Department for
Business, Energy
& Industrial Strategy

Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation

Understanding the opportunities for connected digital twins and other advanced cyber-physical systems

Closing date: 11 May 2022

March 2022

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

Foreword

Innovation is becoming increasingly critical to overcoming the greatest challenges we face as a planet: from tackling climate change and driving sustainable growth, to supporting aging populations and responding to future crises.

As we set out our post-pandemic ambition to cement the UK's status as a Science Superpower, and Innovation Nation, we are both investing more in 'blue sky' science and the technologies of tomorrow.

To achieve this and deliver on our plans for economic recovery and growth set out in "Build Back Better: our plan for growth", the Government is raising public investment in R&D to record levels to drive economy-wide investment in R&D to 2.4% of GDP by 2027.

But realising the benefits of UK innovation will require more than government investment. As set out in the Innovation Strategy, we need to enable innovators to collaborate and commercialise more quickly, cheaply and effectively.

Cyber-Physical Infrastructure will build on areas of UK strength. From our world leading research base to the rapidly growing commercial investment in technologies like artificial intelligence, digital twins, robotics, augmented and virtual reality, sensors and more - the UK is well placed to seize the opportunity presented.

A national capability in cyber-physical infrastructure would mean that every innovator, no matter the size of their organisation, location or access to institutional resources, will be able to design, build and connect across the digital and physical domains.

I therefore welcome your participation in this consultation on a UK capability in Cyber-Physical Infrastructure to help unleash innovation.

To enable this national capability, we need the insights of businesses, academics, institutions, local authorities, civil society and more to ensure that this develops in a manner that serves the interests of an inclusive, innovative and resilient UK.

I would like to thank the large number of contributors to the development of this consultation, and in particular the Robotics Growth Partnership for their leadership in building a community of interest and their compellingly articulated Vision for Cyber-Physical Infrastructure.

And thank you for your engagement with this consultation. We look forward to working collaboratively with you as this area of such opportunity develops.

George Freeman
Minister for Science, Research and Innovation

Contents

General information

Why we are consulting

This consultation has three purposes, to:

- Broaden the UK industry, academia and public sector's understanding of the impact and opportunities of cyber-physical systems
- Explore the potential industrial and commercial opportunity for growing UK global leadership in cyber-physical technology sectors
- Advance our collective understanding of the value of, and options for, an underpinning Cyber-Physical Infrastructure, which could take time, cost and risk out of innovation, and explore the possible roles of government, industry, academia and wider society

Consultation details

Issued: 2 March 2022

Respond by: 11 May 2022

Enquiries to:

Technology, Strategy and Security Team
Department for Business, Energy and Industrial Strategy
6th Floor
1 Victoria Street
London
SW1H 0ET

Email: cpiconsultation@beis.gov.uk

Consultation reference: Enabling a National Cyber-Physical Infrastructure to Catalyse Innovation

Audiences:

We are primarily seeking views from industry, academia and the wider public sector. This includes the range of institutes and other organisations with an interest in cyber-physical systems.

Territorial extent:

This Call for Evidence seeks information for consideration by the UK government but does not contain policy proposals. Responsibility for some of the policy areas covered in this Call for

Evidence may also fall to the Devolved Administrations. Responses to the Call for Evidence will be shared with Devolved Administrations.

How to respond

Respond online at: https://beisgovuk.citizenspace.com/strategy/cpi-consultation

Enquiries:

Email to: cpiconsultation@beis.gov.uk

or

Write to:

Technology, Strategy and Security Team
Department for Business, Energy and Industrial Strategy
6th Floor
1 Victoria Street
London
SW1H 0ET

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We may share your data with other organisations which have a direct interest in the consultation: for example Crown bodies, government departments or BEIS partner organisations.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

Executive Summary

Cyber-physical systems are beginning to permeate the world around us, from smart machines working alongside people in factories, to immersive virtual spaces allowing people to collaborate and socialise globally.

The UK has globally competitive R&D and industrial strength in many of the core elements of these systems including Artificial Intelligence (AI), digital and advanced computing, and robotics and smart machines.[1] For example, equity investments in UK digital twins and AI companies have a compound annual growth rate of 49% and 114%, respectively, from 2018 to 2021.[2]

Here, we present a vision for Cyber-Physical Infrastructure in which connected networks of cyber-physical systems could provide a step change in the economic and social value of these individual systems. Much like the internet, this would not be a single, centralised system. Instead, ecosystems of connected systems would form upon which new products, services and business models could be built.

But this is not an inevitability. There are significant barriers to the emergence of such an ecosystem and particular risks of silos developing if left solely to market forces.

Based on research and engagement with over 100 organisations, this consultation sets out the potential benefits of Cyber-Physical Infrastructure, along with the barriers to reaching these and the possible opportunities for government, industry, academia and wider civil-society to collaborate to overcome them.

Core to this would be:

- **Shared building blocks** which could take time, cost and risk out of the innovation process by reducing the rework that currently is required to develop new applications, enabling more time to be spent on novel elements.
- **Interoperability** of cyber-physical systems and their components through common standards and frameworks, similarly supporting innovation by allowing easier connection between components, systems and sharing of system outputs, reducing the fragmentation of systems.

This document also highlights the breadth of socio-technical challenges that will be necessary to overcome, including within people and culture, technical R&D and infrastructure, security and resilience, connections and interoperability, sustainable markets, and the global considerations.

[1] https://www.gov.uk/government/publications/uk-innovation-strategy-leading-the-future-by-creating-it
[2] BEIS analysis of Beauhurst, January 2022. CAGR can vary in different timeframes given fluctuations in equity investment.

We also identify the opportunities within these areas and set out, based on our engagement to date, some of the possible priority areas where government could collaborate with stakeholders to help realise this vision.

We are seeking challenge and validation of these opportunities, barriers and potential approaches, and invite responses to the questions set out below. Your responses will help inform subsequent policy development and will be key to ensuring that whatever role government plays is inclusive and stakeholder driven.

Section 1 – Introduction

Advanced cyber-physical systems, such as digital twins and smart robotic systems, that sit across the digital and physical worlds are increasingly prevalent and have significant societal and economic benefits – from autonomous drones in agriculture and collaborative robots supporting factory operators, to optimising our supply chains to ensure they can respond to new demands and enabling detailed scenario planning of how infrastructure will respond to extreme weather.

Much like individual computers connecting to the internet, the potential value of these systems increases as they become more connected. Imagine autonomous vehicles in a city, communicating with traffic controls to help reduce pollution and congestion, with both of those systems informing a future smart energy grid where and when electric vehicles will be charged. Innovators across the UK could collaborate across linked virtual and physical laboratories and innovation spaces. Developers and users could interact in real time through virtual reality and shared simulation environments, remotely interacting with smart machines.

This wouldn't be a single, centralised system. Instead, networks of applications will likely form around particular use cases, with interoperability supporting a connected ecosystem of those networks.

Widespread interoperability won't necessarily arise if left purely to market forces, with platforms and providers tending to develop fragmented ecosystems. This can lead to technical lock-in and high barriers to collaborating with new partners. This could be a significant detriment to the UK economy and society if not addressed at this stage. Inclusive industry and academic leadership will be required, and government may have a role to play.

Like the internet, this disaggregated ecosystem of connected systems could be considered an innovation infrastructure on which future products, services and business models are built.

We call this ecosystem capability a 'Cyber-Physical Infrastructure'.

Purpose

This consultation is based on research and engagement with over 100 stakeholders from a range of industries and academia, the wider public sector, not-for-profits, institutions and individuals.

The document has three purposes, to:

- Broaden the UK industry, academia and public sector's **understanding of the impact and opportunities of cyber-physical systems**
- Explore the potential industrial and commercial opportunity for **growing UK global leadership in cyber-physical technology sectors**
- Advance our collective **understanding of the value of, and options for, an underpinning Cyber-Physical Infrastructure**, which could take time, cost and risk out of innovation, and explore the possible roles of government, industry, academia and wider society

In many areas the possible role of government will likely be through existing policies. In others there may be a need for government to explore the options for specific interventions.

Responding to questions

This consultation covers a broad range of topics and you are welcome to reply only to the questions that are of most interest or relevance to you or your organisation.

For simplicity and accessibility, many of the questions are framed to be answered by organisations that may be building or utilising cyber-physical systems. However, we recognise that there will be stakeholders including academics, individual experts and institutions who have expertise and valuable insights to provide, but the exact framing does not reflect your or your organisation's interest in the topic.

Where this is the case, please respond in the way that conveys the insights you wish us to consider in that topic area (for example insights on systematic challenges rather than your or your own organisation's, or customers' needs/barriers).

Innovating in complex systems

Humanity has been on a path of developing increasingly complex physical systems, then digital systems and, most recently, connected digital-physical or 'cyber-physical' systems.

Thousands of years ago, Mesopotamians connected natural and human-made irrigation systems together to revolutionise agriculture and throughout history, societies have developed ever more advanced methods to better understand and improve physical systems.

Thanks to advances in sensors, connectivity, high performance computing and precision robotics, amongst other innovations, our ability to create and connect the digital and physical worlds is greater than ever before.

Understanding and connecting complex systems has been critical to every major human endeavour, from bringing life to arid lands to landing humans on the moon. Now, as we face increasingly 'wicked' challenges such as reaching net zero, declining productivity growth and responding to global health crises, the need to understand, innovate and act in complex environments is the greatest it has ever been.

Enabling the UK's ambitions

Enabling cyber-physical systems to be modelled, tested, built and connected more quickly, cheaply and effectively, as part of a Cyber-Physical Infrastructure, will support the ambition set out in the Integrated Review for the UK to be a resilient Science Superpower.

- **Innovation:** As identified in the Innovation Strategy, by taking time, cost and risk out of innovation, from academia through to businesses, UK science and technology will be able to go further, more quickly. Combined with a business-friendly regulatory environment, this will help make the UK an Innovation Nation and one of the most attractive places to invest and build commercial partnerships.
- **Resilience:** Greater understanding of how complex systems-of-systems such as supply chains, the National Health Service and social care operate and can be influenced, including through improved modelling and simulation, will enable more effective responses to crises and better long-term planning and action.
- **Climate Change:** Our ability to accurately model our environmental and economic systems and explore their possible future states, including simulating policy impacts, will enhance our ability to mitigate climate change and deal with its consequences. Enabling green innovation is also key to this challenge, from fusion and carbon capture to low carbon transport and AI applications.
- **Levelling up:** Driving economic prosperity and security by enabling businesses to start, innovate and grow more easily, and improving the ability to collaborate across the UK, from Anglesey to Aberdeen, Andover to Armagh, will enable more high-quality jobs to grow where people are based.

We will grow the UK's science and technology power in pursuit of strategic advantage by providing the tools and systems that scientists, researchers, inventors and innovators, across academia, the private sector, regulators and standards bodies, need to innovate.

Many organisations are already implementing cyber-physical system innovations such as:

- BMW utilising Nvidia's Omniverse platform to enable global, immersive collaboration in real time across multiple software packages, to improve efficiency of factory planning by an estimated 30% - see page 17
- Rolls-Royce applying digital shadows and machine learning to reduce jet engine maintenance by 1/3 and increased engine efficiency, saving 22,000 tons of carbon to date - see page 20
- Siemens UK designing, testing and scaling production of ventilators from 10 to 1,500 per week in just four weeks using cyber-physical modelling and visualisation as part of the Ventilator Challenge - see page 24

Access to shared building blocks and greater interoperability, including through open standards, could help a wider range of businesses and academics deliver these kinds of innovations more quickly, cheaply and effectively. Enabling innovators to bring together multiple organisations' systems and data securely and easily could unleash a realm of new and more valuable use cases.

For individual businesses, academics and wider society, this consultation seeks to understand the current use of cyber-physical systems, as well as the future opportunities, barriers and role of government, industry, academia and wider society in helping realise those opportunities.

Case study: An Example Net Zero Story

Delivering net zero by 2050 is the ultimate systems and innovation challenge. Cyber-physical systems coming together to build the Cyber-Physical Infrastructure have the potential to make a crucial contribution.

Our energy systems of the future will use highly disaggregated and variable inputs such as wind, solar and tidal, and consumer storage such as electric vehicle batteries. Digital twins could help systems to monitor and autonomously adapt in real time to changes in input and demand. To predict demand, they will need to communicate seamlessly both with other energy systems and the external environment as part of federated cyber-physical systems.[3]

Connections to real-time weather modelling and forecasting will inform not only energy systems, but, for example, urban traffic management. Predicting how people's journey times and routes will vary with weather will enable cities' autonomous traffic management systems[4] to optimise to reduce congestion or emissions. This traffic data will inform real-time predictions of the energy grid, enabling optimisation and reducing unnecessary power generation.

Better information sharing and modelling of the natural environment can inform public policy in delivery of net zero and climate resilience. Whether that's combining ground sensors and satellite imagery to monitor land use for carbon capture[5] or understanding the impact of extreme weather on our interdependent critical utilities[6], better information sharing and connection will inform better decision making.

Innovation will be needed in a wide range of industries from floating offshore wind to more efficient batteries. Tools to enable the design and testing of advanced digital prototypes can reduce the time, cost and carbon required to innovate, whilst in life digital twins can improve efficiency and life span.[7] Accelerating the rate of innovation to speed low and negative carbon solutions will be key to reaching net zero by 2050.

What are Cyber-Physical Systems?

Introduction to cyber-physical systems

Cyber-physical systems bring together the digital and physical worlds, where data from the physical world feeds insight and decision making in the digital world, which can then be implemented either by a person, machine or collaboration of both.

[3] https://es.catapult.org.uk/report/energy-system-digital-twin-feasibility-study/
[4] https://uk5g.org/discover/testbeds-and-trials/smart-junctions-5g/
[5] https://geospatialcommission.blog.gov.uk/2021/01/21/finding-common-ground-the-urgent-need-for-better-land-use-data/
[6] https://digitaltwinhub.co.uk/projects/credo/what-is-credo/
[7] https://www.amrc.co.uk/pages/digital-twin-report

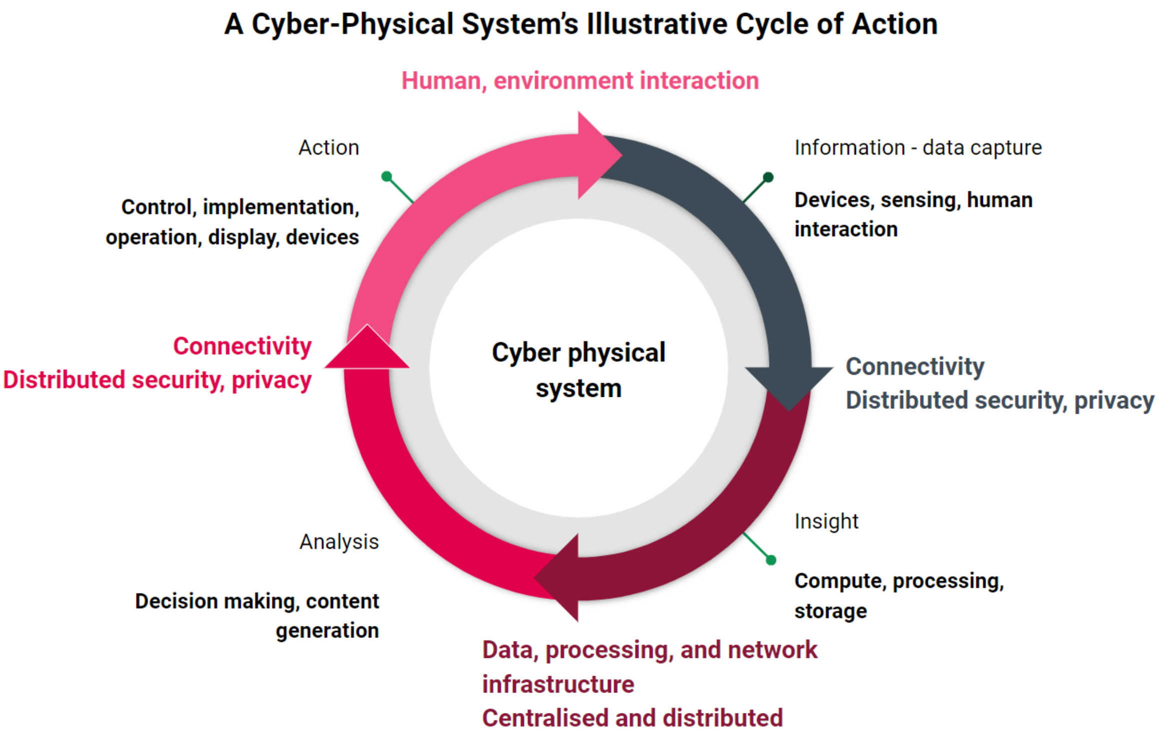


Figure 1 Illustrative cyclical interaction of the digital and physical domains connected by a cyber-physical system (Digital Catapult, 2022)

Cyber-physical systems are already core to our everyday lives. For example, weather predictions collect physical information to inform predictive models. Many human-made creations are now designed and built digitally long before they take physical form. Such systems will become increasingly prevalent, for example in autonomous vehicles and maritime vessels combining static and real-time virtual models to navigate the physical environment, and concepts such as the 'metaverse'. Each application has different considerations around ethics, security, technical needs, interoperability and more.

Initial engagement with industry, academia and institutions has identified three core areas of opportunity where cyber-physical systems could deliver societal and economic benefits:

- **Design, operation and optimisation** – Real- or right-time information on the physical world can inform digital models used to design, test and refine products and services, cutting the time, cost and risk of real-world testing.

  Once in physical operation, this connected system enables automated or autonomous operation of smart robots, connected infrastructure, unmanned vehicles etc. This allows operations to be managed at a scale and speed otherwise unachievable. It also allows for optimisation of complex systems such as urban traffic to reduce congestion or increased efficiency through preventative maintenance.
- **Strategic planning and scenario modelling** – Accurate digital representations of physical systems combined with historical information of their performance and interdependencies is a key tool in planning and scenario modelling.

Bringing together information from multiple systems can enable human and artificial intelligence to improve planning from industry operations to public sector policy making and service delivery.

- **Resilient, flexible and responsive systems** – Smart, connected systems can respond rapidly to changes in need, from reconfigurable manufacturing systems adapting to new output requirements, to fleets of smart machines able to be rapidly redirected to locations or activities.

  As identified in the Integrated Review, greater understanding of whole systems, and the ability to respond rapidly, could greatly increase system and national resilience, particularly in response to exogenous shocks. For this reason, the government committed to developing a national capability in digital twinning.

Case study: Factory of the future, BMW Group and NVIDIA

There are 2,100 possible configurations to a new BMW. With teams and factories spread across the globe, planners and operators need to be able to collaborate across multiple platforms to develop effective new planning processes.

To meet this challenge, a digital shadow of the BMW assembly system has been created using NVIDIA's Omniverse platform. Real-time data produces a simulation of the factory and the platform acts as a single environment where global teams can work together across multiple sites. Planners collaborate virtually with those at the assembly line, utilising motion capture suits to help optimise the line and review worker safety and ergonomics.

This enables complex production scenarios to be modelled, increasing output and optimise efficiency. The cyber-physical approach will reduce production planning time by up to 30%.[8]

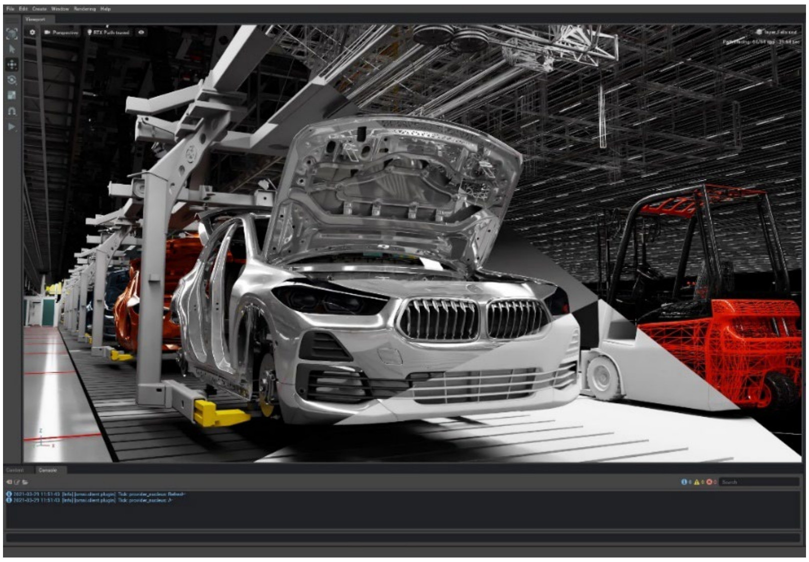


Figure 2 The digital shadow of the BMW factory enables planners and operators to collaborate virtually. Copyright: NVIDIA

[8] https://blogs.nvidia.com/blog/2021/04/13/nvidia-bmw-factory-future/

Case study: The Network Emissions Vehicle Flow Management Adjustment (NEVFMA) toolkit, Aimsun, Highways England, Oxfordshire County Council

The NEVFMA toolkit was developed by Aimsun for Oxfordshire County Council to bring together data from EarthSense air quality sensors (the Zephyr), Yunex Traffic, and National Highways traffic monitoring sensors with information on weather conditions to improve local air quality through better traffic management[9].

Bringing together data from these separate sources into a single model can be used by the public sector to build long term improvement strategies for road networks using new technology (CCAM and ITS). In conjunction with traditional road design the model can enhance public spaces and respond in real time to reduce pollutants through traffic management.

The toolkit developed scenarios for lowering pollutants and averaged daily decreases in emissions of 5% and up to 40% on some days.[10]

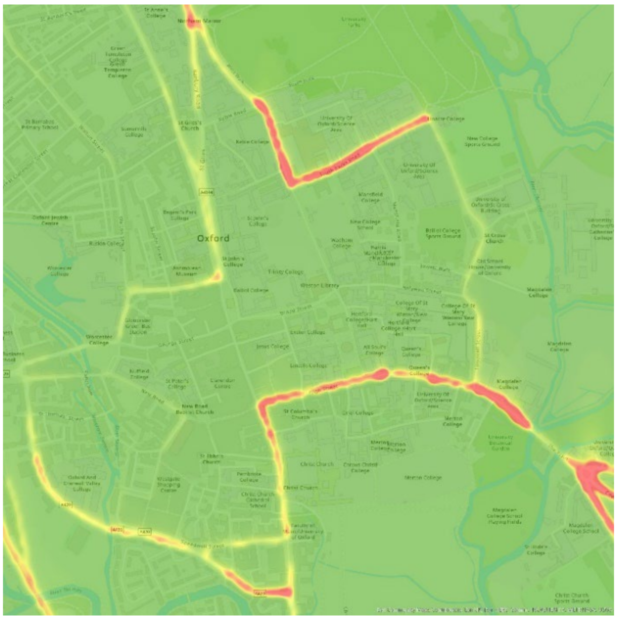


Figure 3 Map of Oxford with high levels of traffic before intervention. Copyright: Aimsun

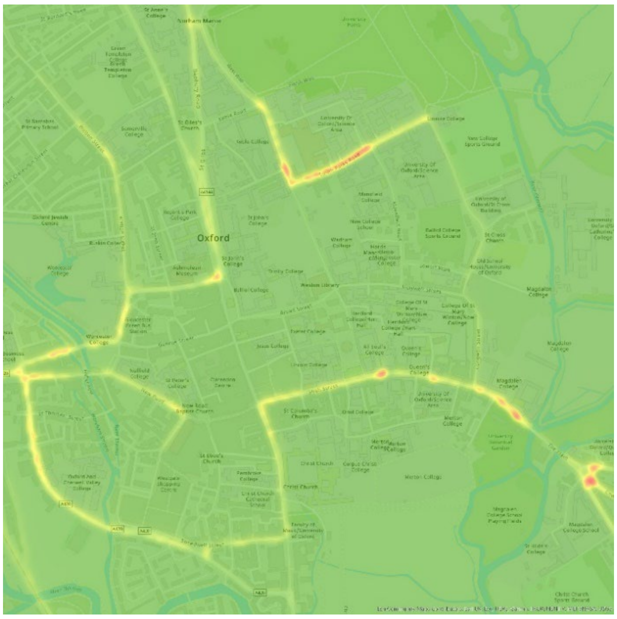


Figure 4 Map of Oxford after intervention with low levels of traffic through traffic management. Copyright: Aimsun

Interoperability and federation

The ability to connect components and systems, and share data securely and reliably will be key to realising the fullest value of cyber-physical systems. This may be smart road systems informing the future energy network where and when electric vehicles will be arriving to charge, taking into account the latest weather forecasts. Or this may be a group of geographically

[9] https://www.aimsun.com/aimsun-live-case-studies/nevfma-oxfordshire/
[10] https://its-uk.org.uk/aimsun-wins-another-award-for-its-nevfma-air-quality-solution/

dispersed innovators collaborating across physical labs through connected physical and synthetic environments.

We have seen in a range of digital and data markets how market development of platforms can provide significant value in isolation. However, the collective value is subsequently limited by the fragmentation of the platforms and their ecosystems. For example, mobile operating systems and their applications ecosystems, social media platforms etc. Therefore, there may be a role for government, industry, academia and wider society to collaborate to enable greater interoperability.

Specific cyber-physical systems

'Cyber-physical systems' encapsulates a wide breadth of applications. However, there are a number of more recognised applications.

Digital Twins

As is often the case with emerging technology, what people mean by 'digital twin' can vary. Figure 5 shows some of the different systems sometimes referred to as 'digital twins'.[11]

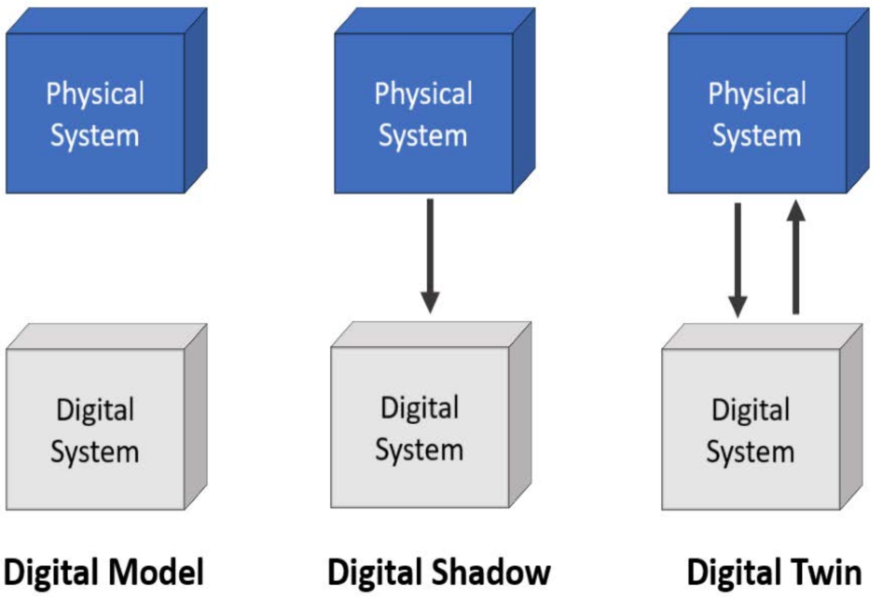


Figure 5 Examples of cyber-physical systems which are sometimes referred to as 'digital twins'

- **Digital Model** – a digital representation of an asset, system or process at a fixed point in time. Commonly used in manufacturing to design virtually before physical manufacturing and reducing the cost and time, for example in Computer Aided Design (CAD).
- **Digital Shadow** – a digital model that integrates information from its physical counterpart. This may be in real- or right-time. This can provide insights into performance, maintenance needs, compliance, scenario planning and future design

[11] https://ieeexplore.ieee.org/document/9103025

interactions. These are often used in systems without autonomous interventions (e.g. predictive maintenance) or any direct interventions (e.g. weather forecasting).

- **Digital Twin** – a digital model with real- or right-time, two-way information flows. This can enable autonomous optimisation, and remote and autonomous operation. These are not yet widespread, but are typically found in autonomously operated environments such as robotics and autonomous vehicles and maritime vessels.

Resilient, flexible and responsive systems could utilise digital twins to understand the impact of shocks and respond either autonomously or with well-informed human decision making. This could enable complex, decentralised systems such as supply chains to better respond to crises.

Case study: Intelligent Engine, Rolls-Royce and R2 Data Labs

Rolls-Royce has over 13,000 jet engines in service globally. Improving reliability and reducing the frequency of unnecessary maintenance can significantly increase efficiency and reduce carbon emissions.[12]

Rolls-Royce created a digital shadow of its engines utilising sensors, flight operating conditions and historical data. This has meant that engines' physical behaviour and maintenance needs can be predicted in real time. This has reduced unplanned grounding of planes by 5% and extended the time between maintenance by up to 50%.[13]

By informing pilots how to fly most efficiently in real time, Rolls-Royce estimates 22 million tons of carbon have also been saved.

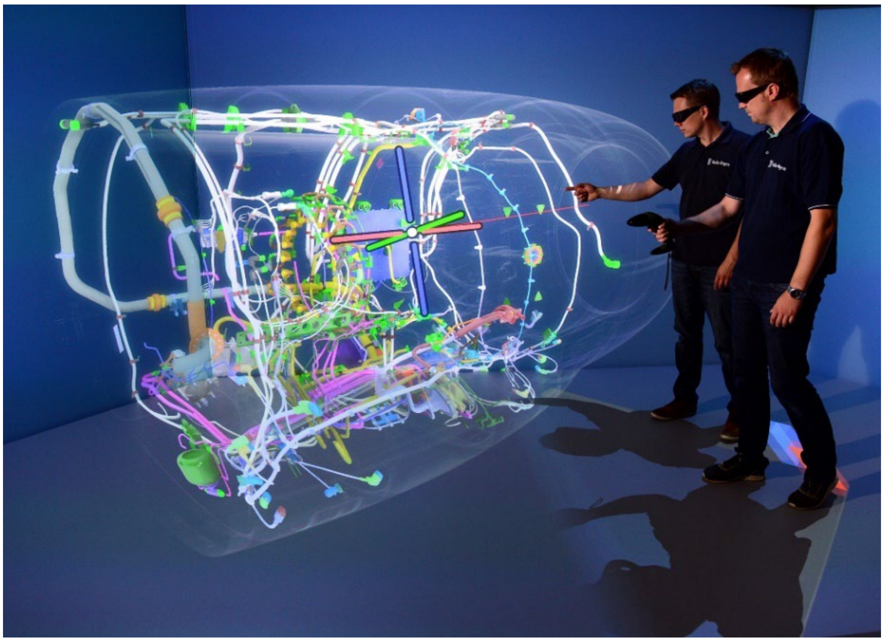


Figure 6 VR headsets are used to view a digital shadow of a Rolls-Royce jet engine. Copyright: Rolls-Royce

[12] https://www.rolls-royce.com/media/our-stories/discover/2019/how-digital-twin-technology-can-enhance-aviation.aspx
[13] https://diginomica.com/how-rolls-royce-improving-engine-sustainability-real-time-data-and-digital-twins

Case study: Smart Grid Pilot Program, Agder Energi, Microsoft Azure, NODES

Increasing demand for electricity with wider use of electric vehicles and variable energy sources like solar panels, requires the grid to be more responsive to shifts in electricity use and distributed energy resources.

Agder Energi, a Norwegian hydro-electricity company is using an Azure digital twin of their electrical grid to operate more effectively.

Sensors on assets like hydro-electric dams and substations feed machine learning analysis, providing real time predictive forecasting of supply and demand. This connects to local and central power markets in an integrated marketplace, capable of real time trading of available network capacity with transparent prices, which in turn informs grid operation. This enables autonomous systems-of-systems optimisation and a more resilient energy system for consumers.

Robotics and Autonomous Systems

Robotics and autonomous systems can operate independently by sensing, reasoning and adapting to their environment. This enables a wide range of applications from surgical assistance and physical rehabilitation, to autonomous logistics across land, sea and air.

Robots can work continuously, often faster than humans and enable people to focus time and training on higher-value jobs.

Communication and intelligence can enable cooperative applications such as autonomous swarm robotics, in which many smart robotic systems work together to achieve an overall outcome. These often replicate group structures and behaviours seen in nature. Examples include search and rescue, autonomous farming, warehouse operations.[14]

More broadly, robots and smart machines can deliver benefits across a diverse range of sectors, from growing crops and providing care and support to those in need of assistance, to working in hazardous environments where humans cannot or should not or working with side-by-side with humans to augment their capabilities.

[14] https://www.frontiersin.org/articles/10.3389/frobt.2020.00036/full

Case Study: Unmanned Aerial Systems (UAS) Swarm pilot, Blue Bear

Multiple unmanned aircraft operating collaboratively as a swarm[15] provides users with greater capability, delivered by fewer people with less equipment. This enables significant cost savings, new capabilities and better use of available assets.

Bringing together swarm connectivity, autonomy and intelligence allows deployment of new capabilities at greater scale increasing efficiency of missions using fewer resources. Drones can undertake missions employing task tailored configurable autonomy, including surveillance and situational awareness, Search and Rescue, inspection/survey of infrastructure and delivery/logistics supply.

Within the swarm, individual drones utilise pre-set rules and task instructions coupled with information from sensors to react to their surroundings and changing circumstances. The drones collaboratively achieve their task objectives – all whilst staying within the applicable rules and operating constraints. Sensors on the drones detect, capture, analyse and relay information in real time to the operator beyond the visual line of sight so they can monitor, and act should the situation demand.[16]

The Metaverse

‘The Metaverse’ describes a specific type of cyber-physical system, particularly focussed on the immersive visual integration of the physical and digital worlds for collaboration, entertainment, socialisation and the accessing of virtual services and operations.

Development has been led by the GAMMA[17] companies, and other tech giants such as Niantic, Epic Games, Unity and NVIDIA. Over the next 10 or more years[18], we may see the emergence of complex, mixed reality internet applications and services. Last year Epic Games[19] hosted a concert in Fortnite attracting 12.3m attendees, demonstrating the appetite for virtual entertainment. Similarly, the Seoul Metropolitan Government recently announced ‘Metaverse Seoul’[20] to provide virtual access to public, economic and cultural facilities. This range of metaverse propositions raises ethical challenges and risks around the interoperability and accessibility of systems, both in public services and non-public services that are still core to people’s everyday lives, whilst the new markets created could be at risk of competition issues.

The metaverse is also an area of particular opportunity for the UK gaming industry. Whilst many of the largest gaming platform companies are headquartered abroad, the UK has a

---

[15] Blue Bear demonstrates simultaneous remote launch swarming technology - Blue Bear Systems Research (bbsr.co.uk)
[16] https://www.kent.gov.uk/__data/assets/pdf_file/0011/105104/Defence-and-Security-Accelerator-case-study-Blue-Bear.pdf
[17] Google, Amazon, Meta, Microsoft, Apple
[18] https://www.bbc.co.uk/news/technology-58749529
[19] https://techcrunch.com/2020/04/24/fortnite-hosted-a-psychedelic-travis-scott-concert-and-12-3m-people-watched/
[20] http://english.seoul.go.kr/seoul-first-local-govt-to-start-new-concept-public-service-with-metaverse-platform/

strong talent pool and over 2,000 game development companies.[21] There is an opportunity to develop a strong UK metaverse capability, which can also support wider cyber-physical system development. For example, Improbable's synthetic environment solution for the defence sector is part of a portfolio of metaverse propositions.[22]

Case study: CrossDrive, University of Salford

Data sets from previous space exploration missions are critical to planning and delivering future missions. However, expert teams, data and tools are located in different countries making cooperation difficult and hindering research. CrossDrive shows how immersive collaboration can unlock the value of people, data and tools through the use of a virtual workspace.

Virtual reality workspaces allow global teams to work together on data gathered from ExoMars missions. The virtual workspaces visually represent Mars landing sites that need to be examined for robotic missions and simulations of planetary rovers and satellites. The workspaces also provide a common platform for research to be presented and discussed.[23]

Figure 7 CrossDrive uses VR headsets to enable teams to explore the surface of Mars. Copyright: THINKlab, University of Salford

21 https://gamesmap.uk/#/map
22 https://www.improbable.io/blog/working-at-improbable-what-we-talk-about-when-we-talk-about-defence
23 http://crossdrive.thinklab-salford.org/new/index.html

Cyber-physical systems in the innovation lifecycle

Innovators may make use of cyber-physical systems in developing new ideas, through ideation, design, proto-typing, testing, production and in-life operation.

Augmented and virtual reality can help visualise designs and operations, providing an intuitive way to interact with the system and making the process accessible to non-technical stakeholders.

Digital models can be used to design and prepare future manufacturing facilities. In response to the Ventilator Challenge, Siemens UK reported using a combination of digital tools including modelling and visualisation to support design, build and operator training. This reduced the time to deliver manufacturing capacity for 1,500 ventilators from the industry norm of over 12 months to 4 weeks.[24]

Prototyping, testing and validation of systems can be supported by digital shadows, which monitor test performance and can be used to inform prototype operation and future design. This information can also inform predictive maintenance reducing the cost and frequency of repairs.

Digital twins may then support the manufacturing and operation. For example, both the manufacturing facilities and their outputs may be autonomously optimised by AI. Connecting with digital twins of other supply chain nodes can enable end-to-end optimisation of manufacturing and supply.

Facilities such as living labs where end users co-locate with design and testing facilities can help ensure key stakeholders are involved in the innovation process. Connection across multiple physical locations and synthetic environments (such as simulations) enables wider collaboration and inclusion.

[24] https://www.theengineer.co.uk/young-engineers-at-siemens-rise-to-ventilator-challenge/

Case Study: A 3D Printed Bridge, Alan Turing Institute

The Alan Turing Institute partnered with Arup, Imperial College London, Dutch 3D printing company MX3D and other industrial and academic partners to design, build and monitor a 3D printed, steel bridge over the Oudezijds Achterburgwal canal in Amsterdam.

They used novel data analytical techniques from samples and prototype tests to inform digital modelling which reduced the amount of steel required. In life, the bridge is fitted with sensors to feed a digital shadow that monitors the bridge's response to corrosion, load changes, and environmental conditions, which will then be used to improve future 3D printed structure designs.[25]

Figure 8 Opening of the 3D Printed Bridge in Amsterdam. Copyright: Adriaan de Groot

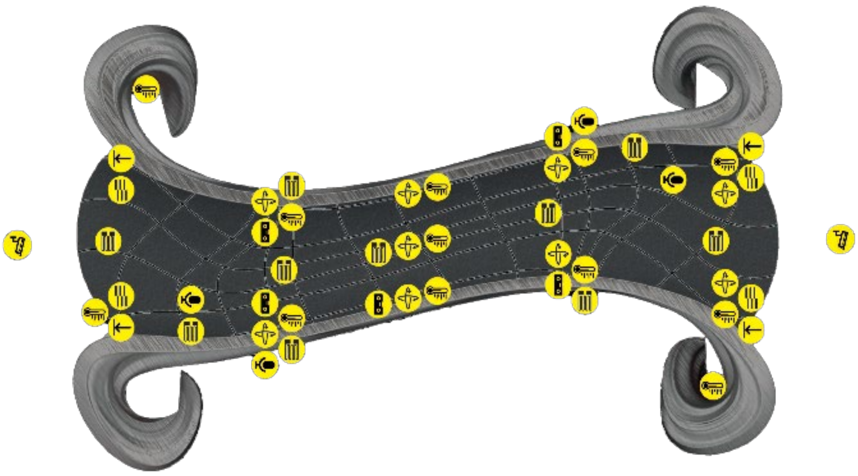


Figure 9 Model of the 3D printed bridge showing the location of sensors. Copyright: MX3D

[25] https://www.turing.ac.uk/research/research-projects/digital-twin-worlds-first-3d-printed-stainless-steel-bridge

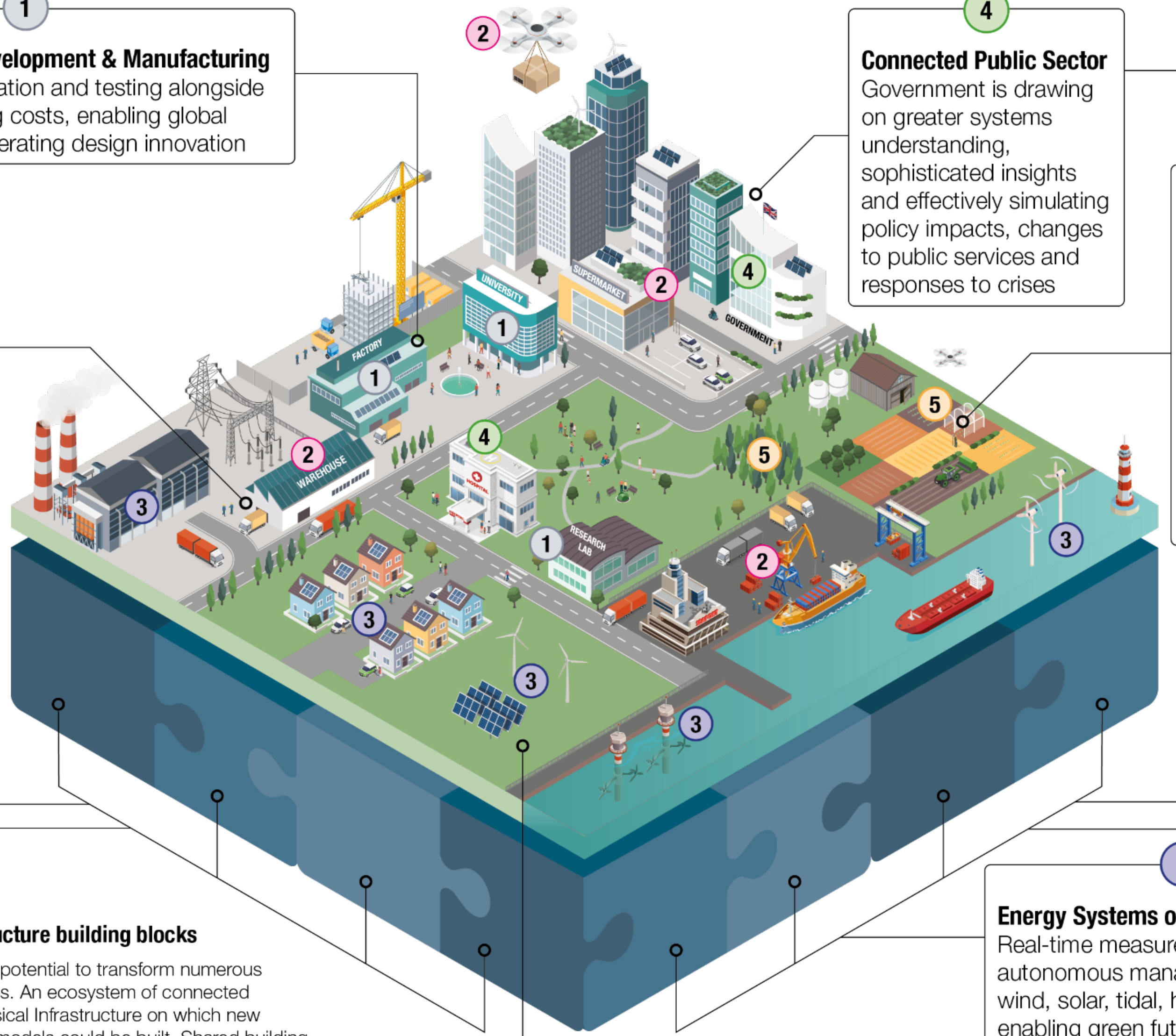
Applications of Cyber-Physical Infrastructure

1

Innovative Product Development & Manufacturing
Virtual design, collaboration and testing alongside smart machines cutting costs, enabling global partnerships and accelerating design innovation

2

Advanced Transport & Supply Chains
From autonomous vehicles and connected public transport, to smart warehouse robots and drone deliveries, seamless connections ensuring transport systems and supply chains are safe, effective and adaptable



4

Connected Public Sector
Government is drawing on greater systems understanding, sophisticated insights and effectively simulating policy impacts, changes to public services and responses to crises

5

Agriculture & Environmental Management
Better modelling, monitoring autonomous management enabling improved environmental quality, animal welfare and agricultural efficiency

3

Energy Systems of the Future
Real-time measurement and autonomous management across wind, solar, tidal, homes and factories enabling green future energy systems

Cyber-Physical Infrastructure building blocks

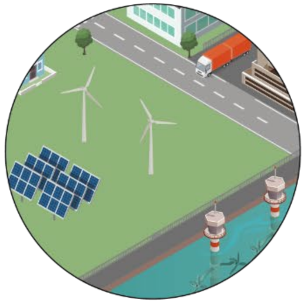
Cyber-physical systems have the potential to transform numerous sectors and enable new use cases. An ecosystem of connected systems could form a Cyber-Physical Infrastructure on which new products, services and business models could be built. Shared building blocks and interoperability of systems will likely be key enablers of this.

Better modelling and appropriately secure sharing and integration of information across the public and private sectors could help transform the delivery of **public services**.

Collecting and combining information across complex services like healthcare and the justice system could optimise capacity and deliver better outcomes.

Better modelling of our natural environment combined with digital twins of our infrastructure could enable better planning and response to extreme weather.

Greater connection of geographic, social and economic data could inform smarter policy making – from where new schools are built to how we protect our natural environment.



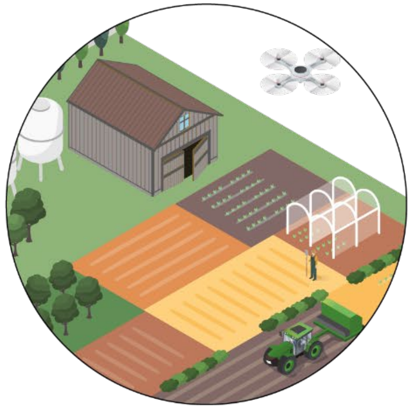
Design and manufacturing companies already use digital twins to design, test and iterate products, saving time and cost, with augmented reality enabling remote collaboration. Smart machines in reconfigurable production lines will help meet urgent needs e.g. medical equipment.

Our **future energy systems** will be distributed across solar, wind, home batteries and more. Real-time forecasting and monitoring of generation and usage will be key to resilience, combined with real time economic models to drive sustainable consumer behaviour.

Smart robots, autonomous vehicles and drones will rely on connections between buildings, the natural environment, vehicles around them, models of weather, road quality etc. to pick, pack and transport our goods quickly and safely.

In-life monitoring from connected sensors can inform predictive asset maintenance, improving efficiency, whilst feeding insights into the next design phase.

Real-time communications between **connected vehicles** and infrastructure, integrated for example with traffic and weather data, will enable better prediction and management of the demands on charging infrastructure and our energy systems.



In an increasingly cyber-physical agri-sector, satellites, drones and intelligent automation can come together to monitor crops, predict yields, perform targeted husbandry tasks (including precision chemical use) and harvest crops.

Better monitoring and understanding of the connection between the **natural and agricultural environments** can help improve land management. For example, helping government and farmers work together towards more sustainable practices such as optimising fertiliser usage or creating and safeguarding wild habitats.

The impact that floods and fires have is currently hard to predict. Combining improved weather forecasting with factors like geology and real-time foliage coverage can help significantly improve forecasting and scenario planning.

Section 2 – Enabling the Cyber-Physical Infrastructure

What is Cyber-Physical Infrastructure?

The need for Cyber-Physical Infrastructure

Whilst individual cyber-physical systems can bring benefits to specific applications, networks of cyber-physical systems could provide significantly greater benefits to both the individual use cases and wider ecosystem.

We are all familiar with how standalone computers provide significant value and networks (such as the internet) both increase the value that an individual computer can deliver and also provide an entire new capability. The internet can be thought of as an infrastructure on which previously unimaginable or unfeasible solutions and business models are being developed.

Analogously, an ecosystem of networked cyber-physical systems could be an infrastructure on which future products, services and decision-making processes are built more quickly and affordably. This ecosystem capability can be termed a ‘Cyber-Physical Infrastructure’.

This ecosystem of connected systems is not guaranteed to arise from individual bespoke applications. We hear from industry that there is significant costly re-work required to develop and connect cyber-physical systems each time, and that the commercial incentives or standards to develop foundational interoperable components and systems are not available.

This infrastructure could be as vital for developing new solutions as roads are for enabling road transport or pipes are for delivering water. Government may have a role in seeding the development of these foundations including shared building blocks and approaches to interoperability.

Building the Cyber-Physical Infrastructure

Cyber-physical systems will connect a range of digital and physical components. Figure 10 shows an illustrative schematic of some examples types of components in each domain.

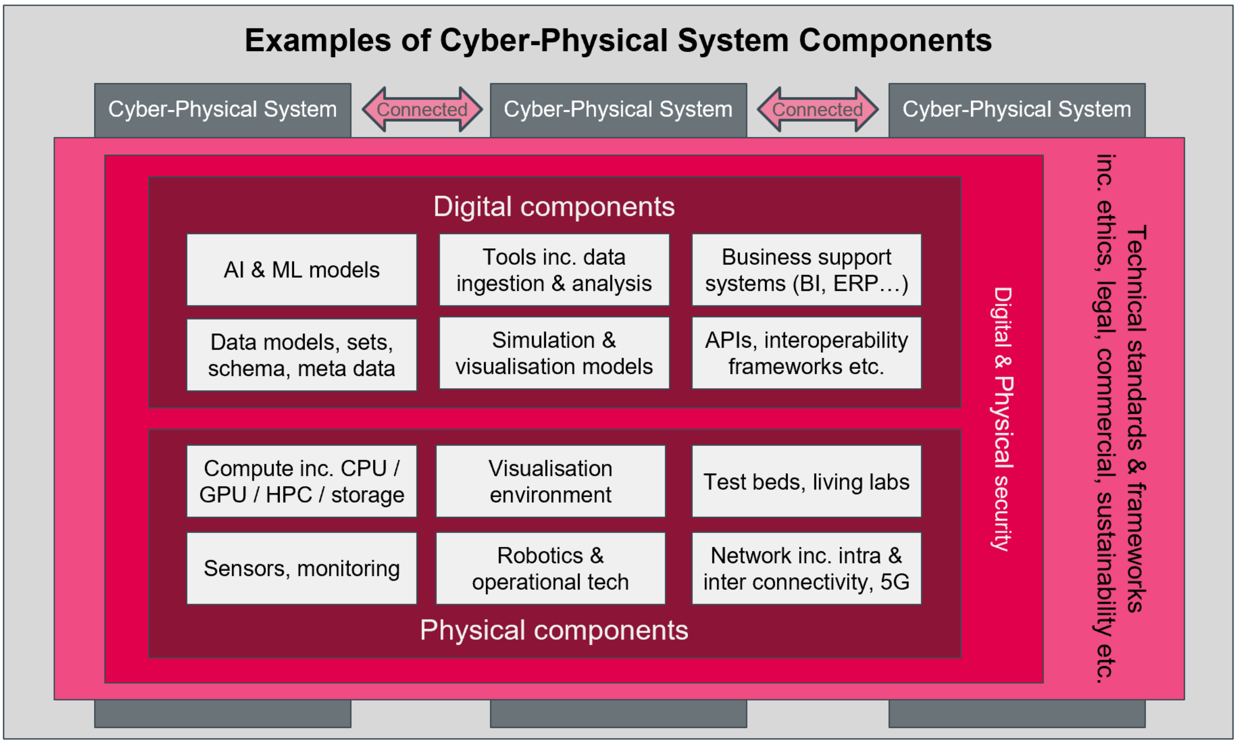


Figure 10 Schematic showing examples of the digital and physical components of cyber-physical systems (Digital Catapult, 2021)

Development of the Cyber-Physical Infrastructure of connected cyber-physical systems could be enabled by:

1. **Shared building blocks** – these could take time, cost and risk out of the innovation process by reducing the rework that currently is required to develop new applications, enabling more time to be spent on novel elements. These could be models, algorithms, frameworks, technical standards, user applications, data assets etc.

   These are most likely to be within specific sub-sectors or application spaces, where common approaches and assets can be re-utilised across systems.

2. **Interoperability** – enabling interoperability of cyber-physical systems and their components through common technical standards and frameworks could similarly support innovation by allowing easier connection between components, systems and sharing of system outputs, reducing the fragmentation of systems.

Cyber-Physical Infrastructure will likely contain a wide variety of connected physical, digital and cyber-physical components and systems, including digital twins and advanced robotic systems, as described earlier. Annex A summarises a selection of these.

Closed and shared elements

Each component (and system of components) will fall broadly into being either 'closed' (used internally or with specific partners, but not more widely accessible) or 'shared' (which includes a spectrum of openness to third parties).

Examples like cloud computing and shared networks have shown how shared infrastructure can widen access to innovations, provide economies of scale and lower barriers to innovation by reducing capital investment costs.

The approach to shared elements will vary by the use case and commercial considerations. In many cases, products ranging from individual data models to fully blown digital twins will be offered as commercial products or services. These may be wholly proprietary or utilise open, standardised interfaces or architectures to support greater integration, interoperability and ease of collaboration.

Some elements may be made available without upfront consumer costs for example freemium or open source models, particularly in pre-competitive environments, and new business models may emerge around these, for example offerings like Red Hat based on open source Linux.

Figure 11 shows how individual cyber-physical systems combine closed and shared elements in both the digital and physical domains, with interconnectivity between systems helping to increase the value and effectiveness of each.

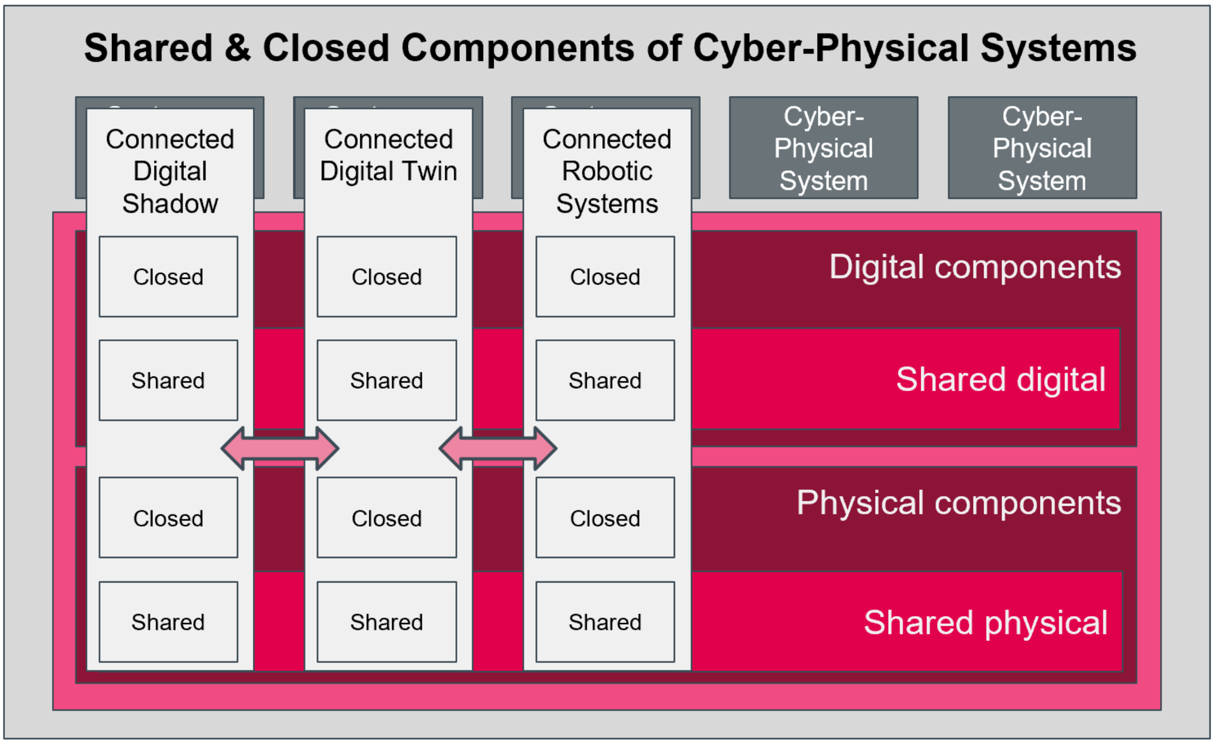


Figure 11 Examples of cyber-physical systems built from elements (both closed and shared) connected across the digital and physical domains (Digital Catapult, 2022)

Questions

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? (Annex A includes some examples of cyber-physical systems)

2 To what extent do you recognise and agree with opportunities for and potential value of cyber-physical systems (identified in section one) and the Cyber-Physical Infrastructure (identified in section two) and why?

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

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

5 a) 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?

5 b) 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?

Section 3 – People and Culture

At least as great at the technical challenges to development, are the socio-technical aspects i.e. how people and systems engage with the technology. Developing trustworthy systems is vital for sustainable technology rollout (see challenges faced by GM crops, 5G).

Within organisations, business models will need to adapt to take advantage of the innovation, efficiency and resilience benefits of cyber-physical systems, whilst sufficiently skilled people from technical through to management and leadership roles will be vital.

Opportunities

The COVID-19 pandemic has increased the public interest in science and technology, whilst also accelerating business digitalisation. These are opportunities that could be built upon.

Challenges

Trustworthiness, ethics and equality

For sustainable adoption, the public and businesses must be able to trust cyber-physical systems, the actions they drive and the use of information – whether that is an autonomous vehicle on our roads[26], optimising operations across connected supply chains or simulation informing public policy decisions.

Developing trustworthy systems will require consideration of existing and new potential ethical and equality challenges, for example, the challenges with algorithmic biases of AI, which are well documented.[27, 28] Greater sharing of information also carries risks to privacy, commercial advantage, national security, democratic rights and more. Accessibility of services, for example to digitally excluded populations, will also be a key consideration, as will the environmental sustainability of cyber-physical systems.

Leadership and culture

Development of Cyber-Physical Infrastructure will not be owned or controlled by government or any other single party. Cross-sectoral collaboration will be vital to avoid building siloed systems, and diversity and inclusivity will be key to developing a culture that works for the broad range of stakeholders.

This coalition should likely include innovators, users, standards developers, institutions, ethicists, citizens, policy developers and more to shape development of both the technical

[26] https://www.tas.ac.uk/
[27] https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version
[28] https://www.gov.uk/government/publications/the-report-of-the-commission-on-race-and-ethnic-disparities

standards and non-technical frameworks and best practices. In the longer term, the global nature of Cyber-Physical Infrastructure will likely necessitate global governance.

Skills

Cyber-Physical Infrastructure will require a broad range of skills, across technical expertise, management, legal, ethics etc. A key part of this will be digital and data skills in the workforce, which are particularly hard to secure.[29] The government recognised the critical role of these skills in the National Data Strategy and has made a number of commitments in the Strategy on digital skills, from school through to post-graduate and in-work development.

There are likely to be specific roles, such as geospatial analysts, with high demand, as well as for individuals with both domain (e.g. health) and technical expertise. Similarly, integrators able to work on converging technologies will be key.

Questions

6 a) 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?

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

Interventions

Government is making significant interventions, particularly in cross cutting areas such as AI, data sharing, and digital and data skills development such as the Centre for Data Ethics and Innovation (CDEI) and Alan Turing Institute. Likely priority actions government could also take specific to Cyber-Physical Infrastructure include:

- Undertaking **government flagship and Collaborative Research & Development (CR&D) projects** to demonstrate, develop, test and trial the business and societal benefits and the safe, ethical application of Cyber-Physical Infrastructure;
- **Engaging in public dialogue** to understand concerns and the best approaches to mitigate them, such as the Geospatial Commission's public dialogue on location data ethics and CDEI's work to understand public attitudes towards use of data;
- Developing and promoting a **coherent public narrative** of the benefits of Cyber-Physical Infrastructure and the risk mitigations in place;
- Collaborating across government, with academia, industry and wider society to help **develop the initiatives and coalitions** that will shape an ethical, public value-orientated, innovation-enabling Cyber-Physical Infrastructure;

[29] https://learningandwork.org.uk/resources/research-and-reports/disconnected-exploring-the-digital-skills-gap/

- Further **exploring the specific skills requirements** that the technology convergence within Cyber-Physical Infrastructure will necessitate.

Case study: Geospatial Commission, Location Data Ethics

Public dialogue is an approach to involving citizens in decision making about policy. Dialogues bring together a diverse mix of citizens with a range of views and values, and relevant policy makers and experts, to discuss, reflect and consider areas of collective agreement on complex issues. They seek to build a shared awareness and understanding of the relevant issues, to enable policymakers to understand different views, opportunities and challenges.

To understand the public's views on the ethics of location data usage, the Geospatial Commission worked with Sciencewise, Traverse and the Ada Lovelace Institute to undertake a public dialogue. This was conducted using 85 people from across the UK over four virtual workshops.[30]

Participants were supported to develop and express their views on issues around ethical principles, privacy and the conditions for public trust, facilitated by online workshops, chat forums, surveys, polls and idea boards.

This found that participants were more comfortable when location data linked with data about people was aggregated and anonymous; that trust in the use of identifiable location data changed depending on whether participants felt the objective was to benefit wider society or make a profit; and that more transparency around how and why data is used and by whom is needed to empower more informed choices.

The report provides evidence on public perceptions about location data use, offering valuable insights into what citizens believe are the key benefits and today's concerns. These findings will inform future guidance by the Geospatial Commission.[31]

Questions

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

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

[30] https://sciencewise.org.uk/2021/07/major-new-public-dialogue-on-ethics-of-location-data-launched/
[31] https://www.gov.uk/government/publications/public-dialogue-on-location-data-ethics

Section 4 – Technical Research, Development and Infrastructure

There are significant R&D and infrastructure challenges to overcome, from underpinning facilities, science and technology to wider socio-technical challenges, including adoption, engagement, public acceptance etc. This section focusses primarily on underpinning technology R&D and infrastructure, which will need to develop in concert with the socio-technical advances.

Opportunities

The UK can build on the significant breadth and strength of existing UK capabilities in the public, private and academic sectors. The UK undertakes significant R&D in the private, academic and public sectors. In 2019, businesses funded £20.7bn of R&D[32] whilst government has committed to increasing public investment to £20bn per year by 2024/25.

The National Digital Twin Programme has been developing a built environment-focussed community of digital twin stakeholders, whilst also developing the underpinning Information Management Framework. This comprises the technical and non-technical means to allow complex, secure and resilient information sharing to take place in right-time.

There are a broad range of investments across underpinning research and infrastructure. From computing investments such as £8m in the DAFNI large scale compute, tooling and visualisation capability and £210m from Government and IBM in the Hartree National Centre for Digital Innovation, to building on the UK's burgeoning AI sector worth £15.6bn and employing more than 35,000 people, supported by government investments of £2.3bn since 2014, including a recent additional £10m investment in the Alan Turing Institute.

UKRI and industry most recently committed £31.2m to four more digital twinning projects including AI-enabled air traffic control and nuclear powerplant component design and operation. £200 million has been allocated to the 5G Testbeds and Trials Programme, which will run until the end of March 2022 plus an additional £300m committed to 5G diversification.

The UK also has a strong record of investing in the commercialisation of these technologies. From 2018 to 2021 on average, more than £600m of equity has been invested annually in UK robotics and AR/VR companies combined, whilst the compound annual growth rates (CAGR) of equity investment in UK digital twins and AI companies are 49% and 114%, respectively, in that period.[33]

[32] https://commonslibrary.parliament.uk/research-briefings/sn04223/
[33] BEIS analysis of Beauhurst, January 2022. CAGR can vary in different timeframes given fluctuations in equity investment.

Challenges

Technical R&D will be required to overcome a broad range of challenges in both the component technologies, such as sensors and synthetic environments, and the integration into cyber-physical systems, such as the technical integration and supporting frameworks. This will need to be supported by significant research in social sciences to overcome many of the socio-technical barriers and also into ensuring we are able to secure the technology, the systems and the data and information produced.

Large increases in the volume of data storage, processing and transfer, as well as increases in both distributed and centralised systems, will require infrastructure, with appropriate security, capable of supporting it. A strategic approach to determining the future needs and how UK infrastructure can best meet these will be necessary.

Interventions

Government, industry, academia and wider society are continuing to invest in the underpinning R&D, infrastructure and application of cyber-physical systems, including in the areas identified above. We are interested in understanding the specific areas where R&D could help your organisation benefit from cyber-physical systems.

Questions

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?

Section 5 – Security and Resilience

Secure and resilient systems are vital to protect the trust in and sustainability of applications and the underpinning information. Risks could arise from malicious actors or inadvertently through system failures. Broadly speaking, these risks are not universally understood by clients and industry, meaning appropriate mitigation measures are frequently not considered or implemented without clear requirements from regulators, industry or end customers. We have seen (e.g. 5G diversification) that late interventions can be costly and disruptive.

Opportunities

There are opportunities for cyber-physical systems to support security, safety and resilience. These include increased autonomous monitoring and assurance of physical and digital systems and improved scenario modelling and planning for response to events such as security incidents and changes in operational demands.

Challenges

New or increased risks

There are a range of risks that come from increasingly connected cyber-physical systems. For example, the increased reliance on autonomous systems and data provides new opportunities for hostile actors to affect outcomes, and increased connection and data availability could give hostile actors greater insights and increase the threat surface and potential scale of impact.

There will need to be technical system requirements to build in security and resilience, for example appropriate autonomous monitoring, fail-safe mechanisms, sufficient physical partitioning of systems, redundancy etc. to ensure that compromise or failure or individual nodes or links does not cause wider system failure.

Wider challenges

There is a need to communicate both the importance of security and level of security inbuilt to both industry and wider public. However, there will be no one-size-fits-all approach. Therefore, industry, academia and public sector (including health service providers and local authorities) requirements, existing capabilities and motivations need to be explored.

Interventions

Existing security work

There is existing guidance and design principles covering personnel, physical and cyber security from the Centre for Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) which apply to the less complex types of cyber-physical systems. There is also some existing legislation and regulation such as UK GDPR. Further work will be required in both areas to take account of increasing complexity. The National Data Strategy also highlighted government's responsibility to ensure that data and supporting infrastructure is secure and resilient, whilst the recently published National Cyber Strategy 2022 sets out the government's approach to protecting and promoting the UK's interests in cyberspace.[34]

The public sector and private sectors also fund security research and innovation including the Centre for Secure Information Technologies and in the case of the former, development of the Information Management Framework.

Other possible interventions to consider

Likely priority actions government could also take include:

- Driving adoption of **existing standards and guidance** including the Information Management Framework in the application of cyber-physical systems in government, industry and academia, which could include incorporating into government procurement requirements;
- **Exploring where new guidance and technical standards** could help develop secure, trustworthy, interoperable cyber-physical systems ;
- Collaborating across government with the wider public sector, industry and academia to **embed security mindedness** into the way projects and programmes are undertaken and into their outputs;
- Undertaking **collaborative R&D projects**, including with international partners, to develop and trial secure approaches to implementing cyber-physical systems and developing Cyber-Physical Infrastructure;
- Working with stakeholders to **pro-actively shape global technical standards** development and ensure appropriate security requirements are embedded.

[34] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Questions

9 a)	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?
9 b)	To what extent do you believe these risks to be perceived or actual?
9 c)	What are the biggest current and future risks you see?
9 d)	Where and how are government, industry and academia best placed to help overcome these?
10	How and where do you currently access support for security risks?

Section 6 – Connection and Interoperability

For cyber-physical systems to realise their potential, suitable mechanisms and commercial incentives for sharing data must be in place. It is important to recognise that cyber-physical systems are one group of data sharing and utilisation applications. Wider approaches to data sharing architectures are being considered across government and improved data sharing could have economic and social benefits across a broad range of applications and sectors.[35]

Opportunities

The nascent nature of many of these markets means there are lower barriers to defining and shaping them to maximise societal benefit than in some well-established markets.

In defining and implementing the UK's approach to standards and regulatory diplomacy, we are able to act more flexibly and directly in the UK's interests post-Brexit.

Challenges

A number of key barriers to data sharing were set out in the National Data Strategy Mission 1 Policy Framework: unlocking the value of data. They are: a lack of incentives to share data; regulatory and legal risks; a lack of knowledge; high costs associated with data access/sharing; commercial, reputational and ethical risks; and a lack of trust from data subjects.

Four thematic areas of action were identified to overcome these: supporting the development and use of good data standards; supporting technologies and institutions that enable data sharing; exploring data sharing incentives and market structures; collaborating with international partners.

These barriers and priority action areas apply more widely to data sharing applications than just Cyber-Physical Infrastructure.

Commercial data markets

The cost of producing shareable data is high, particularly in legacy systems. Additionally, finding buyers, judging fair 'market value' and entering into data sharing agreements can be resource intensive. These challenges reduce the scalable sharing of data in markets.

[35] https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy

Interoperability, openness and standards

As identified interoperability and openness are critical for maximising the societal and economic potential of cyber-physical systems. The ability to move between systems and partners reduces the likelihood of monopolies.

Low cost, scalable mechanisms to connect cyber-physical components and systems, which maintain security, will be key to commercial adoption of both technical standards and the ethical, legal and commercial frameworks and culture of openness.

Conversely, developing interoperable systems and data can increase upfront costs, inhibit innovation or, in some cases, reduce commercial advantage. Therefore, it will not always be the preferred approach. There are a range of potential approaches, from increased use of semantics, meta-data and principles-based approaches, to the need for technical standards.

Case study: Virtual Energy System Programme, National Grid Electricity Systems Operator (ESO)

The future energy landscape will include an increase of offshore wind, the phasing out of coal, a shift to electric vehicles, and smaller, renewable generation. This will increase the variability of energy supply and demand. New tools will be needed to design, forecast and operate the future electricity system more effectively.

To enable this, National Grid ESO is initiating the Virtual Energy System programme with the ambition of creating a shared resource of connected digital twins, developed and owned by different energy system stakeholders. A common framework of standards is being developed to enable an interoperable ecosystem of distributed digital twins.

The programme will be built up through individual use case projects, where a digital twin is developed to solve a particular problem. Data from individual digital twins of assets and systems can then be shared and used to improve operation of the energy system in real time and inform long term planning, such as for infrastructure investments. This shared connection could also enable new business models, policies and commercial offerings.[36]

Technical standards define an agreed way of doing something and are a crucial way to enable interoperability. Trust, safety and resilience can also be strengthened through agreed approaches to security, ethics etc.

The approach to technical standardisation in sectors will likely vary. Some stakeholders prefer development as part of the system of national, regional and internationally recognised global standard developing organisations. Others, often including those within digital technologies, prefer sector specific bodies, such as the Internet Engineering Task Force. Here, technical

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

standards arise when a solution is developed and widely adopted by industry and then codified into specifications.

Case study: Application of the Information Management Framework, National Highways

For National Highways to work effectively across its business, from construction and maintenance to operation and the supply chain, they need access to information held by each other and to understand its quality.

Data is stored across various tools and systems, which has raised barriers to access and interoperability. A common way of showing the properties of each business area’s information and how they relate to others (an ontology) will help enable consistent understanding and interpretation of information across the business, driving efficiency in planning and delivery.

More broadly, applying the principles of the Information Management Framework, which is being developed as part of the National Digital Twin programme, will help National Highways exchange information with third party infrastructure owners and operators. This will enable more effective collaboration.

Integration with legacy systems

In most cases there will be legacy data and systems to integrate with but there can be significant barriers. Technical and institutional approaches may emerge such as technical translation layers, interfaces and technical intermediaries.

Interventions

As identified in the National Data Strategy Mission 1 Policy Framework, there are a range of areas where government could help enable the sharing of data, including:

- Supporting development of **data sharing infrastructure** (e.g. data intermediaries), **data sharing techniques** (e.g. Privacy Enhancing Technologies) and approaches to lower the cost of data sharing;
- Exploring the **role of incentivisation** in data sharing;
- Promoting good data foundations through the **FAIR principles**;

Likely priority actions where government could go further include:

- Identifying opportunities for **public sector flagship projects** to help develop and demonstrate the value and mechanisms for data sharing and help develop the supply chain and ecosystem;
- Exploring opportunities to develop and trial **novel data sharing marketplaces and mechanisms**, including: sandboxes to trial approaches to regulated data sharing;

government procurement marketplaces; and CR&D projects including standards and guidance which support interoperability such as the Information Management Framework;

- Identifying opportunities to **update, influence or create regulation** to make data sharing easier, for example, the recent consultation on reforms to the UK's data protection regime, which are now feasible post-Brexit;
- Collaborating with industry, academia and wider society **to explore the opportunities for standardisation** to support Cyber-Physical Infrastructure and what roles industry, academia, government and wider society could play.

Case Study: Data Intermediaries, Genomics England

Genomics England is a custodian of one of the world's most valuable databases of genomic and clinical data, used to enable better patient outcomes as part of the NHS Genomic Medicine Service, and to support the UK's flourishing research ecosystem.

The data held is highly sensitive, and Genomics England's work demonstrates how data intermediaries can address the ethical and privacy concerns of those who share their personal data, whilst ensuring it is deidentified and shared appropriately to derive public benefit. To do this they employ the following principles:

1.The participant communities who consent for their data to be used for research are involved in and informed of data sharing mechanisms and policy;

2.The consent for data use must be robust and simple;

3. The Caldicott Principles that provide guidelines for good information sharing when using and sharing confidential information[37]; and

4. The 5 Safes framework that provide a set of guidelines to enable safe access to research data must be inbuilt into data sharing and security by design.[38]

The principles ensure Genomics England firmly places patient or participant interests at the core of how data is accessed and utilised for patient benefit. It also pays specific attention to the stability of its systems and services, employing secure technology and safeguards to ensure only appropriate access is granted. This enabling structure provides the data to help diagnoses in the NHS, researchers develop new treatments, and to support the thriving genomics industry in the UK.

[37] https://www.gov.uk/government/publications/the-caldicott-principles
[38] https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/

Questions

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.)?

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?

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

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

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

Section 7 – Sustainable Markets

Cyber-Physical Infrastructure will need to be commercially sustainable and well-functioning technology and data markets will be critical to this.

Opportunities

Whilst building on significantly entrenched markets in many places, many of the markets for these technologies and for data are still developing. In these, there are fewer entrenched standards, business models and marketplaces, and therefore greater opportunities to help shape them to maximise societal benefit.

Challenges

Investment and Development

Where shared building blocks are not directly monetised (including open frameworks and standards), individual businesses may have lower incentives to invest in them. Additionally, without the development of interoperability mechanisms, systems may consolidate around proprietary ecosystems leading to fragmentation and high barriers to data sharing.

We have seen how market models can support open-source assets and open standards. For example, the Linux kernel is sustained by a mix of voluntary developers, donations and contributions of developer time and funding from companies who see benefit in the development of the offering. There may be a role for government to collaborate with industry, academia and wider society in convening and supporting the early development of these elements.

Additionally, the R&D required is often high risk and long term and can require coordination and support to help build demand.

Market Concentration

Technology and data markets are also both at high risk of market concentration. Dominant players can emerge as users are attracted to the already most popular platforms. Similarly, organisations who own assets critical to doing business (e.g. IP, data sets etc.) or that control access to other services (e.g. Google’s search engine dominance of web access) can leverage their powerful positions.

The Digital Markets Unit has been set up within the Competition and Markets Authority to oversee a new regulatory regime for the most powerful digital firms, promoting greater competition and innovation.

Case Study: Online Platforms and Digital Advertising Market Study, Competition and Markets Authority (CMA)

The CMA undertook a study to examine how well digital markets for search engines, social media, and digital advertising are functioning, and the role of Google and Facebook within them.[39] The study highlighted the key role of competition in driving growth and innovation, and the role of pro-competition regulation in enabling this.

The study found Google and Facebook hold powerful positions in the UK digital advertising markets and can gather more data about consumers than rivals. An absence of competitive pressure has inhibited the development of new, valuable services for consumers, whilst consumers also have limited control over the collection and use of their data.

In response, the CMA proposed the development of a Digital Markets Unit (DMU). This has been established as a non-statutory body to oversee a new regulatory regime for digital firms, promoting greater competition and innovation in digital markets and protecting consumers from unfair practices.[40] The CMA is also currently taking forward a market study on mobile ecosystems, investigating concerns that Apple and Google have too much control over key activities such as mobile operating systems, app stores and web browsers.

The final report of the market study is due in June 2022 and will inform the development of the pro-competition regime.

The government consulted on the pro-competitive regime for digital markets in June 2021 and intends to take forward legislation when parliamentary time allows.

Interventions

To address potential competition issues developing within cyber-physical markets, likely priority actions government could also take include:

- Publicly convening, supporting or co-investing in a) **development of shared building blocks** (such as models, algorithms, frameworks, technical standards, user applications, data assets etc.) where there are higher barriers to development, and b) **interoperability mechanisms**, including collaborating with industry, academia and wider society to enable the long-term initiatives necessary to support the development of Cyber-Physical Infrastructure;

[39] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[40] https://www.gov.uk/government/news/new-competition-regime-for-tech-giants-to-give-consumers-more-choice-and-control-over-their-data-and-ensure-businesses-are-fairly-treated

- Exploring with industry how the Cyber-Physical Infrastructure market may develop and how **potential market failures can be proactively addressed** such as through opportunities for codes of practice and self-regulation;
- Explore with industry how government can **help drive investment in cyber-physical systems development** for example:
    - Leveraging **government procurement** of cyber-physical systems and goods and services which comprise cyber-physical systems
    - Supporting **standards development**
    - **Appropriate incentives** for R&D investment, with a strong drive towards development, demonstration and promotion of use cases and business cases to demonstrate the value to users and businesses
- Collaborate with industry to **support demand-side awareness and capability** including the range of non-technical challenges, for example:
    - Business **support for adoption**, such as awareness and upskilling schemes, accelerators and innovation centres etc.;
    - Supporting **development of necessary technical, management and leadership skills**;
    - **Building business awareness** of cyber-physical systems and their benefits;
    - **Demonstrating use cases and business cases** for cyber-physical system adoption.

Case Study: CONVEX, Centre for Connected Autonomous Vehicles (CCAV), Zenzic, Innovate UK

CONVEX is a cloud-based platform to enable the commercial sharing of transport and connected car data among stakeholders in the global connected and autonomous vehicle sector.[41] The aim was to help accelerate research and development of self-driving vehicles through greater data and insights sharing.

The project highlighted the benefits of greater data sharing but also the significant challenges of enabling and encouraging competing organisations to share data. It has shown that detailed understanding of commercial drivers and the specific data that will be shared including ‘how’, ‘why’ and the security approach, is vital to develop an enabling marketplace and building stakeholder buy-in.

[41] https://zenzic.io/testbed-uk/convex/

Questions

14 a) 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)?

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

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

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

Section 8 – Working Globally

The UK market is relatively small and Cyber-Physical Infrastructure will be a global endeavour. Therefore, international collaboration with businesses, academics, investors and other nations will be vital.

Opportunities

Where the UK has relatively advanced capabilities, there may be first mover advantages of being able to export the products, services and standards, driving demand for and alignment to UK offerings, for example with the UK's early progress in development of the Information Management Framework.

The UK already has a top-tier technology investment environment, well-regarded regulatory regimes and forthcoming changes to R&D tax incentives to support data and digital R&D with which to attract businesses.

Case study: The BIM Story

Building Information Modelling (BIM) is a combination of processes, standards and technology through which it is possible to generate, visualise, exchange, assure and subsequently use and res-use information. When fully implemented it forms a foundation for decision-making to the benefit of all those involved in any part of an asset's lifecycle. It also promotes greater transparency and collaboration and thereby a reduction in waste and costs.

The UK Government required that by 2016, public sector centrally procured construction projects would be delivered using BIM. As part of the BIM programme set up in advance of this deadline, Government, the Construction Industry Council and industry worked with the British Standards Institution and others to develop a robust set of standards which have now largely been replaced by the ISO 19650 suite based upon them.

The UK used these standards and its recognised position as a leading nation in BIM exploitation to develop its international construction competitiveness, by collaborating with other countries to shape their digital construction market requirements. This helps improve the quality of their construction, whilst opening up new markets and increasing demand for UK services. Most recently this contributed to the UK-Peru government-to-government construction agreement, which has helped UK firms winning contracts in excess of £100m.[42]

[42] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974105/Global_Infrastructure_Progamme_Prosperity_Fund_Annual_Review_2020.odt

Challenges

Digital and technology markets are globally integrated both through supply chains and the cross-border networking of digital solutions. Therefore, to ensure that standards and frameworks reflect UK democratic values, UK security and privacy requirements and support UK interests, it will be necessary to collaborate with like-minded countries and in international fora to actively shape standards and frameworks, including using the UK's post-Brexit regulatory freedoms.

Cyber-Physical Infrastructure will become a core UK infrastructure, therefore, understanding of the role of international supply chains and their benefits and risks will be key.

Mobility of capital, talent, IP and companies means that we will need to ensure we retain the benefits of UK investments in the UK.

Interventions

Government, working closely with UK stakeholders, is engaging with global standards developing organisations and international partners across a broad range of digital technical standards topics. For example, government has committed to international collaboration in AI and data with the AI Standards Hub and the National Data Strategy's commitments to enabling cross-border data flows. Likely priority actions where government could go further include:

- Identifying opportunities to promote UK leadership and interests in Cyber-Physical Infrastructure through **regulatory diplomacy initiatives** (in many places this will be existing fora and activity in areas that are relevant to Cyber-Physical Infrastructure (e.g. AI, IoT, networks etc.), but there may also be a need for specific Cyber-Physical Infrastructure engagements);
- Developing and promoting a coherent **international narrative** of the UK's vision for Cyber-Physical Infrastructure to drive trust, interest and engagement with the UK;
- **Reviewing and cohering the range of support available** to attract (and retain) people and investment in Cyber-Physical Infrastructure in UK;
- Collaborating with industry, academia and wider society to enable multi- and/or bi-lateral **international collaboration activities including CR&D projects**, to build the UK's international relationships, profile and capability in Cyber-Physical Infrastructure;

Questions

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

17 a) 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.)?

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

18 What international groups and fora are you aware of involved in developing cyber-physical systems and infrastructure (e.g. international industrial groups, standard developing organisations, academic fora etc.) and which of these do you find most relevant?

Annex A – Summarising a range of key Cyber-Physical Infrastructure elements

Artificial intelligence and machine learning	Artificial intelligence (AI) is the capability of a machine to act intelligently, typically similar to human learning and problem solving. Machine learning can be considered a specific approach or application within AI, in which mathematical models are used to enable a machine to learn without direct instruction. Within cyber-physical systems, AI can enable the operation and coordination of smart machines, as well as the operation and optimisation of individual systems or connected systems-of-systems, for example utilising a digital twin.
API	Application programming interfaces (API) enable systems and services to exchange information easily, securely and in a scalable manner by handling requests for information and the responses. They are therefore a key enabler of innovation. By acting as a middleman between systems, they can also increase security as neither system is fully exposed to the other, only providing requests and requested information. This may also include authorisation credentials.
Augmented reality and virtual reality	Augmented reality (AR) adds digital elements to real world elements in an interactive manner (for example Instagram filters or in games such as Pokémon GO). This is often accessed through a mobile phone. Virtual reality (VR) is immersive, wholly virtual visualisation. The entire environment is virtual and is often accessed through VR headsets.
Digital Model	A digital Model is a digital representation of an asset, system or process at a fixed point in time. Commonly used in manufacturing to design virtually before physical manufacturing and reducing the cost and time, for example in Computer Aided Design (CAD).
Digital Shadow	A digital Shadow is a digital model that integrates information from its physical counterpart. This may be in real- or right-time. This can provide insights into performance, maintenance needs, compliance, scenario planning and future design interactions. These are often used in systems without autonomous interventions (e.g. predictive maintenance) or any direct interventions (e.g. weather forecasting).

Digital Twin	A digital twin is a digital model with real- or right-time, two-way information flows. This can enable autonomous optimisation, and remote and autonomous operation. These are not yet widespread but are typically found in autonomously operated environments such as robotics and autonomous vehicles and maritime vessels.
Internet of things	The internet of things conceptualises the connection of a broad range of devices to the internet and other devices. In our homes this may be our central heating system, enabling remote control or devices that help monitor our fitness and activities. This could also include road traffic sensors and connected vehicles. By connecting sensors and actuators (things that make an effect e.g. a robotic arm or connected traffic light), we can better understand our systems, then manage them effectively.
Living labs	Living labs connect researchers and innovators with the range of stakeholders involved in the delivery and end use of products and services, often by embedding the lab within real-world delivery environments. These are usually physical locations but can be enabled and expanded through greater connection of systems and virtual collaboration environments. The aim of living labs is to build greater connection and understanding between the innovators and wider stakeholders which enables wider socio-technical considerations to be considered as part of the innovation process, which can otherwise often focus primarily on the technological.
Shared building blocks	These could comprise a range of assets which are combined to develop cyber-physical systems, such as models, algorithms, frameworks, technical standards, user applications, data assets etc. These could take time, cost and risk out of the innovation process by reducing the rework that currently is required to develop new applications, enabling more time to be spent on novel elements. These are most likely to be within specific sub-sectors or application spaces, where common approaches and assets can be re-utilised across systems.
Simulation and Emulation tools	Simulation is use of a digital model of a real or hypothetical system that can be used to test designs, scenarios and predictions, train algorithms and more. As with all models, the aspects of the system modelled level of fidelity determine how representative it is.

	An emulation is a digital representation of a system (physical or digital, or cyber-physical) that is capable of replicating its behaviours and outputs to such an extent, that applications, tools, devices etc. designed for the system being emulated, can interact with the emulation, with equivalent results.
Robots and smart machines	Robots are physical machines that can act independently of human control by sensing, reasoning and adapting to a given situation or environment. The autonomous capabilities of advanced robots or smart machines mean they are increasingly able to sense and think rather than move in pre-programmed ways. This is opening up new business capabilities and consumer applications from autonomous vacuum cleaners, to fruit-pickers, delivery drones and self-driving vehicles.
Synthetic environment	Synthetic environment is an umbrella term which includes various representations of systems including digital twins, simulations and emulations.

Annex B – Consultation questions

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? (Annex A includes some examples of cyber-physical systems)

2 To what extent do you recognise and agree with opportunities for and potential value of cyber-physical systems (identified in section one) and the Cyber-Physical Infrastructure (identified in section two) and why?

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

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

5 a) 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?

5 b) 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?

Section 3 – People and Culture

6 a) 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?

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

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

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

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?

Section 5 – Security and Resilience

9 a) 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?

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

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

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

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

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?

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

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

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

Section 7 – Sustainable Markets

14 a) 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)?

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

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

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

Section 8 – Working Globally

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

17 a) 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.)?

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

18 What international groups and fora are you aware of involved in developing cyber-physical systems and infrastructure (e.g. international industrial groups, standard developing organisations, academic fora etc.) and which of these do you find most relevant?

This consultation 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 cpiconsultation@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.