

Continuity by design

Mission-critical network and communications

Alcatel·Lucent

SOLUTION BRIEF



Downtime is not an option. When everything is connected and a link fails, real resilience is the continuity that follows.

Mission-critical describes any environment where downtime, a breach or a loss of coordination has consequences beyond cost. These consequences can affect the safety of people, the continuity of essential services or compliance. Real resilience means being able to disconnect and keep operating, because mission-critical operations do not get second chances.

Why continuity matters now

More connected, more exposed

Information technology (IT), operational technology (OT), communications, devices and cloud services depend more and more on one another. A broken link can quickly become an operational disruption.

Modernization cannot mean interruption

Legacy systems must change step by step, without forced replacement, downtime or the loss of specialist systems performing critical jobs.

Cyber risk meets operational risk

Organizations must protect critical infrastructure and keep essential services available, even when public or cloud connections are down.

Skills and resources are stretched

As OT-IT teams do more with less, they need simpler management, greater visibility and AI-assisted guidance to ensure operational continuity. They must also remain in control of every decision.

Three outcomes must hold for continuity, regardless of what fails around them

Coordination	Operations	Control
Connect teams, responders, operators and decision-makers through secure communication and collaboration.	Maintain resilient network and communications infrastructure that help keep essential operations running.	Maintain visibility, security and governance across critical infrastructure, data and communications.



Coordinate under pressure

When something goes wrong, seconds matter. Continuity of coordination depends on two things: Communication and collaboration tools that connect people, and the secure network that keeps those tools available. Teams must be able to communicate and coordinate across OT and IT environments for a fast, effective response.

Coordinate the right response, at the right moment

- Deliver alerts and contextual information across sites, teams and devices
- Coordinate emergency responses quickly and efficiently
- Connect office workers, operational teams, lone workers and field staff in seconds
- Bring your own teams and outside partners together in minutes through shared tools
- Integrate existing safety and security systems such as video surveillance cameras, access control, radio networks, emergency help points (EHPs) and public announcements (PA)

Solutions that support coordination

Targeted or large-scale awareness

Visual Notification Assistant sends the right emergency information to the right people, on the device each person carries.

Immediate response coordination

Dispatch Console helps operators prioritize and route emergency calls and set up conferences.

Protection for mobile staff

Available on DECT or Wi-Fi handsets, Lone Worker Protection sends an alert with the worker's location when a worker falls, stops moving or pulls a cord. If nobody responds, it escalates the alert automatically.

Open integration

Application programming interfaces (APIs), connectors, gateways and developer tools help you connect the specialist systems and terminals you already use.

A resilient foundation

The network and Wi-Fi are designed without a single point of failure, with security built in. Alcatel-Lucent OmniAccess® Stellar Wi-Fi does not rely on a central controller, so communications and notifications continue even if part of the infrastructure goes down. Private 5G complements Wi-Fi to deliver secure, reliable connectivity, seamless mobility and strong coverage, even in large or complex environments.

Collaboration from anywhere

Rainbow™ by Alcatel-Lucent supports secure collaboration between teams and locations. Outside partners can join as guests. Collaboration bubbles (or spaces) combine chat, voice, video and file sharing in one experience.



Keep operations running

Continuity of operations relies on resilient networks and communications, integrated management and AI-assisted monitoring. These tools detect problems early and simplify maintenance. Organizations can keep critical services running during equipment failures, disruptions or when a site is cut off.

Keep essential services available

- Work in harsh conditions with ruggedized equipment certified for industrial environments
- Keep voice communications available during outages or network disruptions
- Find and fix problems earlier, before they disrupt operations
- Maintain and modernize without stopping operations
- Ensure continuous connectivity for critical operations
- Keep critical infrastructure supported for its full lifecycle

Solutions that support operations

Ruggedized networking

Alcatel-Lucent OmniSwitch® ruggedized switches are built to keep working through heat, cold, dust and vibration at industrial and other outdoor sites. Ring and virtual chassis designs (multiple switches working as one) avoid single points of failure.

AI-assisted network operations

Alcatel-Lucent OmniVista® Network Advisor watches the network around the clock to detect issues, explain what is wrong (and where) and suggest fixes. Your team can apply updates with a single click or enable automatic remediation. The AI Virtual Assistant can also be queried in plain language.

Always-on networking

SPB (shortest path bridging) and ring protection automatically find the best route for data and switch to another path in milliseconds if a link or switch fails. Cameras, phones and control systems stay.

Mission-critical communications

Alcatel-Lucent OmniPCX® Enterprise Communication Server Purple delivers resilient voice communications with redundancy, hot standby, call preservation and local survivability.

Maintenance without downtime

Redundant designs let your team upgrade or replace equipment while traffic keeps flowing on another path, so planned work does not stop operations. Data and power over existing legacy cabling connect modern IP and DECT equipment without re-cabling or disrupting services.

Long-term support

Support for **10+** years helps match the hardware lifecycle to the needs of critical infrastructure.



Stay in control

You need visibility for security, and you need ownership for control. Continuity of control means that you decide where data is stored, who can access it, how you show compliance and how fast your infrastructure changes. Modernization should never require you to give up control of data, access, pace or AI.

Keep control of your architecture, your data and your pace

- Protect communications and control where data is stored
- See wired, wireless, internet of things (IoT), communications and network environments in one view
- Contain cyber threats and keep critical operations running during a security incident
- Use your own AI model with your own data, and approve every recommendation before they are applied
- Adopt new technologies without being forced into a specific cloud model
- Prepare your network for future AI and business needs

Solutions that support control

Sovereign collaboration

Rainbow Edge supports private communications and collaboration on premises. Data is stored in your own data center, so you always keep control of your data.

Continuous verification

Zero trust network architecture (ZTNA) means that no user, device or application is trusted by default. Each device, including OT and IoT, is identified and placed in its own segment, so an incident can be contained without crippling the rest of the operation.

Human-decided AI

AI-assisted operations give insights, recommendations and automation. Your team decides what to approve and what to automate.

Sovereign management

OmniVista management tools can run on premises or in the cloud. They give you central deployment, visibility and control of your voice and data infrastructure.

Freedom of deployment

Deploy on premises, in a private cloud, in a public cloud or as a hybrid environment, so you are never forced into a single infrastructure model. Legacy and modern systems can run side by side, enabling a step-by-step migration.

AI-ready data center

AI data center delivers a scalable design, intelligent automation and fast response times for modern AI applications.

Proven continuity across mission-critical industries



Transportation

- Nevada Department of Transportation - United States
- A resilient network supports operations across 5,400 miles of transportation infrastructure.



Healthcare

- John Flynn Private Hospital - Australia
- Integration with a third-party notification server helps the hospital meet regulations and deliver consistent notifications to staff.



Safety and security

- Metz Eurometropolis - France
- Hardened equipment makes it secure and easy to support more than 4,000 connected devices for smart city and transportation applications.



Energy and utilities

- SARP Group - France
- Remote collaboration and visual assistance with field operators improve operations and customer service.



Manufacturing

- Brohl Wellpape - Germany
- Integrated AI and machine learning enable real-time issue detection and troubleshooting.



Why Alcatel-Lucent Enterprise?

Strengthening continuity through data sovereignty and security

Protecting sensitive information requires strong cybersecurity practices, compliance with regulatory requirements and control over where data is stored and how it is managed. At Alcatel-Lucent Enterprise, we:

- Follow National Institute of Standards and Technology (NIST) best practices for secure development
- Apply ISO 27001 standards to our organization and Alcatel-Lucent operated solutions
- Support zero trust principles, granular network segmentation and highly specific security policies
- Conduct specialized security testing and validation
- Hold key industry certifications
- Support sovereign deployment models, including on premises, private cloud, public cloud and hybrid environments

We contribute to European Union proposals for cybersecurity directives. We help customers choose and use the right mix of secure networking, communications and collaboration solutions, and we train their employees in cybersecurity best practices.

Certified solutions, active risk management and trained staff help customers strengthen both cybersecurity and data sovereignty.

One partner for the foundation of continuity

Alcatel-Lucent Enterprise provides networking, communications and collaboration from one portfolio. Our solutions are used in hospitals, energy and utility grids, transportation networks and manufacturing facilities. They keep people connected, operations running and control with the people who own the system.

Continuity is not a hope or a promise. It is an architecture.

Learn more about Alcatel-Lucent Enterprise mission-critical solutions

Always connected. Always operating. Always in control.

Not all solutions are available in all countries.
Please contact your local Alcatel-Lucent Enterprise team for product availability.

www.al-enterprise.com
© 2026 ALE International, ALE USA Inc. All rights reserved in all countries. The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view a list of proprietary ALE trademarks, visit: www.al-enterprise.com/en/legal/trademarks-copyright.
Some visuals in this document may have been generated using AI and are for illustrative purposes only. DID26102301EN (November 2026)

Alcatel·Lucent