Omnion POWER

WHITEPAPER

SECURITY: A KEY DRIVER FOR 5G TRANSITION, AND CRITICAL ASPECT IN NETWORK AND POWER INFRASTRUCTURE DESIGN

SECURITY: A KEY DRIVER FOR 5G TRANSITION, AND CRITICAL ASPECT IN NETWORK AND POWER INFRASTRUCTURE DESIGN

By: Raj Radjassamy, 5G/wireless segment leader, OmniOn Power

When thinking about the benefits of 5G, the first items that likely come to mind are the big three – bandwidth, throughput, and low latency. And while some early adopter consumers are already using a variation of 5G on their smartphones to realize these benefits, the question of when Fortune 1000 companies might make the transition for their enterprise operations still remains.

According to our new report, "Destination 5G: How Global Fortune 1000 CIOs/CTOs Are Charting Their Course," these enterprise 5G transitions may be right around the corner. In our survey of 204 Fortune 1000 CIOs and CTOs, 83% of those surveyed have either transitioned to 5G or anticipate doing so within the next two years.

Two of the primary key criteria for enterprise transition? Security and reliability. In fact, 54% of respondents selected "increased network security" as one of the reasons they are transitioning to 5G – making it the top selected factor. Security and reliability also topped the list of the highest-priority criteria respondents are using to evaluate network providers at 30% and 21%, respectively.

SECURITY FROM THE START

In earlier wireless generations, the network providers managed the network core functions within their own central offices/mobile telephone switching offices (MTSO) and backhaul networks. However, with 5G being more "cloud-centric," the network core functions are on a remote cloud managed by a third party. The fundamental shift to cloud (or "centralized") radio access network (C-RAN) and open radio access network (O-RAN) communication architectures may, for some, imply some inherent security risks. Tampering with or intercepting cloud-based in-bound and out-bound communications versus a traditionally closed 4G network might raise a concern.

Yet, right from the initial releases of 5G standards from the 3rd Generation Partnership Project (3GPP), additional layers of security – in the form of both user authentication, identification, and location encryption – were baked in. This imperative to build a secure, distributed, cloud-based communications foundation set the bar higher for 5G infrastructure providers as well.

For power infrastructure providers like OmniOn Power, it can take a multipronged approach to address security challenges. This includes both built-in hardware protections and network communications and software protocols to enhance secure monitoring.

SECURE AND RELIABLE POWER

The first level of power security is the reliability of power conversion hardware built for robust macro cell or pole-or-post-mounted remote radio heads (RRHs).

OmniOn has drawn on its heritage of powering outdoor cellular, distributed antenna systems (DAS), and small cell wireless networks to develop the next wave of power conversion technologies for the deployment of 5G. These solutions are engineered to meet the unique challenges of 5G, whether that means withstanding harsh environmental conditions or providing compact, efficient power for small cell applications – where every inch is critical and power density is a key concern.

From the vantage of online security, today's powers solutions often feature an always-on capability via power system redundancy and battery backup.

MULTITIERED (HARDWARE AND SOFTWARE) 5G POWER PROTECTION

At the core of protecting cloud-based 5G Remote Radio Head (RRH) networks is continuous monitoring. Macrocell sites are constantly aggregating real-time data from various equipment, relaying that information to a network operating center (NOC). This monitoring offers the first line of defense to detect traffic anomalies indicating possible tampering or disruptions.

The power conversion side of this RRH protection scheme also depends on monitoring and communication between the power module, its controller, and the RRH monitoring functions. This happens on both a software and hardware level via multilayered access control and proprietary communication protocols.

The next 24 months will see the acceleration of corporate enterprise 5G deployments around the world. And with these deployments already in the early stages or on the horizon, it will be essential for network and infrastructure providers to be at the ready with solutions to help ensure reliable, secure communications and power.

To learn more about OmniOn Power's 5G solutions and services offerings, please visit https://www.omnionpower.com/end-to-end-solutions/5g.

To read the full data report, "Destination 5G: How Global Fortune 1000 CIOs and CTOs Are Charting Their Course," click here.

Mobile Europe – June 2020 – How 5G is Both More and Less Secure Than Previous Networks https://mobileeurope.co.uk/features-me/14914-how-5g-is-both-less-and-more-secure-than-previous-networks