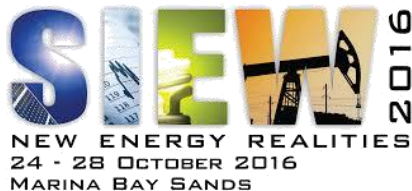


Defence and Resilience Strategies to counter cybersecurity threats to the Power Generation Sector



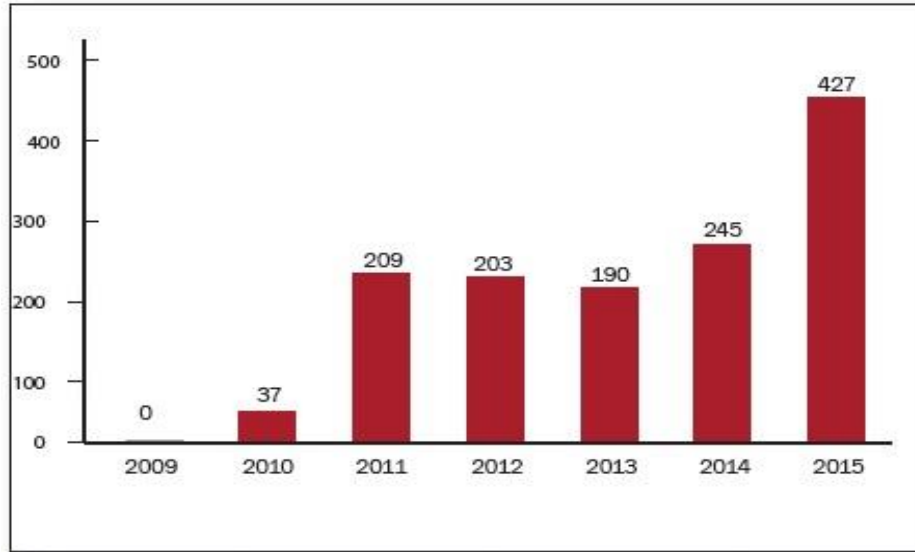
Roundtable I
28 October 2016

Ngai Chee Ban *CISSP*

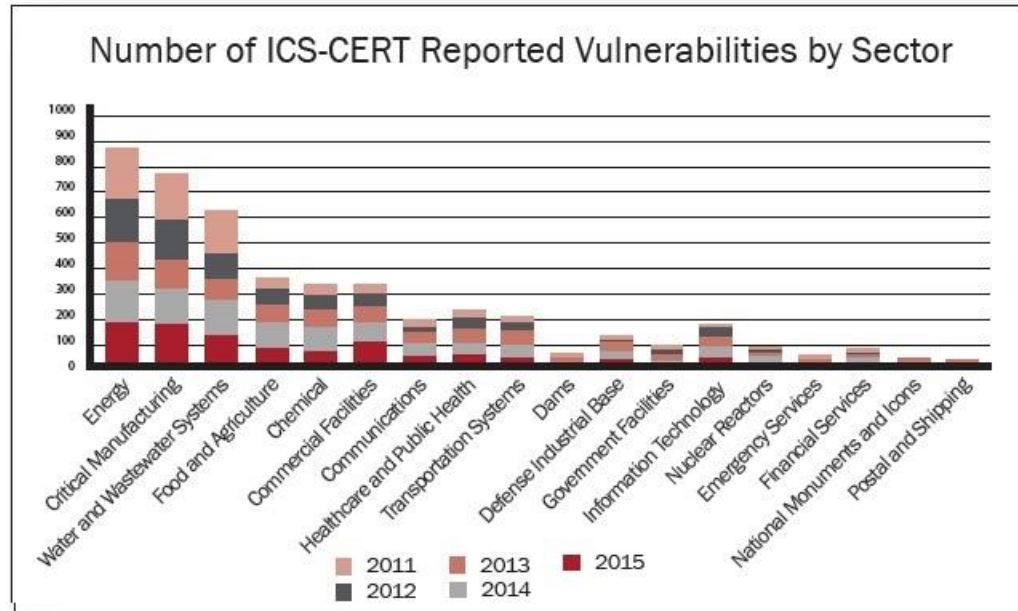
Honeywell Industrial Cyber Security

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

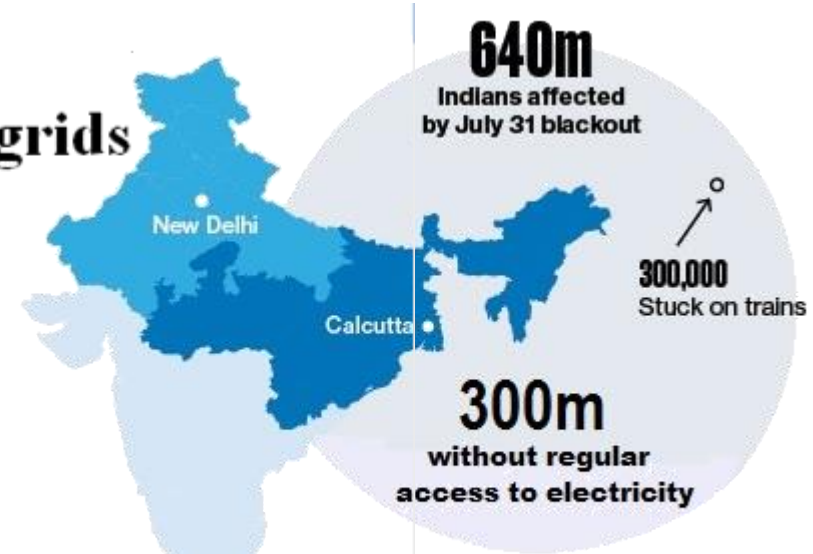


Officials who carried out an audit of critical information infrastructure admit it is "theoretically possible" to cripple India's power grids through a cyber-attack.

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.

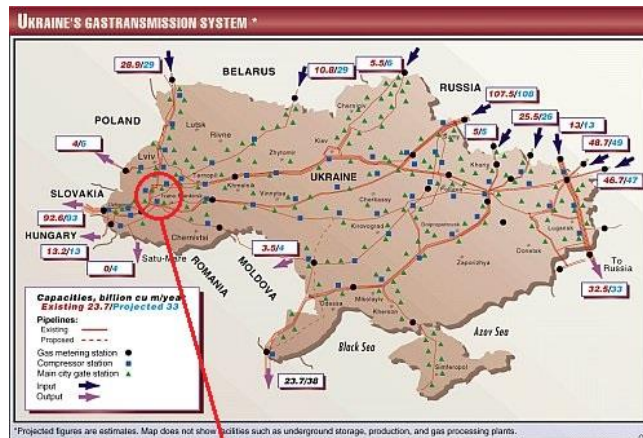
Officials who carried out an audit of critical information infrastructure admit it is "theoretically possible" to cripple India's power grids through a cyber-attack.



Ukraine Power Grid Attacked, 23 December 2015



- 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.



Location of power system outage

Closer to Home: Vietnam, 29 July 2016



Noi Bai & Tan Son Nhat International Airports were affected.



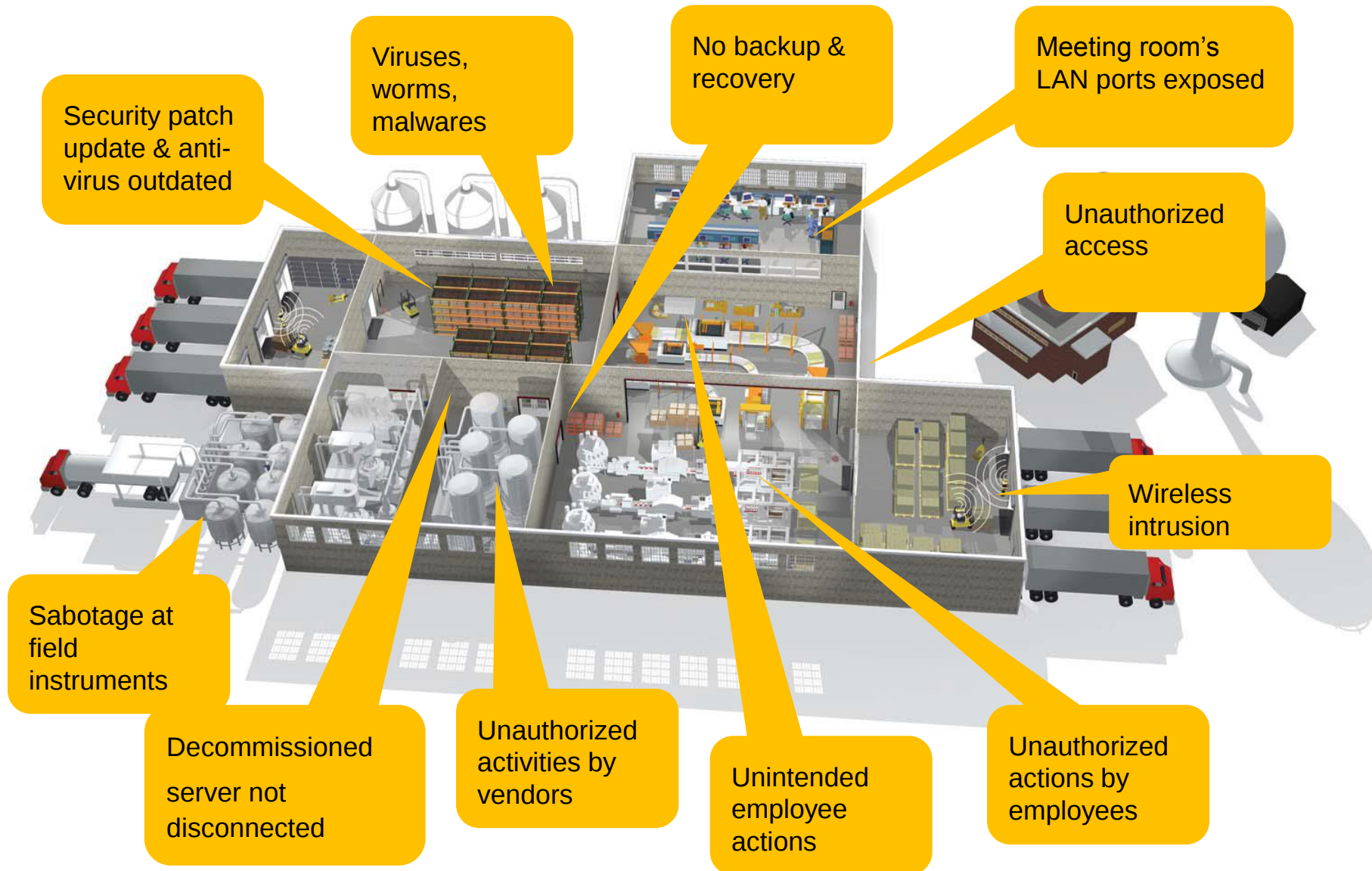
Vietnam Airlines' client & flight information screens were attacked.

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

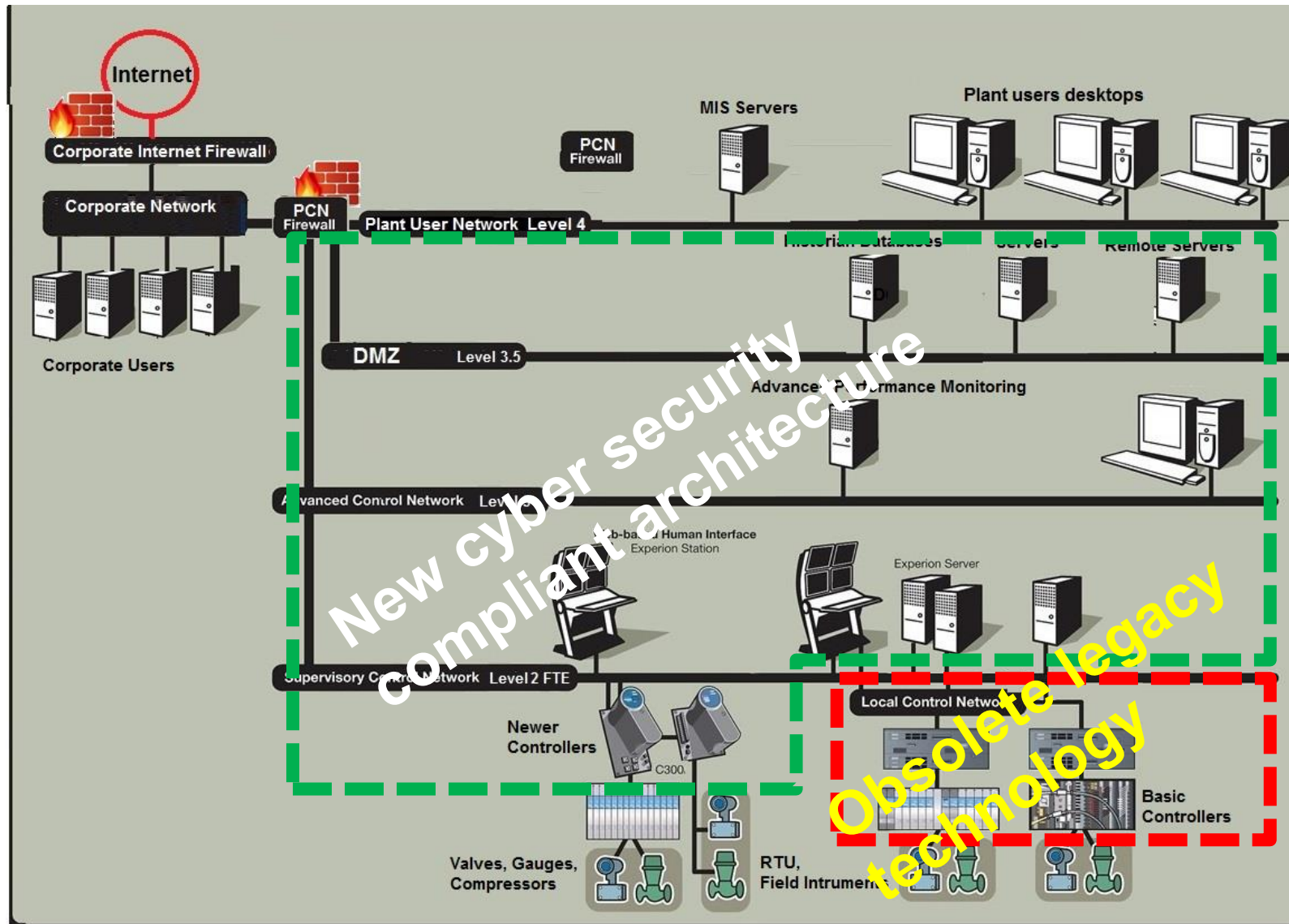


Operational technology (OT) is hardware and software for direct monitoring & control of electro-mechanical systems especially in the industrial processes.

Common cyber security weaknesses at industrial sites



Most Industrial Control Systems' network



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

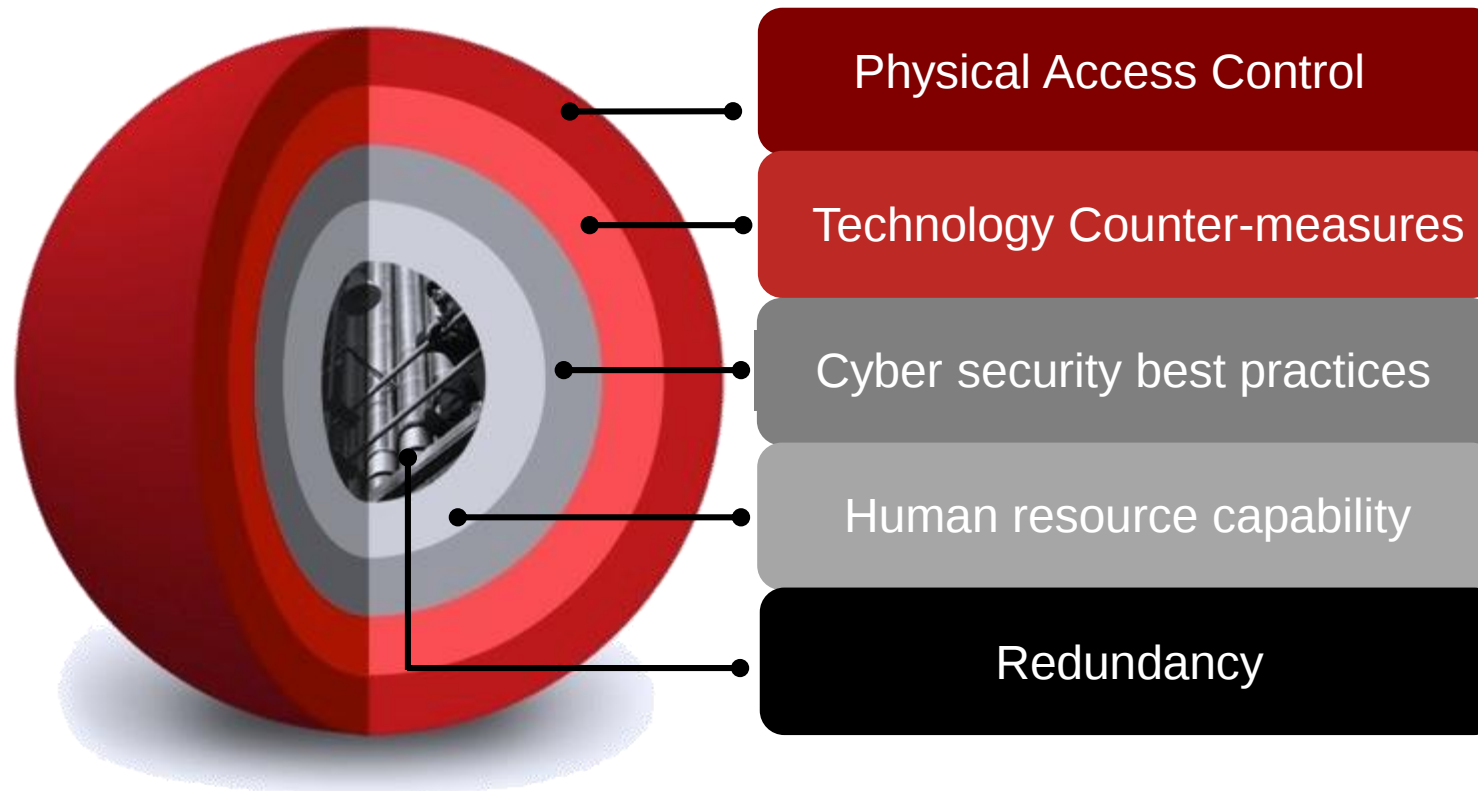
Industrial's OT Perspective on Resilience



- 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



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>

