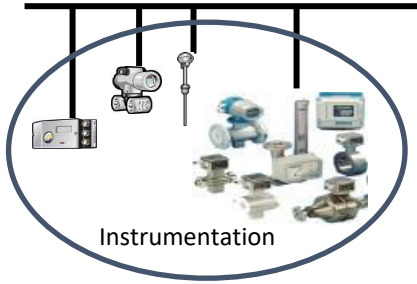


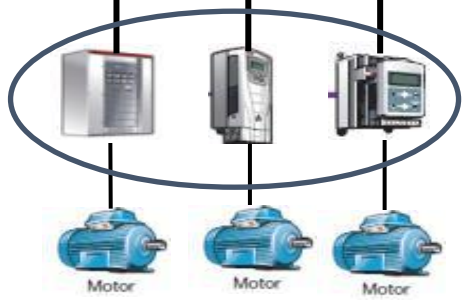






HART COMMUNICATION PROTOCOL
PROFIBUS
Fieldbus Foundation
PROFINET
IEC



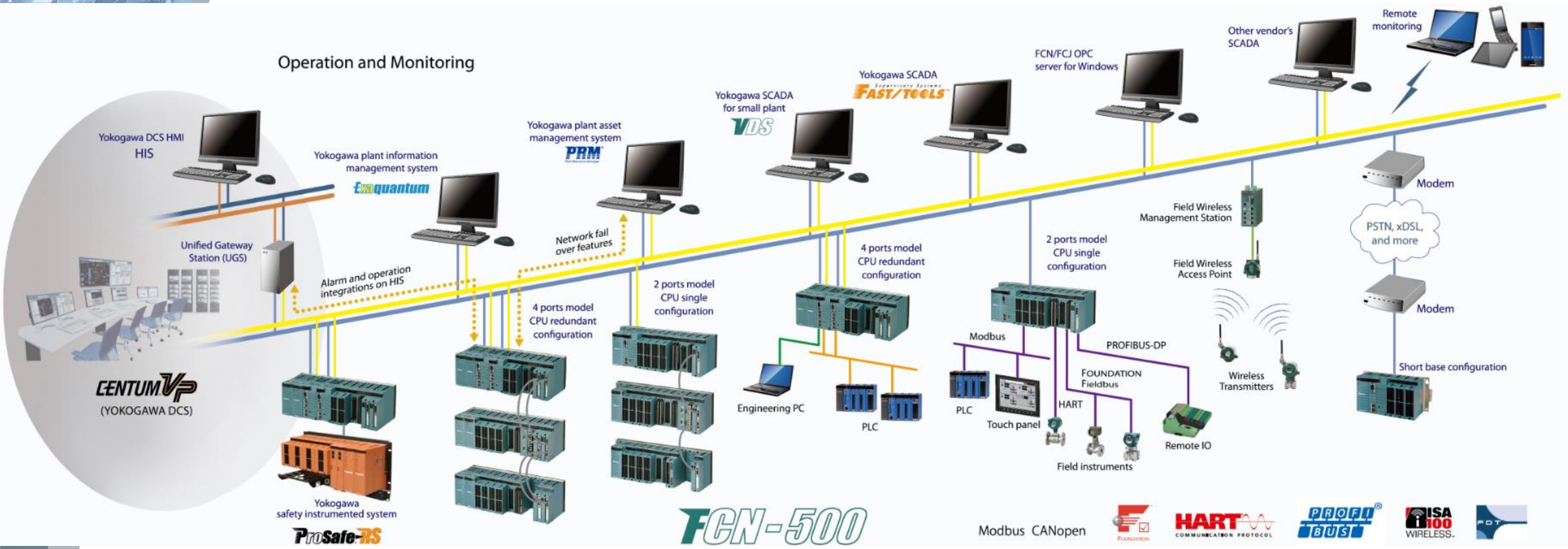


LV Switchgear
Drives
Motor
starters

Protection
& Control
IEDs

YATEC 安華機電

這樣的系統如何封閉?



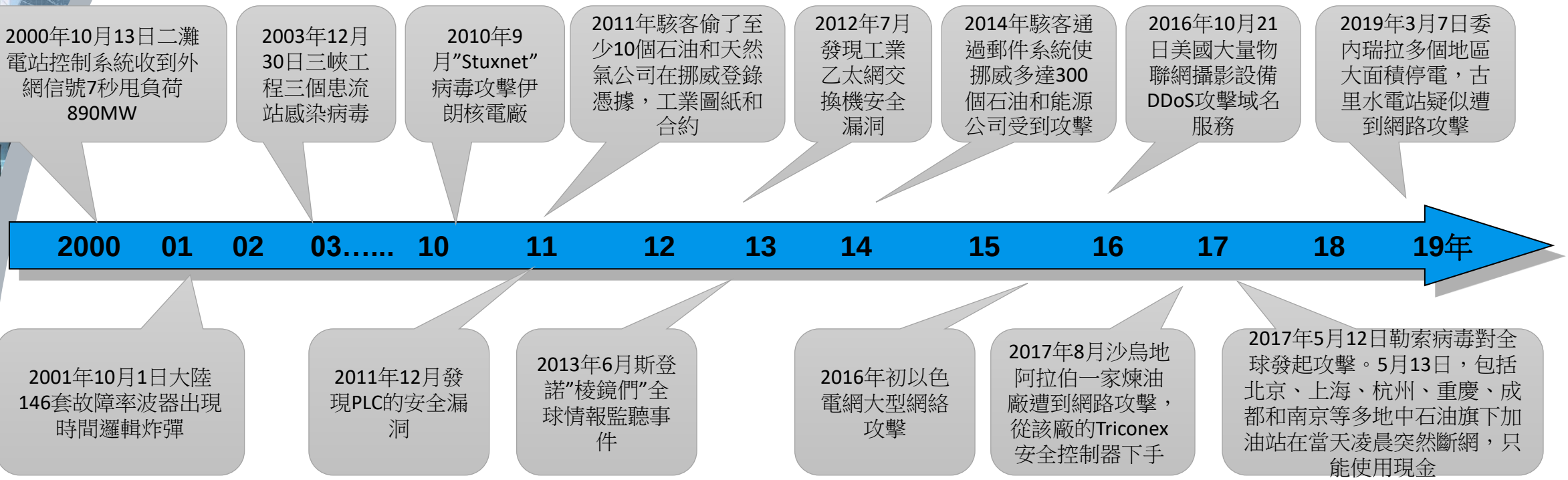
YATEC 安華機電

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……

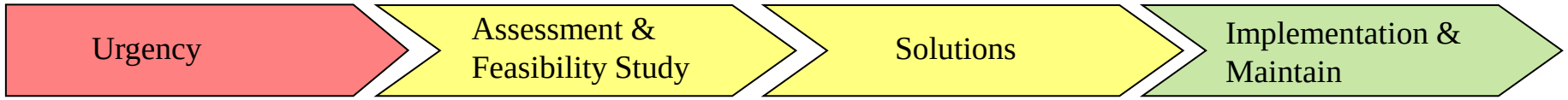
YATEC 安華機電

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。

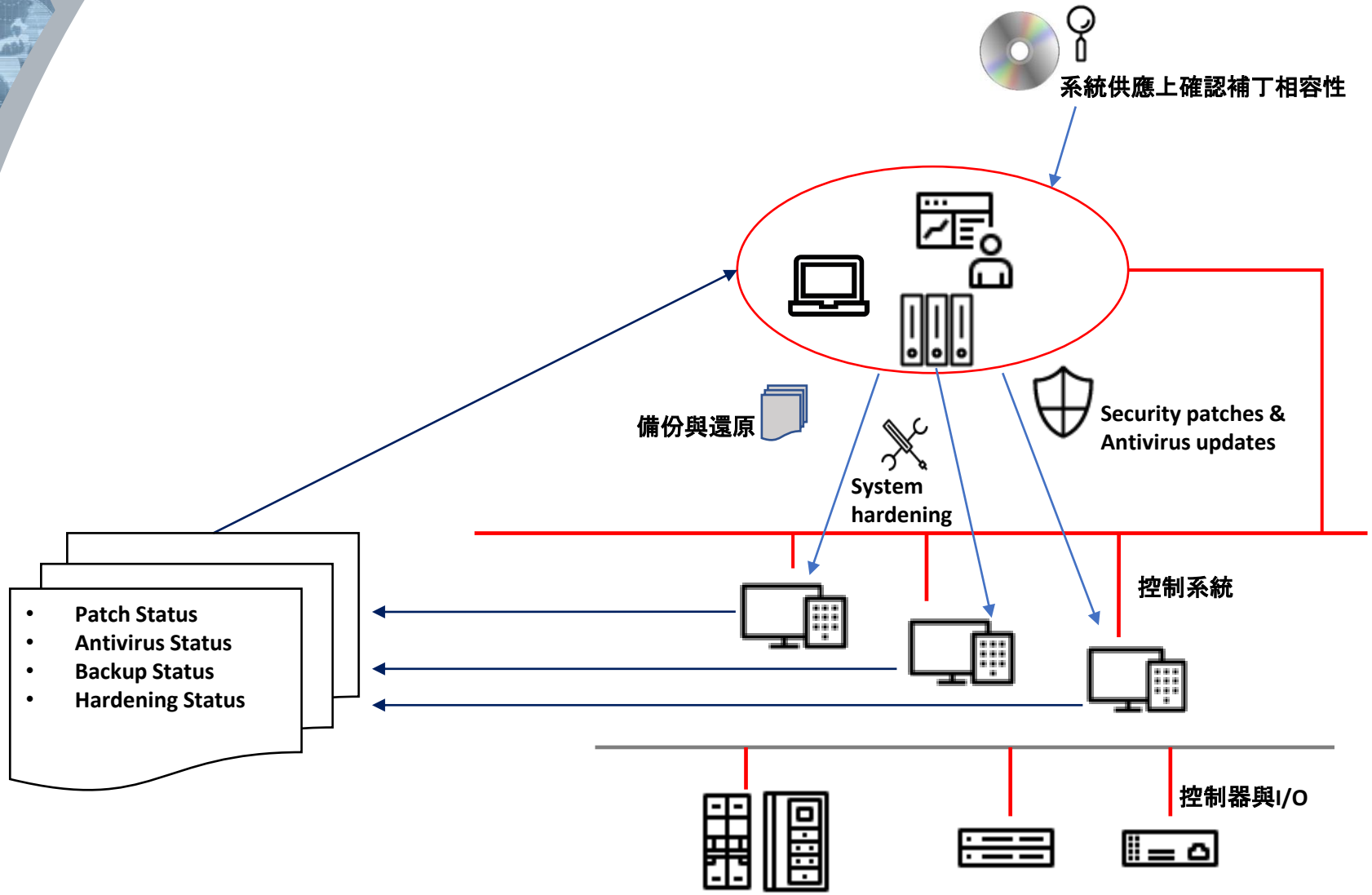
- 有鍵於網路攻擊事件日益頻繁，中電集團高層非常重視，特別是香港對於用電穩定之要求極高，故由董事會直接要求執行資安管理措施，並在2016底完成佈署。其中聘請外部顧問Digital Bond (CLP's cyber security consultant)進行現有系統狀況稽核，並給出建議，在很短的時間下，由ABB建置完成Cyber Security管理架構，同時由ABB及GE分別對自家系統進行升級及必要之補強，以符合Cyber Security要求，全案於2016年底如期完成，並於2017/1交付使用。

Security Assessment

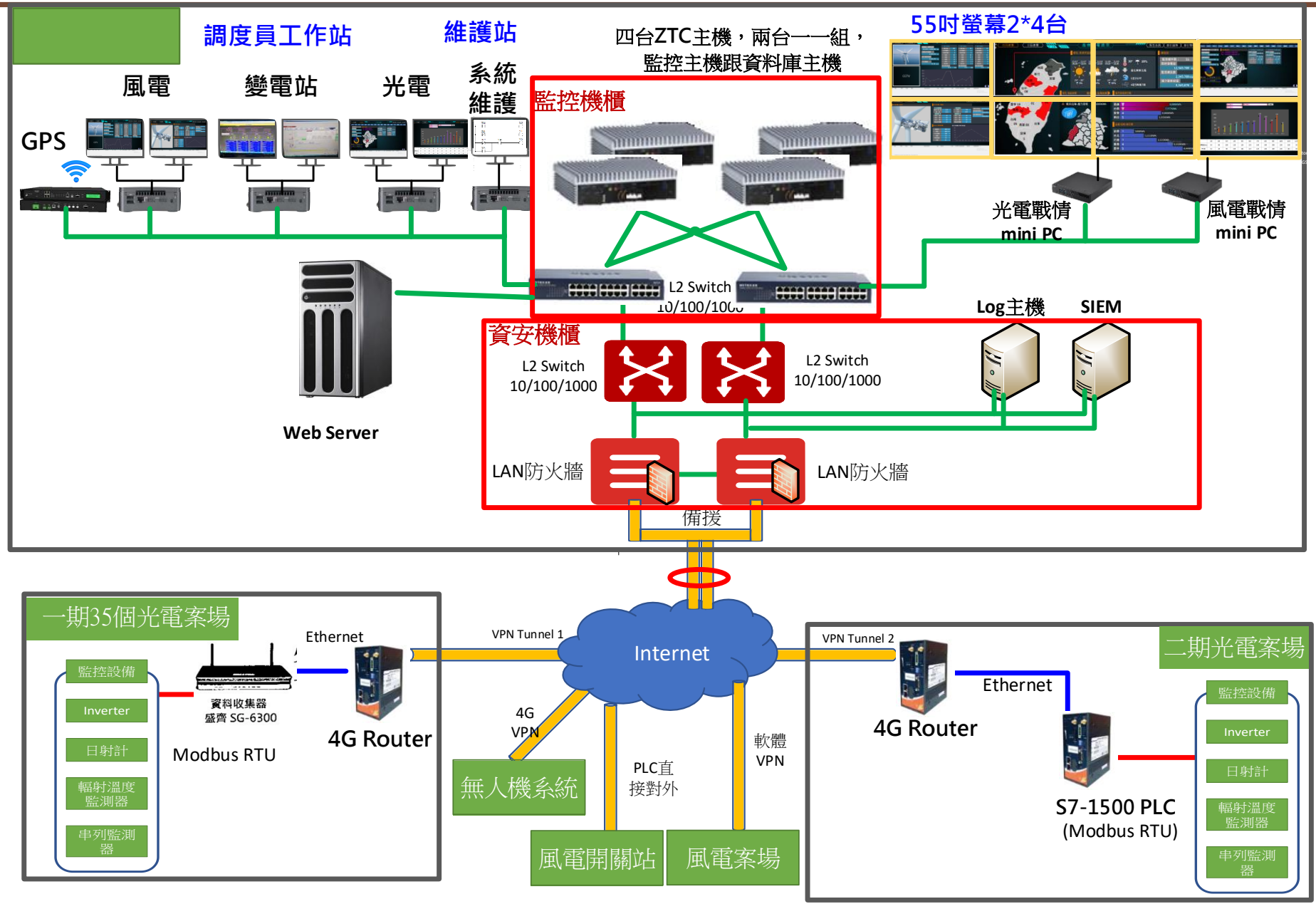
TABLE OF CONTENTS

YATEC 安華機電

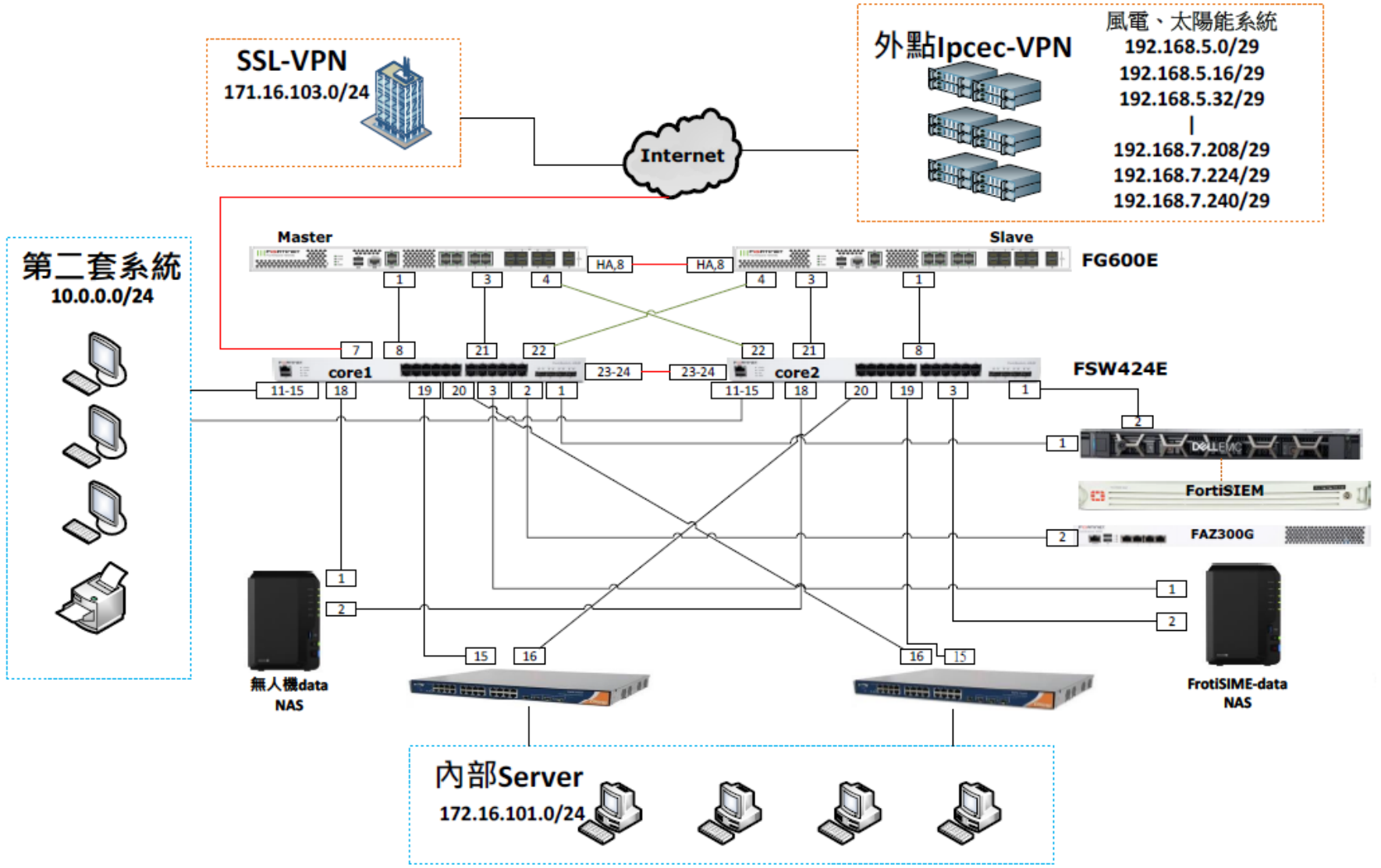
甚麼是對的策略?



新能源監控中心應用實例

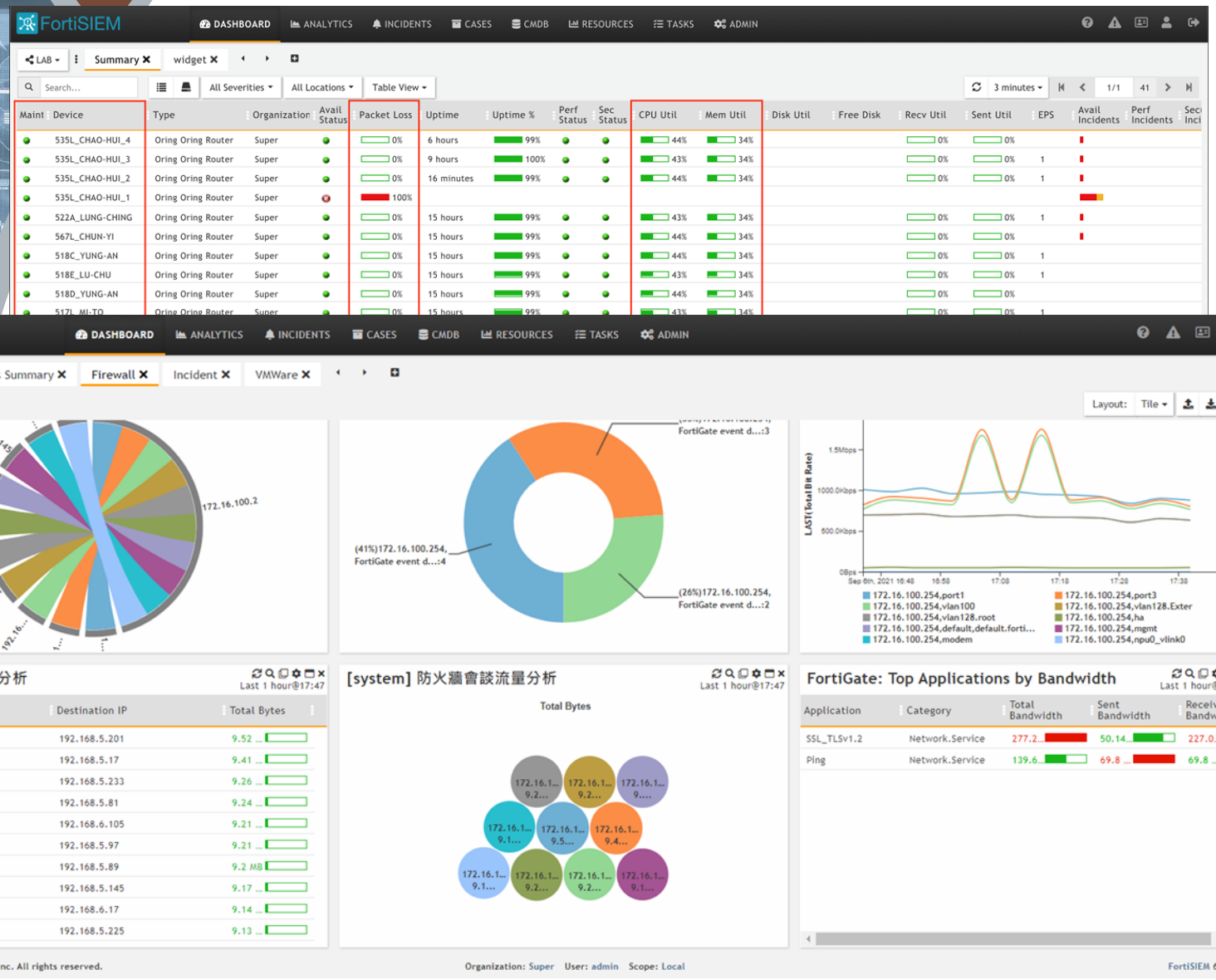


FortiSIEM/FortiGate/Fortianalyzer



YATEC 安華機電

FortiSIEM



- 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。

YATEC 安華機電

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
  - ….

FORTINET

敬請指教

YATEC
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

Secure OT Summit 2022

護航 OT/IT 融合 創新數位發展