WHITEPAPER
PUBLISHED FEB 2024

Building trust in the network digital twin

verizon

InnovationAus.com

Building trust in the network digital twin

Introduction

As networks become increasingly unwieldy, businesses are currently facing numerous challenges when weaving together the data, knowledge, processes and cultures required to get the most from digital twin implementations.

Digital twin technology (essentially, the digital representation of a real product, system or process for simulation, monitoring and integration) is crucial for automating design, testing and provisioning updates.

When replicating any process, front of mind must be the management of quality assurance and security – particularly in mission-critical environments.

But to build trust in the network digital twin, we should first define the parameters. For example, how is a digital twin different to system-information modelling (SIM), which we have been using for decades?

As STaR (science, technology and research) Shot Deputy Leader, Agile Command and Control, Defence Science Technology Group, Duncan Fletcher, explains, “digital twin technology is just SIM combined with live data. There’s a subtlety in putting those two things together that’s opened up the opportunity to make decisions cheaper, faster and more accurately.”

It’s all about finding the ‘ripples’ — to look for those opportunities where the mechanics, whether physics-based or sociotechnical, are modellable.

Can the networks that carry those ‘ripples’ be modelled? Then, the process involves assessing the data that would parameterise that model, which would allow us to tell if the network is available.

The next step is to take the idea of a modellable network that has the parameters available to see if it is projectable in time — and try different courses of action to optimise the decision-making process.

Complexity and fragility intertwine in a network sense

The complexity and fragility of the modern network provided a starting point for an InnovationAus.com roundtable discussion, sponsored by Verizon, about how we can harness the power of digital twin technology while managing risk and complexity.

The sheer size of a modern network is what creates its complexity and fragility. With tens of thousands of devices and components from different vendors, how can we verify a single source of truth that the network is configured correctly and behaving as intended?

The data generated by emerging technologies creates huge advances in capability – and 'data fusion' delivered at the speed at which it is relevant to the success of an operation creates a powerful competitive edge.

But considering the pressure to 'get it right the first time', how can digital twin technology provide the desired functionality and keep the 'data lake' current with the state of the network?

To build trust in the network we must harness the power of digital twin technology while managing risk and complexity.

Leading the way in digital twin technology is the defence sector, which has determined it is an exceptional opportunity to contain many of the models, rules and data that let us use high forms of computing to develop a course of action to arm the decision-maker with better information.

What can the private sector and other government departments/agencies learn from the defence sector – specifically in terms of how to plan and begin to build a digital twin?

A roundtable was hosted by InnovationAus.com with the support of Verizon to explore this topic, comprising the following attendees. This whitepaper is a result of this discussion.

Roundtable attendees

Duncan Fletcher, STaR Shot Deputy Leader, Defence Science Technology Group

Daniel Kalnins, Director of New Build, Willow

Bonnie Shaw, Co-Founder and Chief Impact Officer, Place Intelligence

Damien Manuel, GM of Open Data Regulation, PEXA

Robert Stopajnik, Development Director & Advisor, Digital Twin Victoria

Sharon Wilkes, Senior Manager, Enterprise Risk, Transport Accident Commission

Lachlan Bakewell, Chief Information Officer, Eastern Health

Ian Thorp, Chief Architect, Medhealth

Sylvia Souliotis, Client Partner – Enterprise and Government, Verizon

Will Fooks, Urban Places Market Leader, Stantec

Arvind Vasudevan, Head of Strategy, H&R Block

John Kokkinos, Head of Digital, Maurice Blackburn Lawyers

MODERATOR: **Corrie McLeod**, Publisher, InnovationAus.com

Blurring the line between human and machine

In conflict and competition, predictable elements tend to lose – the challenge for digital twin technology is to separate the tasks a machine can be trained to do and the tasks at which a machine is generally not adept.

Organisations that are leading the charge in terms of digital twin technology are investing in the analysis of people's actions, processes, what their data is doing and where it is going to inevitably find the right answers.

For example, an Australian air traffic control company built a digital twin of its workforce processes to determine staffing levels on incoming and outgoing aircraft. They could model to a point that they could figure out, in real time, how to adjust the system to control stress levels and finances. This approach would have real benefits for an industry like healthcare in terms of machine-learning systems assessing the people and resources necessary to handle rapidly changing situations.

The security challenges of interconnectivity and sharing data in a private and public healthcare setting to streamline efficiencies are primary.

"Humans are significantly better at applying intuition to do clever, unexpected things. [Digital twin technology] frees up people to do deeper, more creative analysis."

– Duncan Fletcher, Defence Science Technology Group

Putting people first in complex business environments

Smart analytics are becoming more important, but they are only as smart as their creators and enablers.

Building trust in the mechanism is dependent on the skills and reliability of its builders. That's why people will always remain at the forefront of deciphering, assessing and implementing technological change.

For example, global technology company Willow collects data into one place to reduce energy and operating costs for one of the world's largest airports in North America, but also collects data on large capital projects for real-time decision making to prevent costly delays and improve construction productivity.

These digital-twin stepping stones create a solid foundation for engendering trust among its adopters and users.

“The biggest challenge we face today has nothing to with technology; rather it’s getting the human users of digital twin technology, who certainly understand the problem, to trust a wholly technological solution.”

– Daniel Kalnins, Willow

Cultural change depends on evaluating the starting point. The person who has to change their behaviour locally will drive the buy-in, trust and ultimately the benefit of the digital twin.

“These new toolsets and skillsets of emerging technologies and data are critical to create digital twins, but these models can only be as effective as the people using them. For twins to drive meaningful change and impact, they must be created within a culture that values their output and is prepared to act on them.”

– Bonnie Shaw, Place Intelligence

Balancing the risk-to-benefit ratio of digital twin technology

The big questions are: How much is the appetite for risk management driving the adoption of digital twin technology? Which companies are using digital twin technology to understand opportunities and drive innovation, versus identifying where risks are, to ensure protection?

The benefit is the ability to model the impacts of different scenarios and systems such as floods, fires and other natural catastrophes. The counterpart is how we protect that information – and, crucially, ensure it’s not a repository that can be leveraged and manipulated.

For example, engineers see the value in the built environment for planning, but they can’t see the value in planning via a digital twin.

Defence, on the other hand, will build a digital terminal of an entire city – plumbing, information and communications technology, communications and restaurants.

That's because defence assesses the risk of adoption to far outweigh the risk of doing nothing.

The Australian Army, for example, is in the process of building a digital twin of its capability acquisition program.

"We're already challenged with misinformation across social media and other day-to-day communication channels – how do we manage it within very complex environments with multiple data points in a way that is not counterproductive?"

– Damien Manuel, PEXA

Security in the geospatial realm

The question remains: How can we apply what's been learned in geospatial digital twins to a 'network' context?

As an open source: we should look to security versus the commercialisation and value of data to achieve cohesion.

There has been little change in this area over the past few decades – it's only the terminology that's changed.

However, in the early 1990s, for example, there wasn't such a need to focus on security.

Data scientists were talking about the same sort of thinking or methodology, but the difference these days, in terms of network and security, is what digital twin technology is going to give us between people, processes and mirroring.

We have the know-how to perform these functions, but how are we going to secure them?

The Australian federal government is opening up its data sets. But also in place are several conditions and hurdles to determine what's in it for the organisation, the community and the government, to fully understand unforeseen issues, as well as the intent and ethics around how the data is going to be used.

From a security point of view, whether or not we're using digital twin technology, we're no longer playing against students with computer science degrees – we're playing against state 'actors', equipped with information, resources and access.

Asymmetric warfare is strategic. It's about using what some may perceive as a smaller, less significant strength to counter their bigger strength via a weak point. It's the smaller, cheaper force being able to equalise without brute force.

In a corporate context, an asymmetric attack might look like a multinational company that spends millions on cybersecurity and resources, then is infiltrated by one employee opening a malicious link in an email.

Particularly with the expanding net of critical infrastructure, there's a concern around the use of the data; separately, such as the security of interconnected devices.

"Thirty years ago, there wasn't such a need to focus on security of data. Today, I get a call a day from a customer about securing their APIs."

– Sylvia Souliotis, Verizon

Using twins in health

The health sector has advanced rapidly since the onset of COVID. We now have the option of telehealth consultations with professionals in disparate locations, digital prescriptions sent to our phones, digital vaccination certificates, and other often essential medical resources.

Security challenges are particularly felt in the health sector as it tries to optimise a federated system while balancing customer expectations and service with security concerns around data. But rather than going ahead in leaps and bounds, as it should, the sector is lagging in digital twin development.

And often the action of 'filling the data lake' is just capturing data for the sake of capturing data – there's a limited understanding of the problem that requires solving, and if the data in the 'lake' will even solve it.

Health systems and data networks cross a number of significant organisational boundaries – state and federal government, GPs, pharmacies, nursing homes and hospitals – so to model the system and adopt a model of that flow so you can reason over disruptions to that flow – you need to build connectivity with data that is crossing boundaries that it has never historically crossed.

And with every different organisation having a strong sense of ownership and responsibility for their patient data, there will naturally be a reluctance to share it externally due to the significant risk of a cyber breach.

A potent example is Medhealth (a collective of health, medical and employment brands), which provides healthcare to large corporate companies and federal agencies, which is exploring patient trends over time.

Medhealth collects a range of health metrics for one of its clients, with the aggregated data being used to create a health profile of the population and trigger interventions that may be required.

"Marrying up data reporting and analytics with security and privacy issues is a significant process in the health sector."

– Sharon Wilkes, Transport Accident Commission

Debunking digital fusion with data at the speed of relevancy

Digital fusion is not just a buzzword, but has real-time implications for how to strategically plan and adapt to the challenges of building a digital twin.

The speed of relevance refers to what data is relevant to the problem that needs to be solved right now, and how many so-called 'injects' are coming through to the decision-maker. If there are too many 'injects' coming through to the decision-maker, the data will eventually become irrelevant (which is represented as information overload).

One of the most significant values of digital twin technology is overcoming data fusion challenges. However, what's valuable is subjective, so the first step is identifying what value looks like for a range of stakeholders.

Citing a Verizon case study example is the building of warships during the supply-chain challenges of COVID. If you roll critical vulnerability forward, how do we get the technology transfer from a location overseas into a location in Adelaide?

The solution: CAD designers who worked on Central Station in Sydney implemented the digital twin in the development of the warships in a blame-free environment, to avoid a five-to-15-year blowout.

Cross-sector learning and a fail-fast, blame-free culture

We should look to the dichotomy between different countries and government cultures for clarity, such as Australia versus the US.

In the US, innovation is the selling point and the case studies follow. But the Australian federal government wants a series of case studies of how innovation has been proven – particularly when it comes to predictive tools – before investing in the technology.

We must do away with the 'failsafe' mindset to enable cross-sector learning around networked digital twins.

Digital twin technology is positioned as an intelligent solution that can predict all the possible outcomes – but often it's just a single-step change that makes one process easier and faster.

While failure may be seen as unacceptable at a governmental level, as Bonnie Shaw quite matter-of-factly puts it: "You can't build muscle by watching someone else lift weights."

"Innovation is not an outcome. Doing things cheaper and faster is an outcome."

– Robert Stopajnik, Digital Twin Victoria

Conclusion

Adopting the lessons learnt at a critical level is the basis for building trust in the digital twin.

The strategic advances gained in the defence sector by adopting digital twin networking have wide-ranging implications and commercial benefits for all industries.

Businesses must find ways to weave together the data, knowledge, processes and cultures required to get the most from digital twin implementations.

At a ‘people first’, geospatial and economic level, leading organisations are developing digital twins of their networks. This practice is not optional, but crucial, as business systems become more complex and technological sophistication is exacerbating risk and security issues.

The major challenge for building trust in the digital twin is connectivity and the pooling of appropriate resources. We don’t yet have collaborative research in the area of digital twin technology because we operate in silos.

This needs to change, and fast, in order to create, enable and build trust in the network digital twin.