Science and
Technology
Facilities Council

Scientific Computing

GridPP
UK Computing for Particle Physics

GridPP Security

David Crooks
david.crooks@stfc.ac.uk

GridPP 48, August 2022, Ambleside

Overview

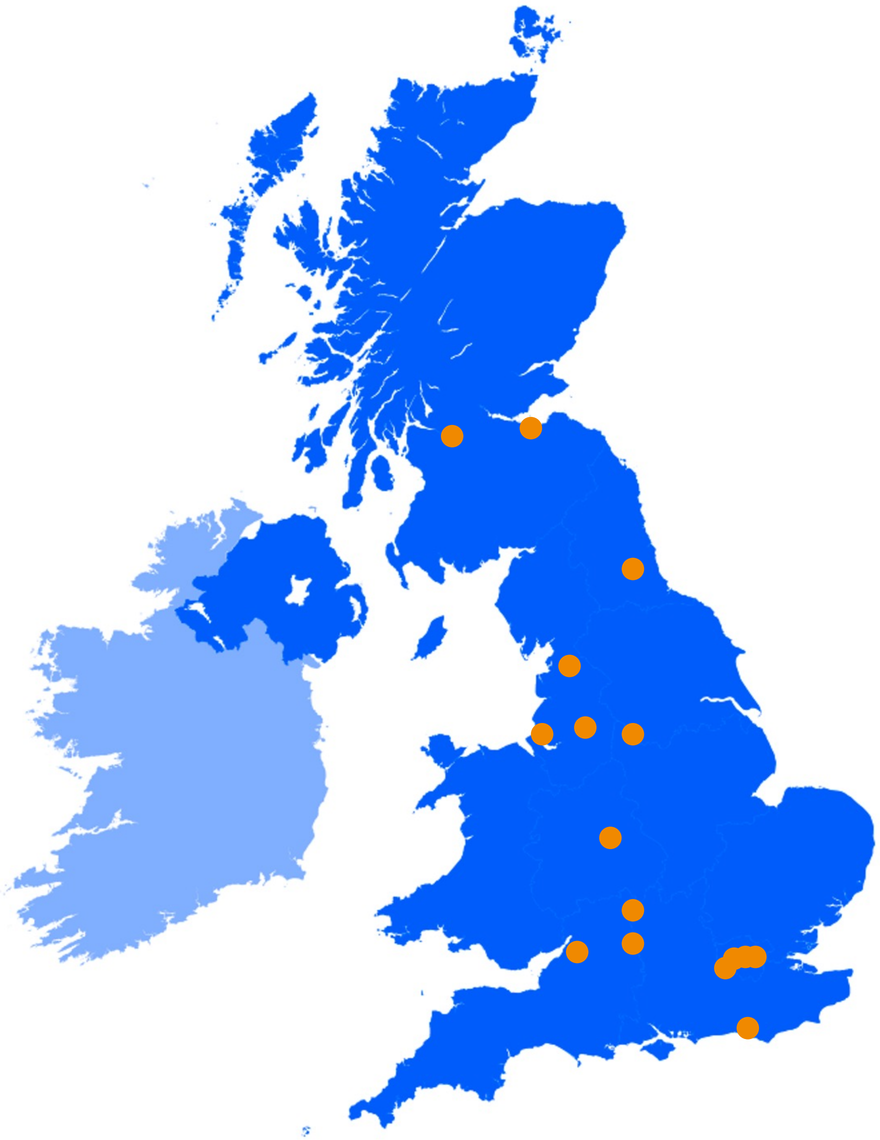
2 Operational Security

3 Topics of current and future interest

4 STFC Cybersecurity

5 UKRI DRI Cybersecurity

6 Conclusions



Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

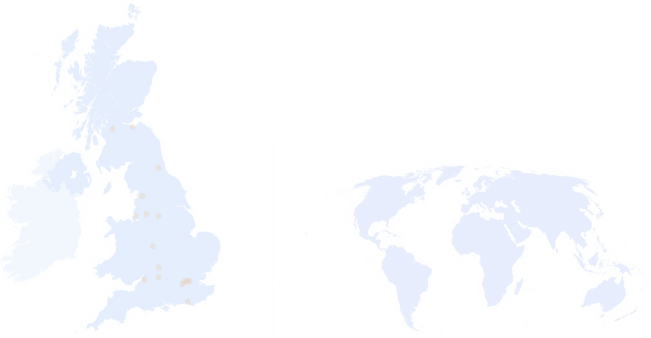
Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Operational Security

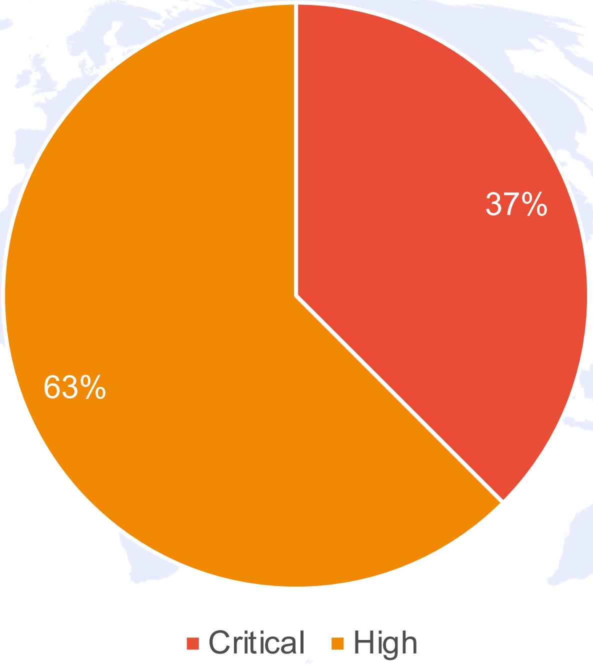


Vulnerability risk assessments

- Since April 2022
  - 15 Tickets created
  - 8 advisories issued to sites
  - **3 Critical**
  - 5 High

Advisories now on

- https://advisories.egi.eu
- NOT the old wiki anymore
- This is now up to date
  - Apart from ones not yet public

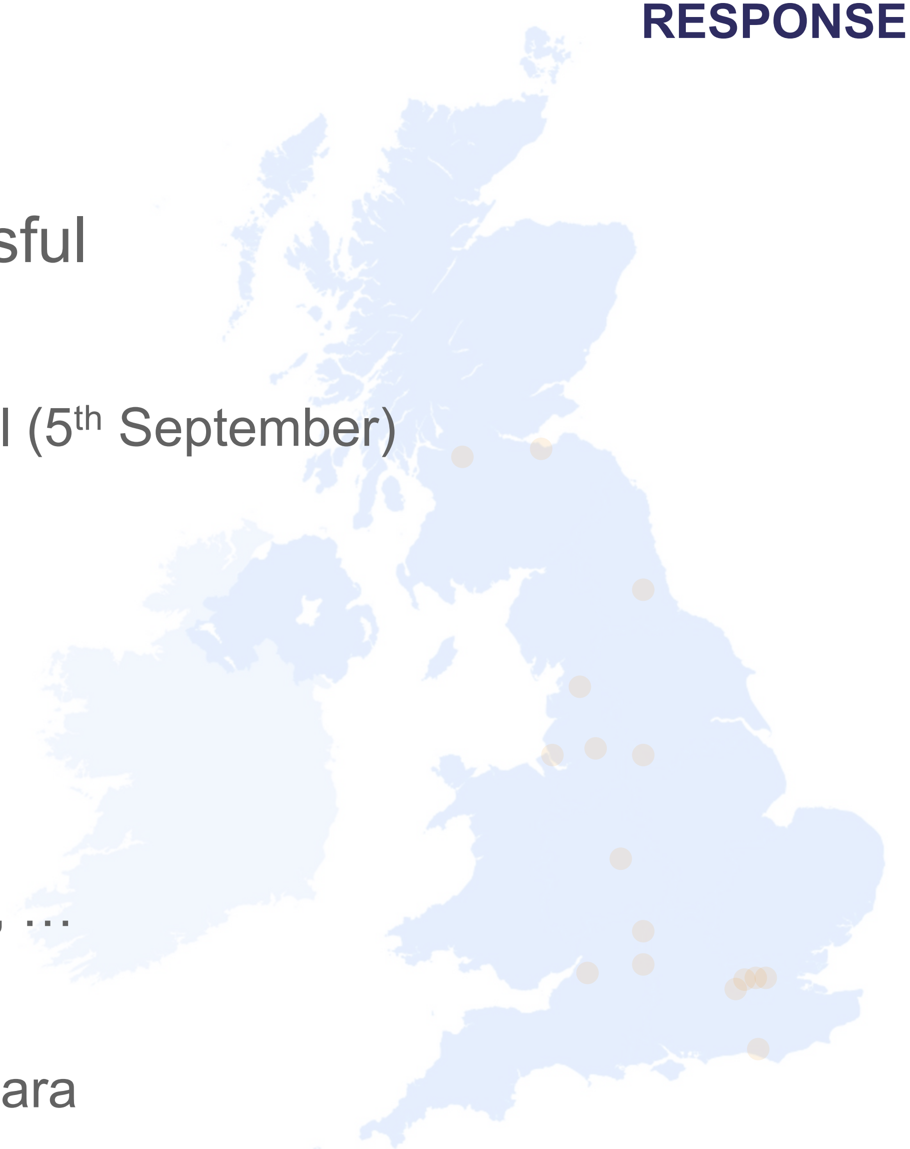


PREVENTION
RESPONSE

IRIS/GridPP Security Team update

- No incidents impacting GridPP since April 2022
- Vulnerability assessment reports continue to be really useful
  - *IRIS: Adding DiRAC status*
- Emanuele Simili (Glasgow) has joined the team and will soon join the rota
  - Welcome Emanuele!
- Plan to create IRIS Security Confluence area using Scientific Computing subscription

Training



- Thematic CSC on Security was incredibly successful
  - Elements will be used at:
    - EGI/Black Sea Universities Network summer school (5th September)
    - EGI Conference (23rd September)
- Need to look at future planning
    - Possibility of repeated schools (bi)annually?
- IRIS/GridPP training (see Matt’s talk ☺)
  - Focus on fundamentals: architecture, risk management, …
  - What can we do F2F/via Zoom/via learning platform?
  - Potential start with architecture/risk/ops: Sven and Barbara

EGI CSIRT SSC Update

- No update on SSC progress for this meeting
- Reviewing status now that Run 3 is underway
- We should also consider other exercises in the context of training…
  - Need to plan these careful including split between F2F/online exercises

PREVENTION
DETECTION
RESPONSE

Site plans

- Previously discussed central logging as a key component to ensure we have in place
  - Pick up now that summer is ending!
  - IRIS Security Forum meeting
- For each site develop an action plan
  - What you feel you would benefit from
  - Where can we support you
  - Next steps
  - Review informally

UKRI Science and Technology Facilities Council

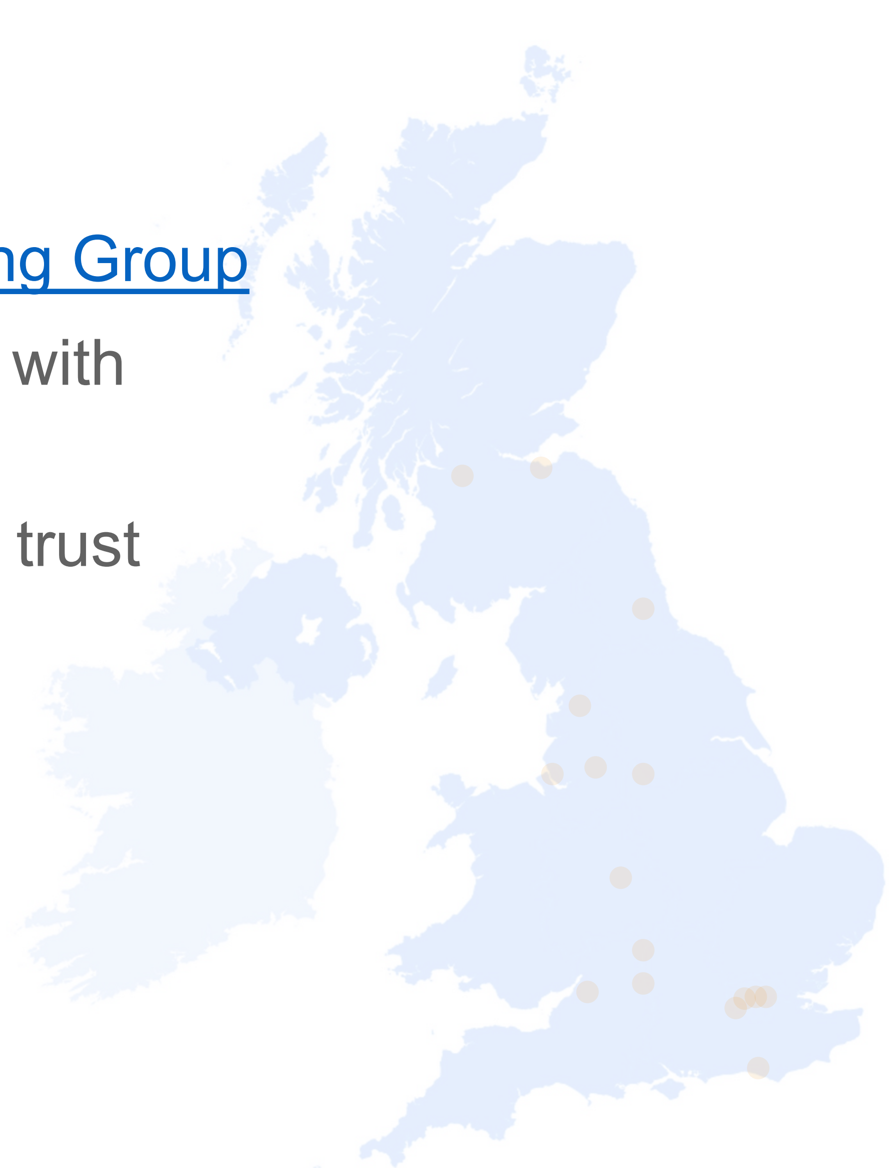
Scientific Computing

GridPP

UK Computing for Particle Physics

Topics of current and future interest

Assurance



- Host certificates: Resource Trust Evolution Working Group
  - Services that serve more than one community with potentially different trust anchors
    - Allowing WLCG to use services with public trust (eg S3)
  - Cloud-based workflows

- Token-based workflows
  - See WLCG Timeline v1.0

Risk management

- Risk assessment and management is at the foundation of information security
- Lots of activity (EOSC Future/STFC/etc) on how we assess and manage risk at the **service** level
- Consider how we could usefully approach this for GridPP

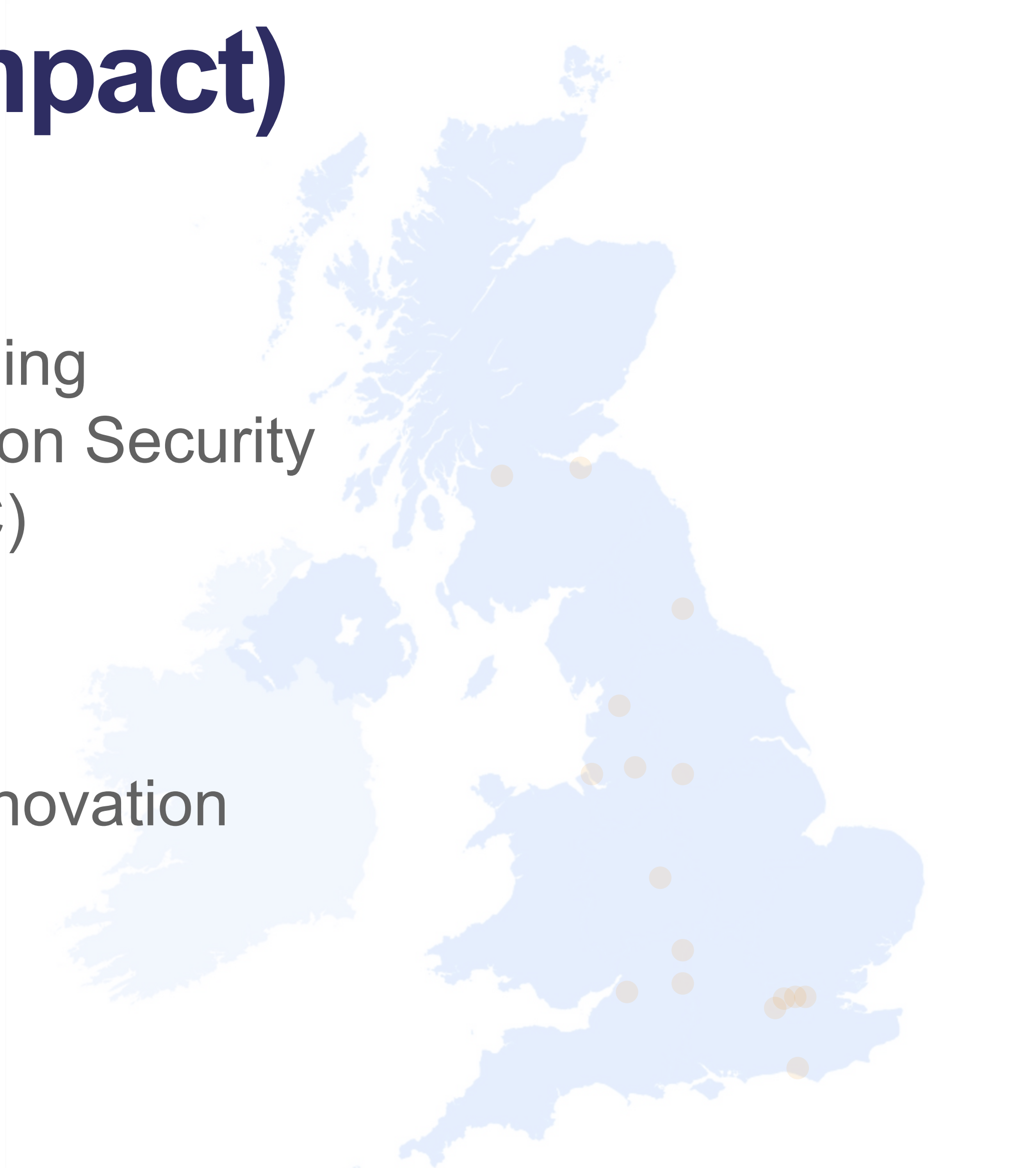
UKRI Science and Technology Facilities Council

Scientific Computing

GridPP
UK Computing for Particle Physics

STFC Cybersecurity

STFC Cybersecurity (and Impact)



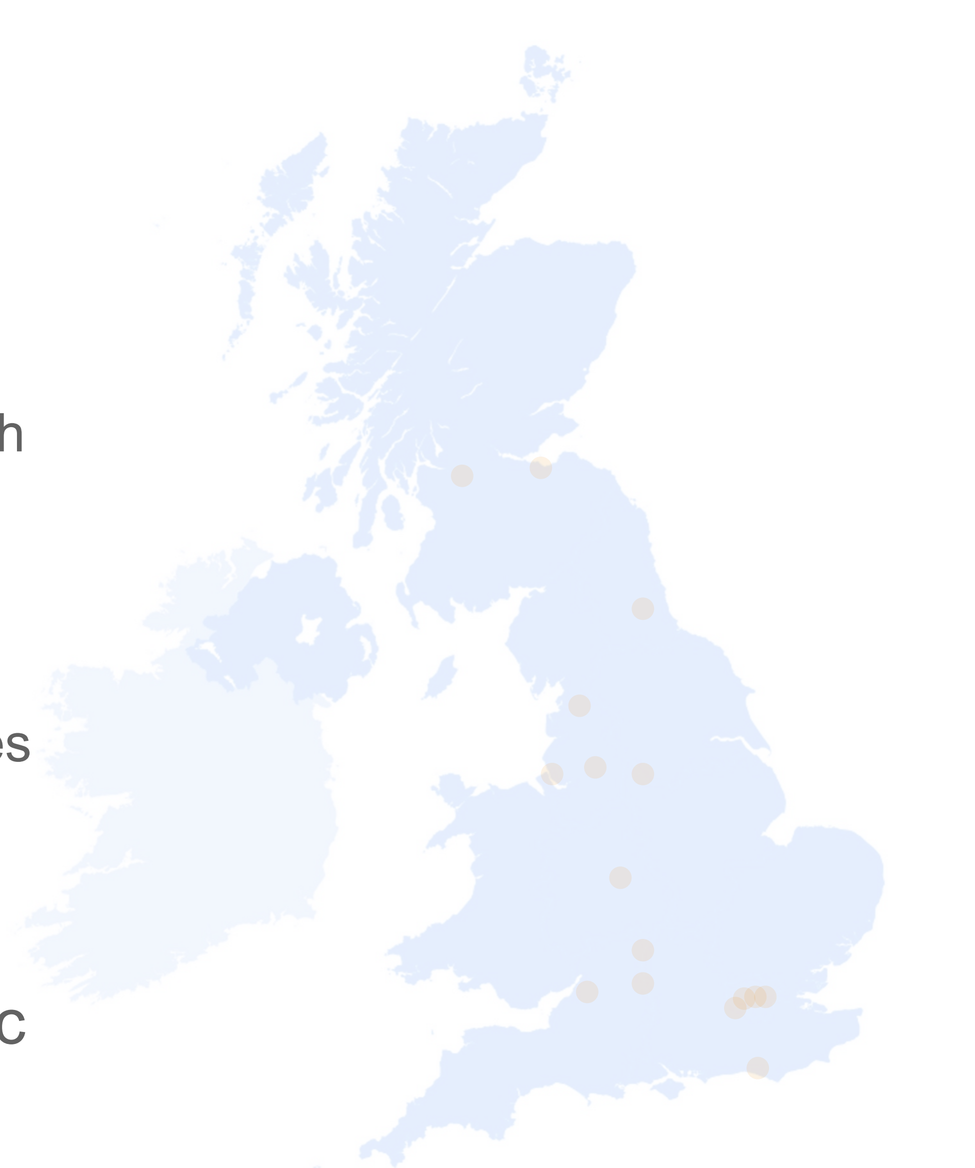
- Building on work in GridPP/IRIS/EGI/WLCG
- DavidC in a position to support STFC in developing cybersecurity capabilities; now chair of Information Security Group (cybersecurity development across STFC)
    - Refocusing that group in light of modern landscape
    - Reviewing overall STFC cybersecurity governance
- Working as part of broader UK Research and Innovation cybersecurity development activities
- Now building a team in Scientific Computing
    - Introducing them to GridPP/IRIS CSIRT work

Scientific Computing Security Engineering

- Important aspect of this team is security engineering
- Security service deployment and management for Scientific Computing, STFC and beyond
  - Owns the development of the STFC SOC
  - Maintenance and development of STFC MISP
- 3 new members joining by April 2023
  - Planning to come to next GridPP ☺

STFC SOC update

- Liam Atherton and James Acris working on Zeek, MISP and OpenSearch integration as graduates
  - Kyle Pidgeon working with Greg Corbett on OpenSearch container deployments
  - Kafka will be pipeline between Zeek and OpenSearch; Logstash proven to be not performant at this scale
  - Rocky 8; building on work creating Aquilon-ready images
- Waiting for final network connection to core network to begin deployment work
- Presented at Networkshop50 and TNC22 with Jisc
  - Very fruitful collaboration!



Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

DRI Cybersecurity

UKRI DRI Cybersecurity Enhancement

- Newly funded DRI Cybersecurity project: FY22/23
  - Includes both resource and capital
- Enhance cybersecurity **across** DRI activities
  - **Augmenting** existing GridPP/IRIS work
- Focus at **organisational** level
  - Working to ensure common, connected capabilities
- Immediate goal is national cybersecurity workshop
  - Work with senior cybersecurity leaders
  - Build detailed plan of work for next FY

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Next steps / Conclusion

Conclusion

1. Landscape and high priority of cybersecurity remain the same
2. Continue to grow the capabilities of the security team
3. Build plans for what will help sites
4. Opportunity to build additional organisational collaboration in DRI context
5. Notable impact of our work on organisational cybersecurity

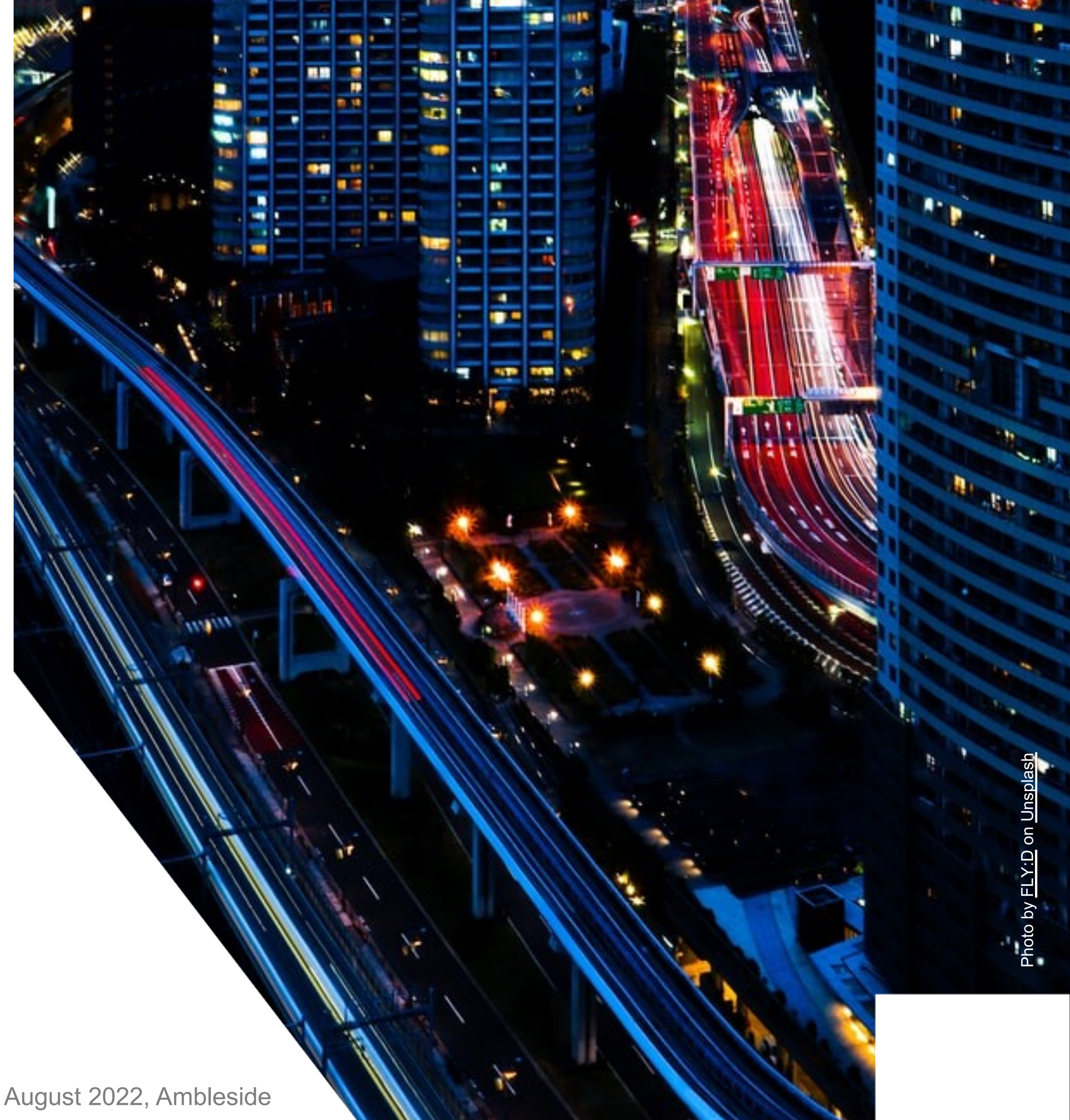


Photo by FLY:D on Unsplash

UKRI Science and Technology Facilities Council

Scientific Computing

GridPP UK Computing for Particle Physics

Science and
Technology
Facilities Council

Scientific Computing

Questions?