Security Considerations for Private LTE Grid Communications Networks

Anterix® ERICSSON ONELAYER Telit Cinterion

April 2025

Table of Contents

1 | Smart Grid Trends and Communications Security Requirements

As rapid digitization continues in American homes and businesses and more pressure is placed on power load demands due to electric vehicles (EVs) and renewable energy integration, utilities must adapt and transform today's electric grid to meet the new smart grid requirements. The smart grid needs to scale to serve more diverse endpoints, for example smart meters and IoT devices, ensuring appropriate power distribution and seamlessly incorporating clean energy sources from distributed resources. Distributed energy, electric vehicles, microgrids, and residential power generation represent a few components requiring monitoring and control capabilities throughout the next-gen electric network. Industrial devices containing internet-connected sensors and actuators are rapidly being deployed throughout the grid. These devices deliver real-time insights that enable automated, fine-tuned performance optimization across the grid. The emerging smart grid requires that the energy sector transforms and digitalizes its operational technology (OT) and information technology (IT) infrastructure.

As the grid advances to become digitized and "smarter," it also becomes more vulnerable to cyber-attacks. These attacks happen continuously throughout the grid on many different levels. Increasingly, utilities have become focused on how to strengthen the grid by leveraging the latest technological and operational improvements.

This paper brings together industry experts to collectively address emerging smart grid infrastructure requirements and how a security-focused architecture comprised of smart edge devices and edge data processing, interoperating networks, secure data flows and controls are necessary to mitigate risk and improve grid resilience.

1.1 | Smart Grid Regulations and Cybersecurity Guidelines

In the context of smart grid security communications in the United States, multiple strategies have been defined already, all of them highlighting the need to enforce and defend national critical infrastructure. The electric grid, including smart grid technologies, is one of the principal elements to be protected across all cybersecurity strategies.

Several other key governmental references and guidelines reinforce this priority:

Executive Orders and National Strategy:

Various executive orders, such as Executive Order 13920 on "Securing the United States Bulk-Power System" outline strategies for protecting critical infrastructure, including the smart grid.

FERC Orders:

The Federal Energy Regulatory Commission (FERC) has issued various orders and regulations to enhance the reliability and security of the electric grid, including Orders 706 and 800, which address cybersecurity standards. Moreover, in 2023, FERC with Order 893 provided incentives to encourage investments by utilities in advanced cybersecurity technology.

NERC CIP Standards:

The North American Electric Reliability Corporation (NERC) has established Critical Infrastructure Protection (CIP) standards that mandate cybersecurity measures for entities involved in the bulk electric system. Recently the National Institute of Standards and Technology (NIST) and NERC released a whitepaper to map the NIST Cybersecurity Framework and NERC CIP standards.

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09292021.pdf

[2] https://www.nist.gov/cyberframework

[3] https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40

[4] https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity

NIST Framework and Roadmap for Smart Grid Interoperability Standards:

Under the umbrella of the NIST Cybersecurity Framework, other guidelines have been developed to ensure interoperability and security within the smart grid, in the "Roadmap for Smart Grid Interoperability Standards" and "Guidelines for Smart Grid Cybersecurity."

2 | Critical Requirements for Smart Grids in Addressing Utility Operations

Wireless communications networks play a key role in helping utilities to meet challenges while also mitigating risks, increasing customer satisfaction, and improving operational metrics.

Utilities have unique requirements for the communications networks supporting smart grids, including:

- Coverage needed across large, diverse areas, including both urban and remote rural environments
- Management, visibility, and control of a large set of network device endpoints
- Unique requirements for IOT device security
- Leverage load planning and analytics to effectively regulate electricity flow throughout the grid
- Security policy control requirements
- Physical security and encryption for remote network assets
- Securely roaming onto adjacent networks to support device connection redundancy, and mutual aid during disaster response

The utility's environment must also be certified via GSMA's Security Accreditation Scheme for Production Environment and Process Security.

3 | How Private LTE Networks Can Deliver Robust Security

Private wireless broadband networks, such as those being deployed at 900 MHz by leading utilities in 15 U.S. states, provide utilities with enhanced network control, helping to mitigate potential threats. Utilities have more control over the network design, build, and operation, as well as end-to-end system security, access, and data visibility. A private network offers a smaller and more visible threat landscape.

By owning and managing a private wireless network, utilities benefit from the ability to customize their network to their specific needs and implement advanced security features. They can integrate cyber tools and capabilities directly from their existing utility data or operations center while selectively enhancing security measures at the network's edge for optimal protection. A private wireless broadband network is becoming an integral part of the utility critical data infrastructure needed to support required increased data speeds, capacity, and security critical to operate modern, safe, and resilient utility infrastructure.

3.1 | 3GPP Standards-Based Licensed Spectrum

Anterix's 900 MHz spectrum is ideally suited to support utility private LTE networks as foundational spectrum, covering wide areas across broad geographies and topographies. As the largest holder of dedicated licensed spectrum in the 900 MHz band (897.5 MHz-900.5 MHz and 936.5 MHz-939.5 MHz) throughout the contiguous United States, Hawaii, Alaska, and Puerto Rico, Anterix is uniquely positioned to deliver solutions supporting secure, resilient, and customer-controlled operations. 900 MHz spectrum is foundational to helping utilities leverage private wireless broadband to support grid modernization.

3GPP technologies such as LTE and 5G NR are increasingly employed in smart grids, primarily operating on licensed spectrum, and historically targeting high-quality mobile data services. These technologies enable widespread, reliable device coverage, providing a single wireless platform for multiple applications. Lower frequencies are often used for IoT because they travel farther and penetrate buildings more effectively. This improves coverage and performance while reducing the need for costly network infrastructure.

The 3GPP specifications provide a comprehensive framework for the security architecture, encompassing aspects such as:

- **Mutual Authentication:** Mutual authentication ensures that both the user equipment and the network validate each other's identities before establishing a connection, preventing unauthorized access.
- **Authorization:** Once mutually authenticated, the network authorizes the devices/subscribers to access specific services and resources based on pre-defined provisioned policies.
- **Encryption:** Encryption protects the confidentiality of data transmitted over the air interface.
- **Integrity Protection:** Integrity protection ensures that the data has not been tampered with during transmission.

These measures are critical in maintaining the integrity and confidentiality of communications within private LTE networks, making them suitable for enterprises and industries with high security requirements. A multi-layered approach to security, combining 3GPP specifications with NERC CIP standards adherence and other optional security standards, fortifies the security posture of private LTE networks, making them resilient against a wide range of cyber threats.

By adhering to stringent 3GPP specifications and NERC CIP standards, these networks enable secure communication with strong authentication, encryption, and integrity protection.

3.2 | Built-in Private LTE Security

Private LTE networks offer a robust solution for utilities, providing enhanced security through dedicated licensed spectrum. Private LTE comes with a broad set of security capabilities and features defined by the global wireless standards body, 3rd Generation Partnership Project (3GPP), to enable delivery of advanced cybersecurity protections. These include network authentication, subscriber identity protection, strong authentication management, and encryption. Utility companies benefit from rigorous access controls and advanced authentication methods, preventing unauthorized access and improving network performance and reliability.

A private LTE network also offers many benefits for physical security applications, including low latency, quality of service, and analytics capabilities. Many utilities are concerned about physical security attacks on substations and other grid assets. Private LTE enables physical security applications like video monitoring with analytics, gunshot detection, and the ability to deliver alerts and dispatch field personnel.

3.3 | Private LTE Support of Security Layers

Private LTE networks provide the necessary tools to protect critical infrastructure, enabling integrity, confidentiality, and availability of communications. Multiple layers of customizable security can be incorporated to align with established cyber frameworks such as NIST or the International Organization for Standardization (ISO). Security features can provide full visibility into connected assets and their behavior, including traffic monitoring and the establishment of device and traffic policies for effective segmentation. Private LTE supports additional security layers, including device threat monitoring and prevention, device URL filtering, traffic monitoring, identification and authentication, implementation of customized network access policies, and network segmentation to permit only authorized host network devices while monitoring device traffic.

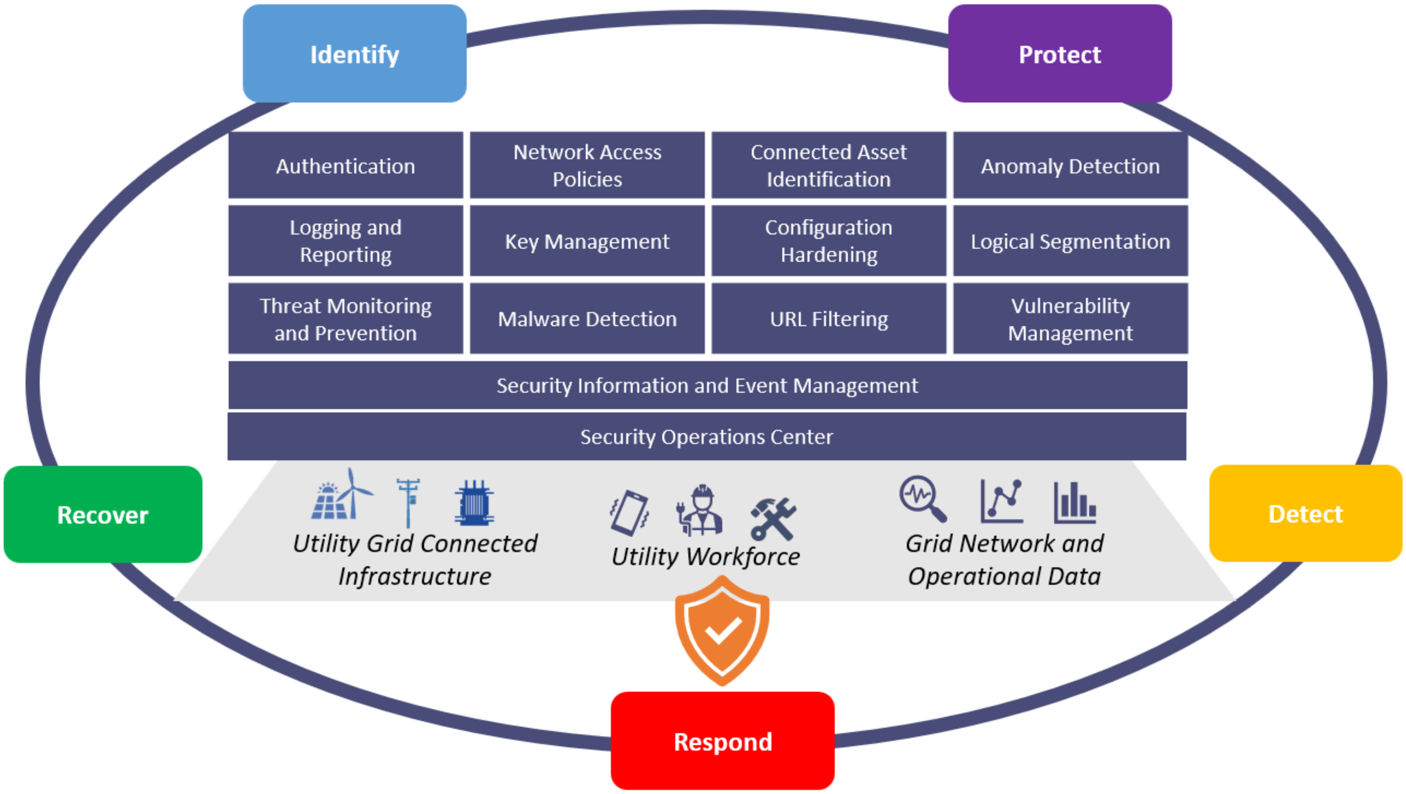


Figure 1: Private LTE security enables multiple security layers to support the mission-critical utility grid

4 | Anterix Active Ecosystem: Testing and Supply Chain Validation

The Anterix Active Ecosystem (AAE) brings together leading companies from across the technology landscape to help utilities harness the value and accelerate the deployment of 900 MHz private LTE networks. This program strengthens and expands the landscape of 900 MHz devices, services, and solutions for utilities and other critical infrastructure industries. Members share technical insights and advanced solutions and collaborate on opportunities for 900 MHz private LTE, all targeted to benefit the utility sector.

AAE members address a broad array of equipment, solutions, and services that utilities require to plan, build, manage, and capture value from their private wireless broadband network investment. This rich and diverse group of innovators is united in their focus in contributing to the success of private LTE. The group includes component manufacturers (devices, chipsets, modules), radio access network (RAN) and core infrastructure providers, software developers, and providers of IoT, cybersecurity, and 4G/5G LTE solutions that are actively collaborating to drive a new wireless communications technology landscape supporting 900 MHz private LTE.

Together with more than 125 AAE members, Anterix and the 900 MHz revolution is dedicated to supporting a long-term roadmap of solutions and services and helping utilities achieve the most value from their private broadband network investments.

Ecosystem Testing and Badge Designations

Anterix works with Ecosystem members to test and validate products for operation on Anterix's 900 MHz spectrum. Upon testing completion, devices that have successfully demonstrated that they are able to connect and operate over networks using Anterix's spectrum are awarded one of two Anterix Active Ecosystem badges:

- **Anterix Active** products that are commercially available and ready to be deployed on Anterix's spectrum
- **Anterix Capable** products that are not yet available for commercial use on the Anterix spectrum, but can be used for demonstrations, laboratory projects, and pilots.

Supply chain security validation is crucial to help ensure the integrity, security, and reliability of products and services, thereby mitigating risks associated with counterfeit components, unauthorized changes, and cybersecurity threats. Anterix recognizes the importance of supply chain security validation and encourages it with the Ecosystem through the badging program for vendors who established best practices, so that only trusted and verified suppliers are integrated into their networks.

Members and customers also benefit from technical assistance, collaborative tools, and marketing support to foster the creation of innovative products and services tailored for 900 MHz private wireless networks, thereby empowering utilities, and the critical infrastructure sector.

5 | Security Collective

The Anterix Security Collective®, an extension of the Anterix Active Ecosystem, brings together cyber-physical solution providers with utility-specific expertise to develop secure 900 MHz private LTE deployments. The members, selected by Anterix, are well-positioned to enhance utility defenses and collaborate to implement comprehensive security solutions. By combining a suite of bundled services with the expertise of the Anterix Security Collective, Anterix can help utilities achieve both operational excellence and robust security, demonstrating a steadfast commitment to the evolving needs and challenges of the critical infrastructure sector.

Members of the Anterix Security Collective provide additional layers of security to private LTE networks with a comprehensive suite of advanced measures tailored to critical infrastructure and enterprise needs. This multi-layered approach combines robust encryption, zero-trust architecture, and continuous monitoring to safeguard the network. Key technologies include multi-factor authentication, which requires multiple forms of verification to reduce unauthorized access, and network micro-segmentation, which limits the lateral movement of threats by dividing the network into smaller segments. Advanced firewalls and intrusion detection systems constantly monitor traffic for suspicious activity, while security information and event management systems analyze security data in real-time for comprehensive visibility and rapid incident response. Endpoint detection and response solutions provide deep visibility into endpoint activities, enabling swift action against malicious activities. These technologies analyze patterns and behaviors to identify anomalies and potential threats that may evade traditional security measures. By leveraging these advanced practices and technologies, Anterix Security Collective members provide technology that enables secure, reliable, and resilient communication infrastructure for private LTE networks, meeting the strict security demands of modern critical infrastructure industries.

OneLayer, a member of the Anterix Security Collective, offers a platform and capabilities that enhance the security of private LTE. OneLayer's platform enables utilities to securely leverage IoT and LTE by extending security visibility and segmentation frameworks like the Purdue model and zero trust Architecture to private LTE, bridging the gap between the LTE packet core and IT and OT security tools. The platform directly integrates with leading cellular packet core technologies, including Ericsson, Nokia, and Verizon to enhance the visibility of the existing security tools and achieve full visibility to cellular devices and non-cellular devices connected behind cellular routers. It enables deployment of granular zero trust segmentation policies with private LTE networks, including geo-fencing devices, track & secure devices with device-level geofencing, and location-based connectivity policies. It extends the Purdue model network architecture to LTE networks and enables compliance with utility regulations such as the NIST Smart Grid Framework.

5.1 | OneLayer Experts Insights and Recommendations

Avishag Daniely, Vice President of Product at OneLayer, emphasizes the critical need for robust security strategies as utilities increasingly adopt private LTE networks to modernize grid communications. Recent industry developments like the Salt Typhoon security incident and new guidance from CISA make it clear that utilities must deploy comprehensive measures to safeguard their infrastructures against evolving cyber threats.

"Utilities stand at the forefront of a transformative era," says Daniely. "As they implement private LTE networks to enhance grid efficiency and pursue new business innovations, securing these crucial communication channels must also be a critical priority. Events like the Salt Typhoon incident are a wake-up call for the industry that adapting enterprise security to address the sophisticated threats targeting private cellular networks is essential to protecting the integrity of critical utility infrastructure."

Among OneLayer's key security recommendations for utilities:

- **Enhance device security:** SIM-based authentication is fundamental, but utilities must not rely solely on this measure. A Zero Trust Network Access (ZTNA) model that includes continuous validation and authorization should be established. This must include devices connected directly to LTE network, as well as devices connecting indirectly through cellular routers.

- **Implement advanced network segmentation:** Utilities must prioritize micro-segmentation to isolate critical assets within their networks. By segmenting their infrastructure, they limit the lateral movement of potential threats, consistent with CISA's advocated approaches for cellular networks.

- **Ensure continuous threat monitoring:** Real-time anomaly detection systems should be employed to provide live visibility of network activities. Utilizing security orchestration, automation, and response (SOAR) capabilities can automate responses to potential breaches, aligning with the proactive monitoring advised by CISA.

- **Strengthen supply chain security:** Proactively fingerprinting all connected devices, conducting careful vendor assessments, and maintaining a secure firmware update process to protect against supply chain vulnerabilities. Adopting security measures in line with NERC CIP standards will further enhance protection.

- **Foster cross-functional collaboration:** Utilities should form interdepartmental teams to address both legal and technical challenges associated with network security. This approach will enable comprehensive visibility and response to emerging threats, in line with best practices highlighted by CISA.

"In this rapidly evolving landscape, utilities need to prioritize both innovation and security. The implementation of private LTE networks provides a solid foundation for future growth, with maximum impact which will only be realized if networks are secured against today's and tomorrow's cyber threats," concludes Daniely.

6 | End-to-End Network Security – RAN, Core

Private LTE system security is defined based on the security domains in 3GPP TS 33.401 LTE System Security Architecture.

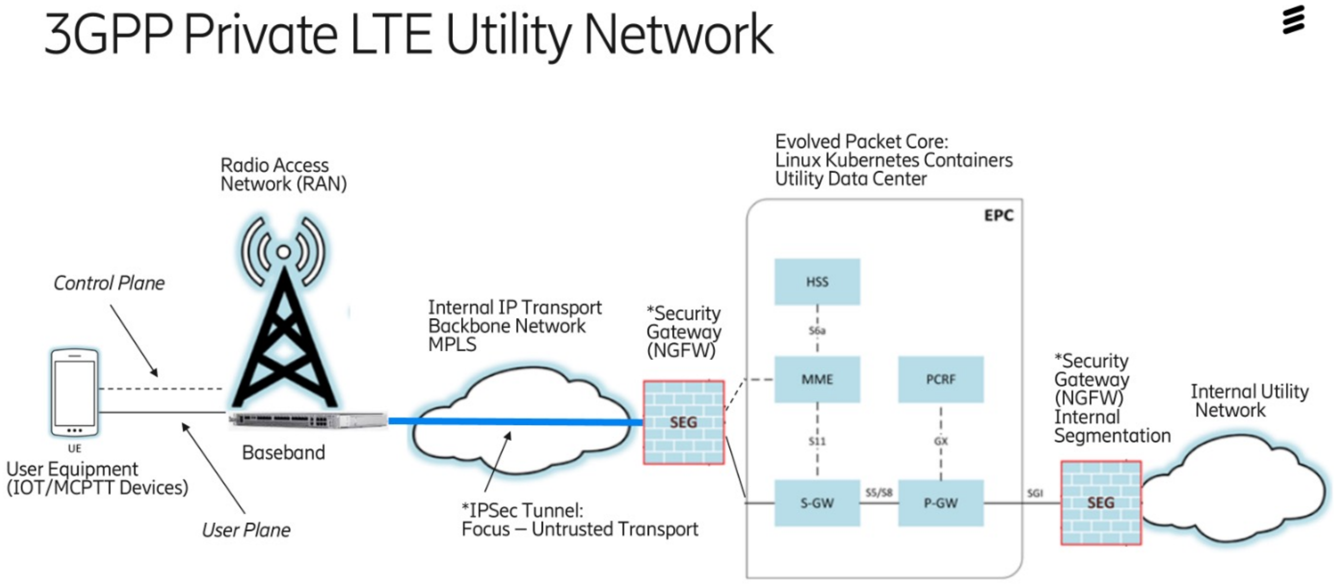

3GPP Private LTE Utility Network
Radio Access Network (RAN)
Evolved Packet Core: Linux Kubernetes Containers Utility Data Center
EPC
Control Plane
Internal IP Transport Backbone Network MPLS
*Security Gateway (NGFW)
SEG
HSS
S6a
MME
PCRF
S11
GX
S-GW
S5/S8
P-GW
SGI
*Security Gateway (NGFW) Internal Segmentation
SEG
Internal Utility Network
UE
User Equipment (IOT/MCPTT Devices)
Baseband
User Plane
*IPSec Tunnel: Focus – Untrusted Transport

Figure 2: Figure 2: 3GPP Private LTE Utility Network

Network access security covers the security features and functionality for RAN. Secure device authentication and authorization uses the 3GPP-defined EPS-AKA authentication method for cellular devices. Standards-based AES encryption is set up for the user data and signaling flows along with AES integrity protection for the signaling as these connections move over the air between the device and the radio node.

Ericsson's RAN supports a hardware-based root of trust that prevents any foreign firmware or software (including software patches) from loading and running on the system. Only authorized signed firmware and software are allowed to execute. All external user access to the underlying operating system and file system is denied by design. Only secure encrypted protocols that use role-based access control (RBAC) are permitted to be used for management of the RAN nodes. All management traffic is authenticated and encrypted using strong PKI certificates using standard secure protocols such as TLS, SSH, Netconf, SFTP, and SNMPv3. All security and audit logs are also encrypted.

Network domain security covers the IP-based transport network that connects the RAN nodes to the cellular core. Over this transport, the management network is segmented off completely from the production network segments that run the user data and signaling traffic. This is done using virtual routers (VR) on the RAN nodes dedicated to each segment which then connect to separate MPLS IP-VPN segments on the utility IP backbone. A security gateway (SEG), which is a next generation firewall (NGFW) supporting cellular-specific protocols and features, can be deployed to protect both user and signaling traffic between the RAN and core using IPSec tunnels and PKI certificate authentication for untrusted transport and core protection. A utility NGFW is also highly recommended at the egress interface connecting the core to the internal utility data center for internal segmentation and security policy control. The core ingress and egress traffic are segmented into distinct network segments that separate the management, user device, signaling, RAN, and all external-facing traffic types. The network manager application implements the PKI certificate infrastructure that supports all of the secure management and communication flows.

User domain and application security cover the end device and the applications that run on those utility devices. The requirements for endpoint device security differ greatly when comparing a traditional cellular service provider to an enterprise running a private network. Ericsson integrates with OneLayer, a security vendor that provides a unified solution for private LTE networks. The One Layer solution provides security controls for the overall endpoint device including network access control (NAC), cellular device fingerprinting, device signaling and data traffic anomaly detection, and full visibility and tracking of all connected devices. The response action includes the ability to segment and quarantine a compromised device with the click of button by utility incident response personnel. Such device security controls are not needed in a larger cellular network provider as they are simply providing a network service to subscribers. Cellular service providers care that the device is authorized to access their network and use their services. Enterprises, on the other hand, require full device security controls for all devices attaching to their private network. Devices should be purchased that are compliant with the CTIA Cybersecurity Certification Program for IoT Devices where they adhere to either level 1 or 2 in terms of supported security controls.

The cellular core implements many security controls. Core security functions include the following: Roaming security is handled via the Diameter Signaling Controller (DSC) in conjunction with a NGFW protecting the roaming traffic between the utility and the cellular service provider. All network functions support security and audit logging via secure syslog. Data at Rest Encryption is handled using file- and disk-level encryption. The core is developed using integrated Linux security features such as AppArmor, SELinux, Seccomp, and host firewall. Operating systems hardening uses CIS control benchmarks for security configuration guidelines. All network functions are installed in accordance with detailed security hardening documents. When dealing with advanced attackers, one of the key required cybersecurity defense solutions is the use of endpoint detection & response (EDR) agents. Such agents can be deployed for all core network functions.

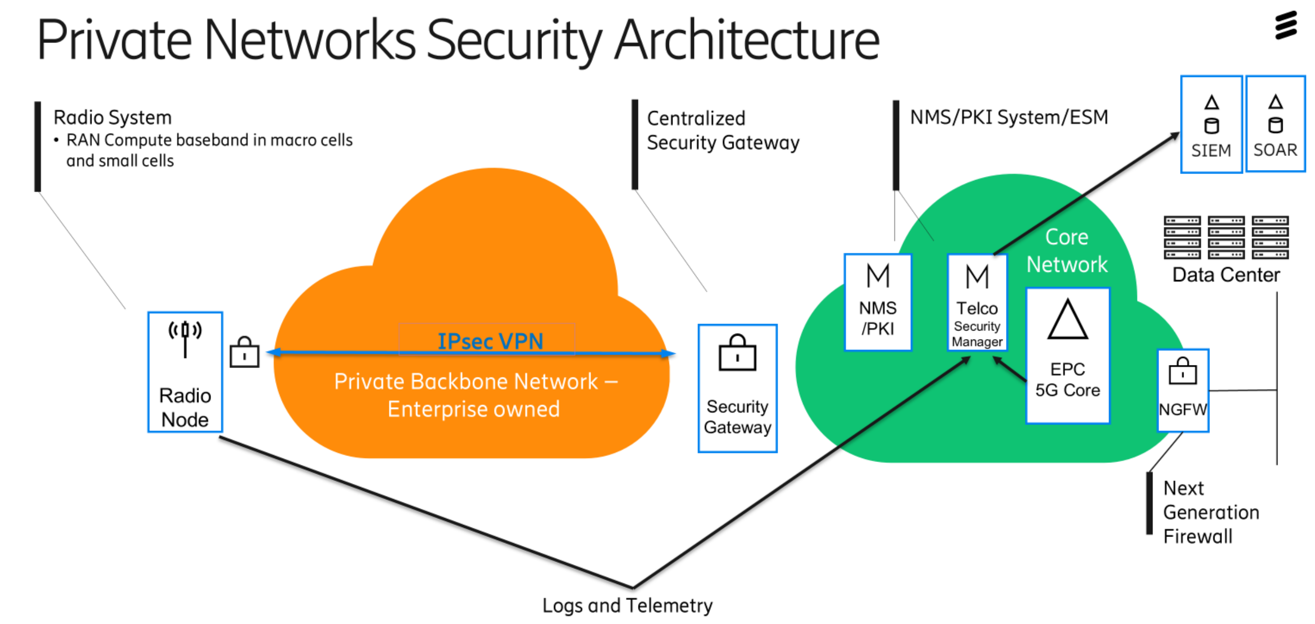


Figure 3: Private Networks Security Architecture

In addition to the above, there are security solutions that integrate with existing utility enterprise systems to close other vulnerability gaps. Cellular network equipment providers offer products that can fill such holes. In the diagram above they are called a Telco Security Manager. Ericsson has the Ericsson Security Manager (ESM). Other telco equipment providers have their own version. The Telco Security Manager fits into the utility security architecture by handling cellular network security use cases that the existing systems such as the security information event management (SIEM) system do not as these systems have been designed and developed primarily for IT networks. The specific use cases are baseline automation to automate and audit security control implementations, threat detection on the management network, false base station detection, and endpoint detection and response (EDR) agents for the cellular core. The ESM is designed to send notifications northbound and work as a telco use case focused adjunct to the utility SIEM. The ESM also has full REST APIs that encompass all its functionality and can be used by the utility Security Orchestration, Automation, and Response (SOAR) for cybersecurity incident response actions.

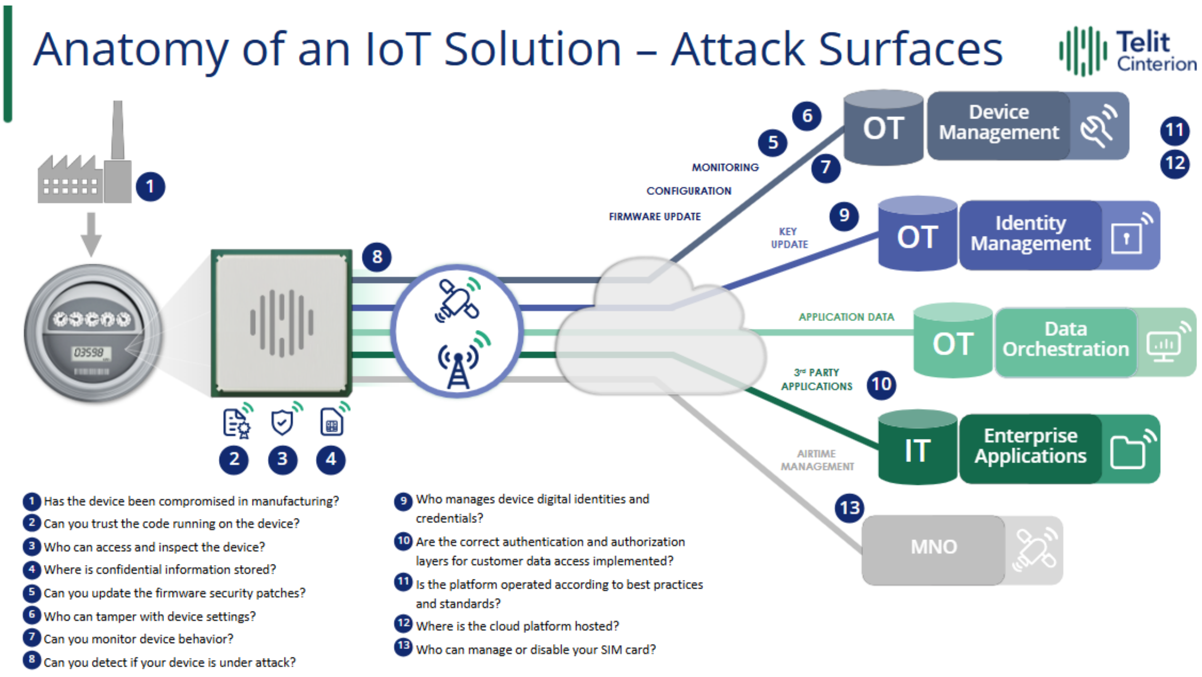
Baseline automation automates the configuration security auditing of all the network elements. If someone should change a security configuration setting, the Telco Security Manager will automatically reconfigure the device so manual intervention is no longer required. This allows for automation of security audits. Threat detection on the management network processes all the management network segment logs from all the cellular devices and reports detected threats to the telco security manager. Attacks such as denial of service against management plane interfaces and authentication guessing will be flagged. False base station detection will alert whenever a radio false base station is active within the utility airspace spectrum. The EDR agent is specifically designed for Linux containerized network function application implementations. The rule set for Ericsson's ESM is built by Ericsson engineering to specifically analyze and protect cellular core applications. Out-of-the-box EDR agents from commercial vendors are not deployable without heavy customization by knowledgeable personnel as they are not designed for cellular cores. Such agents can be used but require much effort and expertise to configure and deploy.

7 | Role of Cellular Modules in the Smart Grid

Private wireless broadband networks are poised to play an even more significant role in enabling the modernization and transformation of the grid, and, by adopting resilient secure connectivity solutions from trusted suppliers, utilities can help to ensure that additional resiliency and security are built into their critical infrastructure. Industrial cellular modules form the arteries of industrial smart grid systems, establishing essential communication links with cellular networks and ensuring the seamless operation of the internet-connected grid network.

Although they may resemble ordinary chips on a printed circuit board (PCB), cellular modules are intricate electronic subsystems equipped with operating systems and thousands of lines of firmware code. They function as industrial communication computers embedded within critical industrial devices, essential for the efficient operation of a nation's vital systems.

Despite their unassuming appearance, cellular IoT modules play a key role in enabling data connectivity by integrating radio access technology and embedded 3GPP protocol support and application processing. They follow a design methodology akin to other electronic components within grid control equipment and metering, serving as crucial entry and exit points for gathering data from industrial sensors and remotely managing actuators via cellular networks over the internet.


Anatomy of an IoT Solution – Attack Surfaces

1 Has the device been compromised in manufacturing?
2 Can you trust the code running on the device?
3 Who can access and inspect the device?
4 Where is confidential information stored?
5 Can you update the firmware security patches?
6 Who can tamper with device settings?
7 Can you monitor device behavior?
8 Can you detect if your device is under attack?
9 Who manages device digital identities and credentials?
10 Are the correct authentication and authorization layers for customer data access implemented?
11 Is the platform operated according to best practices and standards?
12 Where is the cloud platform hosted?
13 Who can manage or disable your SIM card?

Figure 4: Anatomy of an IOT Solution - Attack Surfaces

7.1 | Western Cellular Module Supplier Cybersecurity- Telit Cinterion

Utilities are focused on addressing security risks in their operational technology and IoT systems. Operational Technology (OT) faces an increasing number of attempted hacks, while IoT systems are coming under greater scrutiny. The vulnerability of critical infrastructure in the wrong hands, especially against the backdrop of geopolitical instability, cannot be overlooked.

"A single weak point can compromise the security of an entire IoT system, making a holistic approach essential to safeguarding critical infrastructure," explains Jitender Vohra, Sr. Director Carrier Relations and Product Marketing, Telit.

A substantial number of IoT security problems stem from organizations not considering their technology ecosystem holistically. Cyber attackers will indiscriminately search for vulnerabilities throughout the entire system, and a single weak point can compromise security.

Ensuring robust security requires a layered approach throughout product design, development, security testing, and incident response. A strong product security program helps oversee cybersecurity risks inside connected devices, maintaining trust throughout the product lifecycle. In addition, external cybersecurity assessments and independent security evaluations provide valuable insights into emerging threats and vulnerabilities.

Beyond cellular modules, a complete IoT solution demands scrutiny across various potential attack surfaces. Secure manufacturing of grid control edge devices, device hardening, and digital identity management through key management schemes are all essential components of a holistic security strategy. Adopting best practice operation technology procedures is extremely important in this instance. Effective device management is especially critical for long-lifespan IoT deployments, enabling secure connectivity configurations and reliable over-the-air firmware updates.

Reliable lifecycle management also is crucial for industrial IoT components, just as it is for smartphones. Cellular modules require ongoing security and configuration updates to remain protected throughout their service lifespan. A comprehensive device management platform enables remote connectivity assessments and scalable firmware updates, helping organizations maintain the integrity of their deployments.

Additionally, global mobile virtual network operators' navigating regional networks face complex security challenges. The GSMA has developed standards to accelerate eSIM remote subscription management in IoT applications. Adopting GSMA-compliant solutions for remote profile management of eSIMs enhances security and streamlines deployments. Over-the-air SIM profile management is also driving the adoption of private networks, offering greater flexibility and control.

Placing faith in reputable module manufacturers with an intimate understanding of the security challenges faced by businesses and customers who traverse regional networks becomes crucial to provide integrity, reliability, and safety of these critical components in various industrial systems.

8 | Conclusion - The Future of Smart Grids

To meet increasing power demands and incorporate clean energy sources, the electric grid is transforming into a smart grid network. Utilities need to adapt their operational and information technology infrastructure to support diverse endpoints like distributed energy, electric vehicles, and microgrids. The deployment of internet-connected sensors and actuators is crucial for real-time monitoring and optimization of the grid's performance. As the grid becomes more digitized, it also faces increased vulnerability to cyber-attacks. A comprehensive approach that includes careful cybersecurity planning, can optimize operations while staying ahead of threats to provide greater grid resilience. This paper detailed shared experiences from experts across the industry on the importance of a security-focused architecture, including smart edge devices, edge data processing, interoperating networks, and secure data flows to mitigate risks and enhance grid resilience. With collaboration, trusted technologies, and a proactive mindset, utilities can lead the charge into a smarter, more secure energy future.

Disclaimer:

This white paper is provided for general information and evaluation purposes only. The information contained herein is provided on an "as-is" basis. Anterix makes no representations as to accuracy, completeness, or validity of the information or data provided herein and will not be liable for any errors or omissions in this information or any losses, injuries, or damages arising from its display or use. This white paper does not constitute investment, legal, tax, regulatory, financing, accounting or other advice, and it is not intended to provide the sole basis for any evaluation of a transaction.