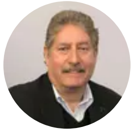
POST

LTE Networks, Interoperability, and Regulatory Requirements: Three Challenges, One Solution

image credit: © Michalsuszycki | Dreamstime.com



RONALD INDECK 1,118
CEO Q-Net Security

Ronald Indeck, PhD Dr. Indeck is the CEO of Q-Net Security, an industry-leading company protecting critical national infrastructure and government systems from cyberattack. He is also a Director...

Member since 2021 5 items added with 5,579 views

Contact

Like (1) Comme

Profile

Oct 11, 2022

173 views

This item is part of the Utility Guide to Private LTE - OCTOBER 2022 SPECIAL ISSUE, click here for more

LTE networks are an important component of modern utility systems, but they remain vulnerable to hacking, as a recent study by Checkpoint Research shows. In that study, they discovered a simple method to compromise the UNISOC chipset, which represents 11% of the global LTE market. This is concerning, especially for companies with facilities in Africa and Asia (two major growth areas) where this chipset is popular due to its price advantage over competitors such as MediaTek, Qualcomm and Apple.

While UNISOC patched the vulnerability reported by Checkpoint in May of 2022, this example highlights the vulnerability of LTE networks to attacks by threat actors, and the importance of implementing security solutions that can protect a utility network from undiscovered "future" threat vectors, as well as those that are already known about.

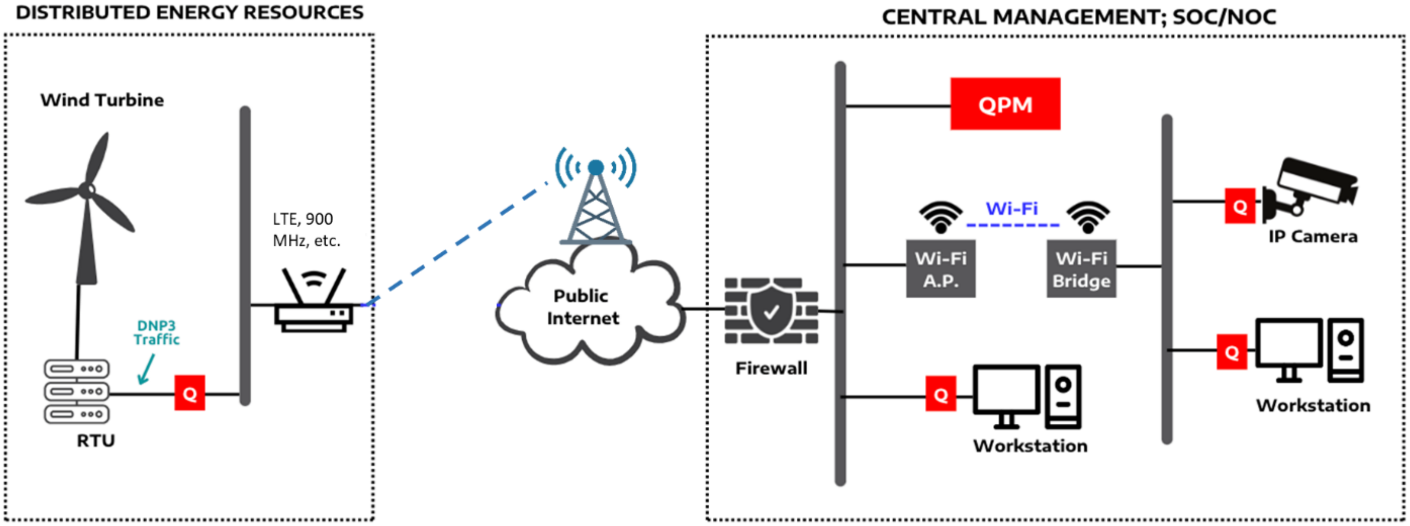
Of course, the utilities industry is not the only place LTE networks are deployed – but unlike many other sectors where a hack may cause inconvenience or cost money, attacks on critical infrastructure such as water and electricity can cost lives.

Managers of IT networks in the utilities sector are thus faced with a conundrum – pressure to implement green energy implementations are which are often remote – such as wind turbines placed offshore, where private LTE infrastructure can be a cost-effective approach to monitoring and control - conflicting with the high potential for damaging cyber-attacks. The risk of disruption is increased if communication networks are set up without implementing cybersecurity improvements that address the demands of new regulations such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA).

A third complicating factor is interoperability – while some elements of utilities infrastructure have state-of-the-art Operational Technology (OT) systems, others may consist of legacy systems that are years or even decades old, where physical devices – such as sensors and actuators – are integrated with collaborative devices, such as laptops, tablets, and smartphones. The resulting patchwork of hardware and operating systems traditionally required constant cycles of patching to stay up to date, and can open vulnerabilities, particularly as IT and OT networks overlap.

Finding a cybersecurity software solution that secures private LTE connectivity along with old and new components whilst complying with regulatory requirements might seem extremely challenging – but there is a simple solution: implement a hardware-based security system instead.

Hardware-based security measures, known as HardSec, use plug-and-play hardware endpoints to secure networks – even complex ones which use multiple communications devices to connect infrastructure of varying ages and operating systems, as shown in the figure below.



These endpoints use Field Programmable Gate Arrays (FPGAs) – circuits which cannot be hacked because there is no software for a malware program to alter. These devices provide the same AES-GCM 256 encryption as traditional software-based solutions, but in addition to being immune to malware, they require no updates, no maintenance, and can work with any operating system – even legacy SCADA devices running Windows NT and Windows 95.

The HardSec approach functions equally well across all networks, including public LTE, satellite, and the Anterix 900 MHz private LTE network. Indeed, as an Anterix ecosystem partner, the Q-Net solution has been validated as "market-ready" to provide endpoint security now and into the future – as its hardware-based solution would defeat even attacks by quantum computers.

This means that cybersecurity managers for the networks that connect key infrastructure can now leverage the advantages of a secure private LTE network, increase the interoperability of their systems, and avoid the onerous burden of reporting cyberattacks to the US government as CIRCA will require them to do – because you don't have to report an attack if it never happens.

Utilities that value reliability can’t afford the constant downtime patching requires, and certainly don’t have time for the disruption of a cyberattack. Gone are the days of tracking intruders through firewalls, IDS, and SIEMs: detecting threat actors as they’re passing through your network is no longer good enough. The future of cybersecurity lies in defense – not detection – and the only defensive solution strong enough for today’s utilities is hardware.