National
Engineering
Policy Centre

Royal Academy of Engineering

APRIL 2022

National Engineering Policy Centre roundtable on cyber-physical infrastructure to catalyse innovation

Introduction

The National Engineering Policy Centre (NEPC) hosted a virtual roundtable on 29 April 2022 as part of the Department of Business, Energy and Industrial Strategy's (BEIS) *consultation* on enabling a national cyber-physical infrastructure (CPI) to catalyse innovation.

CPI including digital twins, connected smart machines and artificial intelligence, are coming into application and playing an increasingly important role. CPI presents real opportunities to enable and accelerate research and innovation in the UK and to deliver wider benefits such as reducing greenhouse gas emissions[1]. Recognising the need for successful development and joining up of physical and digital technologies will help maximise these opportunities.

Physical and digital R&D infrastructures are used by businesses and researchers to undertake a wide range of R&D activities to accelerate the development of new products, technologies, services,

National Engineering Policy Centre

We are a unified voice for 42 professional engineering organisations, representing 450,000 engineers, a partnership led by the Royal Academy of Engineering.

or processes. Shared R&D infrastructure, such as living labs and test beds, play a crucial, enabling role for business R&D. These infrastructures provide access to specialist equipment, data and real world conditions for new products to be safely tested and demonstrated in use with real customers and regulators that would otherwise be unaffordable or inaccessible to companies.

The roundtable brought together the perspectives and expertise from engineering businesses of all sizes and from different sectors, as well as researchers and government agencies. The discussion was focused on shared building blocks, interoperability, and considerations for security and resilience. The Royal Academy of Engineering has also published reports relevant to this topic, including *Internet of Things: realising the potential of a trusted smart world*[2]; *Towards trusted data sharing: guidance and case studies*[3] and *Late-stage R&D: business perspectives*[4].

This paper is a thematic summary of the discussion, covering key points on the role of government, interoperability, standards, examples of valuable building blocks and security and resilience.

The role of government

- Government, industry, and academia all have a role to play, and the discussion began by focusing on the role of government. Concerns were raised around the risk of failure from taking a top-down or centralised approach, with warnings from large IT projects in the public sector that were viewed as poorly executed.
- A key role for government is to prevent market failure and to act when it becomes a risk. The government could act as a convening force, ensuring necessary discussions take place – including on standards, ethics and building blocks – and aiding increased awareness and visibility by bringing stakeholders together.
- Two potential modes of market failure were identified: failure to federate across the sector, and the risk of the market taking an unethical direction. Industry has a fundamental role to play working collaboratively and developing standards to enable join-up across physical and digital technologies. However, past experiences highlighted that industry only tends to federate once their ability to market new products is affected. With strong international competition, a delay in federating the sector could lead to missed opportunities.
- Public procurement can be a powerful tool to set direction and confidence to invest in the sector, as well encouraging adoption of new standards, if made a condition in contracts. The Small Business Research Initiative (SBRI) was suggested as a model to deploy for CPI.
- Joined-up government was viewed as crucial to successful delivery of CPI in the public sector, as thinking will need to be weaved across departments. The Office for Science and Technology Strategy (OSTS) was suggested as a potential candidate to ensure this join-up across government, with a lead role for UK Research and Innovation (UKRI) in coordinating R&D activities.
- From a security and resilience perspective, the government has roles to play both in identifying what the critical national infrastructure of the future will be, and in safeguarding its security.

- Education and awareness-raising of initiatives that already exist were emphasised as a matter of growing importance to avoid unnecessary duplication and use of resources, including public research, investment and local government contracting. Mechanisms enabling easy sharing and access to understand what has already been done would support better practice, progress developing and bringing CPI into wider use.
- Support for initiatives such as living labs and university collaborations would benefit the creation of environments for safe testing closer to the real world (but without the constraints of standards) and to develop the business case. Defining the right risk appetite will be important in order to move fast enough to test and identify problems to solve.

Interoperability

- Sharing mechanisms do not currently exist for CPI data and models. What is shared with whom, for what purpose and at what cost is an important question to address. Different stakeholders will have different needs. Open source and private systems will be required to offer choice and need to work together.
- The development and deployment of CPI is fundamentally a socio-technical undertaking. The technical solutions will be necessary, but not sufficient. Human and organisational factors will also need to be addressed for CPI to deliver on its promise. This includes commercial, legal, regulatory solutions, and organisational interoperability with effective collaborative leadership for government, industry and academia to pull together towards shared desired outcomes.
- Participants discussed the binary view of sharing data and models, with open or closed traditionally presented as the only options. They underscored the need for new models of enabling access that do not depend on making data and models open. These could enable necessary data sharing across sectors and vertically across supply chains and manufacturers.
- Another ongoing challenge is interoperability with existing and legacy technologies. For example, traditional manufacturing machines have out-of-date communication protocols creating barriers to interoperability.
- A federated approach to CPI will need to consider practical interoperability at sensor level and for data sharing, which may require the choice of a common language. Currently, there are many local models that may be challenging to link up.
- However, there are examples of smart cities that are being built through the joining up of heterogenous projects, with examples from Cambridge and Bristol. Interoperability between sensor and actuator protocols is already in progress. The approach can be a mix between federation and aggregation of models. Any future approach should consider issues related to data sharing.
- Examples of good practice to learn from include *Dataswift*, the *DARE UK* project and the use of living labs for safe trialling and testing of new ideas and technologies.

Standards

- The need for standards to enable interoperability, data sharing and security was a focal point of the discussion. Standards were viewed as crucial to ensure the diversity of stakeholders and technologies under CPI can work together, by setting out a common language. This includes standards for data exchange and data quality.
- Standards will need to be agile. The challenge was recognised, considering the pace of change and innovation. Suggestions included setting out standards with a “learning by doing” approach with active feedback loops for improvement or standards outlining high level principles to enable evolution in how they are applied.
- Indeed, beyond the issue of standards there is a general need to manage obsolescence in such a dynamic and fast-moving environment with technologies developing rapidly. This also creates challenges for investability.

- Standards can risk stifling innovation if they are developed or imposed in the wrong way, or in a way that is overly tied to a specific generation of technology. The guiding principle for standards should be that they enable, rather than dominate and control, with standards only used when they are necessary.
- Standards need to be developed in an inclusive way, and it is important that no single player pushes their own standards. SMEs are unlikely to have capacity to participate in efforts to change standards, especially if confronted with lack of appetite for change in that sector.
- Standards will need to be international.
- Common standards would open up opportunities for living labs and to test new technologies in more environments, as it would be easier to connect into existing systems. In turn, living labs are a good way of developing standards in the context of how the technology works, rather than in the abstract.

Examples of valuable shared building blocks

- Participants noted issues arising from data stored with private companies outside the UK. A building block offering secure cloud storage like AWS or Azure would be useful where there are questions of data sovereignty. For example, the US has developed a version of AWS for government, built in a way that is equivalent to ensure all other tools can still be used.
- Physical building blocks such as sensing and robotics technologies have an important role to play. One example from a small scale cyber-physical project noted that they had to develop most robotics components in-house as off-the-shelf products did not meet their needs, taking a few years. Bringing these new technologies to potential users and customers is then challenging as those building blocks need to interface with their models.
- Ways of assuring, benchmarking, and vetting new technologies would be a helpful shared building block. They would support opportunities for businesses marketing new technologies, giving confidence to potential customers on questions of technology and security.
- New delivery mechanisms may be needed to ensure building blocks can be shared, for example using crowdsourcing and pre-competition innovation, with public ownership removing barriers to sharing.

Security and resilience

- CPI was viewed as an opportunity for increased security and resilience, including through the convergence of these two agendas.
  - Self-healing systems and digital twins can support increased resilience and longevity, including with the ability to model for the exception and to support continued operation of a system whilst it is compromised.
  - System diversity helps improve resilience.
  - One of the main benefits of having models and digital twins is the ability to analyse the impact that an attack would be able to have to develop strategies, models and algorithms to respond to events, not just containing the attack but also minimising impact. Investment can be directed to where it will be most effective, improving robustness or system recoverability.
- Connecting systems carries risks and unexpected consequences that will need to be understood and managed. The initial question is important to answer: is it worth having the CPI, or is the default state just as effective with less risk? Then problems and possible mitigations can be considered.
  - Unexpected consequences and cascade effects are likely when complex systems are connected, with cascading effects from attack propagation. Resilience can decrease by making a well-designed and secure system interdependent with another system, for example connecting the electric grid to

telecommunication networks. Any new interoperability model should be envisioned not as traditional security and total defence, but rather, it should consider how to operate with a partially compromised system and have the ability to understand possible cascades.

  - The increased size of a system translates to increased risk of attack.
  - With the use of machine learning and AI, new vulnerabilities are introduced. A very active research community is working to tackle the problem of adversarial machine learning.

- Liability is not well defined for interoperable systems. It is currently unclear where liability sits across these systems, and whether responsibility lies with the manufacturer, user or implementer.

References

1 *Digital technology and the planet: harnessing computing to achieve net zero*, Royal Society (2020)

2 *Internet of Things: realising the potential of a trusted smart world*, Royal Academy of Engineering (2018)

3 *Towards trusted data sharing: guidance and case studies*, Royal Academy of Engineering (2019)

4 *Late-stage R&D: business perspectives*, National Engineering Policy Centre (2021)

National
Engineering
Policy Centre

Royal Academy
of Engineering

THE ROYAL ACADEMY OF ENGINEERING

The Royal Academy of Engineering is harnessing the power of engineering to build a sustainable society and an inclusive economy that works for everyone.

In collaboration with our Fellows and partners, we're growing talent and developing skills for the future, driving innovation and building global partnerships, and influencing policy and engaging the public.

Together we're working to tackle the greatest challenges of our age.

NATIONAL ENGINEERING POLICY CENTRE

We are a unified voice for 43 professional engineering organisations, representing 450,000 engineers, a partnership led by the Royal Academy of Engineering.

We give policymakers a single route to advice from across the engineering profession. We inform and respond to policy issues of national importance, for the benefit of society.

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel 020 7766 0600 www.raeng.org.uk
@RAEngNews

Registered charity number 293074