Science & Technology Facilities Council
ISIS Neutron and Muon Source

The perspective of a small cog in a big machine

Kathryn Baker

6th October 2019

ICALEPCS, New York

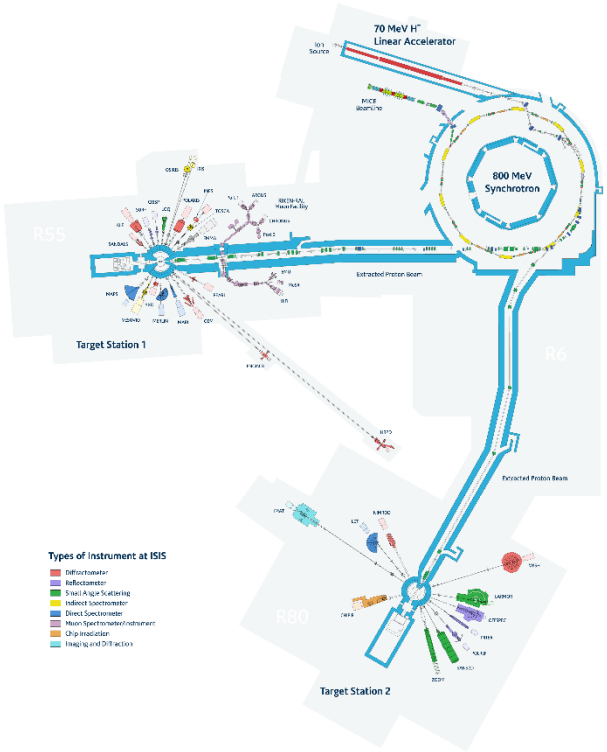
Abstract

The work of the experiment controls group at the ISIS Pulsed Neutron and Muon Source is only a small part of what STFC does. This talk will endeavour to show the difficulties that can be faced between the disparate needs of an organisation like STFC and the practicalities of supporting a science research programme.

Who am I?

- Kathryn Baker
- Senior Software Engineer in the Experiment Controls Group at ISIS Neutron and Muon Source
- The group is responsible for managing/designing/writing/ reviewing/supporting the control software used on the beamlines at ISIS

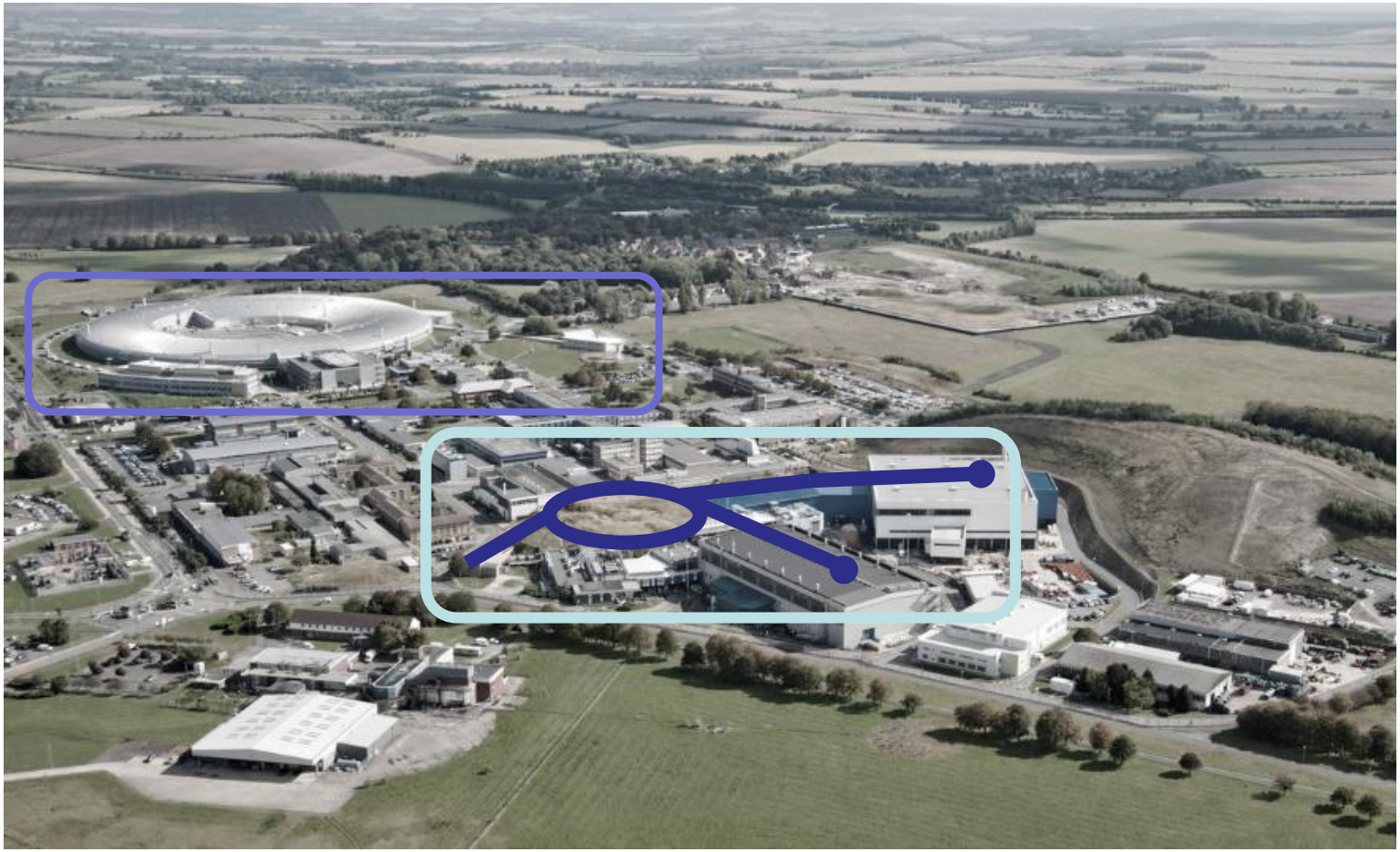
What does ISIS do?



- Pulsed Neutron and Muon Spallation Source
- 2 Experimental Halls
- 30+ Instruments
- In 2018 – 1085 Proposals, 870 Experiments, 500 Journal and Conference Papers

Where is ISIS?

Where is ISIS?



What is RAL?

- Rutherford Appleton Laboratory is one of the sites operated by the Science and Technology Facilities Council (STFC)

What is STFC?

- STFC is one of 7 research councils that are part of UK Research & Innovation (UKRI)
- Manages facilities:
  - ISIS
  - CLF
  - + more

What is UKRI?

- Principally funded by the Department for Business, Energy and Industrial Strategy (BEIS) from the UK Science Budget
- Centralised management of core functions
- Comprised of 7 research councils, Innovate UK, and Research England

Cybersecurity Requirements

- Some are provided by BEIS, namely the expectation to be certified under the Cyber Essentials Scheme
- Cyber Essentials is a Government backed scheme run by the National Cyber Security Centre
- https://www.cyberessentials.ncsc.gov.uk/

Firewalls

- There are boundary firewalls and internet gateways to prevent unauthorised access to/from private networks
- There are approved VPNs and Remote Desktop Gateway Services that will allow ‘offsite’ access to onsite resources

Secure Configuration

- Non-standard passwords for devices that come with them
- Operating System installations that do not include unnecessary applications or services
- Suitable passwords

User Access Control

- Only authorised users have access
- Separate user and administrative accounts – admins can do more than users

Malware Protection

- Protection from malware and viruses supplied by a vendor with good credentials
- The internet gateways also help by blocking sites which are malicious

Patch Management

- Patches applied quickly – for high vulnerabilities within 14 days
- Software should be licenced and supported (still receiving patches)
- Removed from devices when no longer supported

Conclusion

- In many functions it is easy to insist on systems such as cyber essentials
- Sometimes life gets in the way of a good plan