CATAPULT Connected Places

TransIT

Cybersecurity in Transport Digital Twins

9 June 2026

Executive summary

This report summarises insights from the TransiT workshop *Cybersecurity in transport digital twins*, held on 9 June 2026.

The event brought together stakeholders from transport, energy, research, policy and technology to explore how cybersecurity risks evolve as digital twins become more interconnected and more influential in cyber-physical transport systems. The discussion highlighted that cybersecurity is becoming a core condition for the safe, trusted and scalable adoption of digital twins in transport decarbonisation.

In what follows, we translate the event's presentations, discussion and workshop activity into a clear narrative for external academic, industry and policy audiences, focusing on three elements:

What we heard

Why it matters

What it signals next

Key messages from the workshop

As transport systems become more connected, risk increases due to wider attack surfaces and interdependencies between organisations, assets and data flows.

Trust in data, models and outputs remains a major barrier, particularly where digital twins rely on shared data or where outputs influence operational decisions.

Resilience and recovery are as important as prevention, as cyber incidents are expected to occur even in well-designed systems.

Digital twins are increasingly part of cyber-physical system-of-systems environments, where the most significant risks arise between systems rather than from isolated components.

System architecture plays a role in both vulnerability and resilience, influencing how risk propagate, how trust is established and how systems can be secured.

Skills and capability gaps persist across industry, particularly in understanding cyber risk in interconnected digital environments.

Governance, accountability and coordination become more complex as systems scale across organisational and sector boundaries.

Human oversight remains essential, especially in contexts where digital twins inform safety-critical or operational decisions.

Digital twins offer clear operational and decarbonisation benefits, but adoption will depend on improvements in trust, governance, validation and security maturity.

Event overview

The central focus of the workshop was the proposition that cybersecurity is a critical enabling condition for digital twinning in transport as cyber-physical systems become more connected across organisational and sector boundaries.

The workshop was hosted by Connected Places Catapult and opened with remarks from Dr Chris Jones and keynote input from the National Cyber Security Centre. Workshop sessions were hosted and guided by Professor Dimitrios Pezaros and Dr Stefanos Evripidou, whose contributions linked the opening framing with detailed table work and an end-of-day synthesis.

The workshop brought together participants from transport, energy, infrastructure, research, policy and technology backgrounds. The activities were designed for a broad cross-sector audience, including transport and energy infrastructure operators, engineering consultancies, digital twin and technology providers, cyber security and cyber-physical systems specialists, policy makers, regulators and researchers involved in transport decarbonisation.

What we heard – Key insights

Interconnection changes the nature of cyber risk

> **“As our transport systems become more connected, we’re expanding the attack surface that malicious actors might expose.**

A consistent message from the workshop was that cyber risk in digital twin ecosystems is not just a bigger version of existing system risk. The nature of the risk changes as systems become more interconnected. The clearest headline quotation from the discussion captures that concern directly: “*Everything is ripe for attack… being able to attack at any point was essentially what was most concerning.*” Participants repeatedly described environments where exposure is distributed across devices, data flows, infrastructure and organisations.

This concern appeared strongly in discussions of logistics hubs, ports and transport energy hubs. When digital twins are connected or “federated” together, there are multiple interfaces between cyber-physical systems. This introduces cloud dependencies, large numbers of stakeholders and often unclear system

boundaries. In such settings, risk has to be understood in terms of how small faults, poor data or malicious intervention can propagate across systems. That is qualitatively different from protecting one standalone asset or one bounded digital twin.

The implication is that digital twins in transport increasingly need to be treated as components within wider cyber-physical system-of-systems environments. Security approaches that assume clear organisational boundaries, stable ownership models or limited dependencies become harder to apply. Participants were therefore not only raising alarms about greater complexity, but were also pointing to a deeper shift in the operating environment for transport digital twins.

Architecture determines both vulnerability and resilience

> **We can't retrofit security. It can't be an afterthought. It needs to be embedded from the outset.**

System architecture emerged as one of the workshop's most influential themes. Participants observed that "*The more you have in terms of sub-digital twins, the more you are expanding your attack surface*." They also noted that "*Once you start introducing small errors… across multiple digital twins [they] could have major impacts*." Both comments point to the same underlying reality: the architecture of a connected system shapes not only how value is created, but also how exposure grows and how impacts spread.

Participants suggested that the architecture itself, rather than any single threat vector, was the most concerning issue because it determined whether multiple points of entry, trust assumptions and downstream impacts could be contained. They considered issues such as where data sits, how systems are connected, whether information passes through people or APIs, and how digital twins relate to physical assets. Cloud-hosted components can also change the attack landscape.

This gives particular weight to the opening argument from Dr Chris Jones that security must be embedded from the outset.

Governance becomes more complex as the number of actors increases

> **With a large number of stakeholders... you have to be very detailed and keep an eye on the governance aspect.**

While architecture was the main technical theme of the day, governance was the main socio-technical theme. This reflected repeated concerns across the workshop about who is responsible and who is liable for threats or attacks that lead to systems or services being impacted. When systems become connected, ownership and liability need to be agreed from the outset so that multiple organisations can operate coherently and mount a coordinated response when something goes wrong.

"*It's about moving from an ownership perspective to an access principle but that also creates risk*." Participants thought about governance in terms of the operational reality of sharing data, setting boundaries, negotiating trust and determining appropriate access in systems where multiple actors may hold, interpret or act on related data. Questions arose about whether one actor provides the common ground, how common language can be created, and how incident response can function where no single organisation is fully in charge. This suggests that governance in federated digital twin environments is one of the central determinants of whether adoption can happen with confidence.

Trust, data quality and explainability remain major barriers

Trust emerged as one of the strongest themes throughout the workshop. Participants consistently returned to the question of what evidence would be needed before they could rely on insights from a digital twin. Poor data quality and inconsistent data across systems were identified as major barriers, with participants linking trust to data provenance, validation, explainability, traceability and confidence that data accurately represented what was happening in the real world.

Discussions showed that trust is not created by a single technical feature. Participants described the challenge of recognising what 'normal' looks like across connected regional systems, distinguishing local issues from wider network effects, and interpreting anomalies when data is incomplete or conflicting.

These challenges become harder as systems become more federated, increasing the need for clear governance, ownership and analytical capability.

Participants also emphasised the importance of understanding and interrogating outputs from digital twins. Explainability was raised as a key requirement alongside anomaly detection and the ability to determine whether a problem is local or part of a wider regional pattern. This reflected a need to interpret results in context, particularly where evidence is partial or uncertain.

The workshop highlighted that the level of trust required depends on how a digital twin is used. There was greater confidence in applications such as simulation, monitoring and forecasting than in systems that could influence operational or safety-critical decisions. Trust therefore scales with consequence: the greater the impact of a decision, the stronger the evidence, transparency and confidence participants expected from the underlying data and models.

Human oversight remains central

Participants consistently distinguished between digital systems that support decisions and those that make decisions. They saw clear value in digital twins, AI-supported analytics, machine learning and detect-and-alert systems for improving monitoring, forecasting and operational awareness. However, they were much more cautious where these technologies might influence or take responsibility for operational or safety-critical decisions. Human oversight was seen as an essential requirement wherever decisions carry significant consequences.

This distinction remained consistent throughout the discussions. Participants recognised the value of increasingly capable digital systems in providing evidence, identifying risks and informing decisions, but saw a clear boundary between providing advice and exercising decision authority. Several noted that, even in sectors where AI and automation are already used operationally, humans remain responsible for making the final decision.

This suggests that adoption is likely to progress through increasing levels of decision support rather than rapid moves to automation. It also highlights that capability and training become more, not less, important as digital systems become more capable. Effective human oversight depends on operators understanding how recommendations have been generated, recognising when outputs should be challenged, and retaining the confidence and expertise to exercise independent judgement. Without this, there is a risk that advisory systems create complacency rather than better decision-making.

Recovery and resilience are as important as prevention

> **Cyber incidents in transport are not just about data loss. They can disrupt services, impact safety, and undermine public trust.**

One of the strongest messages from the workshop was that cyber security in digital twin ecosystems should be viewed as a resilience challenge, not simply a prevention challenge. "*No matter how well prepared we are, eventually some attacks will happen*." The priority therefore becomes limiting their impact, maintaining essential services, and recovering quickly while retaining confidence in system operation: "*It's about how our systems and societies react… and how we show resilience*."

Discussions repeatedly highlighted that recovery in a digital twin environment is more complex than restoring physical infrastructure alone. Following an incident, organisations may need to re-establish confidence in both the physical system and its digital representation, including determining whether an attack affected one, the other, or both. Participants emphasised the importance of incident response, fallback arrangements and knowing what a 'known good' system state looks like before operations can safely resume.

This suggests that secure digital twinning will require resilience to be designed into systems from the outset. Alongside preventative cyber security measures, organisations will need adaptive capabilities for containment, coordinated response, communication and recovery. As cyber and physical systems become increasingly interconnected, these capabilities become fundamental to maintaining safe and reliable transport operations.

Skills and capability are recurring constraints

> **Innovation and cybersecurity need to be thought about together… especially as we deal with emerging and new technologies.**

Skills and human capability emerged as key constraints across discussions. The challenge identified was not limited to shortages of cyber specialists. Instead, participants described a broader capability gap spanning planners, operators, analysts, engineers, leaders and those responsible for governance and risk. This included the ability to work confidently across IT, operational technology and data-driven environments, as well as to interpret and act on complex system information such as anomalies or performance signals.

The implication is that capability is not just an adoption barrier, but a condition for safe and effective use of digital twin systems. Even where technical solutions exist, organisations may struggle to evaluate, govern or integrate them without parallel development of skills, processes and decision-making maturity.

This reinforces the importance of capability-building alongside technology deployment. It also highlights the value of collaborative forums such as this workshop, which help surface shared assumptions, expose differences in maturity and build a more common understanding of what secure and effective digital twinning requires in practice.

Why it matters – Research and policy implications

Barriers and enablers

The workshop surfaced a cluster of barriers that were technical, organisational and cultural at the same time. These included expanding attack surfaces, weak or inconsistent data quality, low trust in outputs, complex and sometimes unclear governance, skills gaps, lifecycle mismatches between digital and operational systems, and the challenge of maintaining accountability in environments with many stakeholders. Participants also suggested that standards and compliance, while necessary, do not on their own solve the problem if architecture, trust relationships or capability are weak.

The workshop also explored enabling conditions. Participants highlighted secure-by-design architecture, stronger systems engineering practice, clearer trust models, improved validation, stronger governance and common language, greater cross-sector collaboration, human oversight, and the use of digital twins themselves to support testing and scenario exploration. These are the kinds of conditions that could make more secure and trusted use of digital twins possible over time.

Implications for the TransiT programme

For TransiT, one of the clearest implications is that cybersecurity should continue to be treated as an integrative theme rather than as a narrow technical strand. The event showed that cyber concerns in digital twin environments lead directly into architecture, trust, governance, resilience, standards, human oversight and capability. This suggests that TransiT's value lies in continuing to connect technical research with practical questions of operation, coordination and adoption.

A second implication is that TransiT is well placed to help create synthesis across sectors and use cases. Workshop contributions from rail, ports, logistics, planning and energy contexts often pointed towards similar structural concerns, even where technical details differed. This suggests value in drawing together cross-sector patterns around architecture, trust, governance and resilience.

A third implication is that future TransiT work may benefit from going deeper on the themes that recurred most strongly in the workshop: cyber-physical architecture, explainability and baseline setting in federated systems, system-of-systems incident response, governance and accountability, and capability gaps in organisations adopting digital twins.

Economic impacts

The workshop revealed several economically relevant themes. Participants repeatedly associated digital twins with potential operational value in forecasting, predictive maintenance, scheduling, scenario planning, multimodal coordination, charging infrastructure planning and more efficient or responsive use of assets. Stakeholders do see digital twinning as relevant to performance, efficiency and decarbonisation.

Discussions also made clear that governance and assurance requirements will increase the cost and complexity of adoption. In practice it will be important to make the case for cyber security investment as a crucial enabler of long-term value. Digital twins, and in particular confederated systems of such twins, will only generate benefits if all participants can trust in the security of the system. Only if valued input data is fed into it can it provide valuable outputs. Insecure systems will not generate the trust required for such inputs to be shared.

What it signals next – Recommendations and next steps

Signals for policy and industry

For policy makers and industry, the workshop signals that secure digital twinning in transport depends on more than better technical controls. Participants repeatedly pointed to architecture, accountability, common language, data integrity, explainability, institutional maturity and response co-ordination as issues that shape confidence in real deployments. This suggests that policy and industry attention may need to focus not only on what technologies are possible, but on the wider operating conditions that make them governable and trustworthy.

A second signal is that data quality and system interaction risks are seen as especially significant. The event polling and discussion identified inconsistent or incorrect data across systems and unintended outcomes from combined system behaviour as leading concerns. That suggests that policy and industry responses need to address the quality, interoperability and consequences of shared system behaviour, not just classic external attack scenarios in isolation.

A third signal is that readiness will vary. Participants described very different levels of cyber maturity, confidence and resourcing across organisations, especially where smaller organisations or more fragmented environments are involved. This suggests that adoption pathways are unlikely to be uniform. Continued engagement, guidance and capability development may be just as important as technical advancement if digital twins are to scale responsibly across transport systems.

Next steps for TransiT

The workshop concluded with a strong emphasis on distillation and continuation rather than closure. Professor Pezaros drew together the main themes of the day: architecture, interconnection, vulnerability and resilience, highlighting the scale and direction of the challenge. He also invited participants to consider contributing to further research so that the priorities emerging from the workshop could inform future work.

In practical terms, the workshop points towards follow-on activity on system architecture and trust models, explainability and baseline setting in federated systems, system-of-systems incident response, governance and accountability, and capability development across industry and institutions. These themes all emerged directly from the event and would provide a strong basis for future work and external engagement.

TransiT's cybersecurity team highly valued this direct engagement with industry, facilitated by Connected Places Catapult, and have three key priorities following the event:

- **Detailed analysis** – of all the points raised at the event, to ensure their work aligns with industry priorities.
- **Industry engagement** – to continue engaging with industry partners and stakeholders to gather technical and operational insight for TransiT's cybersecurity research.
- **Research** – to accelerate their research focus on the system architecture of TransiT's transport digital twins, and how cybersecurity embeds into this.

TransiT partners

TransiT is a collaboration of eight universities and almost 70 industry partners, jointly led by Heriot-Watt University in Edinburgh and the University of Glasgow. It is supported by the UKRI Engineering and Physical Sciences Research Council (EPSRC), the main funding body for engineering and physical sciences research in the UK, and by the UK government's Department for Transport.

TransiT's other university partners are University of Leeds, University of Birmingham, Cranfield University, University College London, University of Cambridge and Durham University.

Visit https://transit.ac.uk/

Acknowledgements

This workshop was hosted by Connected Places Catapult on 9 June 2026 as part of the TransiT programme. Opening framing was provided by Dr Chris Jones, keynote input came from the National Cyber Security Centre, and workshop sessions were hosted and guided by Professor Dimitrios Pezaros and Dr Stefanos Evripidou from TransiT. The event also benefited from contributions from participants across transport, energy, research, policy and industry.

About TransiT

TransiT is a UKRI-funded research programme and national research hub focused on accelerating transport decarbonisation through advances in digital twinning. It brings together academic research, industry stakeholders and policy actors across transport modes to improve alignment, adoption and impact, with strong emphasis on making research outputs accessible, relevant and usable by those planning, operating and governing transport systems.

TransiT's vision is to harness the transformative power of digital twinning, and associated digital technologies, to decarbonise transport. Cybersecurity is a key component to ensure that these increasingly connected and data-rich systems can support decarbonisation without creating unacceptable vulnerabilities or undermining trust in the systems that depend on them.

Get involved

Transforming infrastructure challenges into opportunities for innovative businesses

Connect with us:

info@cp.catapult.org.uk

cp.catapult.org.uk

@cpcatapult

Connect with TransiT:

info@transit.ac.uk

transit.ac.uk

@transit-hub

We use our networks, technical expertise, and government and industry partnerships to strengthen routes to market and unlock trade and investment opportunities in transport, construction and data infrastructure allowing businesses to start, scale and stay in the UK.