White Paper

The Future of Power Grids

5 Trends and Their Effect on Utility Communications

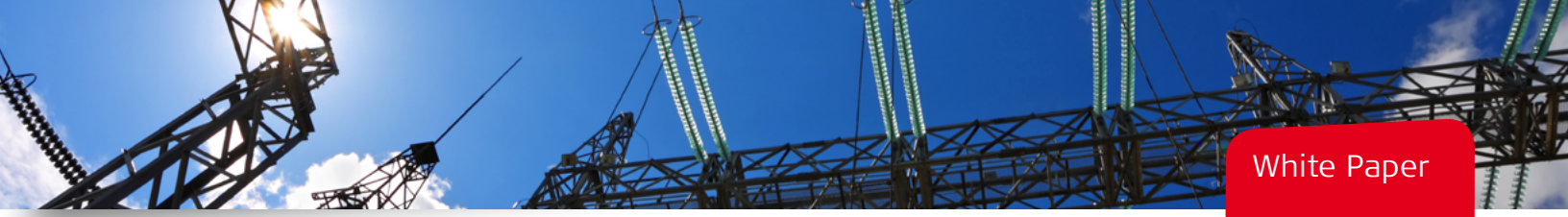
The end of an era – and the beginning of a new one

Power utility networks are becoming smarter, automated and more connected, as they gradually transform into Smart Grids. This transition is designed to allow a reliable supply of electric power to end users, improve power quality, reduce deployment, operational and maintenance costs, and comply with local security regulations. The term "Smart Grid" encompasses power and networking infrastructure, as well as next-gen services and smart applications.

Looking forward, there are several key trends that drive the design of tomorrow's utility networks – most of which are closely connected with the rise of IoT (Internet of Things) – and which need to be accommodated by adequate communication solutions.

RAD

Your Network's Edge®



White Paper

Trend #1

Migration to next-gen communications

Operators of utility communication networks are tasked with carefully executing many changes and upgrades. First, they need to replace obsolete equipment that has been in service for decades, as well as terminated leased line services by Telcos. End-of-life PDH/SDH/SONET multiplexers, for example, are no longer being supported and spare parts are not available. However, this is not a simple case of forklifting, as the underlying technologies, low-speed connections and legacy applications must be kept in service for the time being. Substantial investments have been poured into them and they will not be discarded quickly.

At the same time, there is also a need to move to packet-based technologies. Ethernet and IP have become standard within Telcos and the new generation of substation LANs (IEC 61850) relies on Ethernet connectivity. Utilities must adapt or risk having no service. These somewhat contradicting requirements are complicated further by the need to maintain absolute network and service reliability at all times. As a critical infrastructure, power grids are much less tolerant of network glitches than commercial enterprises.

Figure 1: Transitioning power utility communications networks

Trend #2

Distributed energy and renewables

Traditionally, the power grid has had a straightforward topology with a linear flow: from a small number of generation centers to a larger number of high voltage and medium voltage transformer substations, and finally, to the many consumer locations. This topology, however, is rapidly changing with the introduction of distributed resources like rooftop solar panels and energy storage systems, as well as new distribution points, such as electric vehicle charging stations. Smart new models are being implemented to better balance fluctuations in supply and demand, allowing, among others, for scenarios in which consumer-generated power flows upstream in the supply chain. In addition, renewable energy sources are now mandatory by regulation in many markets, resulting in massive amounts of intermittent wind and solar power introduced into the grid at large substations. Autonomous micro-grids and sub-networks are coming into play as well, representing yet another element in an increasingly complex scheme.

All of the above translates to large volumes of grid assets that need to be managed. To that end, proper communications with all these assets is key.

Trend #3

Automation, remote sensing and intelligent control

The drive to improve efficiencies results in new digital control devices/61850 IEDs, synchrophasors, advanced meter infrastructure (AMI), and the like that provide the "smarts" in Smart Grids and smart metering. Remotely controlling sensors and terminals helps engineers get actionable data from distributed equipment, quickly make informed decisions on capacity shifts, and optimize assets throughout their lifecycle. These live insights require machine-to-machine communications, or IoT. In its true form, IoT goes beyond merely the "connected home" and covers the entire power (smart) grid.

Trend #4

OT and IT integration

As operational technology (OT) networks for command and control of critical functions are evolving, OT platforms and IT domains are no longer viewed as discrete silos.
The need to apply data analytics and forecast trends, as well as provide enablement tools to the field force, compels the integration of OT with IT. For example, a mobile app that shows real-time power usage throughout the grid and is available to all technical staff, everywhere, must involve both operations and information technology resources. Reliable, cost-efficient communications are key to improve efficiency and accuracy, reduce errors and offer faster service restoration. Such integration must provide availability and coverage that meet OT's stringent requirements, which are typically higher than those of IT networks. This would entail, for example, WiFi-enabled vans and ZigBee hot spots with mobile high-gain antennas and roaming LTE devices for field force staff, ensuring always-on connectivity.

Marrying OT with IT, however, introduces new security vulnerabilities that did not exist before.

Trend #5

Cyber security

OT networks were primarily designed with operational safety and reliability in mind. Security was not considered a top priority and, at best, any defense employed followed the "Security by Obscurity" philosophy. These days, however, critical infrastructure networks are more susceptible than ever to cyber threats. The introduction of Ethernet and IP communications, renewables and distributed energy, IoT, and IT and OT integration means that these networks no longer exist "off the grid." Communications need to reach thousands and even tens of thousands more locations than before, creating many more possible attack vectors and attack targets. As a result, they are subjected to hundreds, sometimes thousands of cyber-attacks per day, while even the smallest breach in security could spell disaster. The first confirmed successful hacking of a power grid was the attack on the Ukrainian electricity network in December 2015, which left nearly a quarter of a million consumers in the dark.

The security of critical networks is therefore at the center of attention of industry and

government regulators alike. The first binding regulation was the set of requirements for critical infrastructure protection (CIP), which was introduced in 2008 by the North American Electric Reliability Council (NERC). Since then, the NERC CIP set of requirements has been constantly evolving to make sure power utilities are well equipped to meet new threats. Regulators in other parts of the world are also formulating their own set of directives. The power utility sector is forced to comply with new regulations, or otherwise face stiff fines.

The Impact on Power Utility Communications

In addition to the move to non-deterministic packet environments and upgrades to IP-based systems, power utility communication networks must support grid optimization and efficient demand management. They should include dedicated, low-latency links between sensors, controls and grid assets, provide constant access to real-time data for the grid's many new stakeholders, and ensure absolute reliability with redundancy and resiliency that eliminate single-point-of-failure scenarios.

In some cases, the rapidly expanding connections required and the growing number of distributed market participants involved means that utilities can no longer rely solely on their own private networking assets and must depend on third-party communications service providers. These, in turn, must adapt to provide the highest level of reliability for their services to this market segment, mostly via extended-coverage LTE. While the traffic volumes to and from each terminal might not necessarily be high, the sheer number of the newly connected devices, often housed in limited-space, remote locations and in demanding environments (e.g., extreme temperatures, electromagnetic interference, etc.), involves a completely new skill set and expertise. Power utilities' new communications solutions must provide high availability, cost efficiency, low maintenance, and extreme security.

RAD's Service Assured Networking Solutions

RAD is a leader in secure communications solutions for the critical infrastructure of power utilities. Our Service Assured Networking (SAN) solutions include best-of-breed tools for cyber security and mission-critical communications, as well as for seamless migration to modern packet switched networks and applications. RAD provides field-proven solutions for multiservice operational WAN, ruggedized substation LAN, automation backhaul, Teleprotection, and wireless PTP/PTMP. Furthermore, SAN's multi-layer cyber security ensures that your operational network remains reliable and protected at all times with a rich portfolio of defense tools, including encryption, authentication, intrusion prevention, anomaly detection and integrity verification, among others. For existing networks, RAD also offers a cyber security overlay solution, integrating RAD's award-winning SecFlow SCADA-aware routers and gateways with software from Check Point.

Founded in 1981, RAD has an installed base of more than 14 million units and is a member of the $1.25 billion RAD Group of companies, a world leader in communications solutions.

White Paper

SAN All-Stars

> Operational WAN

Multiservice Access

Megaplex-4

Service Aggregation

ETX-5

DWDM/OTN/Dark Fiber

PacketLight

> Automation Backhaul and Ruggedized LAN

SCADA-Secure Switch/Routers

SecFlow

> Wireless

PtP, PtMP and Broadband Mobility

Airmux

> Management

Planning, Provisioning and Performance Monitoring

RADview

For more information on RAD's SAN solutions for power utility communications, visit www.rad.com

Your Network's Edge®