For more than 30 years, RAD has worked closely with its worldwide energy utility customers to provide field-proven communications solutions that address the automation, Teleprotection and operational core network needs of their transmission and distribution (T&D) grids.

Service Assured Networking: RAD offers secure, reliable, scalable, managed, and performance guaranteed solutions for automation, protection, security, and ICT networking that support multiple deployment scenarios over SDH/SONET and carrier-grade Ethernet networks.

A vast array of capabilities include service provisioning, traffic management, timing synchronization, TDM pseudowire, ongoing performance monitoring, fault management, and various resiliency mechanisms.
In this era of evolving technologies, transmission and distribution utilities face a range of challenges at their high voltage (HV) and medium voltage (MV) substations. Developments in automation and Teleprotection require that old RTUs will coexist next to new 61850-compliant IEDs, Ethernet and TCP-based messaging protocols.

Core networks are migrating to packet-based technologies; fiber optics’ reach is being extended and bandwidth requirements continue to grow.

To address these challenges, substation networking and communications solutions must include support for legacy automation and Teleprotection equipment, while new IEDs and IT devices require Ethernet switching and routing functionality.

In addition, connection to the core network needs to feature cross-generation capabilities, to support current SDH/SONET/ PDH technology and newer PSNs, and finally, security threats and regulation are forcing the adoption of combined protection mechanisms in any new communications solution.
Harnessing RAD’s Expertise for Substation Communications

Our solutions for substation communications are built on RAD’s extensive technological expertise in TDM and packet-based technologies, providing the designers of new MV and HV substations with the technology and tools to address all current and future communications needs. These future-proof solutions support a wide variety of legacy and Ethernet services, as well as comply with IEC 61850-3 and IEEE 1613 standards and incorporate advanced SCADA security firewalls.

RAD’s multiservice solutions for substations meet the communication needs of various departments within the power utility and the systems they operate:

**Automation**
- RTU-to-SCADA connectivity
- Aggregation from multiple substations to control centers

**Voice**
- POTS and VoIP connectivity to a central PABX

**Teleprotection**
- Connectivity between substations
- Serial, fiber (C37.94) differential protection
- Distance contact relays

**Security**
- SCADA firewall
- Video surveillance

**ICT (Telecom)**
- Routing and networking
- IP telephony
“Hybrid” Substation Multiservice Connectivity and Migration

- Powerful cross-generation multiservice TDM and Ethernet capabilities, including TDM DS0 cross-connect and SDH/SONET, Gigabit Ethernet switching and OAM, pseudowire for TDM over Ethernet/IP, and NG-SDH/SONET for Ethernet over PDH/SDH/SONET
- Easily configurable connectivity of all serial automation and Teleprotection devices to either the existing SDH/SONET network, new SDH/SONET rings and, in parallel, to a new PSN
- Dedicated Teleprotection interfaces for differential C37.94 and distance relays
- Supports analog and digital voice and Ethernet IED, or IT devices with versatile rates from RS-232 low speed traffic up to STM-4/OC-12 or GbE
- Guaranteed smooth migration to PSNs by ongoing support for legacy devices
• Support Ethernet-based IEC 61850 substation communications for mission-critical automation traffic within the substation and between SCADA control centers
• Enable co-existence of serial-based RTUs and new Ethernet IEDs with full redundancy over various topologies using fiber optic rings, 2G/3G cellular modems and external radio systems
• Comply with IEC 61850-3 and IEEE 1613 environmental standards
• Seamless communication of the IP SCADA to both old and new RTUs by converting IEC-101 to IEC-104, or Modbus serial to IP, DNP3 and others
• Allow automation and networking departments to build their own secure, dedicated networks over fiber and/or radio links using IPSec encryption and a dedicated, distributed security SCADA firewall suite
Integrated Security and Firewall Tools for SCADA

Multiple Attack Methods Need Multiple Protection Mechanisms

While there are countless ways to attack the Smart Grid utility network, one of four generic attack scenarios is most likely to be used:

Field-to-field physical site breach
The outside high-wire attacker exploits vulnerabilities in the private-public network link using temporary access, or by physically embedding a ‘rogue’ chip into the device.

Control center malware attack
A virus or instruction file is installed (using a USB flash memory stick, network connection, serial interface, etc.) inside a control center and is used to sabotage a field device or a portion of the network. The Stuxnet virus is one example of this attack method.

"Man-in-the-middle“ attack
The attacker resides between two devices in the utility network, gaining access using a public network or cell-based connection, and is able to intercept and control network data without being detected.

Remote maintenance attack
Access is from a remote network device.

<table>
<thead>
<tr>
<th>Protection Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed protection on each end device</td>
<td>Reduces the potential for security processing bottlenecks in the network, and enables creation of application-oriented security, based on the device or network location.</td>
</tr>
<tr>
<td>Port-level access control</td>
<td>Limits access to the network using authentication rules based on MAC addresses, IP addresses and pre-defined access roles.</td>
</tr>
<tr>
<td>L2-L3 filtering</td>
<td>Encapsulates data at both data link and switching/routing layers using virtual tunnels to strip away service identifiers and other critical information that could be used by attackers.</td>
</tr>
<tr>
<td>IPSec L4 VPNs</td>
<td>Ensures that IP-level data transmitted site-to-site via public network interconnection, usually over a virtual private network (VPN), is encrypted end-to-end.</td>
</tr>
<tr>
<td>Remote technician gateway</td>
<td>Provides a standard, secure server that limits remote access to specific devices or sub-networks, and can also hide details of the local network from a remote user.</td>
</tr>
<tr>
<td>SCADA-aware firewall</td>
<td>Provides intelligent, service-level validation of commands to network devices and subsystems via white-listing or similar mechanisms. Able to be programmed logically in order to address local or proprietary process needs.</td>
</tr>
</tbody>
</table>
Additional RAD Service Assured Networking Solutions for Power Utilities

Operational Core Network Using Carrier-Grade Ethernet

Teleprotection Connectivity for Differential and Distance Relays

Distribution Automation & Smart Metering Backhaul

www.rad.com