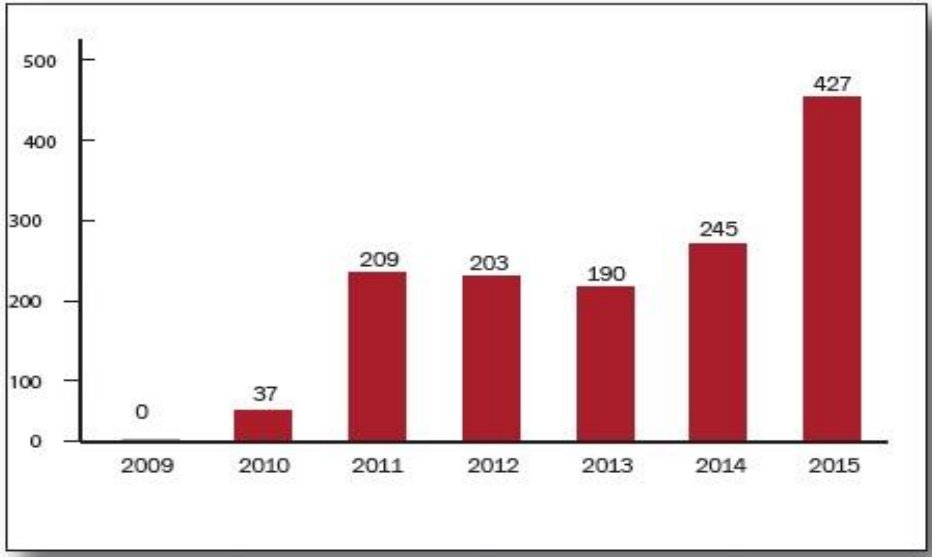
Defence and Resilience Strategies to counter cybersecurity threats to the Power Generation Sector

SIEW 2016
NEW ENERGY REALITIES
24 - 28 October 2016
Marina Bay Sands

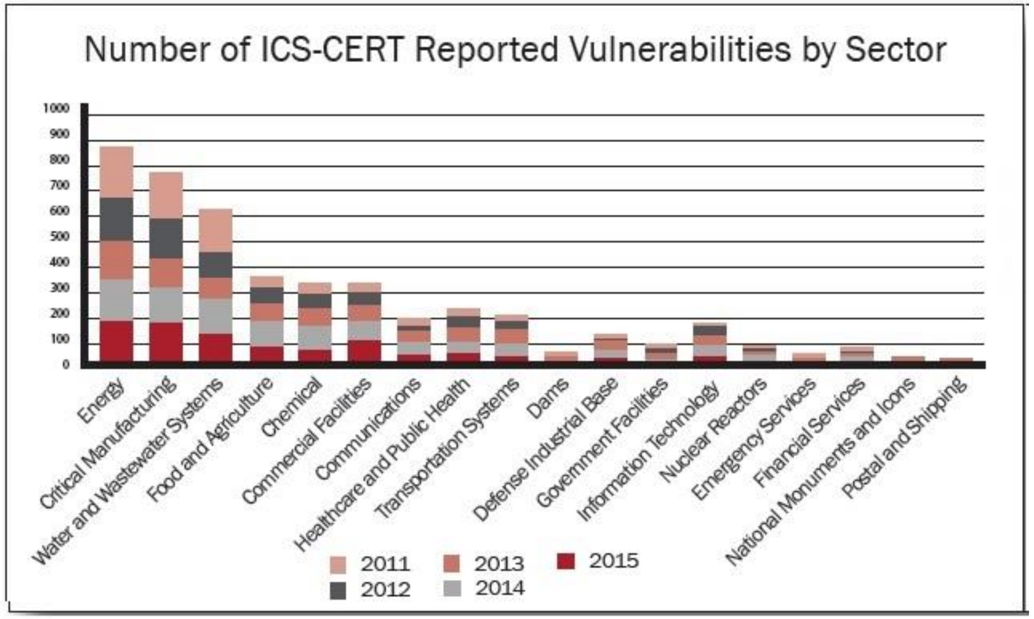
Roundtable I
28 October 2016

Ngai Chee Ban *CISSP*
Honeywell Industrial Cyber Security
Honeywell

ICS-CERT 2015 Vulnerability Report



Number of industrial control systems (ICS) vulnerabilities reported (2009-2015)



Number of ICS vulnerabilities reported in products used in critical sectors (2011-2015)

Source: NCCIC/ICS-CERT 2015 Annual Vulnerability Coordination Report

India Power Grid Failure, July 2012

THE TIMES OF INDIA

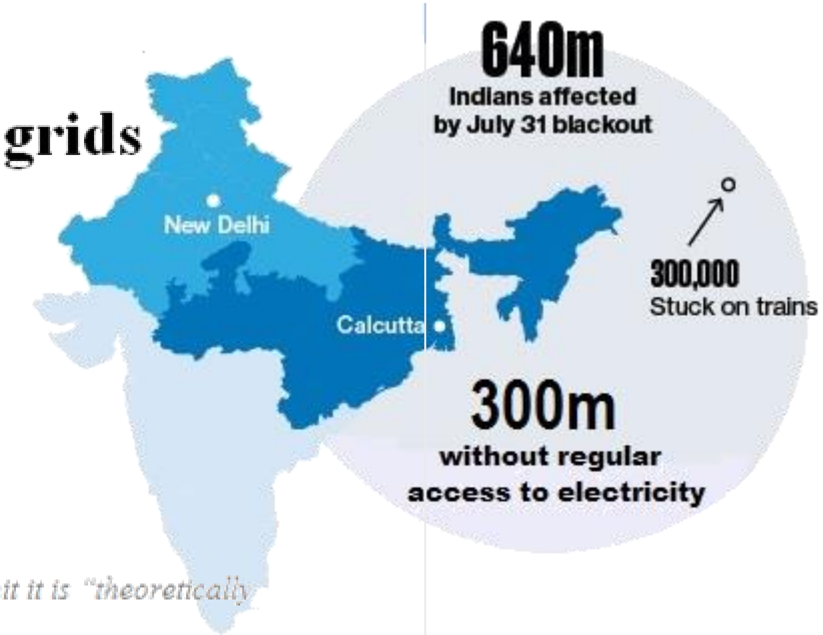
Hackers can cripple India’s power grids

Officials who carried out an audit of critical information infrastructure admit it is “theoretically possible” to cripple India’s power grids through a cyber-attack.

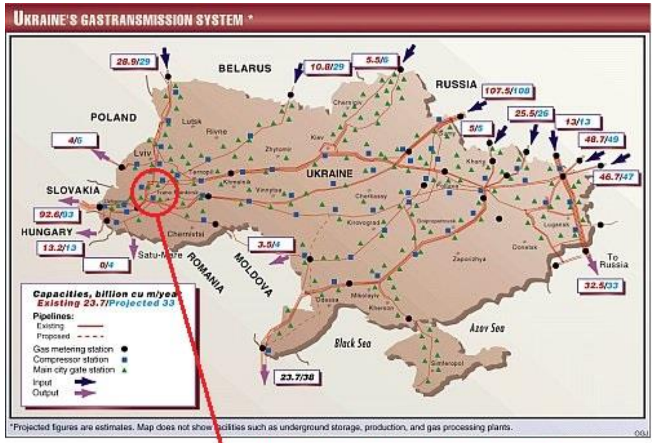
NEW DELHI: It is possible for an adversary or a group of hackers to cripple India's power grids through a cyber-attack, although this is an unlikely reason for the recent power outages that crippled much of north, east and north-eastern India.

Since the first power trip up on Monday, there have been discussions within the security establishment about the possibility of entities trying to carry out a sophisticated cyber-attack to cripple the grids.

Officials who carried out an audit of critical information infrastructure admit it is "theoretically possible" to cripple India's power grids through a cyber-attack.


640m
Indians affected by July 31 blackout
New Delhi
Calcutta
300,000
Stuck on trains
300m
without regular access to electricity

Ukraine Power Grid Attacked, 23 December 2015



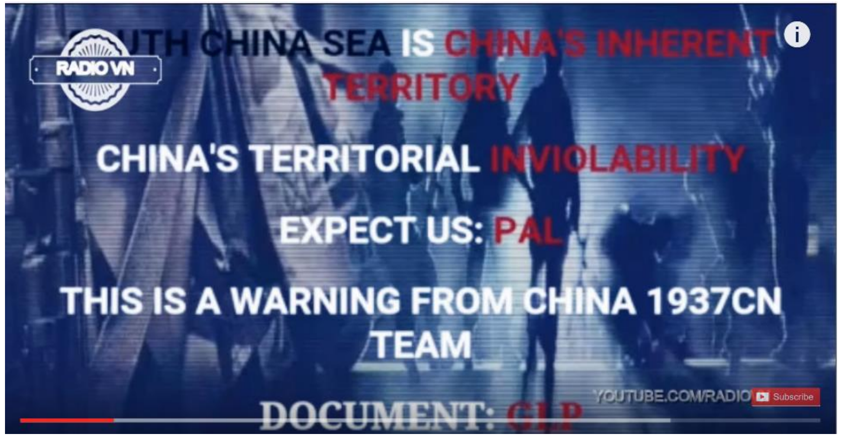
*Projected figures are estimates. Map does not show facilities such as underground storage, production, and gas processing plants.

Location of power system outage

- Remote cyber intrusions at three regional electric power distribution companies.
- More than 220,000 customers/ households affected.
- Malwares "BlackEnergy" & "KillDisk" were found. HMIs in remote terminal units were infected.

Closer to Home: Vietnam, 29 July 2016

Noi Bai & Tan Son Nhat International Airports were affected.



UTH CHINA SEA IS CHINA'S INHERENT TERRITORY

CHINA'S TERRITORIAL INVIOLABILITY

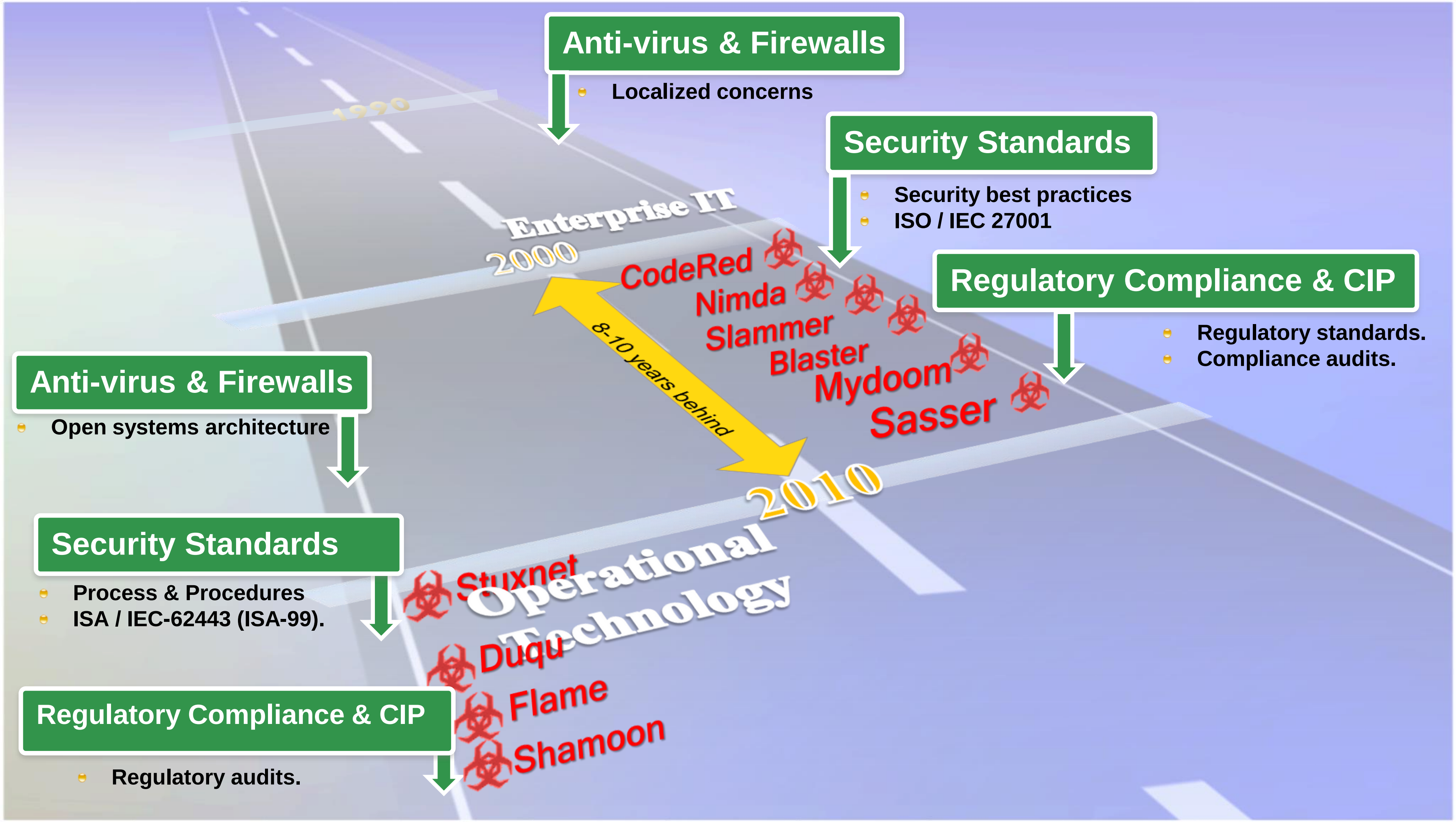
EXPECT US: PAL

THIS IS A WARNING FROM CHINA 1937CN TEAM

DOCUMENT: GLP

Vietnam Airlines' client & flight information screens were attacked.

Industrial's Operations Technology 8-10 years behind Enterprise IT



Anti-virus & Firewalls

- Localized concerns

Security Standards

- Security best practices
- ISO / IEC 27001

Regulatory Compliance & CIP

- Regulatory standards.
- Compliance audits.

Anti-virus & Firewalls

- Open systems architecture

Security Standards

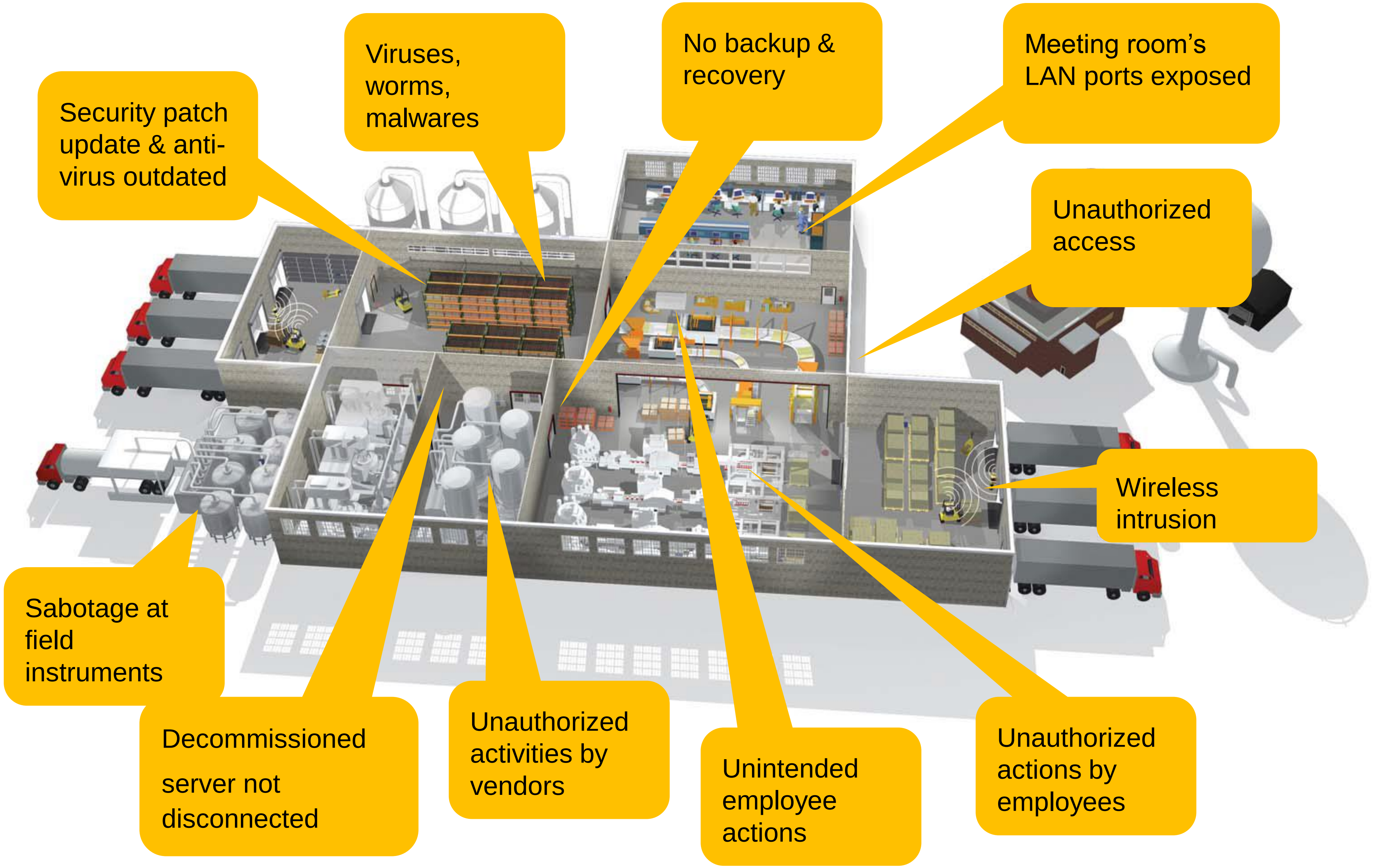
- Process & Procedures
- ISA / IEC-62443 (ISA-99).

Regulatory Compliance & CIP

- Regulatory audits.

Operational technology (OT) is hardware and software for direct monitoring & control of electro-mechanical systems especially in the industrial processes.

Common cyber security weaknesses at industrial sites



Security patch update & anti-virus outdated

Viruses, worms, malwares

No backup & recovery

Meeting room's LAN ports exposed

Unauthorized access

Wireless intrusion

Sabotage at field instruments

Decommissioned

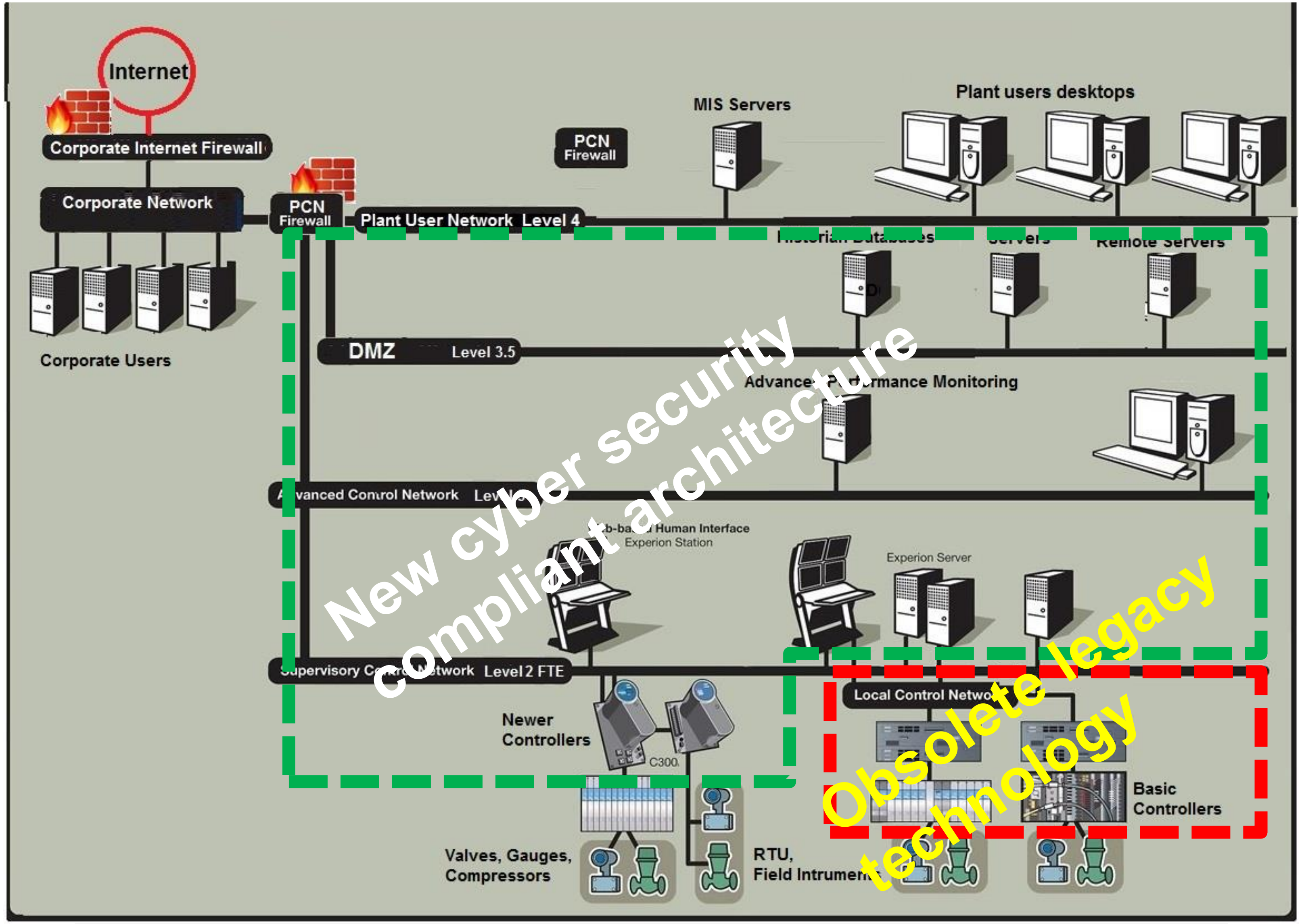
server not disconnected

Unauthorized activities by vendors

Unintended employee actions

Unauthorized actions by employees

Most Industrial Control Systems' network


Internet
Corporate Internet Firewall
Corporate Network
Corporate Users
PCN Firewall
PCN Firewall
Plant User Network Level 4
MIS Servers
Plant users desktops
Historian Databases
Servers
Remote Servers
DMZ Level 3.5
Advanced Performance Monitoring
Advanced Control Network Level 3
Web-based Human Interface
Experion Station
Experion Server
Supervisory Control Network Level 2 FTE
Newer Controllers
C300
Local Control Network
Basic Controllers
Valves, Gauges, Compressors
RTU, Field Intruments
New cyber security compliant architecture
Obsolete legacy technology

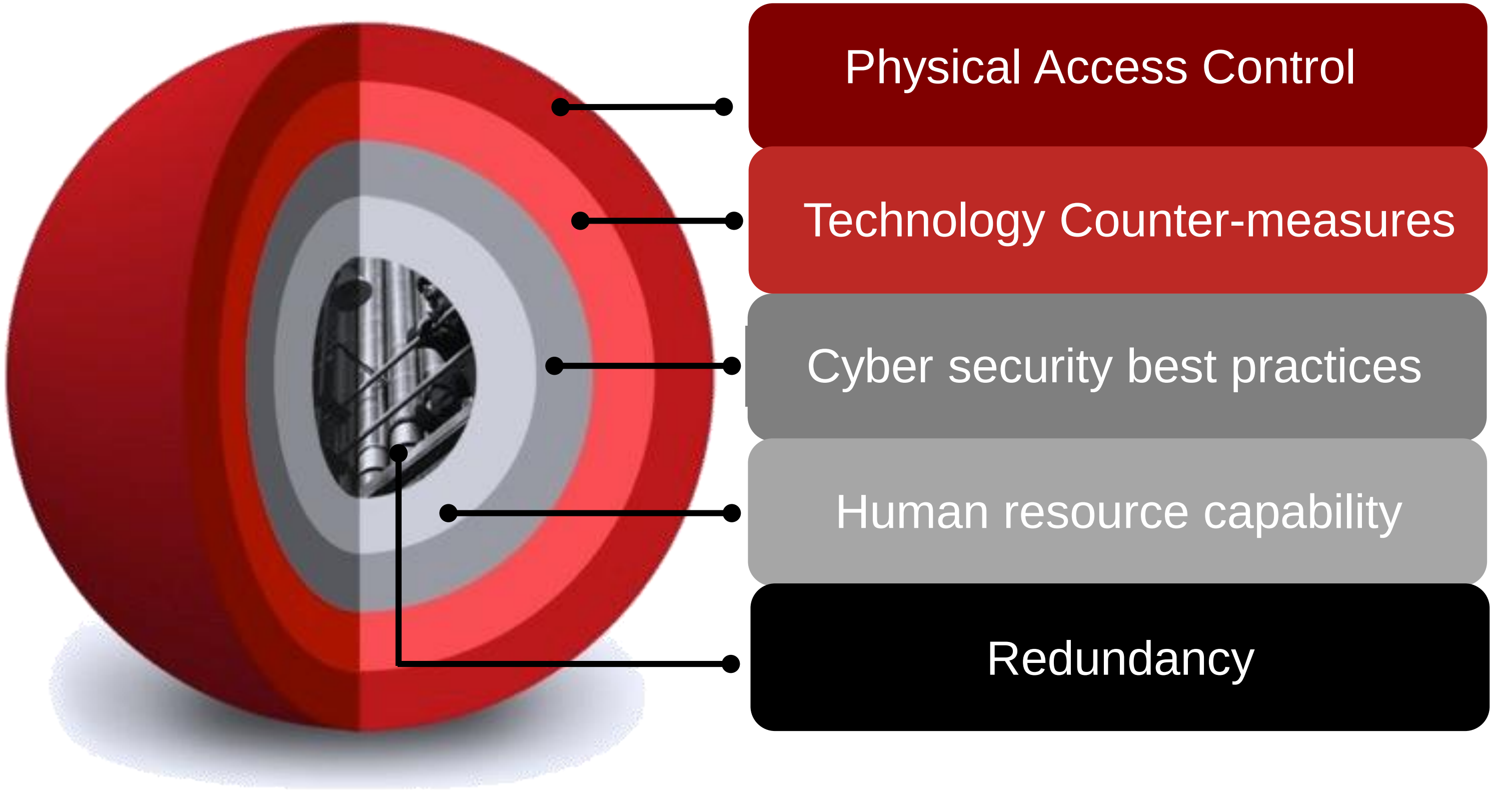
Legacy systems co-existing with new open systems – a Cyber Nightmare

Industrial’s OT Perspective on Resilience

- Japan’s Tohoku Quake, March 2011.
- Ensuing tsunami (6-7m), Refineries flooded (3m).
- Field instruments & RTU submerged, piping leakage & storage tanks burned down. DCS & HMIs totally inundated.
- Resilience in different perspective:-
  - Systems: Virtualization.
  - Process Controls: Automation & Remote Processes
  - Human resource: Remote operations.
  - Heavy machineries, Instrumentations: Supply chain for reconstruction.
  - Business resumption (Recovery Time Objective, RTO) ≥ 10 months.

Cyber Defence vs. Resilience

Cyber protection in ICS is an Eco-system



Physical Access Control

Technology Counter-measures

Cyber security best practices

Human resource capability

Redundancy

Is there another way to look at it?

Conclusions

1. Operational technology (OT) is the technology enabler for the power sector.

2. Recognise fundamental OT vs IT differences:-
   - OT lags IT between 8 - 10 years.
   - While digitization expands, hardware still dominant.
   - Co-existence of legacy technology & new open-architecture systems.
   - OT requires different treatment.

3. Eco-system of cyber threats:-
   - Upstream & downstream vulnerabilities.
   - Human aspect – technology usage maturity.
   - Resource perspective – aging engineers & attritions.
   - Cyber attack - Geo-political factors.

4. Cyber Defence vs. Resilience: is there another way to look at it?

Thank you

Chee Ban Ngai
Industrial Cyber Security, Leader, Asia Pacific
phone: +603 7958 8922
cell: +6012 233 0915
cheeban.ngai@honeywell.com

Follow us:
Blog: http://insecurity.honeywellprocess.com
Website: http://www.honeywellprocess.com
Website: http://www.becybersecure.com