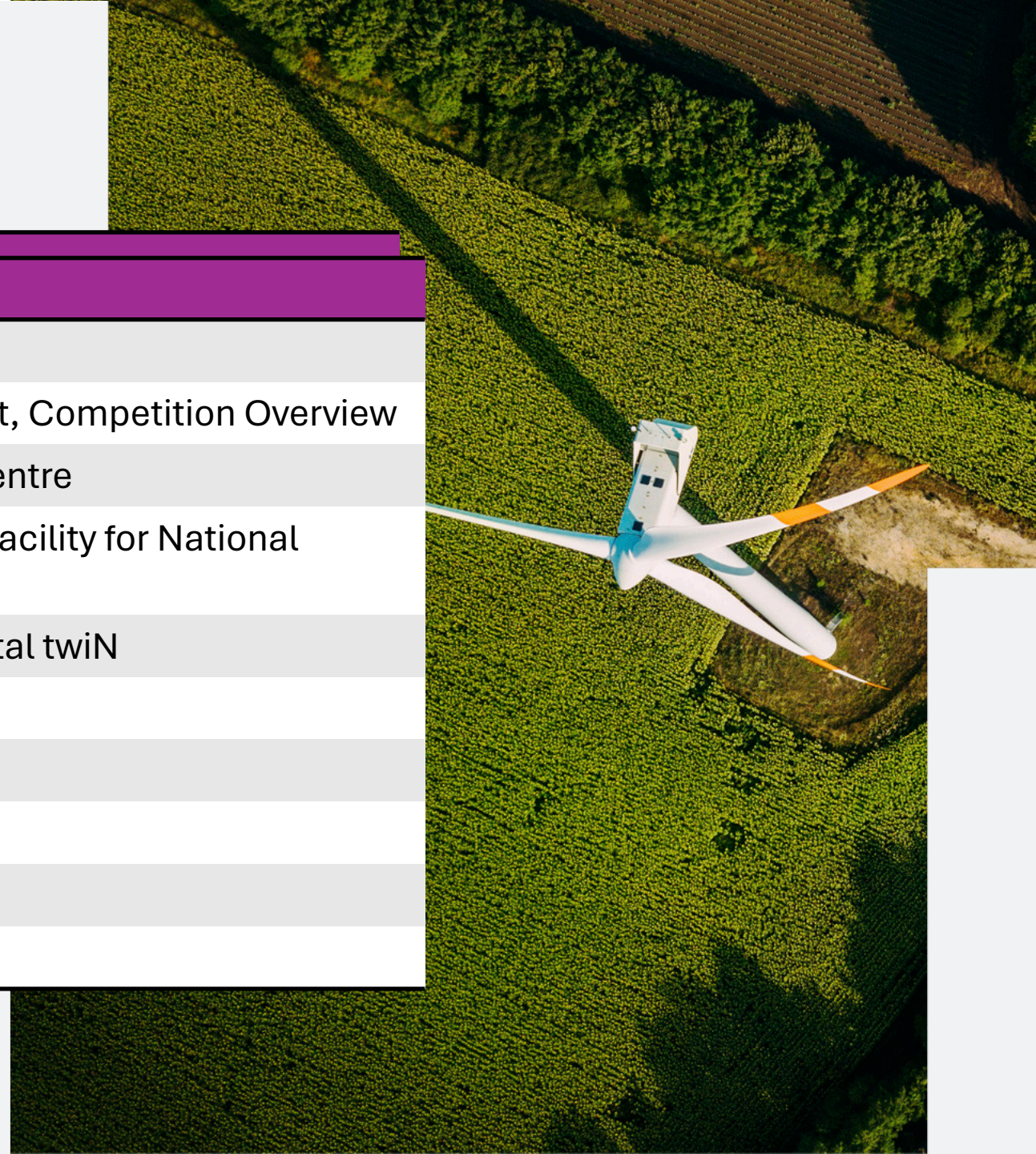
Digital Twin Energy Grids

Competition Launch

Agenda

Time	Item
1100	Mel Cassley, Introduction
1105	Marta Fernandez Aguilar & Kara Cartwritght, Competition Overview
1115	Andrew, NCSC: National Cyber Security Centre
1120	Brian Matthews, DAFNI: Data & Analytics Facility for National Infrastructure
1125	Afia Masood, ENSIGN: Energy System dIGital twiN
1130	Jonathan Eyre, DTNetwork+
1135	Q&A
1150	Break
1155	Breakout Sessions
1225	Wrap-up & Close



Ofgem SIF

UKRI Innovate UK

Innovate UK

Competition Overview

Scope

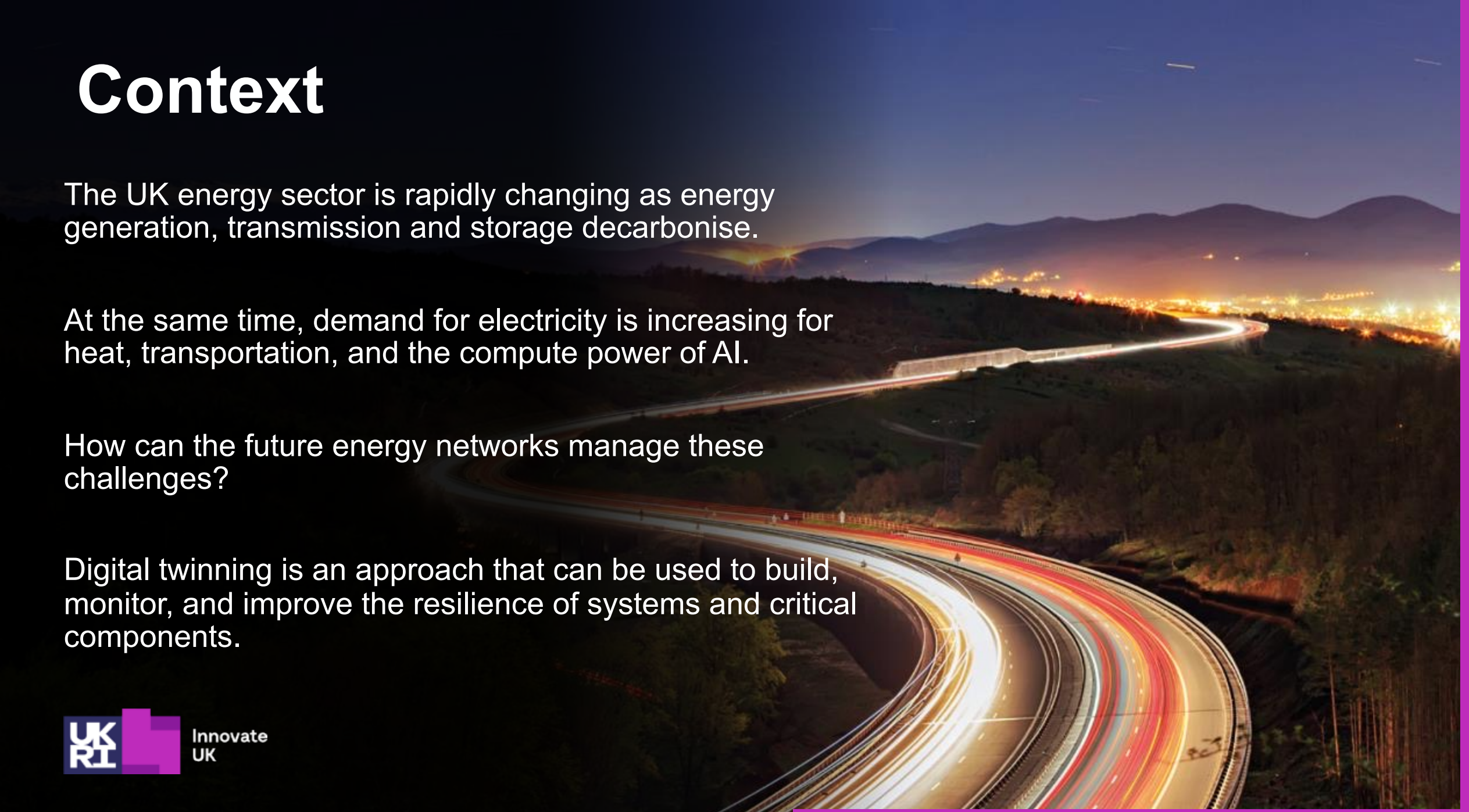
Context

The UK energy sector is rapidly changing as energy generation, transmission and storage decarbonise.

At the same time, demand for electricity is increasing for heat, transportation, and the compute power of AI.

How can the future energy networks manage these challenges?

Digital twinning is an approach that can be used to build, monitor, and improve the resilience of systems and critical components.



UKRI Innovate UK

About this competition

This competition is part of Building a Secure and Resilient World Programme (BSRW).

The aim is to improve the cyber resilience of the UK's energy networks by enabling the development of digital twins and to unblock the current barriers for the development of the digital twin technology.

UKRI Innovate UK

We have developed this scope in discussion with stakeholders and to compliment the OFGEM Strategic Innovation Fund work.

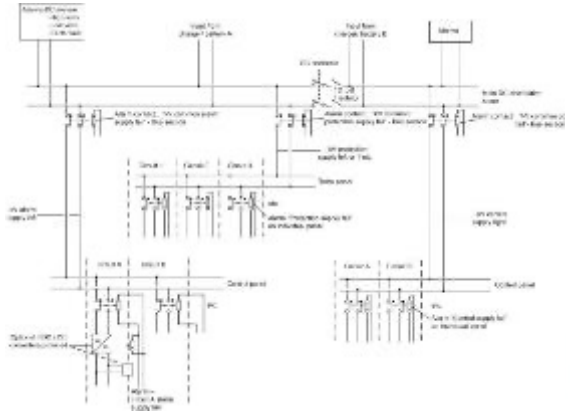
The competition is also aligned to the EPSRC Ensign Programme.

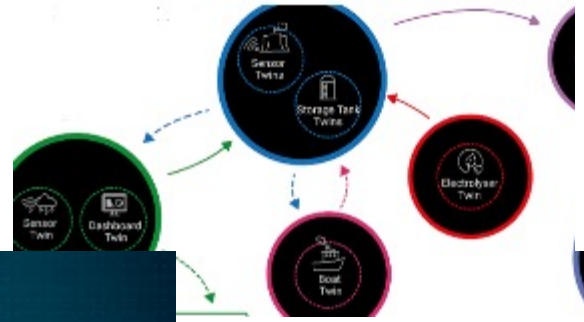
What are we looking for?

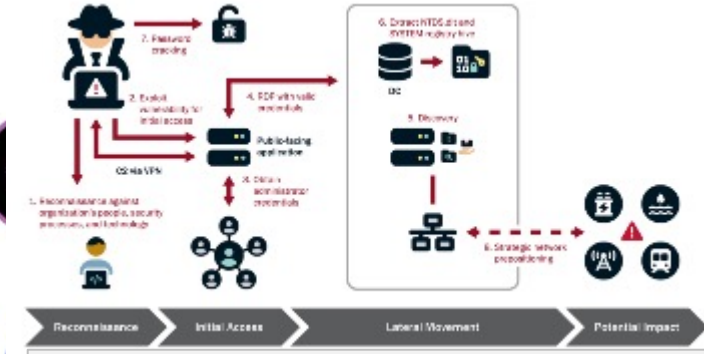
Specific themes

Your project can focus on one or more of the following:

- developing digital twins and their underpinning technologies
- enabling future federated digital twins
- system modelling for data driven decision making
- improving data interoperability, sharing, quality and security
- securing operational and control room technologies
- cybersecurity threat detection, analysis and mitigation
- data driven technologies for grid stability, forecasting, balancing
- demand side response security such as Energy Smart Appliances
- data sharing licensing and legal considerations





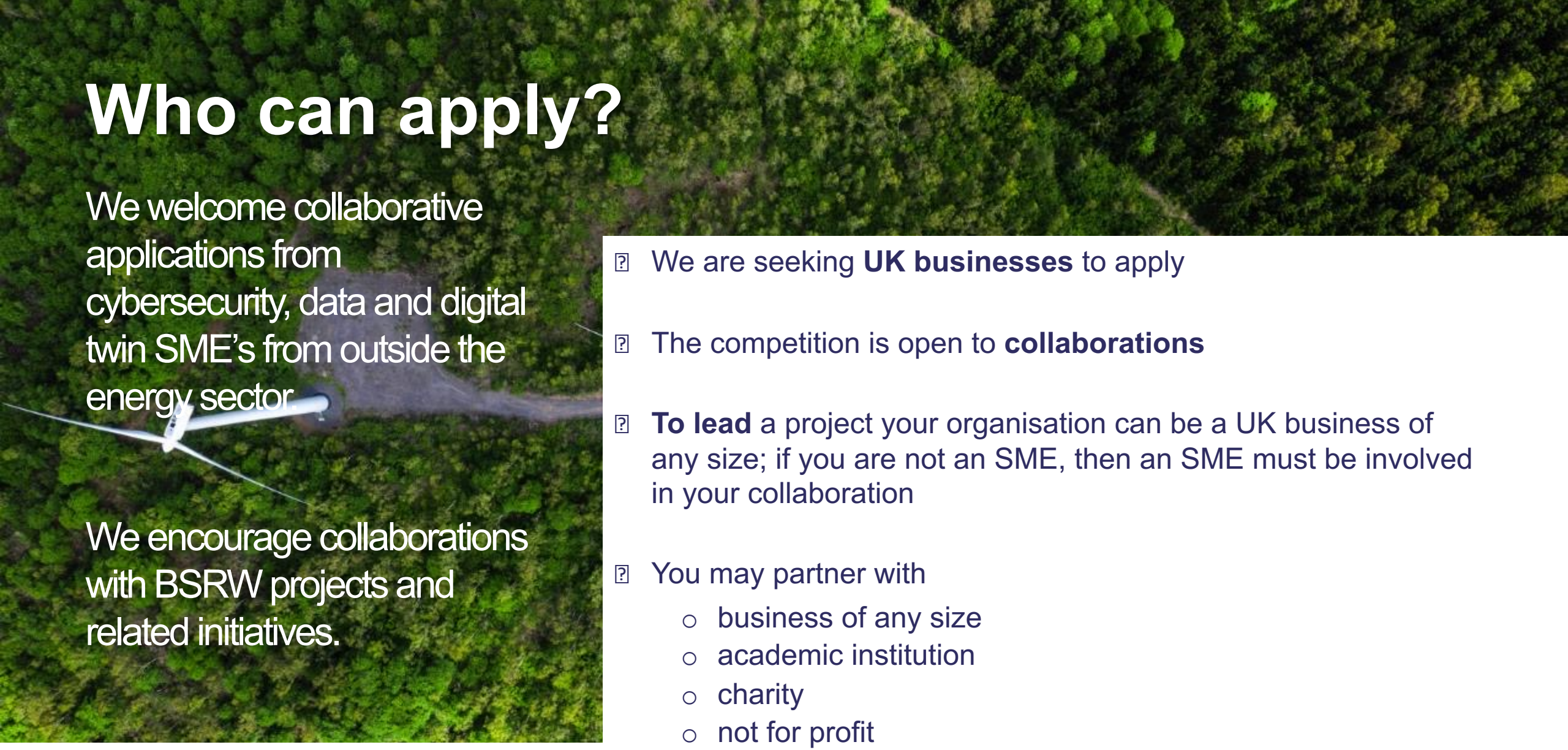


Typical Volt Typhoon Activity – Living off the Land (LOTL) from CISA.gov

ClassOfMoneyTransfer
ClassOfOnlineService
ClassOfOperationalEvent
ClassOfOrganisation
ClassOfPaymentArtefact
ClassOfPerson
ClassOfPersonState
ClassOfRepresentation
ClassOfResponsibleActor
ClassOfResponsibleActorState

Innovate UK

Who can apply?



We welcome collaborative applications from cybersecurity, data and digital twin SME's from outside the energy sector.

We encourage collaborations with BSRW projects and related initiatives.

- We are seeking **UK businesses** to apply
- The competition is open to **collaborations**
- **To lead** a project your organisation can be a UK business of any size; if you are not an SME, then an SME must be involved in your collaboration
- You may partner with
  - business of any size
  - academic institution
  - charity
  - not for profit
  - public sector organisation
  - research and technology organisation (RTO)
  - licensed energy company or regulator

UKRI Innovate UK

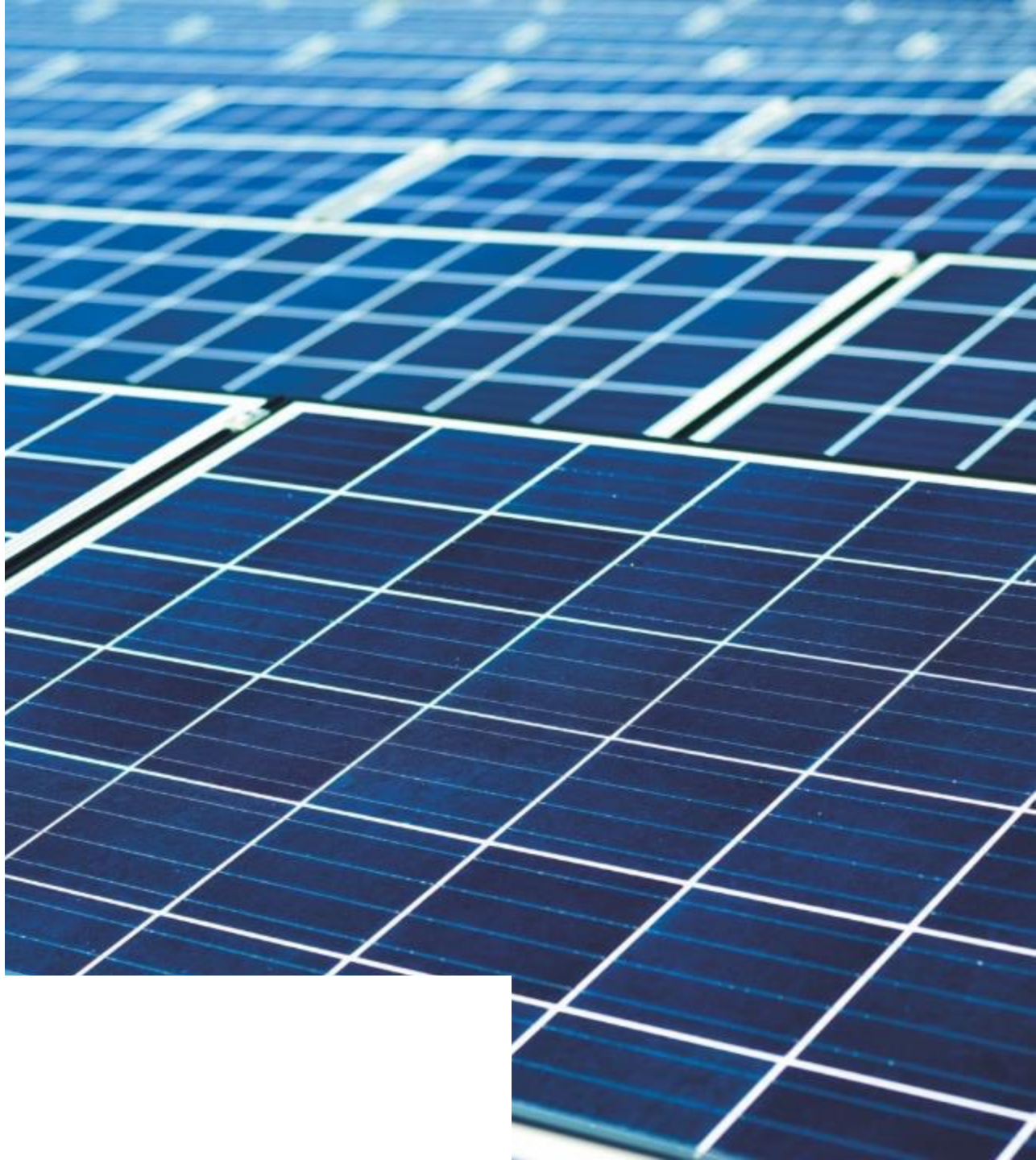
Out of Scope

We are not funding projects that are:

- not in scope for this competition
- do not have an application for cyber resilience of the energy grids
- do not consider interoperability of data
- are only applicable on gas networks

Innovate UK

Scope Q&A



Eligibility criteria

Innovate UK

Eligibility Criteria

Total Competition Grant:	£1.2 million
Open to:	Collaborations only
Project must:	• start by 1 October 2024 • end by 30 September 2025 • include at least one grant claiming SME • carry out all of its project work in the UK • intend to exploit the results from or in ~~England~~ UK (note: text corrected from version shown during live event on 15th April 2024)
Total Grant Funding Request:	between £100,000 and £300,000
Project Length:	between 6 and 12 months
Lead Organisation:	UK business of any size
Subcontractors:	Allowed

UKRI Innovate UK

Key Dates

Timeline	Dates
Competition Opens	22 April 2024
Briefing Event	25 April 2024
Submission Deadline	24 May 2024 at 11:00
Applicants informed	28 June 2024

Innovate UK

Innovate UK

Thank You

@InnovateUK

Innovate UK

Innovate UK

@weareinnovateuk

NCSC
CYBER PHYSICAL

Cyber Physical Challenges and Motivation

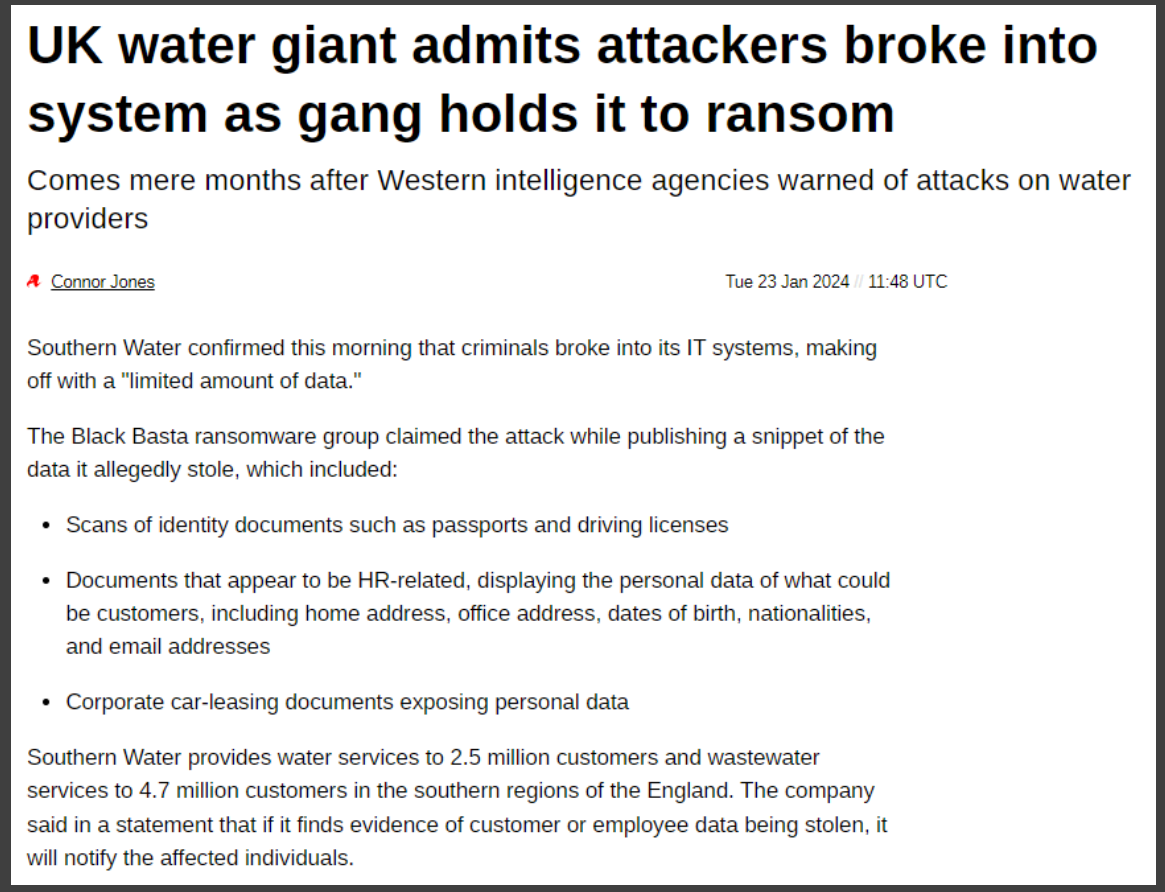
High-Level Research Questions

- How do we build security for products with long operational lives?
- How do we incentivise better security for cyber-physical systems?
- How can we understand the security of a wide variety of cyber-physical assets?
- How do we have confidence in the security of a cyber-physical system?
- How can we utilise emerging technologies in a secure way within cyber-physical systems?
- How do we Build Resiliency Across Systems of Systems?

How do we build security for products with long operational lives?

Designing systems that will operate for 20+ years

- Historical Best Practices
- Dev Ops
- Sustainability
- Skills and Training



UK water giant admits attackers broke into system as gang holds it to ransom

Comes mere months after Western intelligence agencies warned of attacks on water providers

Connor Jones — Tue 23 Jan 2024 // 11:48 UTC

Southern Water confirmed this morning that criminals broke into its IT systems, making off with a "limited amount of data."

The Black Basta ransomware group claimed the attack while publishing a snippet of the data it allegedly stole, which included:

- Scans of identity documents such as passports and driving licenses
- Documents that appear to be HR-related, displaying the personal data of what could be customers, including home address, office address, dates of birth, nationalities, and email addresses
- Corporate car-leasing documents exposing personal data

Southern Water provides water services to 2.5 million customers and wastewater services to 4.7 million customers in the southern regions of the England. The company said in a statement that if it finds evidence of customer or employee data being stolen, it will notify the affected individuals.

Building better ways to get uptake of best practice cyber security

NEWS 18 MAR 2024

Microsoft: 87% of UK Organizations Vulnerable to Costly Cyber-Attacks

James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Just 13% of UK organizations are resilient to cyber-attacks, with the remainder either vulnerable (48%) or at high risk (39%) of damaging cyber-incidents, according to a new report by Microsoft in collaboration with the University of London.

The tech giant said the lack of secure foundations harms the UK's ambition of becoming an 'AI superpower'.

Microsfot urged increased investment in AI technologies and solutions to tackle the growing weaponization of AI by cyber-threat actors.

UK Organizations Fail to Be Cyber-Resilient

How do we incentivise better security for cyber-physical systems?

- Economics
- Policy
- Culture

How can we understand the security of a wide variety of cyber-physical assets?

Wide varieties of technology that is not always easy to manage

- Data Science
- Supply Chain
- Stability

Top Python Developers Hacked in Sophisticated Supply Chain Attack

Multiple Python developers get infected after downloading malware-packed clone of the popular tool Colorama.

By Ionut Arghire
March 25, 2024

Multiple Python developers, including a maintainer of Top.gg, were infected with information-stealing malware after downloading a malicious clone of a highly popular tool, Checkmarx reports.

Called Colorama, the utility makes ANSI escape character sequences work on Windows and has more than 150 million monthly downloads.

To mount their supply chain attack, the hackers cloned the tool, inserted malicious code into it, and placed the malicious version on a fake mirror domain that relied on typosquatting to trick developers into mistaking it for the legitimate 'files.pythonhosted.org' mirror.

TRENDING

1. CISA Releases Malware Next-Gen Analysis System for Public Use
2. Second Ransomware Group Extorting Change Healthcare
3. Microsoft Patches Two Zero-Days Exploited for Malware Delivery
4. SAP's April 2024 Updates Patch High-Severity Vulnerabilities

How do we have confidence in the security of a cyber-physical system?

Even when security is done, we don't know it is being done well?

Daryna Antoniuk

January 25th, 2024

Nation-state | News | Industry | Government

Ukrainian energy giant, postal service, transportation agencies hit by cyberattacks

KYIV — Several state-owned Ukrainian critical infrastructure companies reported cyberattacks on their systems on Thursday.

Among the victims is Ukraine's largest state-owned oil and gas company, Naftogaz. According to its statement, hackers attacked a data center. As of the time of writing, the Naftogaz website and call centers are not operational.

Ukraine's cybersecurity agency told Recorded Future News that it was investigating the incident but did not provide further details. A Naftogaz spokesperson said in a comment that the company's specialists are currently working to resolve the incident and will provide comments on the attack later.

Naftogaz employs 100,000 people in Ukraine and supplies gas to over 12 million Ukrainian households. The enterprise runs 60 subsidiaries in the energy industry.

Assurance

Hardware

Testing

How can we utilise emerging technologies in a secure way within cyber-physical systems?

New technology may not be naturally designed with security in mind, how do we aid this?

- Engineering
- Policy
- Threat Modelling
- Risk

Hackers Earn $1.3M for Tesla, EV Charger, Infotainment Exploits at Pwn2Own Automotive

Participants have earned more than $1.3 million for hacking Teslas, EV chargers and infotainment systems at Pwn2Own Automotive.

By Eduard Kovacs
January 26, 2024

Cybersecurity researchers and bug bounty hunters have earned more than $1.3 million for hacking Teslas, electric vehicle chargers and infotainment systems at the Zero Day Initiative's Pwn2Own Automotive competition.

The first edition of Pwn2Own Automotive has come to an end and Trend Micro's ZDI announced that participants have been awarded a total of $1,323,750 for

TRENDING

1. CISA Releases Malware Next-Gen Analysis System for Public Use
2. Second Ransomware Group Extorting Change Healthcare
3. Microsoft Patches Two Zero-Days Exploited for Malware Delivery
4. SAP's April 2024 Updates Patch High-Severity Vulnerabilities
5. Microsoft Plugs Gaping Hole in Azure Kubernetes Service Confidential Containers
6. Patch Tuesday: Code Execution Flaws in Multiple Adobe Software Products
7. AT&T Data Breach Update: 51 Million Customers Impacted
8. CISO Conversations: Nick McKenzie (Bugcrowd) and Chris Evans (HackerOne)

How do we Build Resiliency Across Systems of Systems?

With a changing technological landscape, we are seeing further integration of these technologies together building a reliance on each other

Daryna Antoniuk

March 22nd, 2024

Malware | Nation-state | News

Sandworm-linked group likely knocked down Ukrainian internet providers

Russian state-backed hackers are likely behind recent attacks on four small Ukrainian internet providers, disrupting their operations for more than a week.

A group known as Solntsepek claimed responsibility for the incidents on its Telegram channel last week. Ukrainian officials told Recorded Future News that evidence implicates the group, which is also believed to be behind the 2023 cyberattack on Ukraine's largest telecommunication provider, Kyivstar.

A spokesperson for Ukraine's State Service of Special Communications and Information Protection (SSSCIP) said that the agency is tracking the threat actor behind the attack as UAC-0165 — the indicator used for a subgroup of Sandworm, a hacking operation run by Russia's military intelligence agency, the GRU.

A spokesperson for Ukraine's State Security Service (SBU) said that the investigation is still ongoing, but there are many indicators suggesting that Solntsepek was indeed behind the hack.

The targets in last week's attack included Triacom, Misto TV, Linktelecom and KIM, which, according to hackers, provide internet services to government agencies and parts of the Ukrainian armed forces. Those providers are relatively unknown in Ukraine, making it difficult to verify the hackers' claim.

NCSC
CYBER PHYSICAL

ANDREW.F2@NCSC.GOV.UK

DAFNI

Data & Analytics Facility for National Infrastructure

UKRI Science and Technology Facilities Council

UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES

UKRI Engineering and Physical Sciences Research Council

DAFNI
Data & Analytics Facility for National Infrastructure

Agenda

- What is DAFNI
- DAFNI's themes
- Link with the Digital Twin Energy Grids
- DAFNI – Data Infrastructure for National Infrastructure (DINI) Project

What is DAFNI?

UKRI Science and Technology Facilities Council
UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES
UKRI Engineering and Physical Sciences Research Council
DAFNI Data & Analytics Facility for National Infrastructure

DAFNI is:

- A hybrid high-performance computing platform
- A secure repository for heterogeneous national infrastructure data and models
- A place for sharing and combining data and models
  - A hybrid high-performance computing platform
  - A secure repository for national infrastructure data and models
- A place to support collaborations and deploy applications
  - A collaborative platform to research multi-system models of infrastructure
- A place as a legacy

UKRI Science and Technology Facilities Council
UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES
UKRI Engineering and Physical Sciences Research Council
DAFNI Data & Analytics Facility for National Infrastructure

DAFNI Themes

Science and Technology Facilities Council
UKCRIC™
UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES
Engineering and Physical Sciences Research Council
DAFNI
Data & Analytics Facility for National Infrastructure

DAFNI Themes

- **UK Research and Innovation - Resilience**
  - Building a Secure and Resilient World – Five strategic themes
  - £4m funded to DAFNI programme working within the subtheme;
    - Strengthening Resilience in natural and built environment in response to short-term and long-term threats via computational modelling
      - Funded the community £1.4m looking into the following
        - Supporting key models, Developing a Resilience Framework and Exploring Resilience Frameworks

- **Department of Science, Innovation and Technology – Data Sharing**
  - £5.3m pilot initiative to address barriers to data sharing, looking into a UK Research Data Cloud
  - Running a Data Infrastructure for National Infrastructure Project (DINI)
  - Focusing on exploring the barriers and opportunities to data sharing
  - DINI Objectives; Situation Analysis, Data Publication support, Enabling Services and Benefits Realisation

BSRW Projects

Developing a Resilience Framework	
USARIS Dr Francesca Pianosi, University of Bristol	Uncertainty quantification and sensitivity analysis for resilient infrastructure systems

Supporting Key Models	
Pywr-WREW Dr Anna Murgatroyd, University of Oxford	A Water Resources model for England and Wales built in Python water resources simulation system
FIRM Prof. Richard Dawson, University of Newcastle	An agent-based model of flood infrastructure resilience – FIRM
SCQUAIR Dr Richard Milton, University College London	Small Changes and Computer-Generated Spatial Interaction Modelling with QUANT

Exploring Resilience Scenarios	
STORMS Dr Xilin Xia, University of Birmingham	Strategies and Tools for Resilience of Buried Infrastructure to Meteorological Shocks
RIWS Dr Ana Mijic, Imperial College London	Resilience Scenarios for Integrated Water
SOFRAMODE Dr Vassilis Glenis, University of Newcastle	Sewer overflow flood risk analysis model DAFNI enabled
NIRD Dr Raghav Pant, University of Oxford	Systemic resilience of interdependent infrastructure networks at the national scale

UKRI Science and Technology Facilities Council

UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES

UKRI Engineering and Physical Sciences Research Council

DAFNI Data & Analytics Facility for National Infrastructure

BSRW/RDC "Sandpit" Projects

Transport (subject to contract)	
ClimaTracks Solutions (Rail) Giuliano Punzo, University of Sheffield; Ji-Eun Byun, University of Glasgow; Qian Fu, University of Birmingham; Tohid Erfani, UCL; Iryna Yevseyeva, De Montfort University; Kostas Nikolopoulos, Durham University	Forecasting resilience of railway network under propagating uncertainty
IMPACT (Road) Dr. Qiuchen Lu, UCL; Prof. Tao Cheng, Mr. Xuhui Lin, Dr Tohid Erfani, Dr Trung Hieu Tran	Improving flood disrupted road networks resilience with dynamic people-centric digital twins
MARS (Airports) Fabian Steinmann, Cranfield University	Flight Diversion Modelling for the UK Aviation System

Energy (subject to contract)	
D-RES Desen Kirli, University of Edinburgh; Laiz Souto, University of Bristol	Provision of distributed grid resilience using EVs during extreme weather events
ForNET Kostas Nikolopoulos, Durham University; Lu Yang, York St John University; Haoran Zhang, University College London	DAFNI Forecasting Services for Energy Networks resilience using EVs during extreme weather events
BRINES Hannah Bloomfield, Newcastle University; Sean Wilkinson, Newcastle University; Ji-Eun Byun, University of Glasgow	Building risk-informed redundancy in energy systems transitioning to net-zero

UKRI Science and Technology Facilities Council

UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES

UKRI Engineering and Physical Sciences Research Council

DAFNI Data & Analytics Facility for National Infrastructure

DINI: Data Infrastructure for National Infrastructure Project

Science and Technology Facilities Council

UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES

Engineering and Physical Sciences Research Council

DAFNI Data & Analytics Facility for National Infrastructure

Project Objectives

A pilot study on the requirements and impact of supporting sharing and analysis of data across National Infrastructure systems, with a focus on energy, water and transport, and the related natural, built and social and economic environment.

1.Situation analysis: Identify the benefits and barriers to data sharing, exchange and reuse for infrastructure systems data and related domains – for example by enabling communities to connect across data platforms for multi-disciplinary research, to deliver impact across themes.

2.Data publication support: Recommend best practises to enable the FAIR publication of and access to infrastructure systems data, including data policy and data sharing agreement templates, and data annotation and terminology including ontologies and the use of Digital Object Identifiers.

3.Enabling services: Pilot data brokering services to catalogue and provide access to infrastructure data and make it available for interoperation and reuse in traceable analysis processes.

4.Benefits realisation: Demonstrate potential benefits via case studies on the use of interoperable data in cross-domain scenarios.

Link with Digital Twin Energy Grids

UKRI Science and Technology Facilities Council
UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES
UKRI Engineering and Physical Sciences Research Council
DAFNI Data & Analytics Facility for National Infrastructure

Our role

Platform

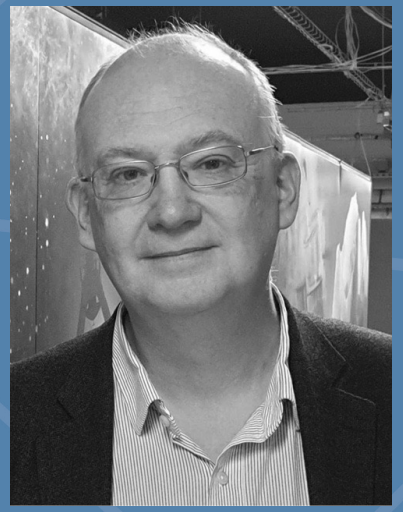
- Provide access to the DAFNI platform and provide training
- Opportunity to collaborate with DAFNI community and researchers

Host a workshop with funded projects

- Addressing the following;
  - Challenges and barriers to data sharing
  - Access to high quality and accessible data in energy networks
  - Explore best practices in data annotation and publication for the sector
  - Exploring organisational, cultural and ethical barriers

Workshop Logistics

- One day workshop in person
- Estimate late August
- More details to follow



Thank you

Dr Brian Matthews
Brian.Matthews@stfc.ac.uk
www.dafni.ac.uk
info@dafni.ac.uk

Any Questions?

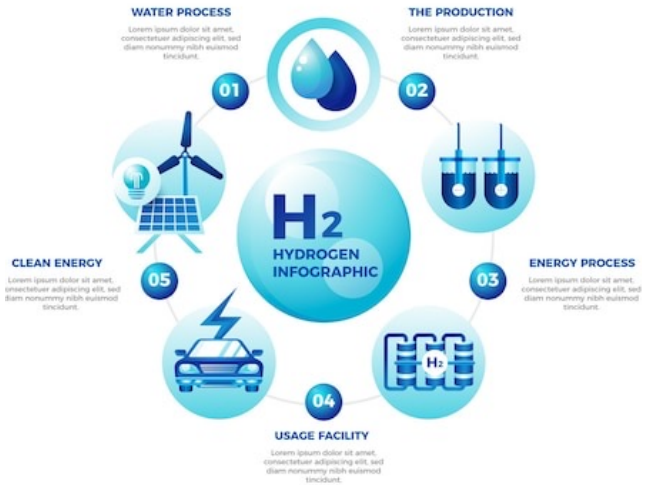
UKRI Science and Technology Facilities Council

UKCRIC™ UK COLLABORATORIUM FOR RESEARCH ON INFRASTRUCTURE & CITIES

UKRI Engineering and Physical Sciences Research Council

DAFNI Data & Analytics Facility for National Infrastructure

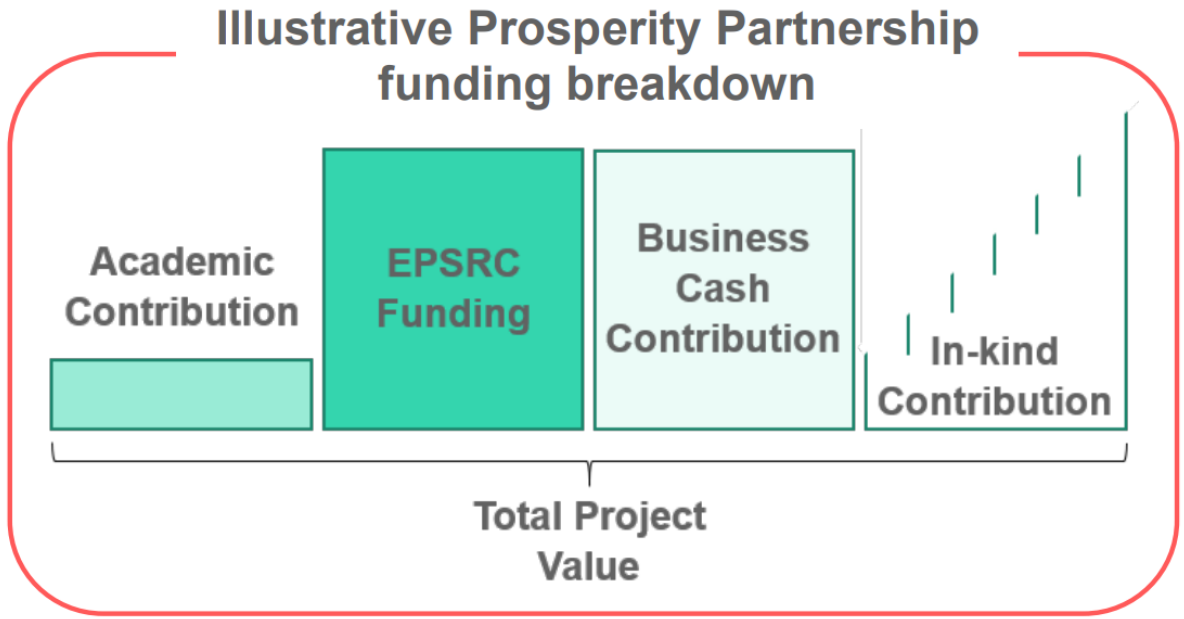
Ensign – Energy System Digital Twin



H_2 image by https://www.freepik.com/free-vector/gradient-hydrogen-infographic_37452070.htm#query=green%20hydrogen&position=5&from_view=keyword&track=ais other images from Unsplash and Pexels (free to use)

What are Prosperity Partnerships?

Large-scale collaborative research programmes funded jointly by businesses and the UK Government through the EPSRC and other UKRI councils. Highlighted as a **Key Action** in the Government's UK Innovation Strategy, these partnerships are an opportunity for businesses and their existing strategic academic partners to **co-create** and **co-deliver** a **business-led** programme of research activity arising from a clear industrial need.



Engineering and Physical Sciences Research Council

Investment: £10mil

Funder

£4,340,128

UKRI Engineering and Physical Sciences Research Council

Co-Funder & Delivery Team

SPEN
£4,519,680

Strathclyde
£1,085,032

SP ENERGY NETWORKS

University of Strathclyde Glasgow

HERIOT WATT UNIVERSITY

University of St Andrews

UNIVERSITY OF LIVERPOOL

Partner & Support Team

£258,467

UK Power Networks Delivering your electricity

Scottish Water Trusted to serve Scotland

CATAPULT Energy Systems

TRANSPORT SCOTLAND CÒMHDHAIL ALBA

The D'Arcy Thompson Simulator Centre WHERE MINDS MEET

Flexitricity

The National HVDC Centre

Logan Energy hydrogen technologies

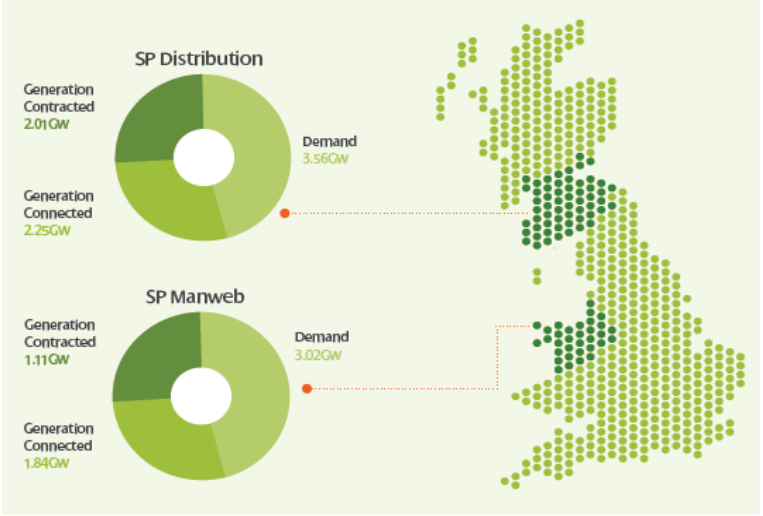
nationalgrid

UNIVERSITY of STRATHCLYDE PNDC

A Strategic and Established Partnership

SP ENERGY NETWORKS

- Transmission and Distribution £5billion investment in the coming 5 years
- Innovation portfolio: Iberdrola £386m in 2021 alone, SPEN £150m;
- 186 SMEs and 13 Universities in the UK;
- Strong links with all partners on major projects, CDT, EDT.



University of Strathclyde Glasgow

- 40+ projects over more than 30 years; PNDC; SPARC; Scottishpower Chair
- Principal Sir Jim McDonald on SPEN's Executive Board.
- Projects: RESCUE, PHOENIX, EFCC, and several others.

HERIOT WATT UNIVERSITY

- IDRIC - Industrial Decarbonisation Research and Innovation Centre
- Energy Revolution Research Consortium;
- Lead major network on EDI

University of St Andrews

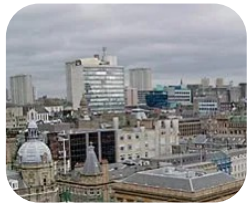
- Hydrogen Accelerator projects and hydrogen vehicle implementation - Hydrogen Train, Hydrogen bus, LOCATE
- Hydrogen production and utilisation basic research activities, Nexgenna

UNIVERSITY OF LIVERPOOL

- Expertise in heat pump and heat storage: FASHION, Green-Ice, and Therma-Pump
- Two EPSRC awards with SPEN support.

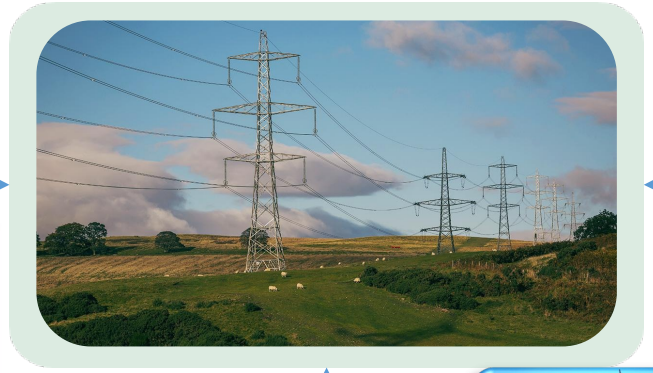
Integrated Energy System-Digital Twin

Industrial Cluster Sub-DT



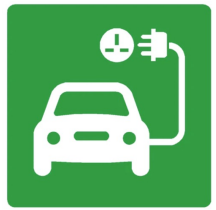
Communication and Interaction

Electrical Network Sub-DT

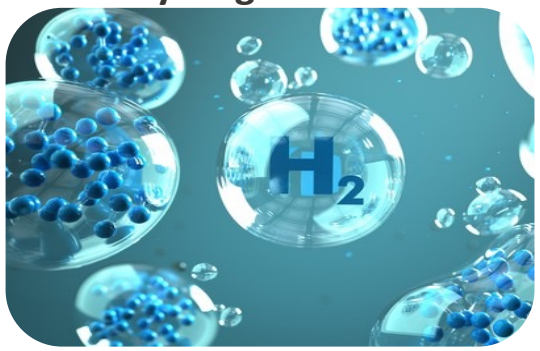


Communication and Interaction

Heat Sub-DT



Hydrogen Sub-DT



Engineering and Physical Sciences Research Council

ENSIGN will create knowledge of future energy system behaviour: electrical system - focussed but with investigations of interactions between vectors – from long to short timescales

Outputs and Organisation

- Integrated set of multi-vector DTs
  - large, energy-intensive industrial clusters, to small domestic and commercial prosumers
  - renewables, storage, electrified heat and transport
  - contexts ranging from rural/sparse to urban/dense
  - represent a range of operational scenarios, from normal, to extreme and emergency contingencies…
- Generate understanding and knowledge
  - how will systems behave and interact?
  - flexibility, opportunities – enhance planning and operation
  - defining the most appropriate use cases very important
- Engagement, dissemination are critical aspects

Engineering and Physical Sciences Research Council

Contacts

Prof. Campbell Booth (Academic Lead)
campbell.d.booth@strath.ac.uk

James Yu (Industrial Lead)
james.yu@spenergynetworks.co.uk

Jill Rymer (Project Manager)
jill.rymer@strath.ac.uk

Afia Masood (Portfolio Manager, EPSRC)
Afia.masood@epsrc.ukri.org

Engineering and Physical Sciences Research Council

Innovate UK

Q&A

Innovate UK

Breakout Sessions

Innovate UK

Break

Innovate UK

Wrap-up & Close