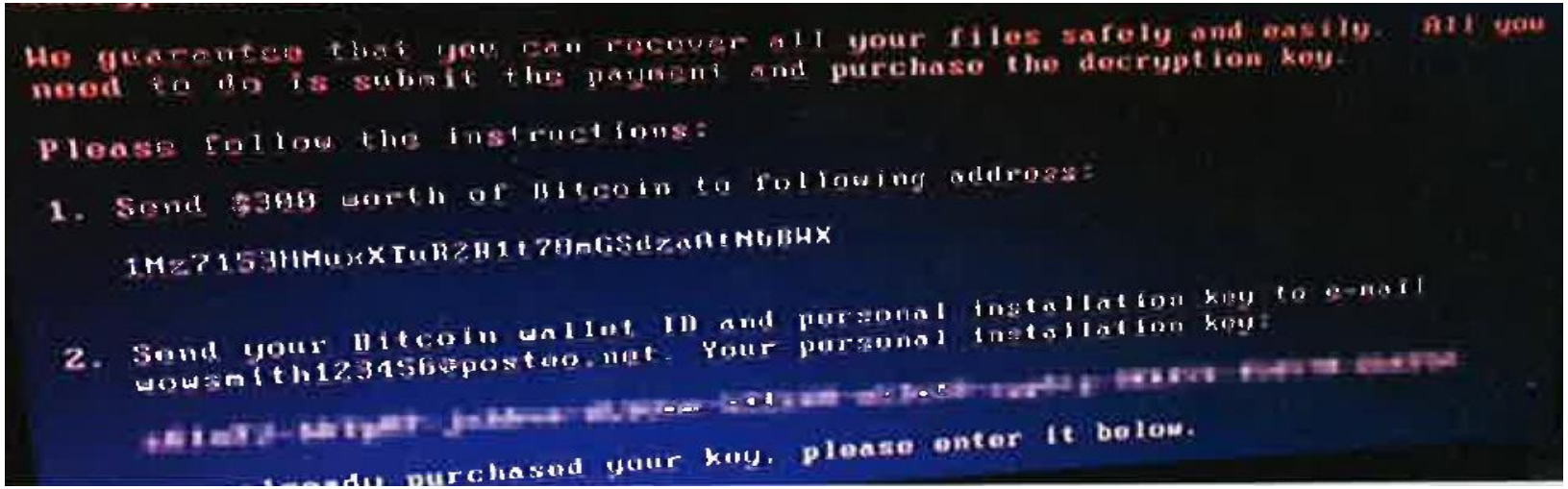
Health and Safety
Executive

HSE

Cybersecurity- Understanding and Managing risk

NEPIC March 2019

Sarabjit Purewal

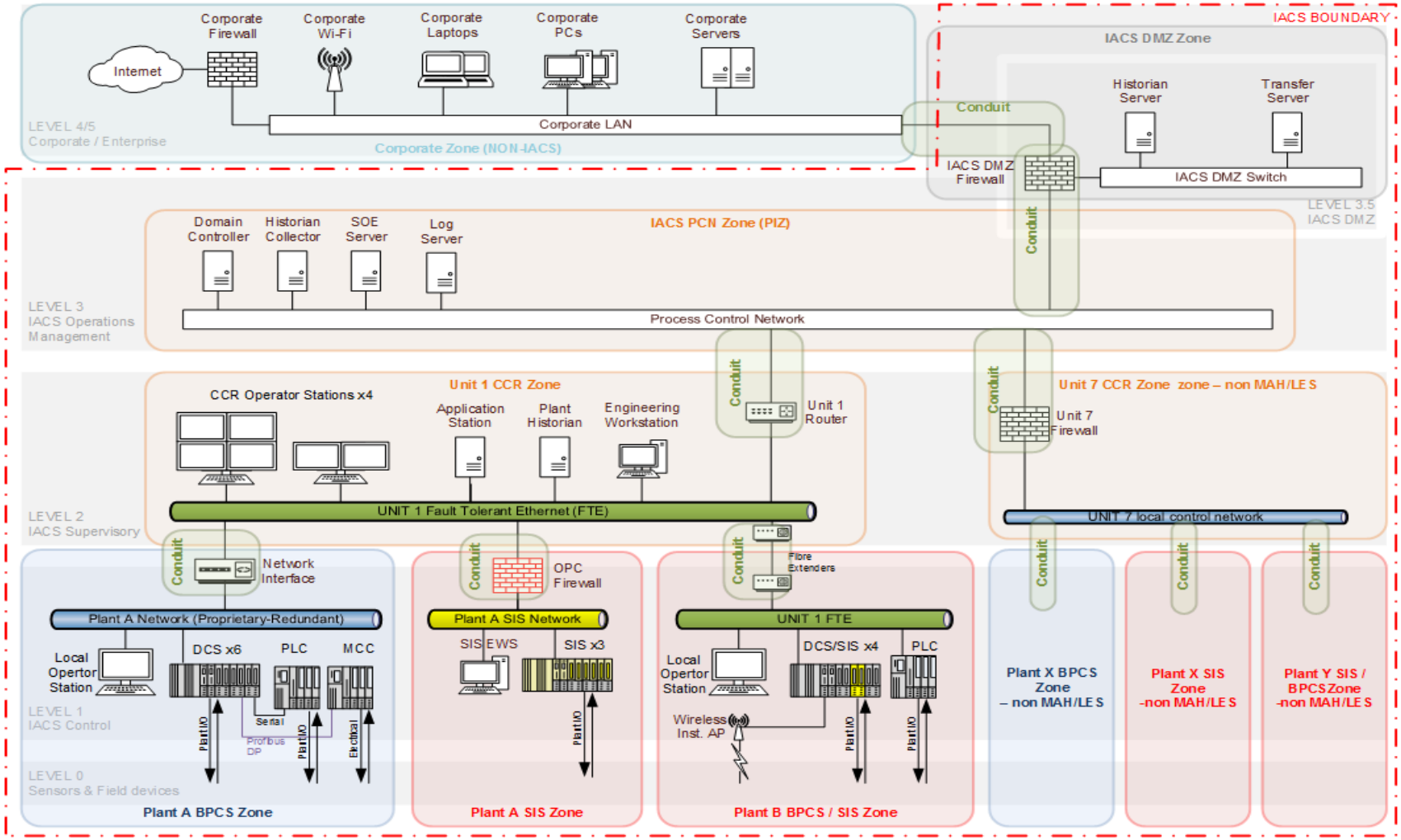


HSEs role in H&S - Independent public assurance

Why cybersecurity is a risk
Technology

- Increased use of programmable systems
- Convergence of technologies used for industrial automation control systems (IACS) and IT systems – OS, network protocols etc.
- Not just plant control systems – also power management, utilities, building management, phones (VoIP) etc.
- Also management systems – e-Permits, e-Procedures…
- Increased connectivity between industrial control systems and business systems and ‘the cloud’ (internet, remote access, cloud services)
- Much greater potential attack space

A Typical Network Diagram



Why cybersecurity is a risk Increased likelihood?

- Increased capability – state actors and criminals
- Availability of hacking hardware and software ‘toolkits’ and coordination – reduced entry level
- Social engineering techniques / Spear phishing
- Average time to detect intrusion into your corporate network is months.
- State, cybercriminals, malicious insiders, hacktivists, terrorists

Ransomware attack hits Chernobyl, Cadbury, Maersk

RADIATION monitoring systems at the Chernobyl nuclear plant were put out of action by a ransomware attack which began in Ukraine on 27 June and hit companies around the world.

Chernobyl workers had to manually monitor radiation after the cyberattack knocked out the operation's Windows-based systems.

The attack, a modified form of existing *Petya* ransomware, dubbed by some security firms as *NotPetya* or *Nyetna* to distinguish it, was first reported in Ukraine. It spread around Russia, Europe and Australia affecting firms including Rosneft, Merck, Reckitt Benckiser and Beiersdorf.

Victims were told they must pay US$300 in Bitcoin to recover their encrypted files.

The Maersk Group said IT systems went down across its business units including its oil and drilling activities, though they were "not operationally affected", while local news in Australia reported that computers at a Cadbury factory in Hobart owned by Mondelez were displaying messages demanding payments to release files.

There is no clear indication of who was behind the latest attack.

The Chemical Engineer (July / August 2017)

Threat Landscape NCSC latest summary for chemical sector

- Lack of investment leading to increasing vulnerabilities
- Links between IACS and corporate networks is growing
- Threat level is growing
- State actors likely to be the greatest threat

Attack highlights

- 2010 Stuxnet
- 2012 Saudi Aramco. Shamoon
- 2013 Blue Termite. Targets Japanese industries including chemical sector
- 2014 South Korean nuclear operators hacked.
- 2015 Black Energy. Disrupting energy distribution company in Ukraine.

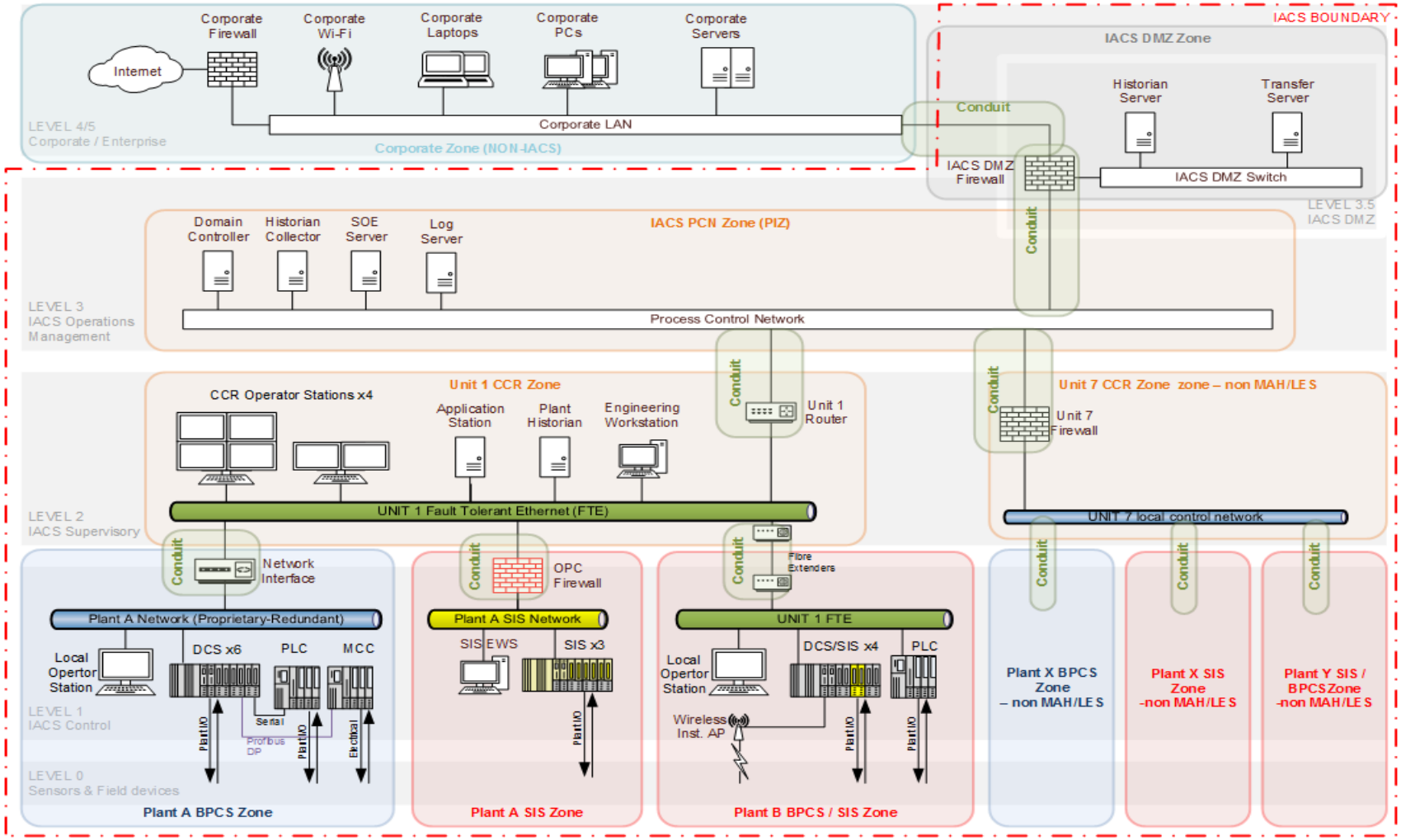
Attack highlights

- 2016 Industroyer. Interrupting part of Ukraine power supply system
- 2017. A chemical company major attack using Shamoon 2
- 2017. TRITON. Compromises petrochemical plant safety system
- 2018. UK Chemical company reports malware incident.

First Step- Do you understand the risk

- Traditional design concepts based upon independent layers of protection, i.e. the likelihood of all the protection layers failing at the same time is very low.
- Risk assessments didn’t consider multiple failings or malicious intent as credible.
- In reality, we know that accidents are more often due to common cause or systemic failures (inadequate functional safety management, competence leading to human error)
- Cyber attack (intentional or otherwise) is another potential common cause failure.
- Risk=Likelihood*Consequence. Determining likelihood is a problem!
- Risk assessment approaches developing. HSE taking a simple approach aligned with IEC 62443. Vulnerability and consequence.

A Typical Network Diagram



Managing Risk

- People
- Processes
- Technology

People

- Are people the weakest link
- Designing around human capability
- Training and competency
- Vetting
- Social engineering

People

- Staff responsible for safety systems should be competent in discharging their responsibilities.
- There is a need to upskill engineers responsible for managing Industrial Automation & Control Systems in cybersecurity.
- IT and OT often managed by different teams need to work together. However, OT need to have more robust controls.

Processes

- Governance, roles and responsibilities
- Risk management
- Asset management
- Controlling Supply chain
- Protecting against cyber attack
- Controlling access
- Staff training and competency
- Security monitoring
- Detecting events
- Recovery from incidents
- Learning from incidents

Technology

- Simple steps can be taken- basic cyber hygiene. For example:
- Do you know what IACS systems you have and how they are connected?
- Have you segmented IACS from other systems (e.g. with unidirectional gateways)?
- Is access controlled to minimum – physical access and authorization (e.g. passwords)?
- Have you removed unnecessary connections, applications, expired users, USB ports that are not required etc.?
- Are you in control of remote and portable connections – e.g. vendor remote access and laptops?
- Do you apply the latest security updates – caution required when it comes to IACS but are we too cautious at the moment?
- Have you got good backups and know how to restore?

HSE experience so far

- First edition of HSE guidance published in March 2017
- Trial inspections run for 8 sites. The main findings and learning included in the second edition of the HSE guidance published in Dec 2018. http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

Learning from HSE field trials

		P	F
A. Managing security risk			
A.1	Governance		
A.2	Risk management		
A.3	Asset management		
A.4	Supply chain		
B. Protecting against cyber attack		P	F
B.1	Service protection policies and processes		
B.2	Identity and access control		
B.3	Data security		
B.4	System security		
B.5	Resilient networks and systems		
B.6	Staff awareness and training		
C. Detecting cyber security events		P	F
C.1	Security monitoring		
C.2	Proactive security event discovery		
D. Minimising the impact of cyber security incidents		P	F
D.1	Response and recovery planning		
D.2	Lessons learned		

RAG Rating

PART (P)	FULL (F)
Most Operators had started to address / partially achieved most objectives (≥6/8)	Most Operators had achieved most objectives (≥6/8)
Some Operators had started to address / partially achieved some objectives	Some Operators had achieved some objectives
Most Operators had not started to address / achieved most of the objective (≤2/8)	Most Operators had not achieved most of the objective (≤2/8)

Leadership

- Cultural shift does not come about without support from the top.
- Senior managers understand and own the risk to the business and provide the right governance, policy, oversight and support.
- CDOIF guidance for senior managers being developed

Key messages

- Cyber is an increasing risk
- Industrial control and safety systems are vulnerable
- There is potential for cyber attack to lead to major accidents and interruption to critical supplies
- Risk should be managed. Need to understand the risk, and manage it through people, processes and technology.
- Cyber security is a rapidly changing topic