High-availability/Low Latency Wireless Communication for Protection, Control, and SCADA applications
Smart Grid Communication Applications and Requirements

Distribution SCADA & Asset Monitoring
1-2 sec reporting

Capacitor Switching
Several seconds

Distributed Energy / VPP Monitor & Control - secs 100ms disconnect

Dynamic Fault Isolation
100 ms comm. time

Smart Home – DSM
Seconds to minutes
Future: 100s of ms…
MicroGrid Control

Monitor the various Distributed Energy Resources - seconds
Execute Optimal Dispatch - seconds
Dynamically Balance Load and Generation - <100ms

All Applications Require Communications
...with varying degree of performance
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Functional Solution</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route between NICs or VPN</td>
<td>Router</td>
<td>Flexible network design options</td>
</tr>
<tr>
<td>Bridge between NICs</td>
<td>Switch</td>
<td>Support of Layer 2 environments (GOOSE)</td>
</tr>
<tr>
<td>Secure server/client, Connection</td>
<td>IPSec VPN</td>
<td>Encrypt &amp; tunnel between sites, meet NERC CIP requirements</td>
</tr>
<tr>
<td>Priority message delivery</td>
<td>Advanced QoS</td>
<td>Meet application SLA via deterministic networking</td>
</tr>
<tr>
<td>High Overall Availability</td>
<td>Redundancy</td>
<td>Improve High Availability and network up time</td>
</tr>
<tr>
<td>RS-232 Modbus, DNP, other</td>
<td>Serial Server</td>
<td>Connect into legacy install base</td>
</tr>
<tr>
<td>High Channel Availability</td>
<td>Multiple RFs</td>
<td>Choices of RF based on application and terrain</td>
</tr>
</tbody>
</table>
RF Solution Space

ISM Band (Industrial, Scientific, and Medical) ... Licensed bands an option
  • Unlicensed 902 - 928 MHz – good penetration ... other bands available
  • 30 Mile radial range ... Low Latency
  • Possible interference ... addressed through frequency hopping/blocking

Public 4G LTE, 3G (Verizon, ATT, etc.)
  • Available infrastructure
  • Operation expense
  • SLAs not available

Private LTE (Band 26) – Licensed ... announced by Verizon & Motorola
  • Large bandwidth (100Mb/sec)
  • Needs infrastructure (some cost)
  • Can be built more reliable than Public LTE

High Channel Availability Solution: Multiplicity of RF bands
Unlicensed Radio Technology Requirements

- Hybrid solution of High-performance 900 MHz Frequency Hopping Spread Spectrum (FHSS) unlicensed radio and Digital Transmission System (DTS)
- Support for low-latency MAC layer transmission (for GOOSE) for low network latency (less than 5msec one-way) with a tunable dwell time
- Data Rates of 125Kbps, 250Kbps, 500Kbps, 1Mbps and 1.25Mbps...fixed or auto-select
- Support networking features including bridging, routing, QoS (GOOSE priority), Firewalling and VPN tunneling
- NOTE: Sensitivity/range is dependent on modulation & terrain
Radio Architecture

ISM Radio

Cell NIC Multi-Provider

Wi-Fi

Serial Server

Ethernet

Switch Fabric

Security...it’s in there...
Device Security:

• Logical Port Disable (e.g. HTTP, SSH, SNMP, etc.)
• Physical Port Disable
• Stateful Firewall
• Tamper Detect ... Magnetometer
• Digitally Signed Firmware
• Secure Firmware Upgrade – via SFTP
Access and Monitoring Requirements

• User Accounts
  ○ RADIUS / AAA Log-in
• Role Based Access Control (RBAC) – 3 roles
• Secure Interface Protocols - HTTPS, SSH, SNMPv3, and NETCONF
• Audit and Logging (SNMP)
• Configuration Files and Restore Points
Performance-Based Uplink Failover

- **Uplink Redundancy**: Any two interfaces (RF or wireline) can be placed in a virtual Bond interface with one as a primary and the other as a backup. Failover can be triggered on:
  - Primary interface going down (Loss of Signal/Status Down etc..)
  - X number of packet loss on primary link
  - Latency/performance degradation on primary link

- **L3 Route Failover**: can also operate at Layer 3 by activating a backup static route in case the Radio device at the end of the primary path becomes unreachable or has a degraded performance

  Cellular network availability could be further improved by utilizing M2M MVNOs that specialize in multi-carrier failover solutions
Quality of Service (QoS)

- Quality of service (QoS) – enables classification of incoming traffic and subsequent prioritization of outgoing traffic
- Useful during congestion...
- Priority can be set via:
  - Ethertype (e.g. – IEC GOOSE)
  - 802.1a tag
  - UDP/TCP Port number
IEC GOOSE over Generic Routing Encapsulation (GRE) via IPSec VPN Tunnel

- **L2 GOOSE over GRE over IPSec** creates an encrypted point to point Layer 2 VPN. The end networks see each others as if they’re on the same “switch”...loss of Multicast property of GOOSE.
- **Packet Format for IPSec Tunnel Mode:**

![Diagram of Packet Format](image-url)

- Original Ethernet Frame
- Ethernet Header
- Payload
- IP GRE header
- Payload
- IPSec VPN Packet
- IP header
- ESP Init V.
- Payload
- ESP Trailer
- Auth Trailer
- Encrypted

- GRE Tunnel Packet
900MHz Topologies: Simple Point-to-Point to Multipoint

Device Mode: Access Point
Modem Mode: 1250Kbps
Network Name: Test

Device Mode: Remote
Modem Mode: 1250Kbps
Network Name: Test

Up to 500 remotes per AP

Works with GOOSE Multicast
IEC61850 GOOSE over ISM/LTE for DA/DG Protection Communication Architectures

Cellular Uplink
- GOOSE over GRE through IPSec VPN LTE Tunnel
- GOOSE over GRE through IPSec VPN ISM Tunnel
GOOSE Test Configuration & Performance Results

- Layer 2 GRE tunneling capabilities, able to encapsulate an entire IEC61850 GOOSE frame inside of an IP packet, and tunnel it securely using an IPSec VPN over a cellular network.

- LTE Performance
  - Congested network (Distributech): <85ms
  - Un-congested network (Dallas suburb): <35ms

- 900 MHz Performance: <5ms...consistently
900MHz Topologies: Simple Store & Forward

Device Mode: Access Point
Modem Mode: 1250Kbps
Network Name: Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Store & Forward
1250Kbps
Test

Remote
1250Kbps
Test

Up to 8 Hops Total, counting the AP

Can address long-haul / complex terrain issues
Automation of Rural Distribution Assets/SCADA

Utility Rural Assets:
- VR, RS, CAP
- Banks, Switches, Reclosers, DS

Network Range Can Be Extended to > 100 miles using Orbit’s Store & Forward
900MHz Topologies: Self-Healing Secure Mesh

Mesh Configuration

- Two methods of self-healing:
  1. **Best Available Path**: Featured above, if SAF and REMOTE modem modes are set to AUTO, upon power up each would scan channels looking for upstream SAF or AP nodes, and would run analytics to pick the path based on the most optimum paths. This calculation may take one and up to a few minutes depending on the size of the network. Upon synchronization, the algorithm runs again only when the signal to AP/SAF weakens or is lost.
  2. **First Available Path**: If a Remote or SAF’s modem mode is set to a specific mode (e.g. 1250Kbps), they will synchronize to the first available/seen synchronization node (AP or SAF), despite the fact that it may not be the most optimum path. This mode is fast, and may bring the network up in seconds.
Mobile Substation SCADA....auto-connect

Auto-switch to “best” carrier
Large Scale Networking Solutions For Utilities

- Distribution Automation
- Distribution Substation
- Transmission Substation
- Mercury WIMAX
- Licensed Narrowband
- 900MHz/Mesh
- Master Station
- Orbit MCR
- Aggregation Network
- Public Cellular Carrier
- Internet
- Cellular AMI/M2M
- AMI
- Licensed Narrowband
- 900MHz/3G/4G
- Distributed Control Center
- Internet
- Corporate HQ
- Control Center
- 900MHz
- Automation and Centralized Applications
- DRM, DMS, OMS, AMI, SCADA, CRAS, Synchronized Phasors, Network Management
- Backhaul: IP, SONET, MPLS
- Multi-Service Utility Backbone
Summary

- The combination of Traditional and Cellular technologies can provide a high-availability solution for critical communication requirements
- Multiple radio topologies are possible
- Very-low latency in the ISM band has been achieved
- GOOSE runs well over Wireless…