Department for
Science, Innovation
& Technology

Cyber-Physical Infrastructure Consultation Response

March 2023

Any enquiries regarding this publication should be sent to us at:
cpiconsultation@beis.gov.uk

Contents

Contents 3

Foreword 4

1 Executive summary 5

2 Introduction 6

2.1 What is Cyber-Physical Infrastructure? 6

2.2 The UK's industrial cyber-physical potential 7

2.3 Why should we care? 8

2.4 What do others think? 9

3 Role of government and actions we are taking 10

3.1 Role of government in supporting key enablers 10

3.2 Government and wider public sector actions 10

3.3 Wider activity 12

4 The UK as a Cyber-Physical Innovation Nation 13

5 Key areas of opportunity 15

5.1 Building on UK Strengths 15

5.2 Sectors 16

5.3 Cross-cutting opportunities 19

5.4 So what 22

6 Key enablers and the role of government 23

6.1 Security & resilience 23

6.2 Interoperability 25

6.3 Recognised value propositions 27

6.4 Frameworks, guidance and standardisation 29

6.5 Skills 30

6.6 Others 31

Annex – Summary of responses to consultation 32

Foreword

From our creative industries to advanced manufacturing and medical robotics, industrial design, Cyber-Physical Infrastructure (CPI), technology & innovation are becoming increasingly key to our future economy.

In the global race for science, research, technology & innovation (SRTI) investment and leadership, the UK's strengths in the field of CPI are a major economic asset that we intend to deepen and better harness for economic advantage as part of this Government's strategic commitment to move the UK to a more strategic SRTI economy.

Through the creation of the NSTC, the new Department of Science, Innovation and Technology, the biggest uplift in public R&D for a generation (a total £52 billion over the next three years); and the creation of ARIA, our £800 million global super lab for world class scientists to explore frontier science and technology; we are making the serious investments for a new era of science and technology led growth.

The pace of technology is also transforming the way in which science, research and innovation is conducted. The inexorable convergence of both our digital and physical worlds is creating an increasingly connected ecosystem of cyber-physical systems forming the Cyber-Physical Infrastructure, enabling a new realm of hitherto unimaginable new opportunities.

So now is the time to secure UK leadership in this new technological revolution, building on the billions of pounds that the private sector has invested in UK robotics, internet of things, AI, machine learning and a suite of associated technologies driving CPI.

To do that we need to bring together the innovators, end users, regulators, researchers, integrators, public organisations and wider society to help shape this technology and sector into one that is innovation enabling, responsible, resilient and helps drive a high-skills, high-wage economy, where innovation is supported and rewarded across the UK.

I would like to thank all those innovators, entrepreneurs, investors and businesses that have already helped shape this agenda and our thinking, and look forward to continuing to work with you and the increasingly large community of collaborators in this exciting field as it develops.

George Freeman

Minister of State, Department for Science, Innovation and Technology

1 Executive summary

From collaborative swarms of drones packing our food, to interactive virtual representations of operational hospitals, cyber-physical systems and their increasing interconnection are transforming our world at an increasing rate[1].

Our consultation last year explored the opportunities and challenges of a national Cyber-Physical Infrastructure, in which connected networks of such systems could provide a step change in the economic and social value of the individual applications.

A significant number of written responses from industry (including both developers and users), academia, the wider public sector and wider society, supplemented by extensive online and in-person dialogue has informed this response.

The strategic value and opportunities of Cyber-Physical Infrastructure were strongly endorsed by respondents, particularly highlighting: Innovation and productivity; Resilience; Climate change response; and Levelling up.

Responses highlighted opportunities across a range of sectors, recognising the breadth and cross-sectoral potential of Cyber-Physical Infrastructure. However, the opportunities within the following sectors were identified most prominently: Energy Systems and utilities; Infrastructure and Built Environment; Manufacturing; Natural Environment; Transport and Supply Chains; and Wellbeing, Health and Social Care. Two cross cutting areas of Research, Development and Innovation, and Net Zero were also strongly identified (see Section 5 for more detail).

There was also a strong call for government to help tackle a number of systemic challenges, through the supporting key enablers, namely: Security & resilience; Interoperability; Recognised value propositions; Frameworks, guidance and standardisation; and Skills (see Section 6 for more detail).

This consultation response sets our vision to enable greater innovation in the UK through a Cyber Physical Infrastructure (see Section 4) and the key next steps that we and wider public sectors partners will continue to take in collaboration with industry, academia and wider society to realise this, including:

- Launching a grant competition to fund one or more organisations working together to develop and host a Cyber-Physical Infrastructure ecosystem accelerating capability
- Continued UKRI funding of a breadth of cyber-physical research, development and innovation including:
  - £3m to develop a multi-disciplinary UK digital twinning research community
  - Additional funding for digital twinning research to support and improve the operation and resilience of the UK energy grid

[1] https://www.gov.uk/government/publications/cyber-physical-infrastructure

  - A suite of Catapult-led Cyber-Physical Infrastructure projects
  - Up to £20m for a research hub in digital twinning for decarbonisation and improved integration of the UK's transport system
  - £7.5 million in cyber security research with partners including the National Cyber Security Centre
  - A Turing Research and Innovation Cluster (TRIC) in Digital Twins
- Department for Transport investing in digital twins for transport
- Department for Business and Trade continuing to lead delivery of the National Digital Twin Programme

See Section 3 for more detail.

2 Introduction

2.1 What is Cyber-Physical Infrastructure?

Cyber-physical systems connect the physical and digital domains. Data shared between physical system their digital counterparts produce insights and feed decision-making: from scenario modelling and collaboration across locations and platforms, to optimisation and even autonomous operation.

They are increasingly widespread and have societal, environmental and economic benefits that are significant in the short term and are expected to be globally transformational in the longer term, as network effects build. Such systems include digital twins and simpler digital models, robotic & autonomous systems, the internet of things (IoT) and augmented/virtual reality (AR/VR)[2]. Examples of applications include:

- Transport for Greater Manchester and VivaCity achieved a 23% reduction in junction journey time by bringing together IoT sensors, Artificial Intelligence (AI), simulation, and connected smart traffic lights[3]
- Rolls-Royce have achieved 30% efficiency improvements of manufacturing shop floor staff through augmented reality and digitalisation of their assets and work flows[4]

The value of individual cyber-physical systems increases with their ability to inter-connect. In the same way that the benefits of computers and phones grew exponentially as they began to connect to each other via networks (e.g. the Internet), so will the value of cyber-physical systems increase at the network effect grows. Imagine a world where we are not only able to innovate and optimise within an urban traffic system, but also seamlessly bring together the

[2] https://www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation-consultation-document-accessible-webpage#annex-a--summarising-a-range-of-key-cyber-physical-infrastructure-elements
[3] https://vivacitylabs.com/smart-junctions-uk5g/
[4] https://www.youtube.com/watch?v=GDhqgMoLMHs

interactions with the built environment, energy infrastructure, weather, social dynamics, local government policy and even vehicles themselves.

An ecosystem of networked systems could be an infrastructure on which future products, services and decision-making processes are built – i.e. a Cyber-Physical Infrastructure, sometimes referred to as the cyber-physical internet. These interconnected systems and the architectures, tools, platforms and data that underpin them, would underpin faster and cheaper innovation by providing the building blocks for innovators to design, test, build and connect their solutions more easily.

In 2022, we ran a written consultation, supplemented by online and face to face engagements to advance the UK's understanding of the impact and opportunities for cyber-physical systems, and the value of, and options for an underpinning Cyber-Physical Infrastructure to unleash innovation. This publication sets out our response including our developed understanding, priorities and next steps.

Case Study: The Augmented Human – The University of Sheffield Advanced Manufacturing Research Centre, Rolls-Royce, Innovate UK

The Augmented Human project demonstrated how connecting the worker to digital systems like MES (Manufacturing Execution System) using AR can lead to improvements in manufacturing efficiency. Core manufacturing software and cloud hosted work packages were brought together with mixed reality headsets, smart watches, smart phones, tablets, and projection tools in the assembly of a Rolls-Royce aerospace engine.

This enabled improved information delivery and operational efficiency by accelerating training and reducing the time spent by engineers away from components, using overlaid instructions and visualisation environments.

The Augmented Human project demonstrated (in a controlled environment), engine assembly productivity and efficiency improvements of up to 30%.

2.2 The UK's industrial cyber-physical potential

UK businesses are already heavily investing in and utilising the technologies that will be core to Cyber-Physical Infrastructure. Between 2018 and 2022, total equity fundraising in UK companies linked to robotics totalled £3.5 billion. For IoT and AR/VR the totals were £6.1 billion and £2.4 billion, respectively[5].

This shows the scale of activity that already exists. The increasing interconnection of these systems has the potential to make this far more than the sum of its parts and this is evident in

[5] BEIS analysis of Beauhurst data

the rapid global growth in convergent systems such as digital twins. Globally, the market for digital twins has a forecasted compound annual growth rate (CAGR) of 40.6%[6].

The world-wide trend towards convergence is clear and the UK has the potential to be at the forefront of developing and realising the benefits to businesses and society, both here and in international markets through our existing capabilities and leading cyber-physical agenda.

2.3 Why should we care?

A global Cyber-Physical Infrastructure is coming – how we want it to develop and whether we want the UK to be at the vanguard or catching up informs the role we will play.

The UK has the opportunity to pursue a resilient, responsible and innovation-enabling Cyber-Physical Infrastructure, with industry, academia, central government and the wider public sector collaborating to build a sustainable ecosystem. Through this, there are significant benefits to seize, including:

- **Innovation and productivity**: quicker, safer and more cost-effective design, testing and optimisation of systems, not limited by geography or physical infrastructure
- **Resilience**: greater systems-of-systems understanding, through scenario planning, monitoring and rapidly reconfigurable tools, enabling rapid response to threats and crises
- **Climate change response**: enabling future energy generation, Net Zero transformation of carbon-intensive sectors (manufacturing, transport etc.), operation of our future energy systems and responding to extreme weather events
- **Levelling up**: enabling individuals and businesses to innovate, collaborate and develop across the UK

As with the Internet and the ecosystem of the World Wide Web, governments themselves will not build this future. Innovators across sectors will collaborate, build and connect. However, the UK government has a clear interest in the ecosystem being secure, resilient and competitive; and in accelerating the benefits both to the UK at large and in delivery of public infrastructure and services itself. There are lessons to be learned in both these domains from the key early roles of governments and how networks, the Internet and subsequent ecosystem developed[7],[8].

The UK has key strengths both in creativity and design, and the research and innovation in advanced technology domains such as AI, digital twins, robotics & autonomous systems,

[6] https://www.fortunebusinessinsights.com/digital-twin-market-106246

[7] 5G supply chain diversification strategy - https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

[8] New pro-competition regime for digital markets - https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets

innovative uses of data, data infrastructure and synthetic environments, many of which were pioneered by sectors such as transport and the video game industry.

Key stakeholder groups are already commencing work (e.g. within the energy sector National Grid ESO, Ofgem, and network operators are each investing in energy grids' digitalisation[9],[10]), but they are calling, including through their responses to the consultation, for government to help address systemic challenges to development and adoption.

Therefore, we care because it is coming and it is incumbent upon us to play an active role in how that happens; there will be risks emerging as part of this that we need to address; there are significant opportunities for the UK's society and economy; and we have received a clear call from key players in the ecosystem to take an active role.

2.4 What do others think?

In 2022, we consulted on the opportunities of Cyber-Physical Infrastructure and barriers to realising them. We received 61 responses from businesses (including industrial users, system integrators, IT majors and small innovators), universities, public sector/research orgs and charities. We also held 12 round tables with over 300 attendees, including many SMEs.

The consultation responses provided strong endorsement of both the opportunities and barriers set out, as well as the role of government in working with industry, academia and wider society to help overcome specific systemic challenges that organic development will not address.

Therefore, whilst the development and deployment of Cyber-Physical Infrastructure will be driven and lead by industry and academia, government has two key roles to play:

1. *Supporting the enablers identified in Section 3 to maximise the value of Cyber-Physical Infrastructure to the UK*

2. *Realising the benefits of Cyber-Physical Infrastructure in priority applications for public sector delivery*

We will work with partners to take and coordinate action in these two areas. See Section 3 for the steps government is taking now in partnership with industry, academia and the wider public sector.

[9] https://www.nationalgrideso.com/future-energy/virtual-energy-system

[10] https://www.ofgem.gov.uk/publications/ofgems-strategic-innovation-fund-pushes-further-ahead-innovation-projects-help-drive-bring-down-consumer-costs-decarbonise-energy-system-and-reduce-dependence-costly-fossil-fuel-imports

3 Role of government and actions we are taking

3.1 Role of government in supporting key enablers

Whilst innovators will be the ones that build Cyber-Physical Infrastructure, consultation responses set out the clear and limited ask for government to help address systemic challenges through the following key enablers:

- **Security & resilience** – supporting the development of systems that can withstand attacks and failures, both at an application level and nationally, such as systemic supply chain risks
- **Interoperability** – ensuring different organisations and systems can connect and communicate as easily as possible
- **Recognised value propositions** – supporting the development and communication of the knowledge of how to develop and apply cyber-physical systems and the value they deliver, to facilitate investment
- **Frameworks, guidance and standardisation** – supporting the collaboration required to develop the common language, approaches and technical requirements for development and deployment, with the subsequent dissemination of this
- **Skills** – supporting the development of technical and non-technical skills required to develop a national capability in Cyber-Physical Infrastructure

These are set out in further detail in Section 6.

We have been working with partners inside and out of the public sector since the consultation launched to help develop their workstreams informed by the insight gleaned through this exercise, make the case for investment and facilitate collaboration.

3.2 Government and wider public sector actions

By no means an exhaustive list, below we identify some of the key actions that the Department for Science, Innovation and Technology (DSIT) and partners are working closely together on to deliver.

Cyber-Physical Ecosystem Grant Competition

Today, DSIT is launching a grant competition to fund one or more organisations working together to develop and host a Cyber-Physical Infrastructure ecosystem accelerating capability. This will promote the agenda with the UK, promote connections, coordination and collaboration between stakeholders (particularly those in industry) and facilitate the development of resources that drive investment, development and adoption of cyber-physical systems.

Up to £200k in total will be made available over the next two financial years to support this. Please see details of the competition.

On data, DCMS are leading activity with partners to explore and test the enablers of greater data sharing, supported by robust UK data infrastructure, as part of the Mission 1 of the National Data Strategy. This includes working with UKRI and the Compute Review[11] to establish the right foundations for data sharing, developing and testing these. Consideration of market-led data standards is also underway, particularly increasing awareness and adoption.

UKRI

UKRI are funding a range of investments in cyber-physical systems research, development and innovation, plus with academic ecosystem forming.

A £3m funding opportunity has been launched under **UKRI's Building a Secure and Resilient World theme** to develop a multi-disciplinary UK digital twinning research community. UKRI will also provide funding for applied digital twinning research to support and improve the operation and resilience of the UK energy grid. In addition, there will be further funding and support for the DAFNI platform to allow researchers to use state-of-the-art modelling, simulation, and visualisation, developing UK capability to reduce vulnerabilities, to respond to and recover from shocks.

The **Engineering and Physical Sciences Research Council (EPSRC)** have launched a call for the leader of research hub in digital twinning for decarbonisation and improved integration of the UK's transport system, with up to £20m allocated to the hub. EPSRC are also investing £7.5 million in cyber security research with partners including the National Cyber Security Centre and intend to make future investments in core research in digital twinning.

EPSRC are the founding partner and major funder of the **Alan Turing Institute**, who have established a Turing Research and Innovation Cluster (TRIC) in Digital Twins[12]. Building on £26m of investment in digital twin research to date, the TRIC will help democratise access to digital twin technology by providing open and reproducible computational and social tools freely accessible to the UK research and innovation communities.

On top of co-funding a wide range of robotics and autonomous systems, AI and ML, IoT, AR/VR and other cyber-physical RD&I projects[13,14,15,16,17], **Innovate UK**, the UK's innovation agency, has invested £5.5m into a Catapult Network led Cyber-Physical Infrastructure projects

[11] https://www.gov.uk/government/publications/future-of-compute-review

[12] https://www.turing.ac.uk/research/harnessing-power-digital-twins/turing-research-and-innovation-cluster-digital-twins

[13] https://www.ukri.org/blog/aiming-high-for-ai-innovate-uks-role-in-supporting-ai/

[14] https://ktn-uk.org/programme/immerse-uk/

[15] https://ktn-uk.org/digital/internet-of-things/,

[16] https://www.ukri.org/what-we-offer/browse-our-areas-of-investment-and-support/robots-for-a-safer-world/

[17] https://www.dsbd.tech/

across energy, manufacturing, transport and digital technology. These projects help develop the ecosystem, supporting companies to meet societal and environmental challenges. Access to this ecosystem enables SME's to commercialise research, turning it into economic growth.

Department for Transport (DfT)

DfT will be working with the Alan Turing Institute, providing an initial £0.5 million to further research the application for Digital Twins in transport including in traffic management and infrastructure optimisation.

National Digital Twin Programme (NDTP)

The NDTP is continuing to work with industry and academia to understand the need for, and develop, the standards, frameworks, guidance, processes and tools that will:

- enable people to gather, process, manage, store and share information in a way that ensures the right information is available at the right time, to the right people and that the quality of the information is understood; and
- enable users to engage with, and visualise, the information in way that meets their needs and support and optimise decision-making.

Outputs are being tested in real world situations through demonstrator work, examining ethical, security, resilience, legal, regulatory, commercial and sustainability considerations, as well as human/twin interfaces, issues relating to education, training and the cultural change required to support wider adoption. The main component of the demonstrator programme taking place on the Isle of Wight and is currently focussed on. infrastructure resilience, emergency planning and responsiveness, and energy demand, use and supply. The programme has £20m of funding for the period April 2022 to March 2025

3.3 Wider activity

As demonstrated by the breadth of cases highlighted throughout, there is significant and growing activity within the wider ecosystem, that we would not be able to list in full nor will we seek to direct. Just as the vision for federated cyber-physical systems envisages democratised connections and information sharing, so the development of these ecosystems must be based around sustainable, collaborative development – not owned or driven by a single organisation or oligopoly.

Government’s role in supporting ecosystem development will be through progressing the key enablers identified, as set out above, and promoting the collaboration and dissemination of information between these broader initiatives.

Within government, there are key supporting agendas that were highlighted through the consultation, including skills, data as set out in detail, along with public procurement, wider security and digital & tech policy, and international technology collaboration. We will bring the capability, assets and resources of central government to bear on this agenda of convergence.

We will work with industry, both large and small, UK and international; with the wider public sector including LAs, regulators, and local authorities; with academia and research organisations; and with wider society to advance the UK's capability and global standing.

The UK's cyber-physical future will be made by innovators across this landscape, and government has a necessarily limited role. But if we can generate and sustain the right collaborations and shared endeavours, we can put the UK in the vanguard of the next major technological sea change.

4 The UK as a Cyber-Physical Innovation Nation

Cyber-Physical Infrastructure could help catalyse the evolution of the UK economy into a more resilient, innovation-based economy – that goes beyond a south-east-centric service-dependent economy to one where individuals and companies across the UK are able to rapidly develop their innovations into scaling businesses.

Reaching a world where cyber-physical systems and the enabling building blocks are readily available and connected across the economy with minimal user effort is a long-term vision, to be fully realised in the 2030s. However, it requires action now to accelerate the timeline and realise the benefits already within reach.

Case Study: Grimsby Living Lab, 5G testbed and DOME - Offshore Renewable Catapult

Offshore Renewable Catapult are using 5G to bring together organisations and assets in and around Grimsby, creating a living lab to build on Grimsby's strength as the world largest operation and maintenance hub for offshore wind.

The 5G testbed for the port of Grimsby and nearby windfarm will provide a demonstration and test zone for Robotics and Autonomous Systems (RAS) and other IoTs. This will enable technology and solution developers to test products such as autonomous robotics, remote sensors, wearable technology and zero emissions vessels.

The Digital Operations and Maintenance Environment (DOME) is a scalable and flexible digital construction space for organisations to develop, demonstrate and test solutions in a high-fidelity virtual environment. The DOME provides a common 'digital world' into which end users input their datasets and models, bringing together SMEs, asset owners, technology developers, Catapults and universities to problem solve and refine new ideas and solutions in a connected, secure and cost-effective platform. The DOME will also allow Human and Hardware-in-the-loop solutions to be simulated in real-time.

Below, we set out the short- to medium-term ambitions that will guide our work with industry , academia and the wider public sector to advance the agenda.

1. Clusters of organisations with clear ambitions for how connected cyber-physical systems will benefit their organisations/sector

   This will be evident through the level of public statements of ambitions and plans to realise the benefits, of which we expect to see tangible progress over the next 6-12 months.

2. Tangible advances in underpinning connected cyber-physical system capabilities (technical and non-technical, inc. security & interoperability)

   Progress will be demonstrated through advancements in technology readiness levels (TRLs) of underpinning technologies and applications, answering of key research questions and development and adoptions of resources such as assets, frameworks, guidance etc. This will be a more gradual development, with significant increases expected in advancements over the next 12 months and research outputs following. Progress will be particularly key in priority sectors highlighted.

3. Value of connected cyber-physical systems demonstrated in multiple applications and sectors

   Moving beyond R&D, seeing the application of connected cyber-physical systems demonstrated in real-world applications will be key to unlocking future investment. Simple use cases are already being promoted, whilst more complex innovations will accelerate over the next 12-24 months, with opportunity to measure the number, scale and value of them.

4. National Cyber-Physical Infrastructure collaboration across sector boundaries, with shared understanding of common needs and enablers

   Collaborative fora are already propagating and we would expect to see an increase in the number, membership and outputs of these over the next 12 months. Progress can also be assessed through increases in collaborative projects across sector boundaries in that period.

5. Emerging UK leadership in cyber-physical systems development and adoption

   Increases in the number of international collaborations (combinations of academic/industrial/governmental) and the growth in investment in UK companies developing and deploying cyber-physical systems may be useful indicators of the UK's standing in this domain. International comparisons of the UK's capability and international recognition could also be useful measures. The geographic spread of organisations and projects within the UK itself will also be an indicator of the strength of sustainable capability. We would expect these measures to show progress over the next 18 months.

To drive progress against these ambitions, we will work with partners to deliver the next steps set out in Section 3.

5 Key areas of opportunity

5.1 Building on UK Strengths

The UK already has significant strengths in numerous component technologies that will help realise the opportunities of Cyber-Physical Infrastructure including artificial intelligence, digital and advanced computing, and robotics and smart machines[18],[19],[20]. This is underpinned by world leading financial services industry and thriving investment ecosystem, with the largest Venture Capital market in Europe, larger than France and Germany combined[21]. Cyber-Physical Infrastructure will help enable transformational societal, environmental and economic benefits that are more than the sum of the individual technological parts.

Unlocking the economic value of data, a key element of Cyber-Physical Infrastructure, is a focus of UK government activity, identified within the National Data Strategy. We are exploring how data interoperability and availability can be best supported, including the roles of data infrastructure, the use of good data standards, data intermediary ecosystem, and privacy enhancing technologies. Under the 2022 to 2025 Roadmap for Digital and Data, work is underway within government to transform digital public services, deliver world-class digital technology and systems, and attract and retain the best in digital talent.

The UK's regulatory system is also forward looking and a key facilitator of innovation. For example, the Digital Regulation Cooperation Forum brings together four key regulators to collaborate and engage with innovators in digital platforms[22]. The Information Commissioner's Office recently published a Horizons report exploring how emerging technologies such as next generation internet of things (IoT) and immersive technologies interact with data protection regulations[23].

The Regulators Pioneer Fund has made more than £25m available for initiatives that help businesses bring innovative products and services to market. Not only will regulators be key in the deployment of cyber-physical systems, but the systems themselves offer the chance to accelerate innovation in regulation, including through enabling regulatory sandboxes, and advances in monitoring and controls and more.

For example, the novel approach to air traffic management being developed by air traffic control services provider NATS and the Alan Turing Institute offers revolutionary new capabilities to support safe and efficient air space regulation[24]. The Centre for Connected and Autonomous Vehicles has funded numerous such projects alongside industry, including the

[18] https://www.gov.uk/government/publications/national-ai-strategy
[19] https://www.digicatapult.org.uk/expertise/publications/post/digital-future-index-2021-2022/
[20] https://www.gov.uk/government/publications/uk-innovation-strategy-leading-the-future-by-creating-it
[21] https://www.gov.uk/government/news/uk-tech-sector-retains-1-spot-in-europe-and-3-in-world-as-sector-resilience-brings-continued-growth
[22] https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum
[23] https://ico.org.uk/about-the-ico/research-and-reports/tech-horizons-report/
[24] https://www.nats.aero/about-us/research/n/project-bluebird/

Smart Mobility Living Lab, where live feedback between the real and digital worlds can accelerate testing and increase safety of new technologies, such as self-driving vehicles[25].

UK government is also a major investor in infrastructure and public service delivery. As part of this investment, there is the opportunity to collaboratively design, develop and disseminate the shared ‘building blocks’ (e.g. models, algorithms, frameworks, technical standards, user applications, data assets etc.) of Cyber-Physical Infrastructure. This will help both the ecosystem and public services design, build, implement and connect solutions more quickly, easily and cost effectively.

Case Study: Made Smarter Digital Supply Chain Innovation Hub - UKRI, Digital Catapult

The UKRI funded Made Smarter Digital Supply Chain Innovation Hub is a £20 million programme led by Digital Catapult with support from the National Physical Laboratory, the High Value Manufacturing Catapult and TWI. The hub works with a range of industry stakeholders across sectors such as Sainsbury’s, BAE Systems and Nissan, to tackle long term challenges and opportunities for supply chains in the UK and beyond. This means enabling the building blocks for innovation and interoperability in industrial supply chains, helping to bring numerous actors together into a collaborative environment for R&D and data innovation.

This year the Hub is launching its Interoperability Flagship Programme, seeking to develop an AI based solution to enable data exchange across supply chains. Cutting edge AI/ML techniques in combination with foundational data/semantic models will help to infer and guide connections between system interfaces and generate interoperability dynamically across supply chain systems. This will help to enable supply chain digitalisation, optimisation and sustainability in support of UK priorities such as climate response, productivity, national resilience.

5.2 Sectors

Responses were received from organisations who operated in a broad range of sectors, identifying opportunities within nearly every major sector in the UK. The following sectors were highlighted most strongly in responses[26]:

- Energy Systems and utilities
- Infrastructure and Built Environment
- Manufacturing

[25] https://smartmobility.london/

[26] Response levels are not an analytical assessment of (e.g.) sector potential, as respondents are self-selecting with a natural tendency to highlight opportunities within their own domain. However, this does provide insight on the opportunities within domains and gives some indication of appetite of organisations within domains, based on their engagement with the consultation.

- Natural Environment
- Transport and Supply Chains
- Wellbeing, Health and Social Care

The true potential of Cyber-Physical Infrastructure lies in the ability to collaborate across sectors. The value of the sectors identified lies in the ecosystems of engaged organisations within them who are motivated to work within and across boundaries, to realise the benefits they have identified.

The development of Cyber-Physical Infrastructure will likely be driven by domain specific initiatives, iteratively developing alongside the cross-domain interoperability necessary to realise the wider value. Therefore, we need to encourage individual ecosystems to take action, whilst facilitating the incremental connections to other ecosystems.

There is also a vital role for local actors, including Local Authorities, in driving the place-based collaboration and convergence of these sectors. We have seen, for example with the 5G rollout, that the deployment of infrastructure and adoption of use cases can be greatly accelerated and made more than the sum of their parts through local leadership.

Case Studies: Transforming Healthcare

As hospitals evolve to deal with increasing demand and complex care needs, cyber-physical systems are playing an integral role in delivering more effective, efficient and personalised care.

Smart Hospital - Hitachi Vantara

Hitachi Vantara’s partnership with an NHS Foundation Trust shows how digital shadows and AI and IoT can optimise hospital performance and care.

A digital shadow of the hospital acts as a digital control centre where hospital staff can access patient data and monitor the health and flow of patients in real time.

Machine learning and AI generate predictions of demand, admissions, patient length of stay and discharge. These insights are used to support proactive demand and capacity management and flow, enabling a ~10% improvement in efficiency. Real time location sensors can monitor patients, assets and staff unobtrusively to automate workflows, improve productivity and manage high-risk scenarios. For example, combining these and LiDAR technology in smart patient rooms can detect a medicated patient trying to get out of bed and at risk of harm, and automatically trigger intervention by medical staff.

The digital shadow of the hospital also enables clinicians and managers to model potential changes in patient care, simulating new systems before they’re trialled safely, quickly and cost effectively.

Infectious disease management – AxoMem, a member of the Digital Twin Consortium

During the height of the COVID-19 pandemic hospitals were faced with the challenge of providing high quality and efficient care while limiting the spread of the virus. AxoMem developed digital twinning technologies to assist the management of infectious disease in hospitals.

This 3D Disease Outbreak Surveillance model of the hospital showed the location of infectious and non-infectious patients across the hospital. Spatial analytics were applied to anonymised patient data to understand the progression of the virus, review historical movement, and risk-stratify patients potentially exposed to the infectious patients. The ability to interact with the digital representation in “4D” (time and space) and integrate deep analytics provided new models for epidemiologists and clinicians to build insights about causes and progression of disease.

Case Study: Smart Junctions - VivaCity, Transport for Greater Manchester, Immense Simulations

VivaCity’s Smart Junctions was developed to improve congestion and air quality, while optimising traffic flow and user experience for different types of road users through an AI based traffic signals optimisation system.

Sensors detect and classify road users, with 5G transmitting this information to a simulation to give a real-time view of the junction. Historical and real-time data is used by an algorithm, developed using AI-based reinforcement learning techniques, to produce an optimal control strategy. This is fed back to the traffic controller at the junction, enabling optimised signal control based on demand.

In Manchester, the Smart Junctions project led to the reduction of journey times by up to 23% for motor vehicles at a site. Smart Junctions reduce the need to develop new infrastructure to meet capacity and support decarbonisation goals by optimising existing transport infrastructure to reduce congestion and associated air pollution.

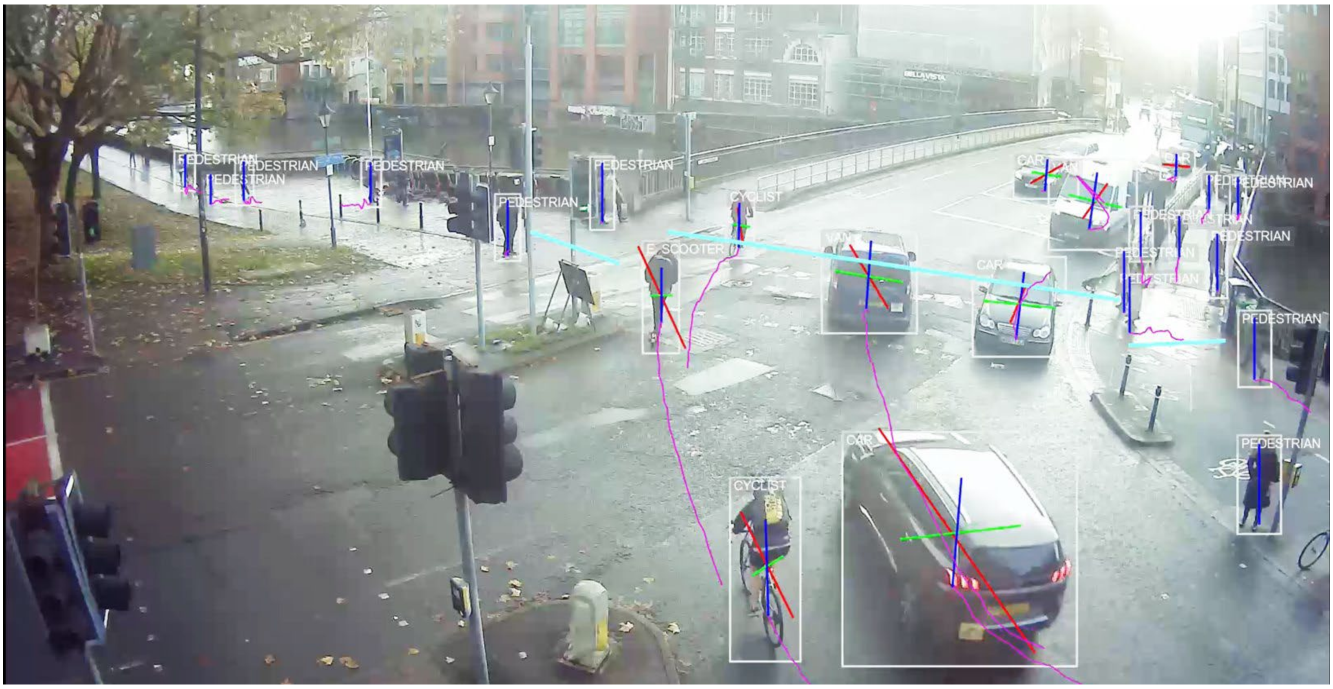

Figure 1 Visualisation of sensors classifying different road users alongside traffic lights which can be connected for autonomous operation, VivaCity

5.3 Cross-cutting opportunities

There are also areas of opportunity that cut across sectors. These can provide vital incentives and direction to cross-sector collaboration. They are also areas where government has a particular mandate and breadth of existing activity to leverage.

- Net Zero
- Research, Development and Innovation

Case Study: Enabling nuclear fusion with CPI - Remote Applications in Challenging Environments (RACE), The UK Atomic Energy Authority (UKAEA)

Fusion power plants will only be feasible with fully remote operations. UKAEA, through its cutting-edge centre for Remote Applications in Challenging Environments (RACE), are developing the connected design, testing and implementation of robotics, digital twins, IoT and VR-AR required to make nuclear fusion power plants a reality.

Within the unique Joint European Torus (JET) Remote Handling Systems, two snake-like robotic booms with arms and grippers act as the operators’ hands utilising haptic ‘touch’ feedback. VR allow the operator to see what is happening in real time with AR used to increase situational awareness. Digital twins are used for operations, strategy development, training and data management.

UKAEA is also leading RAICo, the Robotics and AI Collaboration, with the Nuclear Decommissioning Authority and University of Manchester, and has opened the RAICo1 facility in Whitehaven, Cumbria. Projects include collection of operational data using quadrupeds and drones to feed digital twins, in-situ robotic decommissioning, and increasing use of machine learning enabled handling strategies.

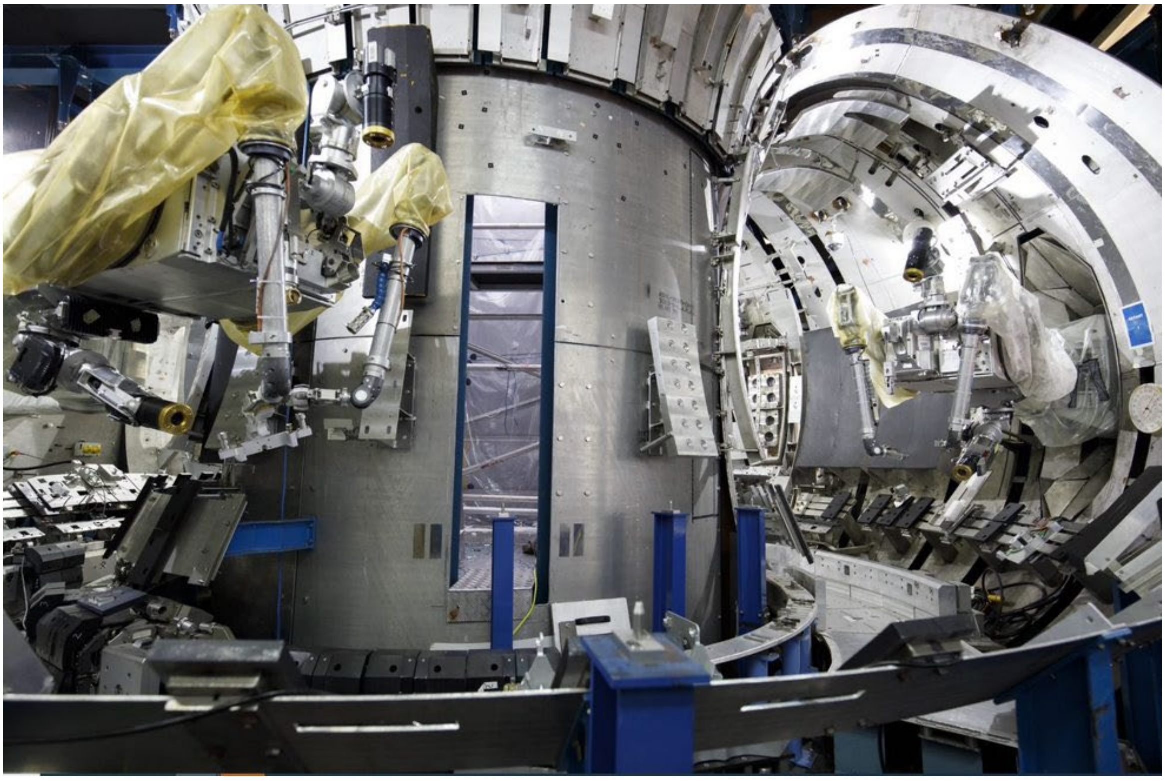

Figure 2 View of nuclear fusion reaction with robotic booms, UKAEA, RACE

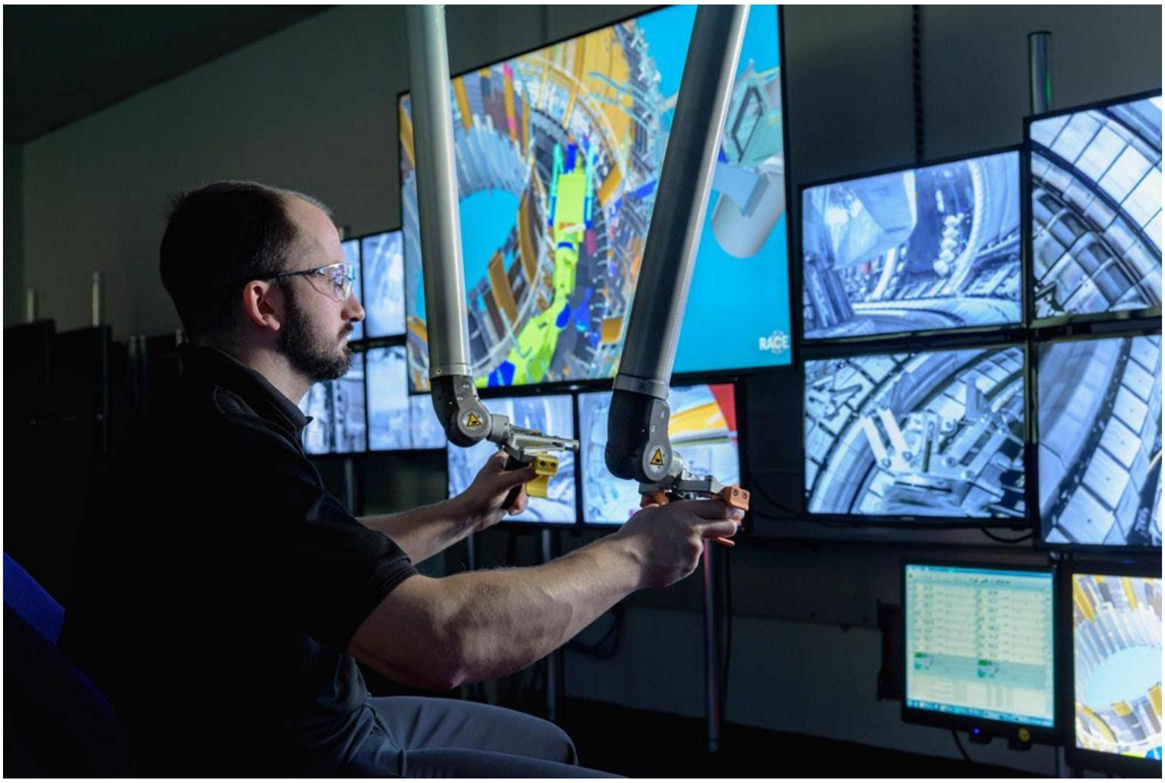

Figure 3 Operator remotely controlling the robotic booms and using VR to visualise the fusion reactor, UKAEA, RACE

Case Study: Smart Biosphere - Biosphere Foundation, Environment Agency, Devon County Council, Siemens Digital Industries Software

The Smart Biosphere project in in North Devon has been created to help stakeholders determine how energy and resources can be used more efficiently and also sustain a cleaner environment.

Smart Biosphere provides real-time monitoring of the catchment area to view environmental conditions and their inter-connections with local land use, wastewater infrastructure and water courses. Remote environmental sensors, AI and ML, IoT and satellite earth observation are used to collect and glean insights from data on issues such as soil health and carbon, pollution run-off, water quality, flood management and flood risk.

For example, sensors in the watercourses and in the ground measure critical variables that allow stakeholders to quickly detect issues such as bacterial build-up, sewage, flood risks, fertiliser run-off and industrial discharges harmful to aquatic ecosystems.

The system is scalable and replicable and can save both water regulators, farmers, and the water industry millions in terms of reduced pollution, improved efficiencies and safeguarded investments.

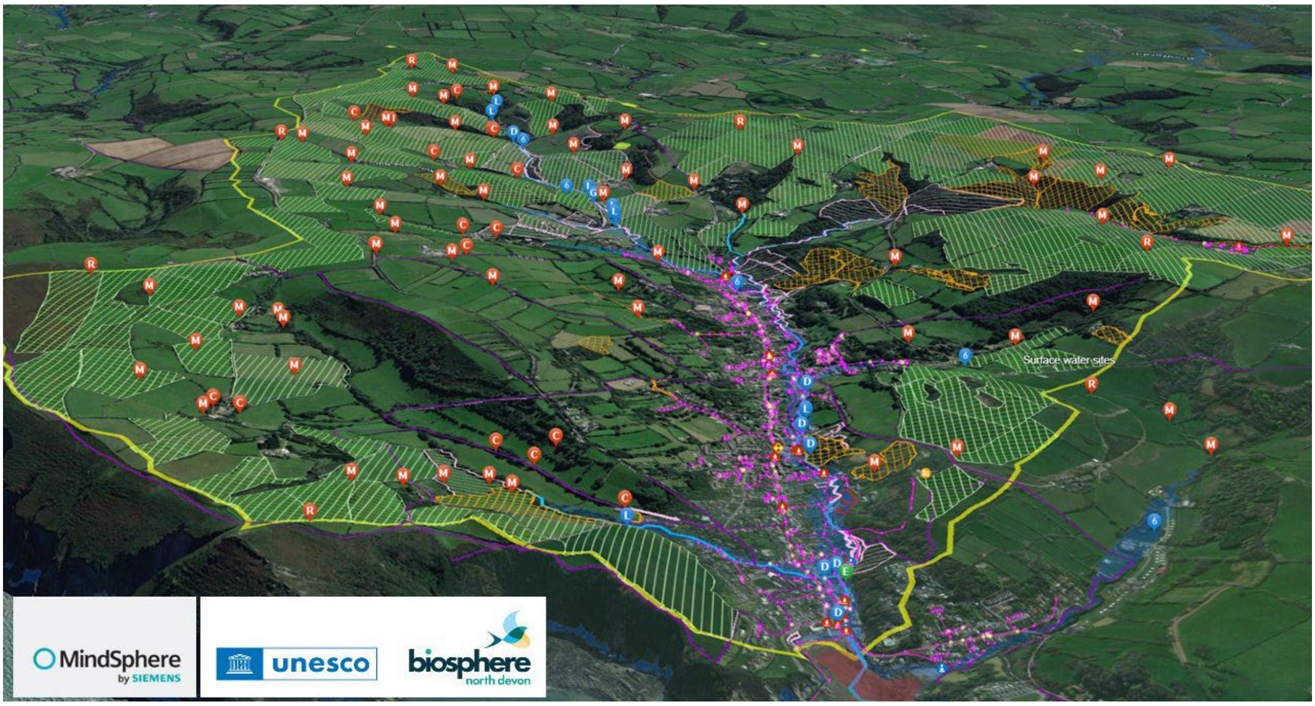

Figure 4 SMART biosphere deployment of sensors to monitor and predict environmental change, Biosphere Foundation

5.4 So what

In seeking to tackle systemic barriers to realising these opportunities, we will prioritise government's own efforts to act where:

1. **There is high potential for impact**

   This will drive engagement and action by ensuring that there is strong demand for development in these areas and individual organisation can clearly see the opportunities. It will also ensure that we are targeting investment to maximise societal, environmental and economic returns.

2. **Where government and partners can leverage influence, resources and initiatives**

   We will seek to maximise the impact of our activity by leveraging government and partners' strengths, including utilising and building upon existing and planned activity. We will work to deliver benefits to these activities through increased innovation, efficiency and collaboration, whilst also using these developments to build the components of the UK's Cyber-Physical Infrastructure.

6 Key enablers and the role of government

6.1 Security & resilience

Along with interoperability, security and resilience of systems and data came through as one of the two biggest enablers to development and adoption of cyber-physical systems and the building of a Cyber-Physical Infrastructure.

Responses provided strong endorsement of the challenges identified in the consultation including new opportunities for hostile actors to affect outcomes and an increased threat surface from greater connection. They also highlighted the critical importance of systems being secure and resilient if they are to be safe for humans who engage with or are potentially affected by them.

Concerns identified in responses particularly centred around respondents' poor understanding of the risks and a need for solutions that enable trust even with a low level of technical understanding. Risk aversion was highlighted as a key barrier to realising the potential of Cyber-Physical Infrastructure. High profile security incidents could significantly damage trust in cyber-physical systems and the organisations using them. Cascading failures, where the impact of compromised systems grows potentially exponentially via other connected systems, were frequently identified as a major resilience concern.

Not only is this a barrier to adoption, but government has a particular interest in the security of Critical National Infrastructure, along with the possible impacts on non-critical but highly impactful infrastructure, such as 'smart cities', where cyber-physical systems are key enablers.

Concerns over supply chain resilience (as have materialised for examples within telecoms with high risk vendors) were not strongly identified in responses. This is likely due to both the nascent state of Cyber-Physical Infrastructure and the macro-scale of supply chain risks, such that individual organisations do not feel that it is an immediate risk to their own operations. However, learning from national experience, this is nonetheless a material risk for government to work with partners in addressing.

The lack of skills and tools available to help address these emerging risks was identified as the primary challenge in addressing this. The skills needs range from technical through to senior leadership.

This reflects the findings of research commissioned by DCMS, which highlighted the lack of cyber security skills across the public and private sector as a key barrier to connected place deployment and showed that connected places stakeholders relied most heavily on internal expertise and government guidance to ensure effective security controls and measures for governing their connected places[27].

Existing CPNI and NCSC support and guidance[28],[29], such as the Connected Places Cyber Security Principles, were welcomed, as was the National Cyber Strategy and funding commitments within it. However, it was recognised that a) guidance is typically high level, and b) the emerging threats within the cyber-physical domain will increasingly fall in the gap between physical and digital security guidance and tools, which is not currently well served. Consultation respondents were consistent in highlighting both their anticipation of new, more complex risks that federated cyber-physical systems will pose, but also the lack of specific understanding at this early stage.

Therefore, to advance the security agenda within this nascent environment, we will work with internal and external partners to fully understand the risks and threats of the cyber-physical ecosystem. In developing our approach to understanding and then addressing these security and resilience risks, including through the funding of research and development, we will adhere to the following high-level principles, which are appropriate at this stage of Cyber-Physical Infrastructure development.

The two case studies that follow highlight how such principles inform the development of specific interventions in collaboration with industry, academia and the wider public sector.

Cyber-Physical Security & Resilience – High-Level Principles

1. **Security as an enabler** – security and resilience should be considered as critical enablers of the value that cyber-physical systems can deliver

2. **Secure by design** – security and resilience should be built into design, including research and development, from the outset

3. **Necessity** - There will be risks and threats we need to understand and mitigate with security controls that will require addressing feasibly with respect to cost and deliverability

4. **A systems approach** – assessment of security and resilience risks and threats should consider the whole, connected system

5. **Learn from existing best practice** – the broad domain of cyber-physical systems means that there are is significant relevant best practice to utilise and build upon

[27] https://www.gov.uk/government/publications/uk-connected-places-survey
[28] https://www.cpni.gov.uk/advice-guidance
[29] https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Case study: Security Policy Development in Consumer Internet of Things (IoT)

Connected technologies pose complex security policy challenges, with policy and interventions maturing over time as the risks, suitable mitigations and understanding of each continue to evolve.

For example, as IoT devices became more prevalent, government worked with industry, cyber experts, consumer associations and academia to develop the Code of Practice for Consumer IoT Security, published in 2018, which provided parties involved in the development, manufacturing and retail of consumer IoT with guidelines to ensure security of products by design. In 2020, a Call for Views was published on proposals for regulation. This informed the 2021 Product Security and Telecommunications Infrastructure Bill, which became an act in 2022 and enables the UK to set a security baseline for consumer IoT products.

The security requirements in the Act have been derived from and align with key provisions within ETSI EN 303 645, the leading international consumer internet of things security standard. The standard was introduced in 2020 by ETSI, with the UK government contributing significantly to its development and continuing to act as Rapporteur. It has since been adopted in codes of practice and domestic schemes internationally including by Singapore, Australia, India, Finland, Germany.

6.2 Interoperability

Interoperability of components and systems was the other critical enabler of Cyber-Physical Infrastructure identified through responses to the consultation. This includes both the technical interoperability of physical and digital interfaces (both the technology and the data), and the non-technical interoperability required for cooperation such as common frameworks, commercial models, ethics etc.

At the individual organisation level, this is key to reducing the ‘friction’ (incurring time, cost) of connecting components and systems, whether internally or between organisations. At a macro level, interoperability is a key enabler of competitive, innovative ecosystems. For example, the forthcoming Digital Markets, Competition and Consumer Bill will give new tools to the Competition and Markets Authority to remedy harms to competition in digital markets, which could include the ability to require interoperability. By prioritising interoperability of cyber-physical systems from the outset, we aim to mitigate the need for similar such policy interventions in the future.

Key data and systems interoperability challenges identified included the lack of common standards, formats, open protocols and tools across domains, along with general poor data quality and lack of semantic interoperability. Variance in regulation across borders was also highlighted.

There are also commercial concerns around interoperability. Greater interoperability would alter the competitive landscape and commercial advantage of some organisations. There are also concerns about the risk to intellectual property and data ownership when sharing and processing increased amounts of data.

In some cases, interoperability will be facilitated by frameworks, guidelines or standardisation, whilst in others, shared building blocks that are reused between parties will enable this and reduce the effort of re-work for new solutions. These shared building blocks could include shared models, algorithms, frameworks, technical standards, user applications, data assets. In the consultation we discussed the spectrum of different approaches to 'sharing' possible.

Whilst standards are not the sole enabler of interoperability, there was significant feedback on the need for and timing of development of standards. The prevailing view was that there are a broad range of data and technology standards that already exist and will underpin large elements of Cyber-Physical Infrastructure, however, there will likely also be a need for additional cross-sector standards to support the vision of a national Cyber-Physical Infrastructure.

But now is too early for that level of alignment. Attempts to standardise prematurely risk inhibiting innovation without facilitating the collaboration and scaling they are intended to enable.

The current need is for the fora and frameworks that enable innovators and users to collaborate on the research, development and innovation of connected cyber-physical systems. The challenges exist in the common frameworks between disparate stakeholder groups (replicating the challenges Industry 4.0 faces bringing together manufacturing, telecoms, robotics, IoT, AI etc.). Use cases that drive test and development, will develop the approaches that will subsequently mature into standards.

As highlighted above, activities set out in the National Data Strategy and the 2022 to 2025 Roadmap for Digital and data are accelerating the UK's development of the capability and tools required to maximise the value of data through better interoperability, availability and use.

Case study: Energy System 'Digital Spine

Following on from the Energy Digitalisation Taskforce's recommendation to 'deliver interoperability' in the energy sector[30,31], the Government awarded funding to Ove Arup, Energy Systems Catapult and the University of Bath to deliver a feasibility study into an Energy System 'Digital Spine', due to conclude in August 2023[32].

This study is exploring the needs case, benefits, and costs of an Energy System 'Digital Spine', a proposed piece of digital infrastructure aiming to connect energy system

[30] https://es.catapult.org.uk/news/energy-digitalisation-taskforce-publishes-recommendations-for-a-digitalised-net-zero-energy-system/

[31] https://www.gov.uk/government/publications/digitalising-our-energy-system-for-net-zero-strategy-and-action-plan/energy-digitalisation-taskforce-report-joint-response-by-beis-ofgem-and-innovate

[32] https://www.gov.uk/government/publications/energy-system-digital-spine-feasibility-study

participants through the real-time transfer of data. The Energy System ‘Digital Spine’ could provide the means to collect, standardise, present and exchange energy system data in a simple and secure way, supporting the delivery of a modern decarbonised digital energy system.

Case Study: National Underground Asset Register, Geospatial Commission

Each year, 4 million holes are dug to access the pipes and wires buried underground with an estimated 60,000 utility strikes. These strikes cost an estimated £2.4bn a year through injury, project delays, and disruption to traffic. Whilst data on underground assets is freely available for certain groups, obtaining it requires contacting multiple sources, with the data provided in different formats and scales.

The Geospatial Commission is building a digital map of the location of underground pipes and cables - the National Underground Asset Register (NUAR). It will be a secure data-sharing service that will provide an interactive, standardised digital view of the underground assets in a given location.

NUAR will streamline the data-sharing process between the 650+ energy, water, telecommunications and public sector asset owners and those who carry out excavations, reduce the risk of potentially lethal utility asset strikes and promote more efficient management and maintenance of underground assets.

Secure data sharing is enabled through the platform. To safeguard against misuse, sensitive assets and sites are flagged with users required to go through additional measures to access information e.g. additional guidance, or contact/permission requirements. The project is envisaged to result in savings of £350m per year through improved efficiency and safety of underground works when operational.

6.3 Recognised value propositions

As with many emerging technology applications, the recognised value propositions are critical enablers of further investment and development. This is particularly true where the value of Cyber-Physical Infrastructure lies in federated systems. Whilst demonstrating the value of individual use cases is feasible, the bigger picture requires significant technical and non-technical challenges to be brought together and overcome.

As we’ve seen from Ford’s production line in automotive manufacturing and the application of transistors in radios, right through to the internet itself, value propositions will likely be developed and matured within specific sectors and sub-domains. Therefore, development with an eye to future proliferation and the capability to communicate and adapt them to wider settings will be key.

Iterative development of both use cases and business cases will be key to advancing this agenda, with proof of return on investment (ROI) a critical goal within this. The diffuse realisation of benefits across federated systems is a complicating factor, whilst the high upfront cost of many of these approaches is a barrier. As always, senior understanding to the strategic benefits and practical implications is critical to driving investment, but this is currently held back by lack of understanding due to the complexity and lack of tangible business cases.

Case Study: SHAPE UK: Shipping, Hydrogen and Port Ecosystems –- IOTICS, Portsmouth University, Connected Places Catapult

Portsmouth International Port (PIP) aims to become the first carbon neutral UK port by 2030. To achieve its net zero goals, port managers need to understand the impact of interventions, new technologies and alternative fuels on the port's operation.

The project produced a digital ecosystem of the port with organisations sharing data from their existing digital shadows covering real-time data for air quality, water quality, weather, energy transition and port traffic.

The ability to share data selectively through the digital ecosystem encourages organisations to do so, since they retain complete control over their data and assets. This allows partner organisations to benefit from valuable information while protecting the intellectual property of individual organisations. For example, by sharing data on real-time change in air quality, the change can be attributed to a particular port activity, allowing interventions to be designed and tested to address the cause.

As the port evolves its net zero solutions, the ecosystem is the foundation for measuring effectiveness, flexing to include new sources and reusing existing ones.

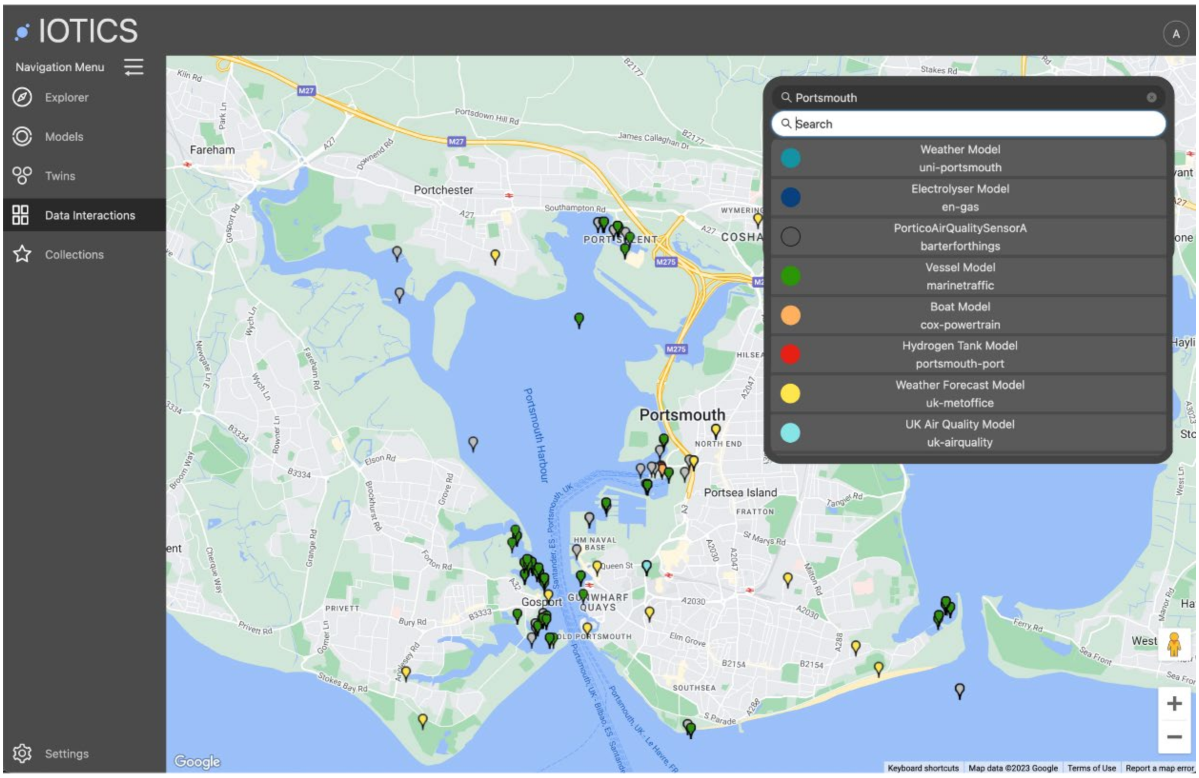

Figure 55 A view into the digital ecosystem showing eight IOTIC Spaces and the digital shadows they contain around Portsmouth, IOTICS

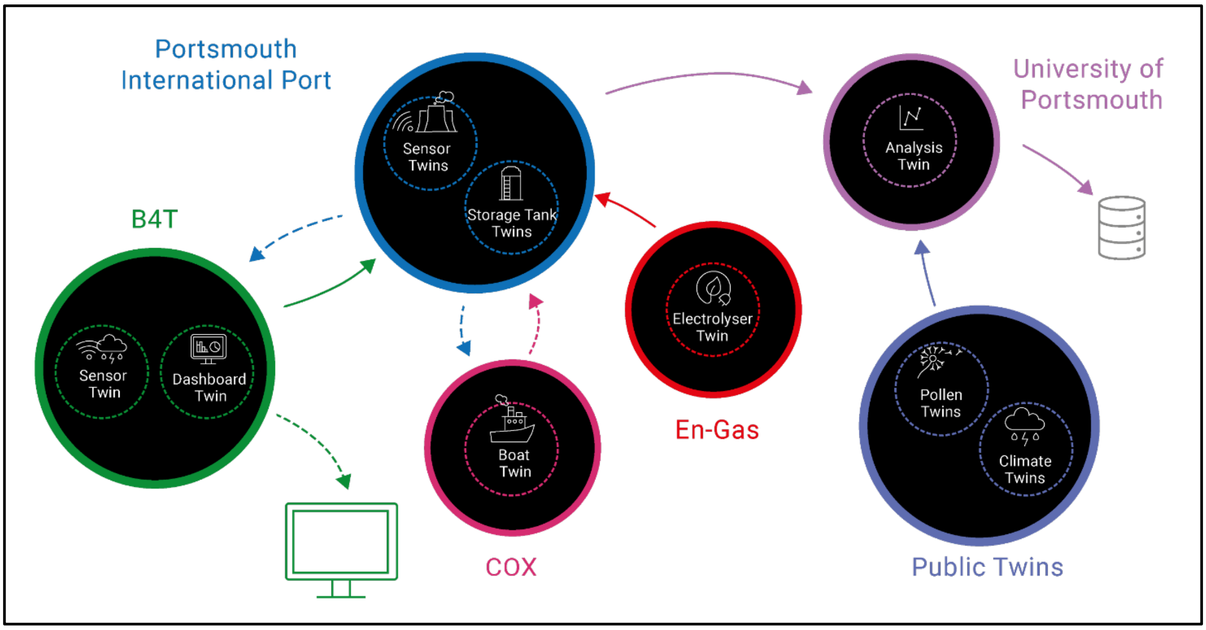

Figure 6 Diagram showing the decentralised, federated architecture underlying the digital twin ecosystem, showing the digital shadows of sources and consumers of data, IOTICS

6.4 Frameworks, guidance and standardisation

Common frameworks, guidance and standardisation are fundamental enablers of not just interoperability, but also security and resilience, best practice, assurance and validation, cross-sector collaboration, market-scaling and more.

Written responses strongly endorsed the value of technical standards in reaching the long-term value of Cyber-Physical Infrastructure. However, dialogue on standards presented a nuanced picture, confirming the value of standards but that it was too early to consider specific ‘Cyber-Physical Infrastructure standards’, as the need, scope and, most importantly, key stakeholder groups are not sufficiently mature yet.

Instead, the importance of developing the ecosystems where frameworks, guidelines and eventually standardisation can be collaboratively scoped and developed was highlighted. This requires sector and domain specific ecosystems to coalesce around specific challenges, whilst also facilitating the collaboration between these individual ecosystems.

This is not to say that standards work should wait. Work will be iterative and develop at different paces within the wider ecosystem. There are areas within this space with mature needs and stakeholder groups working to scope standards or who have already developed standards that will contribute to the wider Cyber-Physical Infrastructure development. The developing cyber-physical ecosystem will be key to advancing this.

Case Studies: Building the CPI Ecosystem

FutureScope Cyber Physical Systems accelerator cohort, Digital Catapult

Digital Catapult has launched its first cohort around virtualisation and cyber physical systems as part of its FutureScope acceleration programme, supporting UK startups and scaleups working in Digital Twins, the Metaverse and other cyber-physical systems to overcome business challenges, attract investment and explore new opportunities as part of the value chain and building blocks for a cyber physical future.

This includes high growth and innovative UK startup companies such as Extend Robotics, CuteCircuit, Focal Point VR, Virtual Speech, GroundWaves, SpaceForm and RideCommerce.

The Digital Twin (DT) Hub, Connected Places Catapult

The DT Hub was created in March 2020 by the Centre for Digital Britain at the University of Cambridge. In 2022, it transitioned to a cross-sector partnership between industry and the Catapult Network, hosted at the Connected Places Catapult. Working closely with the National Digital Twin Programme, it provides a network for digital twin collaborators including developers and suppliers, asset owners and operators of digital twins, investors, policy makers and more to help advance the cross-sector vision for connected digital twins.

An open access 30 minute Gemini Call is hosted every Tuesday to showcase advances in digital twinning innovation and provide network, policy and programme updates.

6.5 Skills

Skills was highlighted as a critical enabler across the breadth of technical and non-technical set out in the consultation. From data engineers, software and hardware developers, systems architects and security experts, to organisational change, legal, procurement, and cross-domain skills, there was recognition of both the existing and growing needs.

Unlocking the potential of technology and growing the digital economy through a world leading digital workforce is a high priority for the government. Action we are taking includes launching a Digital Skills Council of government and industry to address the digital skills challenges facing employers, and expanding our support for postgraduate conversion courses in data science and artificial intelligence (AI) by announcing additional funding to deliver scholarships for underrepresented groups.

Through the National Cyber Strategy we are enhancing the nation’s cyber skills and through delivery of the National Data Strategy we are focused on ensuring students are better prepared for data-driven lives and careers. Government also provides a number of ways for adults to reskill for roles in the cyber sector, including Skills Bootcamps, the DCMS cyber retraining programme and the CyberFirst bursary scheme.

Case Study: Digital and Technology Solutions Apprenticeship MSc, Cranfield University

Launched in 2022, the digital and technology master's programme brings together the technical and managerial skills required for industry to transform their business models through digital solutions.

The programme enables individuals to develop innovative approaches to meet industry challenges using AI/Machine Learning, digital twins, AR/VR, data analytics, and data management, which will help to develop a national Cyber-Physical Infrastructure. There are already two cohorts enrolled with another two cohorts joining in June 2023 and October 2023.

6.6 Others

Whilst the five key enablers above are where we will prioritise our efforts, that is not to ignore the range of other barriers and enablers that were set out in the consultation and highlighted in responses.

Concerns about privacy, loss of commercial advantage, and legal and regulatory impacts were all identified as particular areas of risk as systems become more connected and data is shared more widely.

Structural challenges such as access to RD&I funding, access to infrastructure, complexity of procurement, lack of commercial incentives, the organisational and cultural change, plus social trust and acceptance required to facilitate the development and adoption of a Cyber-Physical Infrastructure were highlighted by a range of stakeholders.

As with the key enablers, none of these are unique to this domain, though they have their own specific aspects within it. Therefore, we will ensure that they are part of the work we take forward with partners, particularly seeking to leverage the range of initiatives already underway in and outside of government that are seeking to address them.

International collaboration was identified as a critical underpinning of cyber-physical system development by respondents. The most frequent barrier to international collaboration were the differences in regulation of data sharing between jurisdictions. The role of government to help develop and align frameworks and standards for cyber-physical systems internationally was highlighted. In line with this, the AI Standards Hub pilot was announced in 2022 and is trialling this form of engagement[33].

[33] https://www.gov.uk/government/news/new-uk-initiative-to-shape-global-standards-for-artificial-intelligence

Annex – Summary of responses to consultation

Below is a factual summary of the written responses to the consultation received and aggregate information on respondents where provided. Please see the consultation document for the full context of questions. Section and question numbering aligns to that in the consultation.

Aggregate information on respondents

The consultation received 61 written responses.

Respondents by organisation type:

- 20 Businesses
- 17 Universities
- 8 Public Sector Organisations
- 5 Individuals
- 4 Trade Association, Membership Organisation or Representative Bodies
- 3 Research Institutes
- 4 Other – such as Non-profit organisations, Learned Society, National Academy or Professional Body

Within businesses respondents, the largest group were established businesses (age of organisation as 30+ years) who identified the size of their organisation as having 250+ employees, but we also received responses from a range of micro and small businesses that were established from 0-10 years. Smaller organisations were more prominently represented in the online and face to face engagements.

Respondents by region organisation HQ (or individual if not an organisation) is based, where available[34]:

- 20 London
- 7 North West
- 7 South West
- 5 Scotland
- 6 West Midlands

[34] Note, a number of responses were received from the UK entities of large, multinational organisations. We have used the HQ location of the UK registered entity that provided the response for this regional breakdown

- 4 South East
- 2 Yorkshire and the Humber
- 1 East Midlands
- 1 East of England
- 1 Northern Ireland
- 1 Wales
- 3 Outside of UK
- 1 Not available

Section 2 - Enabling the Cyber-Physical Infrastructure

1. What type(s) of cyber-physical systems are you currently employing, for what purpose(s) and to what extent to do you develop in-house or source these systems?

The majority of respondents said that they used Internet of Things, digital shadows and digital twins, AR/VR and AI/ML. Other cyber-physical systems (CPSs) include autonomous systems, models, living labs, synthetic environments, simulation and emulation. Respondents said CPS developed with a mixture of in-house development and externally sourced, reflecting the complex and multi-component natures of these systems. Respondent, frequently reference the use of open-source software.

2. To what extent do you recognise and agree with opportunities for and potential value of cyber-physical systems and the Cyber-Physical Infrastructure and why?

86% of respondents agreed strongly and 14% partially agreed to the potential value of CPS and Cyber-Physical Infrastructure (CPI). No respondents disagreed with the value outlined in the consultation. Respondents identified interoperability as the biggest value of CPI, enabling the linking of systems and infrastructures across locations and organisational boundaries. CPI has significant value in enabling hybrid facilities for testing, development and validation and could be an enabler for automation and manufacturing. Several respondents identified sustainability applications such as environment monitoring, emissions management and circular economy applications. Some respondents also said CPI could provide value to system resilience and training.

3. Where do you see the biggest long-term opportunities for cyber-physical systems in your sector or domain?

Sectors of particular opportunity identified were: built environment, connected places, climate response (including net zero), energy systems, health and social care, infrastructure, manufacturing, natural environment, RD&I, supply chains, transport and utilities. Common themes in responses include the opportunity for disaggregated and decentralised systems (e.g. supply chains, natural environment, future energy systems, transport), research and innovation-particularly in remote collaboration, design and manufacture of new products, significant efficiency benefits through automation, optimisation of processes, better modelling of systems to inform scenario planning, testing, validation, certification, assurance, benefits to enabling small orgs to innovate and drive adoption, training using real world data, immersive experiences and improved system resilience. New opportunities identified include enabling safety for example by reducing the requirement for people to be in hazardous environments and a greater ability to identify risks.

4. What are the biggest barriers and risks to you developing and/or adopting cyber-physical systems?

Respondents identified a lack of standard approaches for connecting CPSs as the biggest barrier to development, including standards for best practice, interoperability and security. Many respondents identified the skills needs and lack of common vocabulary and guidance is hindering CPS development and deployment. Other barriers identified are related to legal concerns such as data sharing, a loss of commercial advantage and intellectual property and privacy concerns from collaboration across organisational boundaries. Several respondents said there is a need to develop trust in CPSs such as trust in processes and decision making. Infrastructure barriers include access to compute and platforms to develop and connect CPSs, and knowledge on how to upgrade legacy systems and manage data quality.

5a. How much value do you see in shared building blocks (e.g. models, algorithms, frameworks, technical standards, user applications, data assets etc.) and specifically what building blocks and for what purposes?

53% of respondents saw enormous value in shared building blocks, 33% great and significant value and 13% saw some value. The benefits of shared building blocks are identified as: providing industry with confidence to make investments, helping to benchmark and vet new technologies, a reduction in duplication, support for SMEs and start-ups to participate in CPI and assist with security, safety, verification and assurance. Respondents said shared building blocks should be developed for interoperability, enable effective workstreams and ensure accessibility and trust e.g. through open source and security.

5b. What are the roles of government, industry, academia and wider society in supporting development of these shared building blocks within your sector or domain and how could they best be developed and maintained?

The majority of respondents framed answers on the role of government, industry, academia and wider society in developing CPI more broadly rather than the development of shared building blocks specifically. Respondents said government can help set the strategic direction for CPI, embed CPI in RD&I programmes, public procurement (incorporate standards and guidance) and large infrastructure projects. The role of government working with regulators to develop regulation for Critical National Infrastructure safety, security and ethics as well as develop skills and shape new business models was highlighted.

Several respondents outlined the importance of collaboration between industry and academia for example through industry identifying challenges and working with academia and organisations to develop innovation in response and when creating CPS, industry could incorporate more open, common elements and build and use open source. Respondents strongly felt academia was well placed to drive interoperability through its commercial neutral role and can feed into standards and novel way of using data. Research institutions were identified through their similar neutral capacity as well placed to drive interoperability, shared building blocks and knowledge sharing.

Section 3 - People and Culture

6a. What are the key technical and non-technical skills requirements for your organisation, sector or domain to develop, implement and/or utilise cyber-physical systems?

Respondents said the technical skills required include engineering, AI/ML, data analysis, application development, hardware development, information management, cloud computing, software development, systems architecture and cyber-security. Several respondents said that engineers and developers should have a good understanding of cyber-security to allow security to be built into CPS.

Several respondents said non-technical skills are required to support organisations to shift from the development of CPS to business viability. This needs interdisciplinary skills to communicate the value proposition and commercial viability of CPS. Non-technical skills include digital transformation, business model change, project management, digital literacy, operational research, non-specialist end user skills, legal and procurement. Cross-domain skills were also identified alongside the importance of senior leaders' understanding of strategic opportunities and implementation challenges.

6b. To what extent do you feel you have access to these necessary skilled people or are able develop them within your own organisation?

Most respondents said they were able to recruit people with the right level of skills to a limited extent. Higher education equipped people with some technical skills needed such as data science and software engineering. However, respondents said further training within organisations is often necessary for employees to develop sector and use case expertise. Several larger organisations said they were developing skills in-house through their own academies with software and training programmes in place to up-skill workers where needed.

Smaller organisations encounter difficulty training in-house, leading to some hiring consultants to support the skills gap. This was identified as an additional challenge for example for start-ups and local authorities due to the cost. The skills gap for smaller organisations and academia is associated with competition with larger organisations for skilled people. Several respondents noted that this creates a risk that skills development is taking place in silos and is limited to larger industry organisations. Some respondents said that apprenticeships, graduate training programmes and degrees that focus on CPS development and CPI would be beneficial and help overcome the skills gap.

7a. What are the challenges and risks you see around the ethical, sustainable, trustworthy and equitable development and adoption of cyber-physical systems?

Risks such as loss of privacy, discrimination, loss of intellectual property and ownership of personal data, bias in AI, algorithms and data were identified. There is also challenge related to the liability of problems created by connected CPSs. For example, where would liability across federated systems of CPSs, individual components and third-party users.

The majority of respondents highlighted the challenge of developing trustworthy systems and said building trust in CPSs and their outputs was key to the success of CPI. Some respondents said security is a key enabler. Both concerns about known security risks and a lack of knowledge about CPSs can be cause of mistrust of specific CPSs and CPSs in general. Interaction with CPSs and an understanding of CPS outputs and how they are achieved were identified as approaches to building trust. Two types of trust were identified by respondents: competence trust (trust in the functioning of a system) and moral trust (trust that the system will work in the best interest of people).

The equitable challenges of CPS were less explored. Some respondents identified digital exclusion as a challenge, for example, the elderly and those with limited internet connectivity are at risk of missing out on the benefits of CPI due to limited skills and accessibility to CPSs. Other respondents said CPI development favoured larger organisations that have the resources to develop CPSs.

The sustainability challenges of CPI were less identified by respondents. The risks identified are carbon emissions from CPSs primarily from the energy consumed.

7b. Where and how are government, industry and academia best placed to help overcome these?

Most respondents identified the role of government in supporting standard development and supporting good information sharing practices. Several respondents said government should fund or incentivise research including for example how CPI can benefit minority and underprivileged groups. A common theme was collaboration between government, industry and academia to encourage transparency in the development of CPI through the involvement of stakeholders and potential end-users of in the development and design process. This can help to address ethical concerns, enable trustworthy systems and ensure inclusion. Several respondents said there should be transparency between government, business and the public to build trust in CPI.

Section 4 - Technical Research, Development and Infrastructure

8. Where do you see greatest needs for R&D advances that could help your organisation, sector or domain to exploit the benefits of cyber-physical systems?

The majority of respondents said technical advances in data science is needed and said advances were required in data interoperability and integration, the way data is managed, modelled (complex, federated systems) and data quality. Security and resilience was also strongly reflected in responses with development of secure and CPS and assurance of CPS security. Respondents said knowledge sharing was important to understand how organisations can connect to other CPSs. Other R&D advances include AI/ML, use case development, standards development (security and interoperability), sensors, communications, Human/CPS interaction, robotics, tool kits, testbeds, multi-source integration, low latency systems, infrastructure needs.

Section 5 - Security and Resilience

9a. To what extent are concerns about security risks a barrier to the development and deployment of cyber-physical systems in your organisation, sector or domain?

All respondents identified security as a significant, high-level barrier, but specifics were more limited due to the emergent nature, range of risks and lack of expert knowledge and experience for many of CPSs. Several respondents said security had to be built in the development of CPSs from the start and maintained. Respondents identified several impacts of a security breaches: compromise of sensitive information, loss of trust, compromise of safety and business critical systems, and liabilities. Security concerns meant that many organisations were risk averse to implementing CPSs and data sharing. Respondents said there was tension between the agility required to develop CPS and the security assurances required.

9b. To what extent do you believe these risks to be perceived or actual?

Most respondents said risks were actual rather than perceived and said there is a need for security risks to be recognised and understood by non-security professionals. Respondents said the perception of the security risk was important as it could be a barrier to CPS development and adoption. Security is needed to develop trustworthy systems and should be incorporated into the development of systems from the start. Respondents said there is a requirement to equip organisations with the right tools to make right security risk management decisions for their risk appetite.

9c. What are the biggest current and future risks you see?

Few respondents distinguished between current and future risks. The common risk identified include the extent of harm caused and the damage of trust from security incidents, increased connections and interactions between components leading to increased threat surface and the risk of cascading failures, compromise of an asset and information, injection of faults or information poisoning, and ransomware attacks.

9d. Where and how are government, industry and academia best placed to help overcome these?

Respondents identified roles for government, industry and academia to a limited degree and were generally unsure how security problems could be addressed. Some respondents said government could support security training and develop clear requirements for secure systems. Industry and academia could work together to ensure security solutions meet needs and are fit for purpose. Academia could play a role in building security into projects from the start. Developing approaches to make the security of specific CPSs intelligible to non-security experts was identified as important.

10. How and where do you currently access support for security risks?

Many respondents were unclear on where advice and support on security risks could be obtained from. Larger organisations identified NCSC and CPNI guidance but said advice was primarily focussed on high level threats. Respondents said more tailored advice would be helpful but they were unsure about where this could be accessed. Respondents often said they relied on internal expertise to support security risks, whilst many respondents said they hired external specialists or relied on the process contained in standards. Respondents said that novel security problems were difficult to manage and the importance of developing skilled people to understand risks.

Section 6 - Connection and Interoperability

11. What are your current approaches to connecting cyber-physical systems (e.g. bespoke integration, conformance to industry standards, use of single-provider solutions, shared/common architectures and interfaces with partners etc.)?

Many respondents said they create bespoke solutions to connecting CPSs within their own organisations, often on a use case basis. Typically they utilise industry standards e.g. DIS, HLA. The use of bespoke solutions is often due to lack of interoperability of existing offerings or open standards to connects CPSs. Several respondents identified the risk of bespoke solutions becoming redundant and the challenge of training people how to use bespoke solutions. It was recognised that bespoke solutions can realise the benefits of specific use cases but will not lead to the scalable approaches needed for CPI.

12. What value and risks do you see in greater interoperability and sharing of data between your and/or your partners' cyber-physical systems, and for what purposes?

Many respondents agreed with the benefits of interoperability posited in the consultation. Benefits include: a reduction of replication of CPSs and data, aiding research and support sectors like education and healthcare; coordination and optimisation with partners e.g. supply chains; and management of complex systems of systems for example enabling scenario modelling, predictive action and optimisation. The use of existing CPSs can lower the cost of development of new CPSs and encourage sector investment. Greater analysis can take place with a large sample size of data, better data sets for models that can lead to the creation of complex models e.g. for infrastructure.

The majority of respondents identified security and resilience as the main risk of interoperability. Respondents said security could be undermined by less trustworthy components and systems, and lead to risks such as cascading failures, data poisoning, sensitive information being revealed and data misuse. Several respondents said the benefits of interoperability can be undermined by the poor data quality which could lead to a loss of semantic integrity through data manipulation and conversion. The loss of Intellectual Property and commercial advantage for businesses was also a concern to counter the benefits of greater system federation and information sharing.

13a. What are the current barriers to greater interoperability and data sharing between your and other organisations' cyber-physical systems?

The majority of respondents said a lack of common frameworks, standards, open data protocols and tools makes interoperability difficult and resource intensive. Responses primarily focussed on data sharing challenges. These include a lack of semantic interoperability, poor data quality or inconsistent data formats. Some identified data sharing a potential commercial risk. A lack of standard vocabulary and terminology also means there is an educational barrier to collaboration. Several respondents also said compliance with data privacy laws and existing regulations and legislation is a barrier to interoperability.

Respondents identified that CPSs are generally created with a specific purpose and time scale for operation in mind which restricts their capability to be integrated into wider systems, including interoperability. Respondents said that the difference in maturity and types of connectivity of both individual CPSs and organisations more broadly was a barrier to collaboration.

Several respondents said barriers to interoperability for businesses were related to intellectual property and establishing a business need and unique selling point for collaboration and data sharing. Other business barriers include the perceived complexity of interoperability and the financial cost and risk of making CPSs interoperable.

13b. What are specific examples of data that you need but can't access?

Several respondents would like access to data sets related to CNI, population data and data related to privately owned assets. Respondents also said they would like access to Government data such as National Health Service and Office For National Statistics data for CPSs that are for public use and benefit. Other sensitive data includes environmental impact assessments, long-term population survey, survey data for animals and vegetation in protected areas.

13c. Where and how are government, industry and academia best placed to help overcome these?

The majority of respondents said government can play a large role in overcoming barriers of interoperability and collaboration. Government can reduce barriers to data sharing through creating a culture of trust, promote open-source technologies and incentivise open sharing protocols and repositories to support equitable access for organisations at different levels of CPS development.

Government can incentive data sharing through tax incentives and support data sharing through education and skills development. Several respondents said collaboration between government, industry and academia can help to build standards for data sharing that are specific to CPI with government working to coordinate the development of legal, regulatory, commercial and technical frameworks. It was identified as a risk that without government-supported coordination frameworks and approaches would continue to proliferate, without moving towards coherent interoperability. Demonstrators and use cases can show the value of CPI and support a business case for organisations to develop CPS and show how data can be shared safely and securely.

Section 7 - Sustainable Markets

14a. What are the specific challenges you face to securing investment to develop, procure or implement cyber-physical systems (investment from within your own organisation or from external funding sources?

The majority of respondents said that limited use cases and difficulty in the development of a business case for CPS development were the greatest barriers to investment. Respondents said business case development is difficult because of the long-term benefits of CPSs and that they often accrue to diffuse parties. In the short-term, development requires high upfront costs making investment difficult to justify and reducing the incentives for individual organisations to lead in the development of CPSs.

Respondents also said that limited senior understanding of CPSs made investment difficult. The long-term funding needed for CPS development and often short-term nature of funding, including government grants, for CPS projects made R&D funding difficult. Respondents also said the current scope of R&D competition funding is not built for the cross-specialism and domain nature of CPS. Others said a lack of clear pathways for organisations of what they should invest in and how to realise benefits made investment in CPSs and R&D competition difficult to participate in.

14b. Where and how are government, industry and academia best placed to help overcome these?

Overall respondents said government, industry and academia should work together to drive cohesion for CPI. The majority of respondents said government should play a lead role in overcoming barriers by convening stakeholders and funding long term R&D to develop proof of value for foundational and reusable elements of CPSs and support living labs. Some respondents said it was important for government to ensure the regulatory environment supports investment and application of CPSs. Respondents said it was key for industry to invest in skilled people needed for CPI and develop value proposition for customers to invest in CPSs and provide use case challenges for academia and providers to solve.

15a. What are the specific barriers you face to developing, procuring and adopting cyber-physical systems?

Respondents said limited general terminology, common understanding and guidelines was an overarching barrier to CPS development, procurement and adoption. Key barriers to developing CPSs identified were related to the nascent nature of the technology making the value proposition difficult to define, and limited knowledge in academia related to industry in this area and approach. There are also challenges related to the high cost of funding CPS development and siloed R&D funding which is focussed on component technologies or a particular CPS rather than CPI.

Procurement barriers identified include large organisations being risk averse to procuring from SMEs and device procurement not positioned for R&D e.g. devices need to be purchased in large quantities and limited customer awareness. Challenges to adoption include poor data quality and low trust in data, a lack of standardised approaches to CPS development, lack of trust between organisations and a cultural aversion to sharing data, commercial and security concerns, legacy system integration, matching technology to organisation needs, lack of expertise in CPS and the complexity of systems can deter adoption.

15b. Where and how are government, industry and academia best placed to help overcome these?

Respondents said collaboration between government industry and academia is key to overcoming barriers. Collaboration could focus on interoperability and standards development, address ethical, safety and privacy concerns and prove feasibility and value of CPI. The majority of respondents identified a need for government to help overcome system challenges and valued the role of government to set the strategic direction for CPI. This could be through facilitating coordination across domains and sectors, promoting best practice, funding RD&I and demonstrators for use case and value proposition development. Respondents said it was necessary for industry and academia to collaborate together to find solutions to challenges and develop demonstrators to understand the value of CPI across sectors.

Section 8 - Working Globally

16. If you currently source cyber-physical systems, do you source from UK providers, non-UK providers, or both?

Most respondents sourced components through UK and non-UK providers. Many solutions are often sourced globally due to the dominance of global vendors. Smaller organisations and start-ups often use bespoke in-house or local solutions for CPSs but may rely on global vendors for some solutions. A risk was identified that UK providers cannot compete with non-UK providers because of the cost of products despite UK expertise in specific areas. Many respondents also use open-source hardware which is global in nature. Importantly, services and solutions even if sourced in the UK will typically need to align with global standards to maximise the export market of UK businesses and support interoperability.

17a. What are the specific barriers to cyber-physical collaboration with partners outside of the UK (examples of collaboration include connecting cyber-physical systems, sharing data, providing services, procuring services etc.)?

Many respondents felt a lack of international standards and variations in data sharing regulations globally made working with partners outside the UK more difficult. However, some of these barriers also make collaboration with partners in the UK also difficult e.g. compliance with GDPR. Uncertainty related to long-term funding was also a barrier.

17b. Where and how are government, industry and academia best placed to help overcome these?

Respondents primarily focused on the role of government with working with international partners to help shape international standards and align regulations including on data sharing and security. A role for government to provide leadership in collaboration and value demonstration was also identified.

18. What international groups and fora are you aware of involved in developing cyber-physical systems and infrastructure and which of these do you find most relevant?

The international groups and fora identified by respondents are listed below:

Government/Government Funded projects	Research Institutions	Academia	Standards Organisations	Membership Organisations
CADDE (Japan)	Australian Cooperative Research Centres	École polytechnique fédérale de Lausanne (EPFL)	BSI	AI, Data and Robotics Partnership
Cyber Physical Systems for Europe (CPS4EU)	Connected Everything	Lisa Yang Center for Bionics at MIT	European Standards Organisations - CEN and CENELEC	BIM forum
ERNCIP – the European Reference Network for Critical Infrastructure Protection	Future Artificial Intelligence and Robotics for Space Hub	Singapore University of Technology and Design (SUTD)	Institute of Electrical and Electronics Engineers	CPS-VO (Cyber-Physical Systems Virtual Organization)

Government/Government Funded projects	Research Institutions	Academia	Standards Organisations	Membership Organisations
EU Industrial Data Spaces	International Cyber Security Center of Excellence (INCS-CoE)	The Health Sciences and Technology Institute at ETH Zurich	International Electrotechnical Commission	Cyber Physical Security Convergence Forum
European Commission Destination Earth and Digital Twins of the Ocean	ODI	The Max Planck Institute for Intelligent Systems in Tubingen	ISO	Digital Twin Consortium
European Space Agency-EU, ESA DTs	UK Through-Life Engineering Services Council	Wyss Centres at Harvard	National Institute of Standards and Technology	Eclipse Foundation
GAIA-X			NATO Modelling and Simulation Group	EU Robotics network
Industrie 4.0			Simulation Interoperability Standards Organization	European Open Science Cloud
Japanese Government vision of Society 5.0				IFAC Technical Committee on Hybrid Systems and Discrete Event Systems
Digital Twin of Republic of Korea				Industry IoT Consortium

Government/Government Funded projects	**Research Institutions**	**Academia**	**Standards Organisations**	**Membership Organisations**
National Information Exchange Model (US)				National Robotics Network
The Alliance of Internet of Things Innovation (AIOTI)				Open Geospatial Consortium
The Digital Twins of the Ocean (DITTO) Programme of the UN				Research Data Alliance Research Data Alliance
The EU Sphere project				Robotics Growth Partnership
The IoT European Research Cluster (IERC)				SPRINT Robotics
United Nations activities on sustainability and smart cities				SmartGrid Forums (CNI Focus)
WMO Information Systems (WIS)				The Digital Twin Forum
				The Institute of Electrical and Electronics Engineers
				The International Academy for Production Engineering
				World Wide Web Consortium

This publication is available from: www.gov.uk/government/consultations/enabling-a-national-cyber-physical-infrastructure-to-catalyse-innovation

If you need a version of this document in a more accessible format, please email alt.formats@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.