Security of SMRs

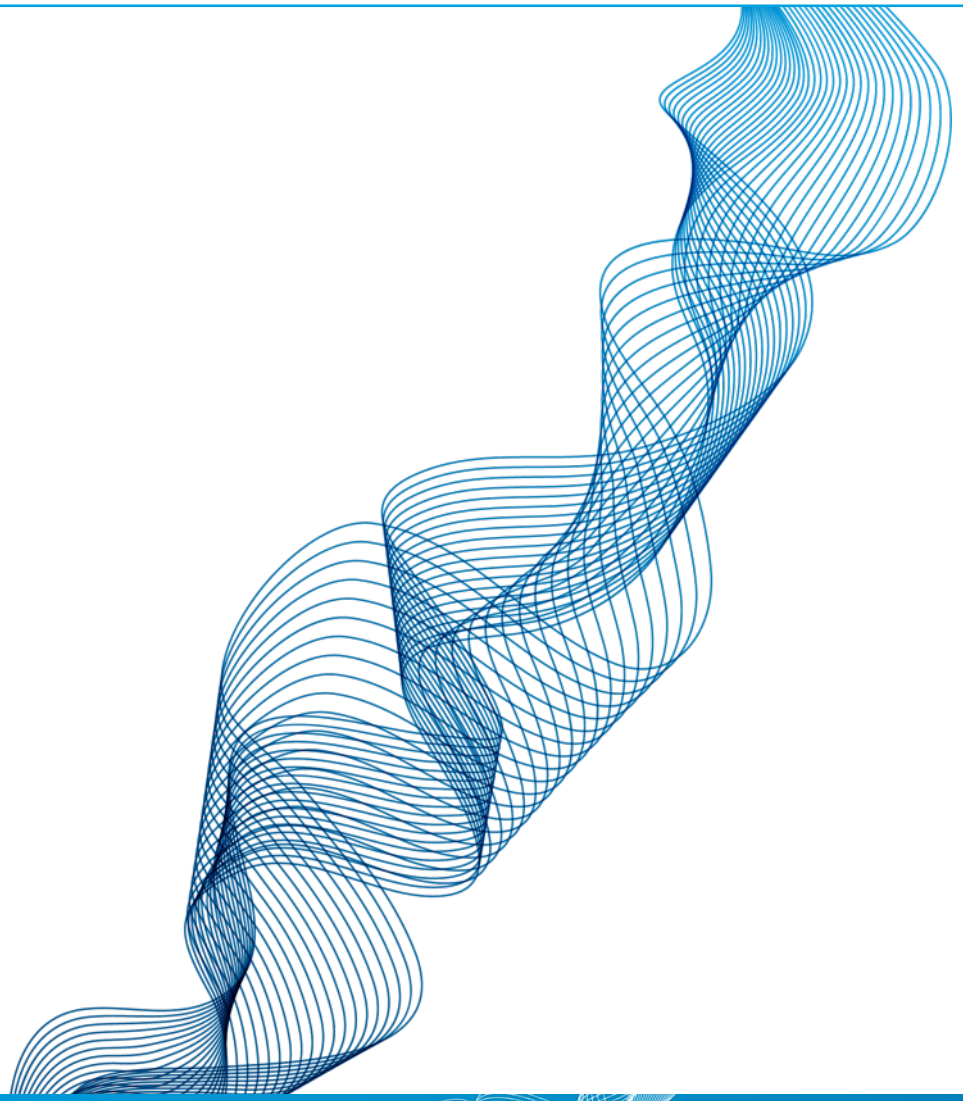
Cyber Security and the Insider Threat

Christopher Cope - Chief Information Security Officer, NNL

NATIONAL NUCLEAR LABORATORY

Scope

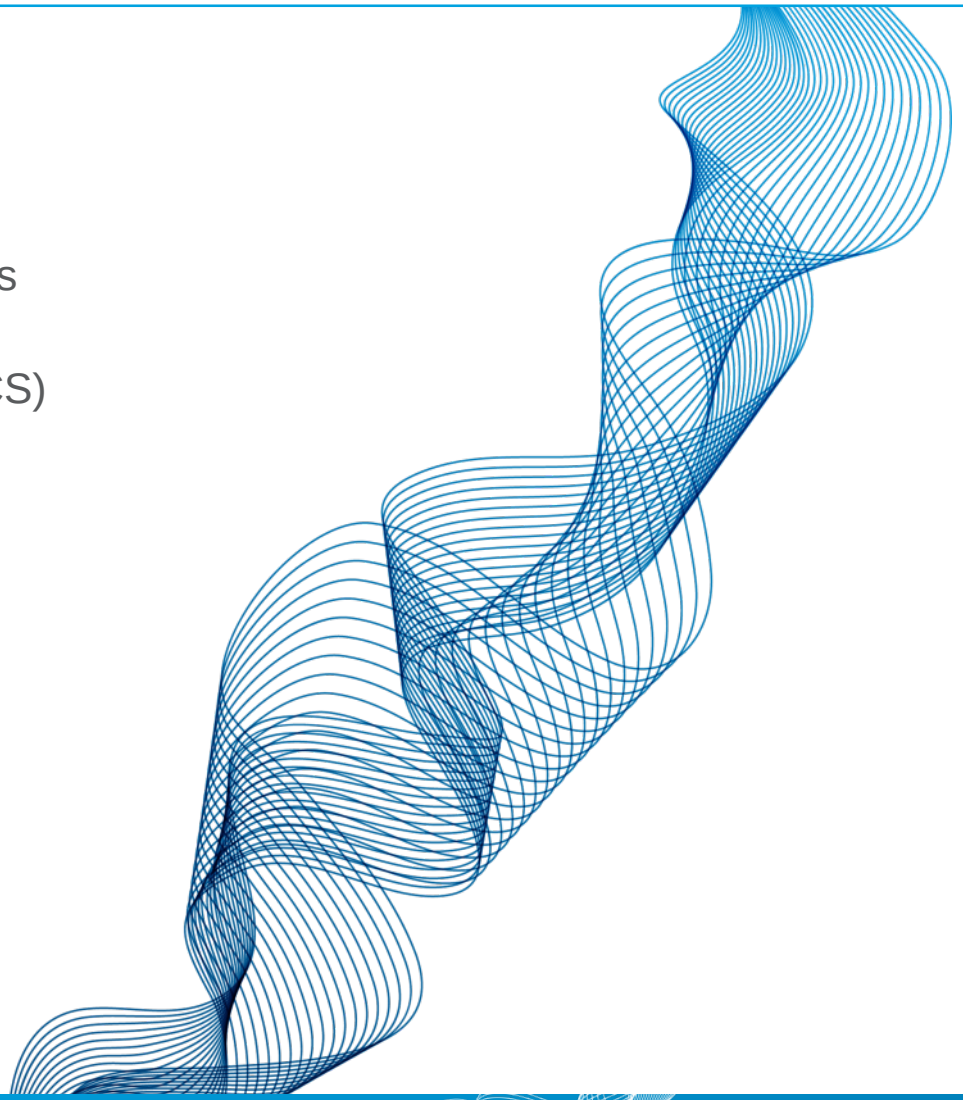
- What is operational technology?
- Security considerations of operational technology
- Specific issues for SMR
- Insider threats
- Summary and discussion points



What is operational technology?

Huge variety of Operational Technology:

- Nuclear Instrumental and Control (I&C) Systems
- Industrial Automation and Control Systems (IACS)
- Automated Access Control Systems (AACS)
- Closed Circuit Television systems (CCTV)
- Building Management Systems (BMS)
- Fire, criticality, evacuation and site emergency alarms
- Nuclear Material Accountancy (NMAcc) systems



Security considerations of operational technology

Significant differences with IT:

- Longer in service times
- Bespoke

IT security principles must be applied with caution

When the hackers struck power company workers reported being unable to control their own computers

Ukraine power 'hack attacks' explained

US investigators have accused Russia-based hackers of being behind an attack that caused blackouts across Ukraine in December.

The team said it was not possible to say whether it was the "Russian government or a well-funded [non-government] team".

However, one of the experts involved in the probe has warned that the UK and other countries could be vulnerable to similar cyber-attacks.

Read more

29 Feb 2016

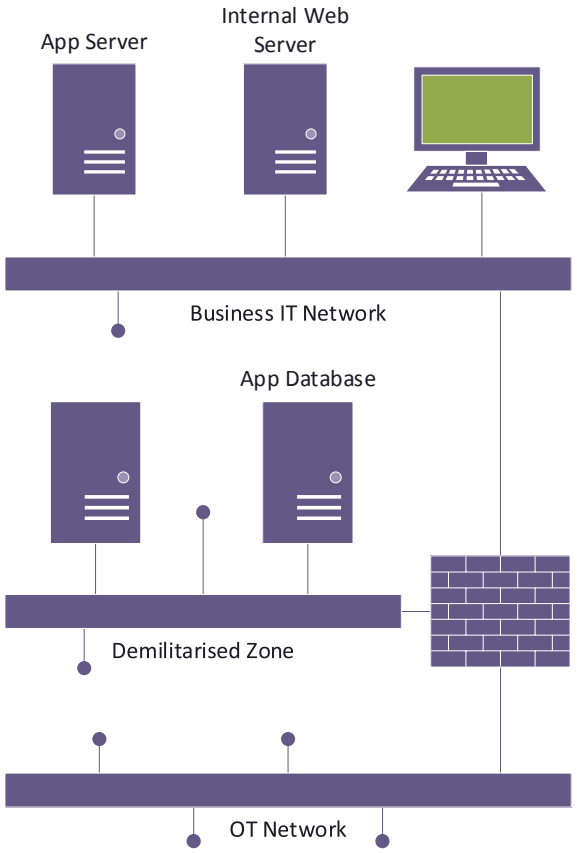
Share

BBC News Website, June 2016

Security considerations of operational technology

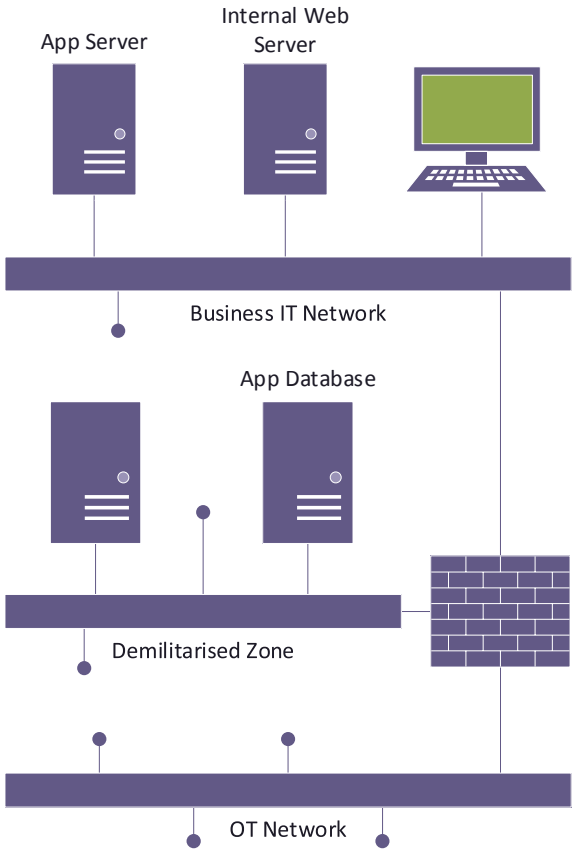
Security considerations of operational technology

Information flow for management and analytics



Security considerations of operational technology

Information flow for management and analytics



Increased Risk

SMR cyber security

Traditional reactors are built on site

SMRs are built elsewhere and then assembled on site

Supply chain security now a factor

SMRs are smaller, but that may not decrease security requirements.

Remote monitoring necessitates connectivity

How will regulation be applied?

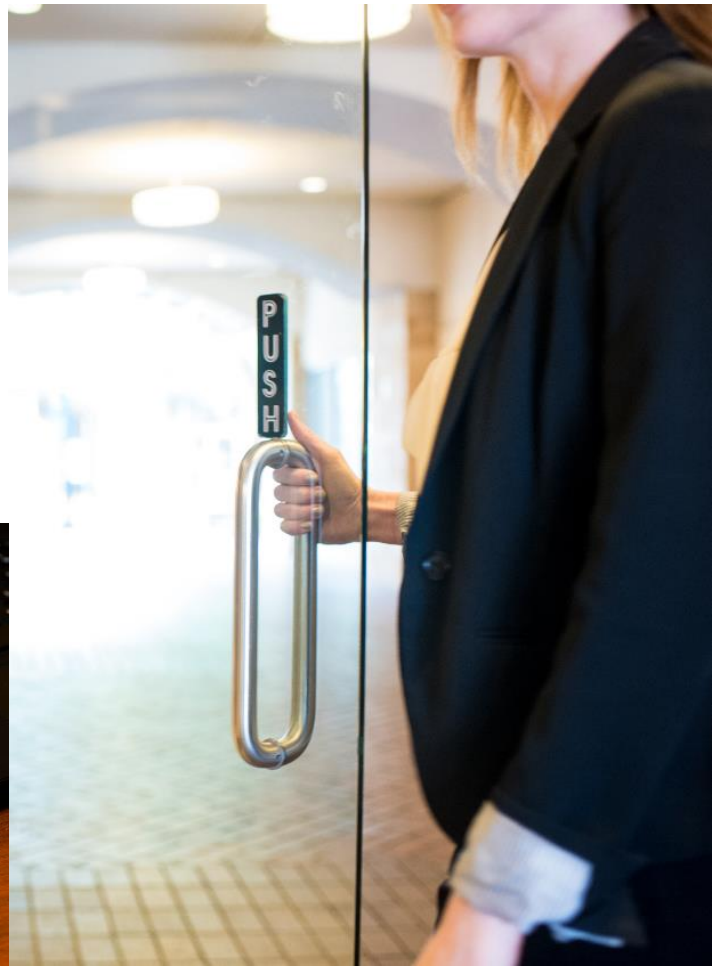
Opportunity for security by design

Insider threat

Human factors play a critical role in security

Authorised people can act deliberately, accidentally or be duped/ coerced

Social engineering



Insider threat

1 **Digital Transformation**

IT-OT Convergence
Data Analytics
Algorithms

2 **Cloud Computing**

AKA "I don't know where my data is."

3 **Internet of Things**

Devices of unknown provenance and the dissolution of boundaries

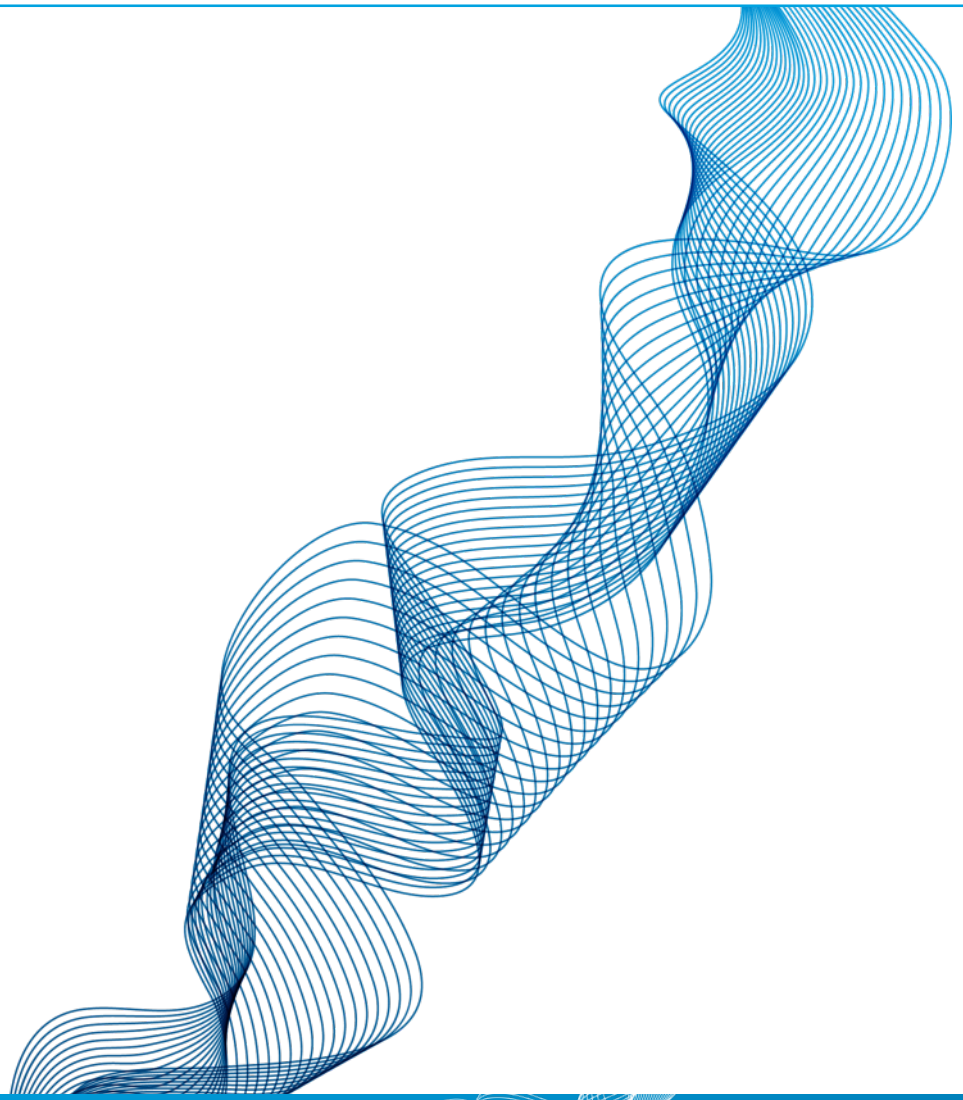
Summary/ discussion points

Operational technology faces cyber threats

- How can we better understand those threats?

Security controls for operational technology can’t precisely mirror those for IT

- What standards can be applied?

Insider threat remains a consideration

- How can we reduce risk and maximise benefit from workforce?