IoT Communications over Satellite

Satellite communications provide a perfect fit for countries with limited cellular infrastructure, as well as in rural areas and difficult terrains such as over mountains. In some industries, for example shipping, satellites are the only option for ongoing communications. However, delay-sensitive applications, such as streaming, are difficult to support with satellites.

Most satellite internet services come from geostationary satellites that orbit the planet at 35,786 Km or 22,236 miles. As a result, the data's round-trip time between the user and satellite – also known as latency – is high, too high to support such applications.

Starlink satellites, on the other hand, are in a low orbit, offering a significantly lower latency of around 25~36 ms compared to +600 ms of other satellites. Starlink also provides download connection of 100-300 Mbps and upload speed of 10-25 Mbps. By delivering high-speed, low-latency bandwidth, it offers a good fit for IoT communications, and can be used as both a primary and backup link.

Other relevant points of interest include:

- Start Tracker – custom-built navigation sensors survey the stars to determine each satellite's location, altitude and orientation, enabling precise placement of broadband throughput.
- Antennas – each Starlink satellite uses 4 powerful phased array antennas and 2 parabolic antennas to provide increased capacity.
- Ion Propulsion Systems – efficient ion thrusters, powered by krypton, enable Starlink satellites to orbit rise, maneuver in space, and deorbit at the end of their useful life.

RAD

Your Network's Edge®

RAD's Solution for Encrypted SCADA Backhaul over Starlink Satellite

RAD's SecFlow IoT gateways include Starlink support to provide utility organizations with unrivaled flexibility in connectivity options, as well as advanced security, redundancy, and protection schemes.

Water and power remote terminal units (RTUs) and intelligent electronic devices (IEDs) are securely connected to the SCADA HMI over satellite and LTE connections, serving as primary and backup links. IPsec ensures IEC 61850 GOOSE and IEC-104, DNP3 data security with scalability for up to 100K IPsec tunnels. With easy configuration and various resiliency options, users can minimize downtime while benefiting from automated deployments for end-to-end service monitoring.
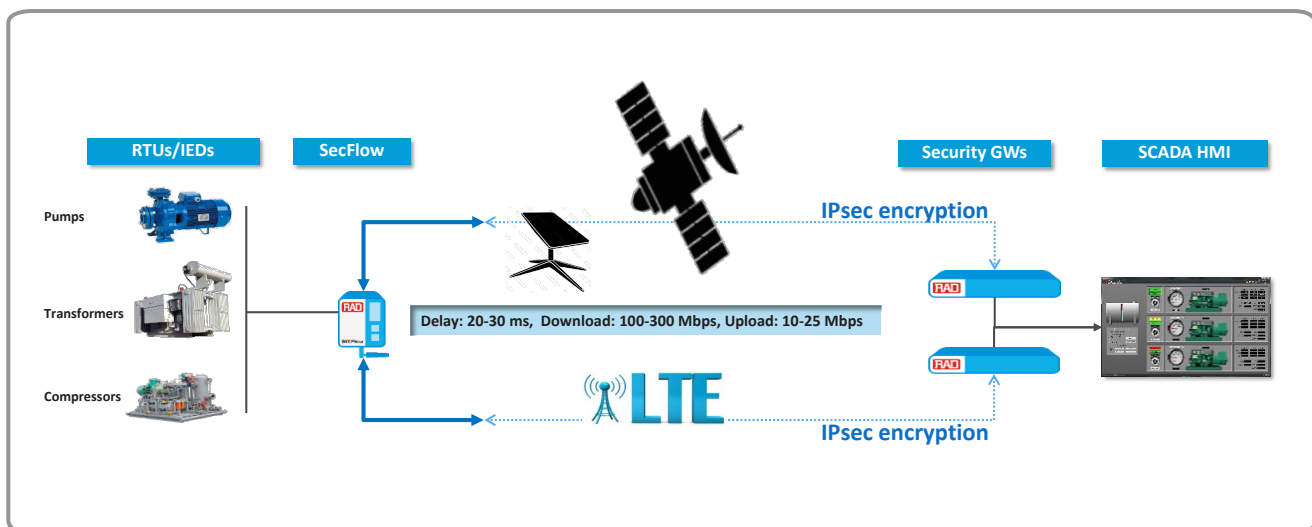

Enhanced Performance & Reliability

The SecFlow enables users to enhance performance and reliability through various mechanisms:

- **Layer 3 load balancing**: Distributing L3 traffic, packet-by-packet, over several links. The weight of each link can be configured, in case one of the networks provides lower bandwidth than the other. Packet sequencing addresses the issue of out-of-order packets at the receiving end.

- **Packet duplication**: This operational mode duplicates L3 packets and transmits them over multiple networks. In case one network loses a packet, the packet will arrive at the Multipath Gateway via another link, thereby ensuring zero packet loss. Again, packet sequencing addresses the issue of out-of-order packets at the receiving end.

- **Layer 2 over Layer 3 tunneling**: A virtual bridge in the SecFlow-1p receives packets and forwards them to the Multipath client. The client then encapsulates the L2 packets over L3, encrypts them using SSL and transmits them over the WAN link available. If the SecFlow-1p is also connected to an existing fiber network (G-PON, SDH, SONET, MPLS), the packets are also forwarded to this native interface, without a L3 encapsulation for fast transmission to neighboring substations.
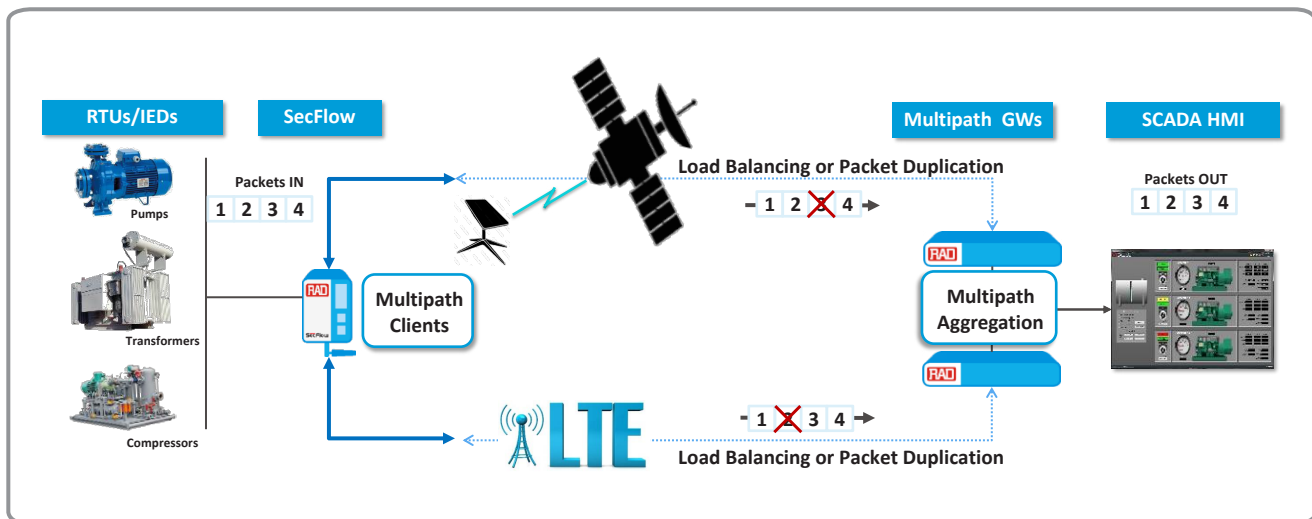
This solution therefore eliminates packet Loss and provides millisecond switchover time. Also important, the links are configured with priorities and are revertive.

Solution Highlights

- Reliable broadband IoT connectivity with low latency for very remote sites. Optional secondary link for secure mission-critical services.

- Secure backup and failover for primary LTE, copper, fiber, GPON links over Starlink satellite services, with critical service availability assurance.

- Additional security layers, such as firewall and encryption as well as load balancing and link duplication for uninterrupted services availability.

For more information on RAD's IoT solutions, contact us at market@rad.com

RAD
Your Network's Edge®