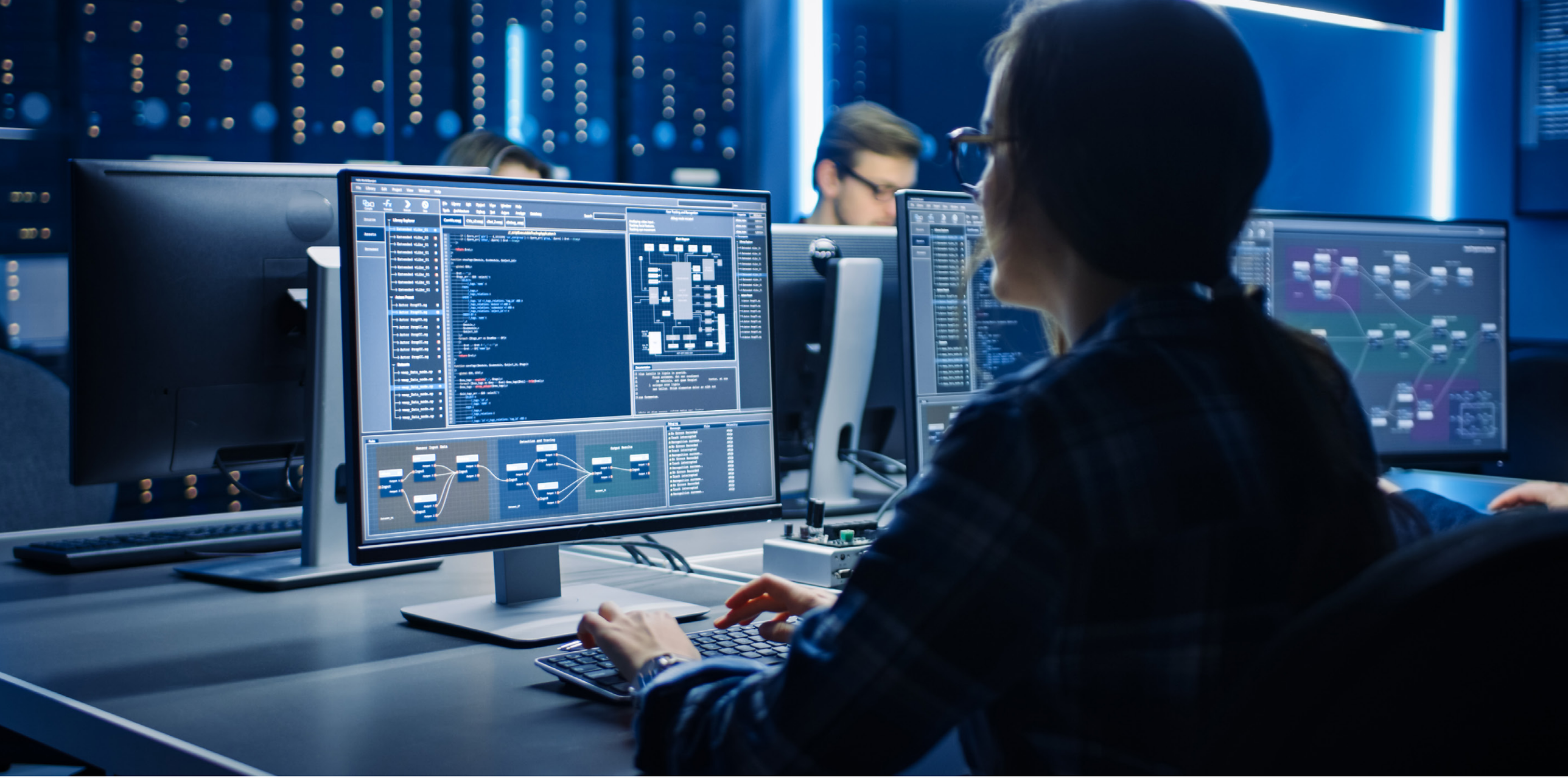


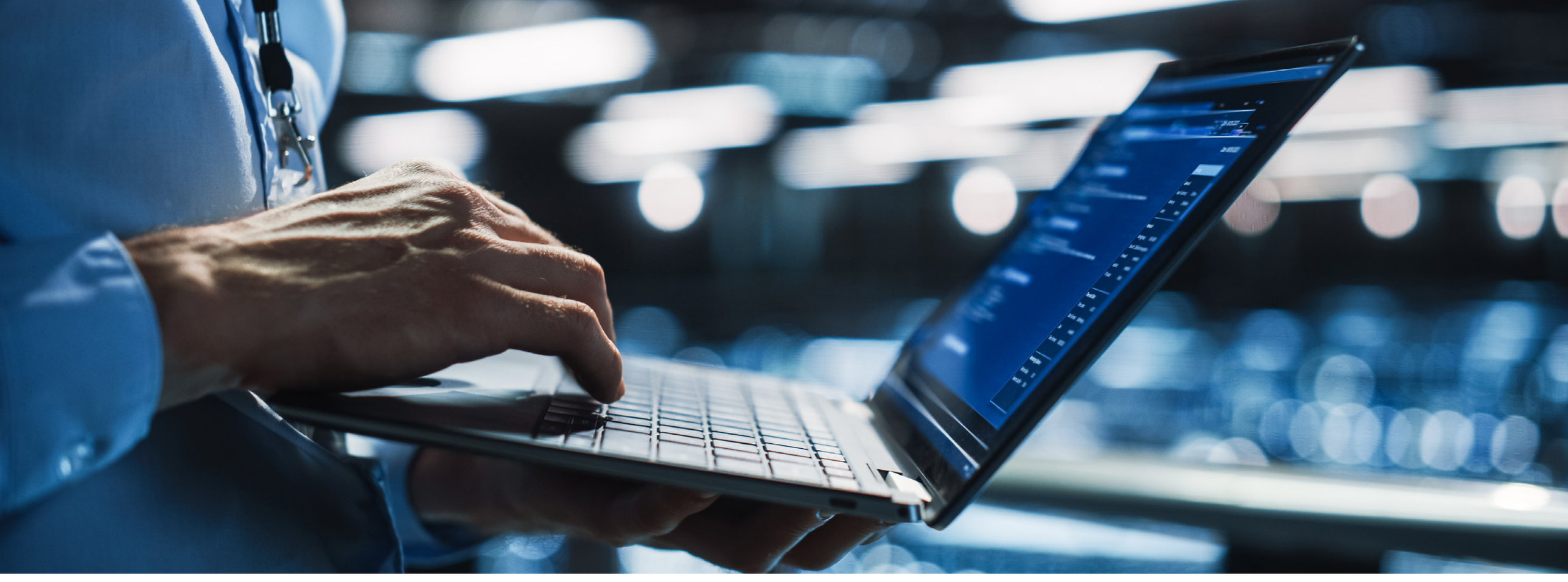
Making resilience and security a priority

Alcatel-Lucent Enterprise solutions for government

Alcatel·Lucent Enterprise

eBook

Table of contents



Overview

With growing global challenges and increased cyber and physical risks, governments must prioritise risk management, safeguard critical infrastructure and protect citizens. According to CloudSek cyberattacks against the government jumped 95% in 2022.[1] The expectation is that government business continues whatever the situation and that citizens are kept safe. In today's global climate, it's more important than ever to maintain data security, protect data sovereignty and ensure service availability.

Public sector and why ICT is more critical than ever

In recent years, digital transformation in the public sector has rapidly advanced, with an increasing number of citizens accessing digital services. Digital transformation has also enabled government employees to adopt a work-from-anywhere workstyle. There is growing pressure on governments to accelerate digital transformation further. According to a Deloitte article, seventy-seven percent of government agencies say that digital transformation initiatives pushed during the pandemic are already having a positive impact on their organisation.[2]

Alcatel-Lucent Enterprise works with governments globally and recognises the significance of safeguarding citizens, operations and buildings against cyber and physical risks. Our solutions consider security and data privacy at every stage of the design process and are built with resilient options to fit every type of organisation. This eBook provides insights about resilience and security for your ALE communications, cloud, and network solutions.

1 Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says. CSO United States, January 2023.
2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Why IT/OT collaboration is critical

Before we explore how you can improve resilience and security with Alcatel-Lucent Enterprise solutions, it is important to acknowledge the changing Information Technology/Operational Technology relationship. In the past, IT and Operations teams didn't collaborate closely, each had their own functions and responsibilities. These two worlds are now converging and must work as one. IT and Operations teams that aren't aware of each other's activities, or that don't coordinate and collaborate, put the entire organisation at risk.

Let's consider, for example, the vast number of Internet of Things (IoT) devices that are rapidly being deployed in many government agencies and smart cities. When IT isn't aware of the operations team implementing new IoT devices, they can't ensure the devices comply with the organisation's security policies. IoT devices come with highly variable levels of cybersecurity features and may not be equipped with the latest protection mechanisms, or their capabilities may not have been fully implemented. These unauthorised "shadow IT" devices could run any software and be infected with viruses and malware. Left unchecked, they can easily introduce new vulnerabilities and attack vectors into the network. We are now seeing the emergence of IT/OT collaboration required to ensure network security and resiliency.

Resilient and secure network solutions

The network infrastructure is integral to the functioning of government organisations as well as the provisioning of services for citizens. Due to the sensitive nature of the information contained in government networks and the critical services governments run, downtime or disruptions in network services can have severe consequences, making resilience and security the priority. Reliable and secure networks are essential for governments to deliver effective public services, protect sensitive information and ensure smooth operations.

ALE Digital Age Networks are resilient and go beyond what many other technology providers offer. We embed security in our network and solutions from the earliest stages of design with no additional licensing costs.

6 Best practices for choosing network solutions

1. Adopt a zero trust security strategy. Macro- and micro-segmentation of your network is crucial to maintain a resilient infrastructure. A phased approach for micro-segmentation ensures the proper implementation and helps avoid disruptions.
2. Consider adopting a Shortest Path Bridging (SPB) solution for redundancy and security, as this approach dynamically reroutes traffic across multiple paths in case of failure while creating an efficient, containerized network. SPB enhances security with MAC-in-MAC encapsulation, eliminating IP addresses to prevent IP spoofing and packet analysis attacks.
3. Consider leveraging virtual chassis capabilities to enhance reliability in critical areas—as this enables network redundancy and resiliency—along with supporting in-service software upgrades (ISSU), and allowing for dedicated mesh or ring interconnections. The virtual chassis presents a cost-effective solution to simplify network management while ensuring high availability.
4. Consider implementing the Virtual Router Redundancy Protocol (VRRP). VRRP enhances network resiliency by providing a backup virtual router that can seamlessly take over if the primary router fails.
5. Implement a solution that ensures that you have all configuration backups from network switches, and can restore them should the worst case happen or when the need arises.
6. An enhanced security step is to have Secure Diversified Code that randomizes the location of different segments of code on your switches, dramatically increasing security. This can be paired with an independent verification and validation (IVV) process, conducted by a third-party cybersecurity expert, that analyses and tests the operating system to identify and eliminate any potential vulnerabilities, backdoors, malware or system exploits.

Invest in resilient and secure network solutions

Investing to ensure your network is resilient and secure always makes sense. However, understanding where best to invest can be complex and take time — planning is key. Before you get started, here are some key areas to consider ensuring you get the security and resiliency your organisation requires:

- Review and update your network design to ensure your organisation's requirements are reflected in the network, including the appropriate level of resiliency for sensitive and critical areas that impact essential government services. For critical areas, consider adding backup servers and multiple connections where possible and applicable.
- Consider the increasing importance of incident response time: For example, we use artificial intelligence (AI) and machine learning (ML) capabilities for our Alcatel-Lucent OmniVista Network Advisor to identify and resolve issues faster. This tool ensures problems are resolved before they impact end users, by proactively identifying and addressing network or security issues. It expedites troubleshooting and improves network security through configuration audits and administering alerts in real-time about any sudden changes in network behaviour.
- Consider hardened switches for harsh environments. The Alcatel-Lucent Enterprise family of ruggedised Ethernet switches is specifically designed to excel in challenging environments and extreme temperatures. These switches are built with ruggedised components and housed in sturdy enclosures, ensuring durability and reliability and have the same Operating System as the rest of the ALE switches. To enhance security and protect sensitive information, some models of switches are equipped with intrusion alerts and alarm relays that enable the connection of external alarm systems. Some models even support MACsec for secure data communications between the two ends. With Virtual Chassis capability in ruggedised switches, you can gain improved redundancy, resiliency and scalability.

Resilient and secure communications solutions

Communications are crucial for governments to interact with citizens, stakeholders and other government agencies, as well as for the dissemination of important information. Communications systems must be available in times of crisis, when citizens need government assistance most. Resilience and security are evolving, and regular reviews will help keep your Alcatel-Lucent Enterprise communications solution safe and available.

ALE communications solutions are secure-by-design. That means we consider security during every step of product definition, development and delivery. All hardware and operating systems are hardened, and Denial of Service (DoS) protection is built in. We comply with recognised certifications and accreditations for global security and privacy standards (ISO 27001, ISO 27017 and ISO 27018). As well we adhere to industry-specific security and privacy standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and Hébergeurs de Données de Santé (HDS) for health data hosting in France, as well as regional security and privacy standards, such as the General Data Protection Regulation (GDPR) in the European Union.

6 Best practices for your communications solutions

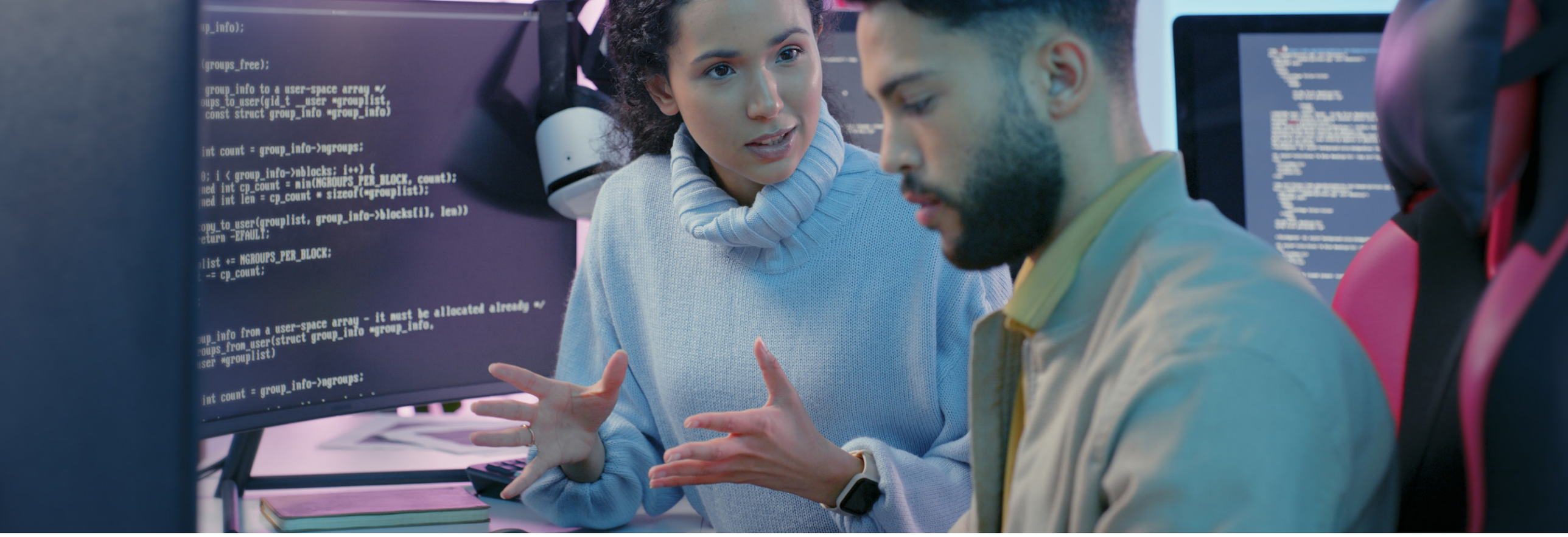
The following are 6 best practices to help ensure you fully optimise the resilience and security built into your ALE communications solutions.

1. Ensure you have the latest software version or the right patches in order to have the latest security enhancements for better protection.
2. Consider a solution that includes alarm monitoring and remember to perform regular updates with the right thresholds. Verify that notifications around communication system failures or quality alerts are sent to the appropriate individuals.
3. Review and enforce a strong password policy, preferably using external authentication with a RADIUS server. Implement user reminders to help prevent toll fraud, which is still a threat in many countries.
4. Provide employees with security awareness training and ensure they are aware of risks and prevention measures.
5. Ensure you have an automated remote system backup to help avoid configuration data loss.
6. Consider a specific VLAN for voice. Separating voice from other traffic reduces the chance of contamination, which can potentially disrupt operations and even government services.

Invest in resilient and secure communications solutions

Over the last few years, the global environment has shone a light on the importance of government-citizen communications. Following are some key areas to consider for government agencies planning to invest in communications solution to enhance resiliency and security.

- Redundant and resilient architecture. Your architecture should be fully redundant and resilient. Duplicating call servers in critical areas, implementing remote site redundancy and duplicating critical application servers can provide additional protection.
- Create a workflow using Rainbow and/or Alcatel-Lucent Visual Notification Assistant (VNA) with automatic triggers (trigger being human, IoT or system) to notify key people of system issues so they act quickly and speed up the recovery process
- Deploy strong encryption. Encryption is based on industry standards designed natively into the solution, without any impact on the voice quality and performance



- Implement Rainbow™ by Alcatel-Lucent Enterprise, the ideal collaborative tool to complement ALE communications solutions. Rainbow offers a comprehensive set of features including voice, video and instant messaging, empowering seamless communications and efficient collaboration. With Rainbow, you can exchange images, videos and video surveillance feeds, enhancing contextual awareness and enabling better decision-making. Rainbow also provides hybrid communications with secure connectivity between on premises and cloud. It ensures resilient communications, keeping you connected to colleagues and customers using Rainbow, providing uninterrupted connectivity even in challenging situations. Hybrid communications also have the advantage of cloud and on premises operations being run from different locations for ultimate resiliency to keep communications open.
- For agencies with more stringent security requirements, Rainbow Edge offers an on premises alternative with a private cloud instance. The instance can be hosted in any data centre, providing complete control over servers, storage and networks, empowering agencies to customise and configure the infrastructure according to their requirements. Personalised security policies can be implemented, and resources can be managed autonomously. This level of control provides complete visibility and authority over the infrastructure, enabling agencies to make informed decisions and optimise performance in alignment with their objectives.
- Define a secure distributed workforce communication strategy. ALE provides multiple options for communications and collaboration for distributed, mobile and work from home employees, including:
  - Rainbow
  - IP Desktop softphone
  - ALE Softphone
  - Deskphone with embedded VPN and can be mass deployed with embedded security (VPN)

Protecting people and assets

ALE offers flexible, secure and highly available real-time communications and notification systems. These solutions can integrate with public safety or smart city control centre operations, streamlining call dispatching and prioritisation, facilitating contextual information exchange with IoT data, and enhancing collaborative efforts among first responders and various stakeholders enabling improved decision-making and coordination.

The ability to interconnect IoT devices within buildings, venues and cities, combined with analytics and AI, is fundamentally transforming the communications landscape. Through the integration of sensors, video surveillance, Rainbow workflow and AI, the shift from a reactive to proactive approach is possible, enhancing process efficiency in terms of time and cost. This integration facilitates a comprehensive understanding of the context, supports decision-making processes, and subsequently reduces emergency response times. Additionally, functionalities like Asset Tracking and control of smart locks and lights streamlines operations. Furthermore, the ability to record communications and log actions simplifies post-event analysis, enhancing security processes and mitigating potential liabilities. To achieve these advancements, a connected environment with ubiquitous Wi-Fi access and effortless IoT onboarding is crucial.

For time-sensitive, secure and highly available real-time communication platforms, a robust infrastructure is vital to ensure seamless operations. Your technology infrastructure should encompass appropriate software, high availability networking protocols, and the flexibility to incorporate rugged network switches which can seamlessly integrate into your ecosystem and withstand harsh environmental conditions, including limited airflow, shocks and extreme weather temperatures. Opting for rugged equipment ensures longevity in such challenging locations where non-rugged equipment would be less durable.

In the field of physical security systems, the stakes are high. Each minute and every piece of video footage could be crucial for authorities in identifying wrongdoing, pinpointing the source of an incident, or understanding the cause of a disaster. A robust video surveillance infrastructure is essential. The networking infrastructure should not only provide sufficient bandwidth and Power over Ethernet (PoE) for surveillance cameras but also seamlessly integrate with video surveillance management systems. This integration ensures an efficient and reliable surveillance network with smooth operation and easy troubleshooting. The operations team should be capable of promptly resolving any video issues, particularly in environments where every video frame is critical. Alcatel-Lucent OmniSwitch® solution integrations, accomplished through plugins with major video management systems, enable you to achieve this vital objective.

Furthermore, there are situations where asset tracking or locating individuals or equipment within your organisation becomes necessary. An effective asset tracking solution relies on its ability to easily and accurately locate people and assets. Such a system also enhances safety and security by enabling the quick dispatch of assistance when the location of individuals is known. With the Alcatel-Lucent OmniAccess® Asset Tracking solution, staff and equipment can be located quickly and shown on a floor plan map. Asset tracking also provides information about usage patterns, knowing if assets are over utilised or underutilised can provide valuable information.

Data sovereignty and security

Alcatel-Lucent Enterprise surpasses other technology providers in implementing best practices required for end-to-end cybersecurity. At ALE we:

- Follow the National Institute of Science and Technology (NIST) best practices and recommendations when performing risk assessments on new features and when implementing cybersecurity features, such as native encryption, in our solutions
- Have Common Criteria EAL2+ certification
- Apply ISO 27001 standards to all our cloud-based solutions
- Support ZTNA, granular network segmentation, and highly specific security policies to reduce the risk of unauthorised activities
- Execute highly specialised, security-specific tests, such as penetration tests, on our products
- Ensure our products achieve key industry certifications, such as HDS, HIPAA, and the Family Educational Rights and Privacy Act (FERPA)
- ALE International complies with European Union Network and Information Security Directive (NIS 2).

As recognised cybersecurity experts, we contribute to European Union proposals for cybersecurity directives. We also leverage our cybersecurity expertise to help customers choose and implement the right mix of secure unified communications and collaboration solutions to meet their needs and we train their employees in cybersecurity best practices.

DID23070401EN (March 2025)

Alcatel·Lucent
Enterprise