



★ Defence in Depth

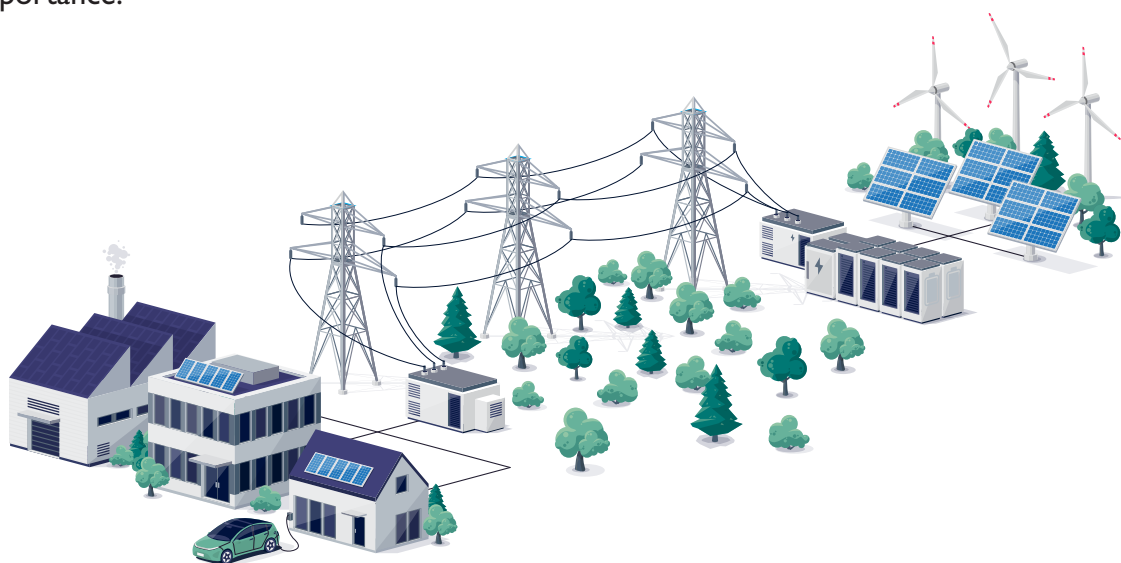
Achieving security end to end

Robust Industrial Networks

Defence in depth for the world's most demanding applications

Across the globe we are seeing strategic infrastructure owners investing heavily to improve networked resiliency and achieve greater climate neutrality. The need for more resource-efficient control and optimisation of processes has never been more pressing as we respond to the large-scale deployment of electric cars and integrations with a range of decentralised renewable technologies.

Increasing levels of integration and therefore digitalisation will result in unprecedented levels of interactions with digital assets from a large and diverse set of stakeholders. With many more distributed edge devices, the need for deeper security across devices, the network, the cloud, and connected systems has never been more critical and of more strategic importance.



Securing infrastructure in an insecure world

The surge in cyberattacks on infrastructure like power and water companies intensifies the need to take a new approach to security. The attacker who tried to poison a Florida city's water supply in 2021 was stopped by a vigilant supervisor, but [later analysis](#) of the water company's infrastructure found even more vulnerabilities that had gone undetected.

Attacks on state-owned utilities in [Brazil](#) resulted in the theft of more than a thousand gigabytes of sensitive internal data, which attackers offered for sale. The same criminals went on to disable the [Colonial Pipeline](#), which supplies almost half of the fuel needs of America's East Coast. While most of the \$4.4 million ransom paid was recovered by the FBI, it was too late to stop the panic-driven petrol shortages as motorists raced to fuel up.

Critical Infrastructure companies must be better connected than ever to deliver on their strategic objectives.

What's needed is a new approach to securing that connectivity, to deliver protection at all levels.

Pressures within and without

Infrastructure companies face pressure from more than just attackers. They must also:

- Abide by legislation, such as Europe's Network & Information Systems (NIS) Directive, which tightens requirements to secure their systems and limit damages from any attacks; fines for non-compliance can exceed €19 million
- Advance digital transformation initiatives that will support the smart grid and smart city, and improve the customer experience
- Drive efficiencies with improved remote access for authorised engineers, without leaving doors open for attackers
- Leverage their investment in extensive legacy equipment that's still fit for purpose



Defending against attack with Defence in Depth

The concept of Defence in Depth is borrowed from the military. In the context of securing the infrastructure provider's communications network, this means:

- Deploying an enriched cybersecurity architecture with multiple redundant solutions
- Using several independent methods to achieve layers of protection
- Recognising and prioritising the network's weakest point: remote assets

With Defence in Depth as its default design strategy for IT and Operational Technology systems -- from RTU to SCADA master and everything in between -- the provider can:

- Leverage automation to secure its infrastructure at scale and at pace
- Trust that individual devices can self-protect and self-isolate in the event of attack
- Integrate with industry standards and recognised cybersecurity protocols and tools

Each connected device must be capable of defending itself. This makes the WAN gateway a vital first line of defence.

Security from the bottom up: protect the weakest points

Attackers often avoid highly-defended Network Operations Centres and instead try to hijack remote assets. They may attempt to spoof their identity and modify routers that connect RTUs and other remote systems to the wide area network, and onwards to the NOC.



Self-defence for connected remote assets

Infrastructure providers are increasingly deploying hardened WAN gateways that do more than just provide modem capability and protocol conversion for the RTUs, switches, and other mechanical infrastructure across their estates. To stay ahead of cybersecurity threats and risk of financial loss, they're seeking solutions that offer microcontroller-level security, isolated cryptographic engines, and advanced capability to monitor, deploy and defend every connected device.

The Merlin series from Westermo- security from the bottom up

Developed by Westermo, the Merlin series of industrial cellular routers for remote sites are the first in the industry to feature comprehensive hardware-level cybersecurity, including:

Tamper-proof secure boot

Highly secure boot process that prevents the router from functioning unless it can validate the digital signature of the router's operating system.

Trusted Platform Module

This microcontroller-based chip keeps cryptographic keys separate from the file system. If the device is stolen, the keys cannot be retrieved. TPM also securely identifies the device to the network and supports standard cryptographic engines.

Zero-touch deployment

The router's management software is Activator, which pioneered the zero-touch deployment methodology. Manage and update thousands of devices securely from one management domain, and automate asset verification for security at scale.





Network and inventory monitoring

The router's alerting system presents the full operational state of the device and provides early warning of anomalies that could indicate an attack, such as spikes in a device's CPU activity or network traffic loads.



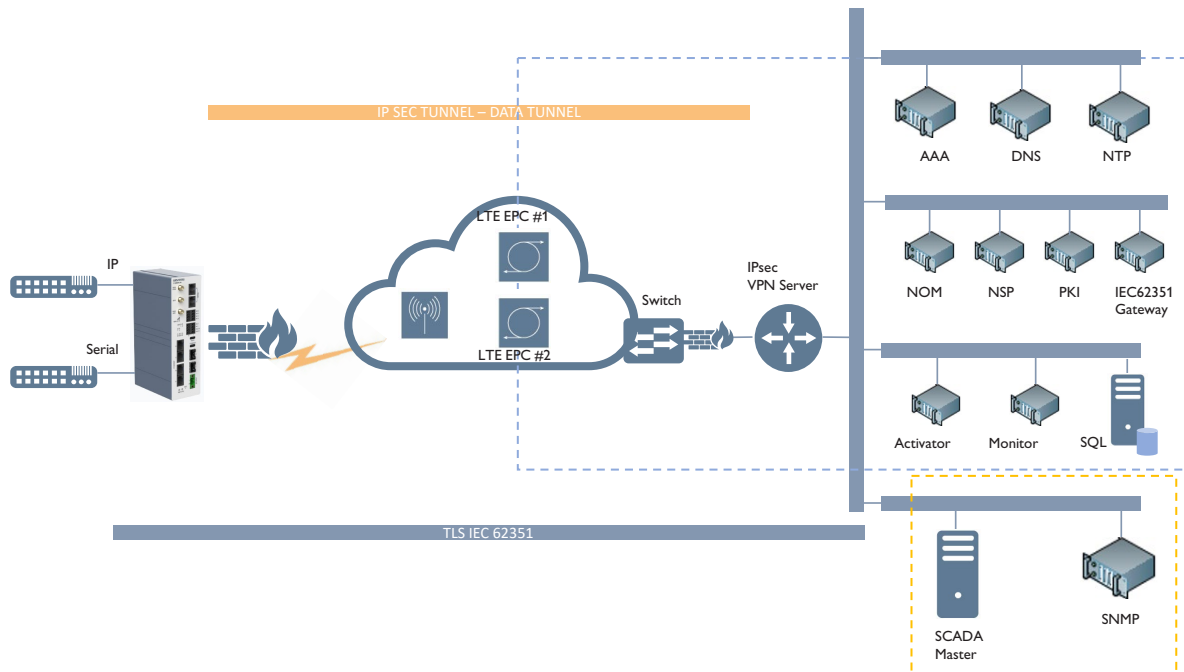
Securing end-to-end communications

Infrastructure that supports end-to-end encryption gives providers another layer to a Defence in Depth design strategy. The Merlin series simplifies encryption at scale, even in complex legacy environments, and supports the latest encryption algorithms:

-  Transport Layer Security (TLS – IEC32351-3 extension): encrypts traffic from the gateway at the remote site to the SCADA master at the Network Operations Centre
-  IP Security Virtual Private Network (IPsec VPN): provides additional security across the wide-area network for sensitive traffic
-  Supports flex VPN, Open VPN, and auto-enrolment with PKI (SCEP)
-  Private keys used for VPN are protected with Trusted Platform Module



Future-proofing for private cellular networks



As providers prepare for initiatives like the smart grid that demand more visibility and control, there's growing interest in private LTE networks as an alternative to commercial mobile networks. In a private LTE scenario, the utility operator's wireless traffic runs over a dedicated network built on spectrum allotted by the communications regulator. Private LTE also keeps sensitive information on the internal WAN, instead of using commercial infrastructure that cyber-attackers may be more likely to target.





Typically, the 450 MHz or 410 MHz spectrums are made available for private LTE. One characteristic of this spectrum is the benefit of better penetration and reach compared to the higher frequencies found in commercial LTE networks. Using LTE bands that are not normally accessible to the public ensures that sensitive information is kept separate from the public domain and provides an additional level of defence that will defeat all but the most determined cyber attackers.







Westermo and private LTE

The Activator zero-touch platform has been used to deploy large-scale utility networks for customers operating private LTE networks, in many instances scaling in excess of 10,000 sites.

Westermo customers are implementing private LTE for connectivity and control of applications including:

-  Smart grid
-  Distribution automation
-  Smart metering aggregation
-  SCADA

The Merlin series includes features designed to meet the proven needs of utilities:

-  TPM for security
-  Integrated RTU/SCADA protocols that reduce need for external RTUs and simplify large deployments
-  High galvanic isolation for longer life in electrically hostile environments
-  Support for TLS and IPsec encryption – TLS has been shown in a research study funded by the University of Strathclyde Power Networks Demonstration Centre to consume less bandwidth; useful where bandwidth conservation is a priority.



ACTIVATOR

Deploying secure boot and TPM to protect the water supply

★ Customer story

Westermo is working with a national Irish water authority to upgrade the security of its mission-critical infrastructure.

Estate

Water treatment, quality monitoring and other facilities nationwide

Challenge

Improve security of water infrastructure against cyberattack

Solution

Live demo of Merlin series illustrated:

- Secure boot (the router will only run-factory-approved firmware loaded in our facility in Ireland)
- TPM for secure cryptographic key storage

Partnership

Westermo and its access business unit is working in collaboration with a water company's consulting engineers, integrators and company engineers to deliver leading edge solutions.



About us

Westermo is a leading supplier of industrial data communications equipment to the world market. Development and manufacturing takes place in Sweden, Ireland, Germany and Switzerland. Sales are conducted through offices in key markets as well as through distributors and OEM customers worldwide. Westermo was founded in 1975 and is a wholly owned subsidiary of Beijer Electronics Group AB, listed on the Nasdaq Stockholm stock exchange.

Westermo acquired Virtual Access (Ireland) Limited in 2019 – its ruggedised equipment is designed and built for the most mission-critical applications and is trusted at scale by utilities across the globe. When strategic infrastructure owners need to deploy, manage and secure tens of thousands of devices across their distributed networks – they come to us and we deliver.

