

Connectivity 4.0 series – part 2

Building resilient mission-critical services

Your road map to implementing tomorrow's networks and connected technologies to support, modernise and secure mission-critical infrastructure and services.

vocus.com.au/brilliant-connectivity

VOCUS



Contents

Why more enterprise operations are mission-critical	4
What is Connectivity 4.0?	5
Build resilience into your digital transformation	6
Deliver Connectivity 4.0 anywhere — even at the bottom of the ocean	7
Close the digital divide with LEO satellites	8
Why mission-critical services rely on ubiquitous connectivity	10
Provide connectivity where you need it with private LTE	12
Mitigate the critical infrastructure risk	14
Five key cybersecurity recommendations	15
Next steps for building mission-critical services	16
Re-architect your infrastructure for the future	18

Why more enterprise operations are mission-critical

In a time of rapid change, the importance of ensuring the resilience of mission-critical services cannot be overstated. Organisations can face an array of challenges at any time — ranging from cybersecurity attacks to extreme weather events and the effects of geopolitical instability.

What's more, the COVID-19 pandemic and other recent disruptions have shown just how dependent society is now on a broad range of goods and services, effectively redefining what mission-critical means today.

Recent amendments by the Australian Government to the Security of Critical Infrastructure Act 2018 (SOCIA) reflect this change. These amendments include additions to the longstanding definition of 'critical infrastructure', which has traditionally been limited to conventional infrastructure like electricity, water and gas. The term now includes 11 core sectors, including:

- financial services and markets
- communications
- data storage and processing
- defence
- food and groceries
- higher education and research
- healthcare and medical
- transport
- energy
- space technology
- water and sewerage.

Shifts in government and society attitudes have raised the stakes for many organisations, lifting customer expectations to unprecedented levels and bringing new meaning to the term 'mission-critical services'.

It's therefore more important for more organisations to take meaningful measures — and even adopt new operating models — to ensure their services operate continuously and reliably, no matter what external events or forces threaten to compromise them.

Enter Connectivity 4.0, a new era in which network technologies and business needs have evolved and come together to make fast, resilient and ubiquitous connectivity a reality.

In this paper we reveal why embracing Connectivity 4.0 is an imperative for businesses today. We explain how it can help organisations build the future-proof networks and connected technologies needed to support and secure mission-critical infrastructure and services.

What is Connectivity 4.0?

Just as the transition to Industry 4.0 is revolutionising business by integrating digital services and processes into every aspect of operations, Connectivity 4.0 can revolutionise the way those services connect with each other and the world around them.

Connectivity technologies have evolved through several eras, from the original public switched telephone network to early computer networks, the internet and beyond. And as businesses have become more connected, they have adopted an increasing range of technologies. However, choosing those technologies has traditionally involved balancing performance with flexibility and availability.

Connectivity 4.0 is a new era in which these technologies have evolved to the extent that organisations no longer need to compromise. Together, these technologies can provide ubiquitous connectivity across terrestrial and subsea fibre, regional 4G and 5G mobile services, satellite coverage, and private long-term evolution (LTE) campus networks.

What's more, you can choose a mix of technologies that provides both fibre-like performance and unprecedented resilience, along with the network flexibility and availability your business needs.

Connectivity 4.0 is paving the way for high-speed, low-latency applications like autonomous vehicles and widespread sensor networks. But it's also driven by the need for ubiquitous connectivity for core business needs right now — including building mission-critical services, enhancing the employee experience, and achieving environmental, social and governance (ESG) objectives. It does this by unlocking a new level of pervasive connectivity, enabling organisations to reimagine what's possible like never before.

For more details about this new era in connectivity, see [Connectivity 4.0: the new business imperative](#). In this paper, we explain Connectivity 4.0 in-depth — the technologies driving it, how it works and why you need to embrace it, so your organisation can reimagine what's possible like never before.

Build resilience into your critical networks

Given the extensive digitalisation of today's enterprises, technology leaders play a huge role in ensuring mission-critical services operate continuously and reliably. This means embracing geographically diverse infrastructure to avoid 'single point of failure' weaknesses, adopting infrastructure-level security systems to strengthen organisations' resistance to cyber attacks, and building redundant connectivity solutions for increasingly complex, distributed corporate networks.

The challenge for technology leaders is to build resilience into the digital innovations and transformations that enterprises began or accelerated during the pandemic. Forward-looking enterprises, for example, are fast-tracking the transition to Industry 4.0 by adopting connectivity and digital technologies that greatly improve their agility and drive efficiencies through automation.

And then there are technological issues to resolve, such as how to best optimise architectures for hybrid cloud environments, deliver value from more advanced technologies such as artificial intelligence (AI) and the Internet of Things (IoT), and connect new and expanding digital ecosystems.

Connecting data from widely distributed applications and platforms is vital to unlocking the full potential of these technologies, delivering the insights and productivity enhancements that organisations need.

Next-generation Connectivity 4.0 solutions are critical in providing the performance and resilience needed to support today's complex data integration requirements.

Increasingly, connectivity solutions are enabling not only information technology (IT) solutions but also integrating operational technology (OT), such as supervisory control and data acquisition (SCADA) and other industrial control system (ICS) platforms that manage manufacturing, mining and other industrial processes.

IT networks have typically evolved separately from OT environments, but in today's service-focused environment the two are converging more than ever before. They also typically integrate IoT equipment, such as temperature and water-level sensors, valve controllers, monitoring cameras equipped with AI-driven object detection, and more.

Connectivity 4.0 solutions are needed to support this convergence, delivering scalable and resilient converged networks capable of carrying all manner of traffic according to the performance requirements of new applications.

Deliver Connectivity 4.0 anywhere — even at the bottom of the ocean

The mining and natural resources sector provides myriad opportunities for connectivity innovation, with Vocus helping to develop innovative solutions to ensure connectivity across mission-critical settings such as offshore gas drilling rigs. Here, the forces of nature and physical challenges of industrial environments require innovative connectivity solutions.

For example, how do you extend robust connectivity to a massive, floating platform many kilometres offshore and regularly lashed by violent storms and waves?

Vocus achieved this by working with a submarine cable specialist to create a multimillion-dollar terminal box that was secured to the ocean floor hundreds of metres below the gas rig's planned location. The connection was pre-cabled, with a fibre-optic cable run from the mainland to the terminal box, long before the rig's installation.

Then, once the massive rig had been moved into place, unmanned aquatic vehicles ran another cable down from the rig to the terminal box.

The vehicles plugged in a high-speed, reliable connectivity service that supports the rig's business systems, SCADA and other industrial controls, as well as delivering services to the residential quarters.

Developing such solutions is about much more than simply connecting a fibre service. A rig's massive steel platforms are a challenging environment for deploying conventional wireless connectivity. Extensive site surveys are needed to identify potential coverage blockers.

"We've done a lot of work to create solutions for customers that are using IT-type features of the networks but in fact solve operational problems as well," says Phil Martell, Head of Strategic Network Development with Vocus. "There's a lot of service and operational thinking required to make that all work — and we have tried to create an infrastructure capability rather than just delivering a single service."

Having that infrastructure capability means the connectivity provider can operate and configure a gas rig's network completely remotely. That includes turning ports on and off as new services are required, monitoring traffic for security anomalies, adjusting bandwidth flow and management, and disabling ports based on access-control restrictions.

Close the digital divide with LEO satellites

While innovative fibre solutions provide connectivity to remote locations, rapid innovations in wireless technologies, such as satellite, are adding alternatives to increase network reach and resilience.

Although geostationary satellite data services have been available for many years, their utility in mission-critical networks has been limited by their relatively slow speeds, high cost, and the high latency created by their position more than 36,000 kilometres above the Earth.

However, the launch of high-speed low Earth orbit (LEO) services has changed all that. LEO services fly smaller satellites at an altitude of around 500km to 2,000km – close enough to Earth that they can deliver fast, high-powered data communications services with very low latency.

LEO constellations require complex integration of hardware and software systems. Unlike geostationary satellites, which appear stationary when viewed from Earth, LEO satellites must orbit the Earth extremely quickly to maintain their altitude, requiring specialist tracking antennas to maintain connection.

Operators like SpaceX are addressing this with its Starlink service, building global mesh networks comprised of thousands of satellites, launched dozens at a time by low-cost, reusable SpaceX launch services.

Starlink's performance is advertised as being between 100 and 500 megabits per second, with latency as low as 20 milliseconds when accessed from almost any place on the planet. This enables organisations to build high-speed networks anywhere they might be operating, whether on land or at sea.

“LEO has created something that didn't exist in the satellite industry before – low-cost services and high performance,” says Ashley Neale, Development Manager, Space and Satellite, with Vocus. As part of his work, Neale helps space and satellite operators use Connectivity 4.0 solutions to tap into the capabilities of their networks.

“When you've got a truly ubiquitous, low-cost and high-performance network, you can connect proper metro-grade broadband anywhere in the world,” he says. Neale points out that the ability to bridge the longstanding digital divide is allowing businesses to extend connectivity anywhere in Australia or around the world, without having to rethink their network architecture.

LEO services also provide new options for improving the resilience of Connectivity 4.0 services, as they are safe from unpredictable weather and other continuity threats.

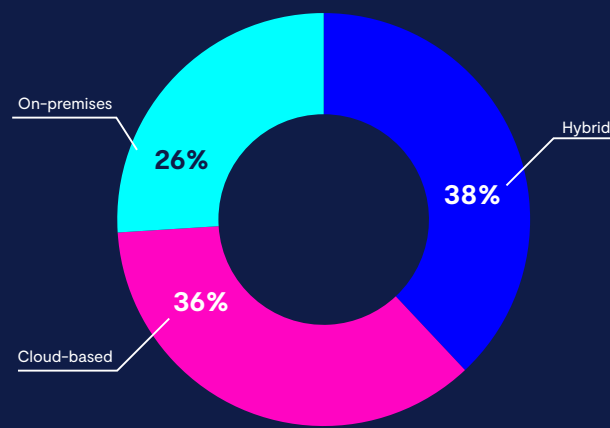
On a gas rig, for example, the LEO data service could be used as a backup to undersea fibre cabling. This maintains critical connectivity even in the event the fibre is accidentally broken by wave action, physical wear and tear, or an explosion or other accident.



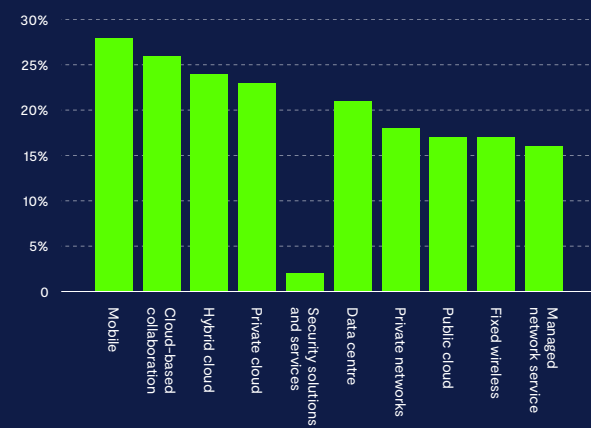
Why mission-critical services rely on ubiquitous connectivity

Cloud migrations have long been fundamental to digital transformations, but they are even more vital for mission-critical services. New Vocus research has found that three in four companies are either solely dependent on cloud services or are using hybrid cloud environments for their mission-critical operations. What's more, cloud-based applications and workloads are often widely distributed and interconnected, making robust, ubiquitous connectivity essential.

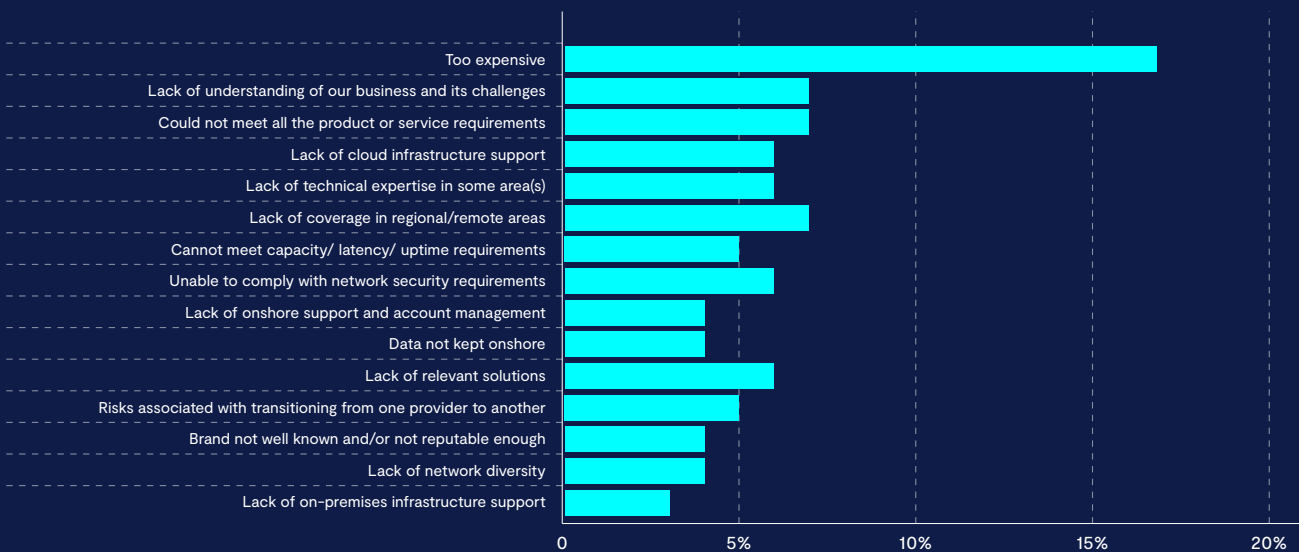
Infrastructure for mission-critical operations



What solutions will organisations invest in?



Top considerations when selecting telcos



Source: Vocus research, 2022



Provide connectivity where you need it with private LTE

Another transformative wireless technology is private LTE, which is conceptually a successor to Wi-Fi networks but uses longer range mobile communications protocols to deliver high-speed coverage to specific areas — for example, at a mine, solar farm, or large industrial complex.

Private LTE networks are built using similar components to commercial mobile networks, with base stations mounted on towers scattered across the coverage area. Two large base stations can provide blanket coverage across a 12km radius, with mini base stations added in areas of high usage, such as where there are a lot of workers or an array of connected equipment.

“Private LTE gives you the ability to take standard telco infrastructure and customise it to make those solutions work in the most remote areas,” says Martell, who notes the ability of such networks to connect operational technology in ways that have never been possible before.

Private LTE is transformative for businesses that have previously been forced to rely on whatever commercial 4G or 5G mobile signals manage to reach their site location. With the right site survey and engineering work, it’s possible to build private LTE networks that provide high-speed connectivity to every part of a commercial environment or industrial operation — even deep underground.

The implications of this degree of connectivity are significant, with the potential to link every piece of equipment within the coverage area, including workers’ smartphones.



An environmental field worker uses wireless technology to collect data on fire damage in Rockingham Lakes Regional Park.

In addition, the technology’s extremely low latency offers new capabilities to connect devices such as autonomous vehicles, which must be able to react instantly to commands or changes in their environment.

Containerised private LTE networks are also being used to rapidly provide connectivity in areas that suffer interruptions to normal coverage — for example, when bushfires destroy commercial mobile base station towers, or floods inundate a region.

The potential to rapidly restore communications in such areas makes private LTE as important to emergency services operators as it is to businesses seeking to extend connectivity to industrial sites.

In such industrial environments, private LTE has already filled another crucial part of the Connectivity 4.0 platform — providing flexible, robust terrestrial communications backed by service characteristics and control that legacy wireless infrastructure cannot supply.

By connecting a private LTE network to LEO satellite backhaul, it’s possible to combine the respective and complementary strengths of both technologies to build robust connected campuses anywhere on Earth.

“We think private LTE will be really critical in terms of the way companies manage their infrastructure assets and operational requirements in order to deliver productivity dividends,” says Simon Parker, Head of Strategic Projects with Vocus.

“The technology suits any organisation that has a range of requirements around workplace activities, like autonomous vehicles and active predictive maintenance. It creates opportunities for precision monitoring and control, even at facilities that don’t have people in them but are operated remotely.”

Mitigate the critical infrastructure risk

Connectivity 4.0's flexibility and ability to integrate new technologies to meet operational business requirements is becoming increasingly important. Already, it's helping businesses adapt to the infrastructure, security and other risks created by ever-changing global circumstances.

Increasingly, it will also play an essential role in helping organisations address the Australian Government's expectation that they protect the integrity of critical infrastructure. This has been the subject of extensive consultation and reform in recent years, as new threats accumulate.

A raft of recent SOCI amendments have imposed significant obligations on operators of critical infrastructure. These include new requirements around ensuring the security and resilience of the systems they administer.

To meet their security obligations under SOCI, operators must undertake a range of improvements to security risk management – including more quickly responding to and reporting cybersecurity incidents.

They must also participate in a central Register of Critical Infrastructure Assets managed by the Cyber and Infrastructure Security Centre.

Increased reliance on connected and online systems really makes businesses more vulnerable to attack," says Anita Sheridan-Roddick, APAC Group Sales Manager with managed security service provider Seccom Global. She notes that "companies have had to be more strategic, diligent and vigilant when it comes to maintaining security".

Ever more resourceful cyber criminals have taken advantage of the disruption of the past few years, escalating attacks such as ransomware

and distributed denial of service (DDoS) to become major threats to business continuity and real-world tests of corporate resilience.

Reports of ransomware attacks alone increased by 15% during the 2020–21 financial year, the Australian Cyber Security Centre (ACSC) observed in its latest [Cyber Threat Report](#). The report also warned about increasing risks from targeting of supply chains, rapid exploitation of security vulnerabilities, exploitation of the pandemic environment, and business email compromise attacks, which cost businesses over \$50,600 per incident, on average.

Recognising the intensifying attack climate during the pandemic and as a result of growing geopolitical uncertainty in Ukraine, Taiwan and elsewhere, the ACSC has joined similar organisations around the world in entreating businesses to [improve their security practices](#).

A sound connectivity strategy is an important element of these efforts, Sheridan-Roddick says. These include infrastructure-level innovations such as SD-WAN services, network segmentation to create private data networks, secure access service edge (SASE) architectures to protect edge-computing devices, zero-trust authentication services, and automated detection and incident response to strengthen organisations' resistance to security attacks.

"We're having a lot of conversations with customers around asset and vulnerability management," she says. "And while the risks are the same as before, they're just amplified."

There is no doubt that the risk of state-based attacks has increased, but also the risks from your general, run-of-the-mill cyber criminals."






"They are running companies now," she continues. "Rather than being just one person sitting in the dark launching attacks. It's organised crime – and the risks to our national security and national infrastructure are very real."

With around one in four of the cyber incidents reported to the ACSC now related to critical infrastructure or essential services, businesses operating in many of these sectors are on notice about the risks posed in the new environment.

Because many rely on extensive OT environments as well as conventional IT, they will need to invest heavily in

Five key cybersecurity recommendations

The ACSC recommends that organisations adopt an "enhanced cyber security posture" that includes the following five measures:

-  Patching applications and devices
-  Implementing mitigations against phishing and spear-phishing attacks
-  Ensuring staff report all suspicious emails received, links clicked and documents opened
-  Ensuring that logging and detection systems are fully updated and functioning
-  Reviewing incident response and business continuity plans, including clear and well-understood response plans for ransomware attacks.

 Reports of ransomware attacks alone increased by

15%

during the 2020–21 financial year which cost businesses over **\$50,600** per incident, on average

Source: ACSC, Cyber Threat Report 2021

supporting infrastructure capable of extending SOCI-compliant controls from one side of their business to the other – and even out to close supply-chain partners.

"We're going to have more volatility in terms of GDP and asset prices, and at the same time, cyber and disruption risks continue to increase," says Daniel McCormack, Head of Thought Leadership (Research) with Macquarie Asset Management, part of Macquarie Group.

"For businesses, being flexible is absolutely key. You need to be able to respond to those pressures and opportunities very quickly – and Connectivity 4.0 embodies that flexibility to support businesses going forward."

Next steps for building mission critical services

1 Build for redundancy

Ensure you have the right combination of terrestrial and satellite options to ensure continuous connectivity to all of your sites, then look for opportunities to support new, low-latency applications by adding local wireless and private LTE services.

2 Design to manage risk

In today's volatile geopolitical and economic climate, business success requires careful attention to cyber security, operational continuity, supply chain, and other kinds of risk — so make sure you have considered how your partners can work together to use Connectivity 4.0 to minimise this exposure.

3 Reimagine your future

Embracing Connectivity 4.0 will open up new opportunities to tap the benefits of automation, AI and other technologies. Keep your mind on the future and never stop thinking about how new capabilities will enhance your business for the future.



Re-architect your infrastructure for the future

Change and disruption were part of doing business before the pandemic, but they have reached new levels since then. And with no end to economic, market and supply chain volatility in sight, organisations must be more agile than ever.

At the same time, society's definition of what constitutes 'mission-critical services' has broadened, further raising customer expectations. The pressure is on organisations to support these services with highly resilient operations and infrastructure. Connectivity 4.0 is the glue that can bind this infrastructure together with fast, resilient and ubiquitous connected solutions.

Many of today's organisations have grown organically over many years, and their infrastructure has too – often creating challenges in sustaining mission-critical business requirements. Much more than simply replacing old technology with new technology, Connectivity 4.0 solves this issue by providing the opportunity to re-architect and modernise infrastructure for a hybrid-cloud future. Ubiquitous access to high-speed, low-latency and highly reliable connectivity lets you reimagine your business from the ground up – not in terms of what it used to be, but of what it could be.

That's just the start. By embracing Connectivity 4.0, your organisation will be well placed to tackle other fundamental business challenges, such as transforming the employee experience and achieving sustainable growth. And by unlocking a new level of pervasive connectivity, your organisation can reimagine what's possible like never before.



We thank the industry experts and Vocus experts for their contribution to our report.



Daniel McCormack

Head of Thought Leadership (Research),
Macquarie Asset Management,
Macquarie Group



Anita Sheridan-Roddick

APAC Group Sales Manager,
Seccom Global



Phil Martell

Head of Strategic Network
Development, Enterprise &
Government, Vocus



Simon Parker

Head of Strategic Projects,
Enterprise & Government, Vocus



Ashley Neale

Development Manager, Satellite and
Infrastructure, Vocus

Vocus, Australia's specialist fibre and network solutions provider, owns and operates 25,000kms of secure, high-capacity fibre connecting all Australian mainland capitals with Asia and the USA. Vocus' network includes the 4,600km Australia Singapore Cable (ASC) from Perth to Singapore via Indonesia and the 2,100km North-West Cable System (NWCS) from Port Hedland to Darwin, connecting offshore oil and gas facilities. Vocus owns a portfolio of well-recognised brands catering to enterprise, government, wholesale, small business and residential customers across Australia.

vocus.com.au/brilliant-connectivity

VOCUS