Summary: Network management systems have been widely accepted and implemented by the telecommunication industry, contributing to improved operational visibility and adding defense-in-depth for cybersecurity. This Secure Pathways for Resilient Communications (SPaRC) technical bulletin explores the benefits of deploying a network management system across electric utility communications infrastructure.

CONTEXT

Modern operational communication networks increasingly rely on distributed, data-intensive operations that depend on secure, high-performance networks. Many operational networks have evolved over time, expanding and updating communications technologies to support primary underlying infrastructure operations. Today, the need for communications to support electric utility operations has become the de-facto standard and is a growing dependency. Communication networks must not only deliver reliable, error-free communications for control and monitoring but also scale with updated and new operational processes while supporting high-precision timing and withstanding evolving cybersecurity threats. While firewalls and endpoint protections address perimeter and system-level risks, they often lack visibility into the internal workings of the network itself. A network management system (NMS) addresses this gap by monitoring the network and establishing a baseline of performance, which can be used as an established reference to ongoing network situations and events.

The Secure Pathways for Resilient Communications (SPaRC) program is deploying an NMS to actively monitor network infrastructure on the SPaRC network, establish operational performance baselines, and detect anomalous or malicious activity. A NMS supports both engineering and security teams by providing actionable insight into network health, performance, and potential risk exposure.
By monitoring the performance and health of network devices and communication pathways, operators can maintain a known good performance baseline and detect deviations that may signal faults or threats. These capabilities are especially valuable to operators' managing networks that consist of owned, leased, and third-party facilities in support of critical infrastructure.

NMS FUNCTIONALITY AND BENEFITS

1. Operational Benefits for Utilities

- **Situational Awareness**: Maintains real-time visibility of devices and links across substations and other field sites
- **Performance Monitoring**: Continuously tracks latency, jitter, packet loss, and throughput, which is vital for good quality-of-service communications and timing protocols like precision time protocol (PTP)
- **Fault Isolation**: Quickly identifies root causes of outages or degraded performance
- **Proactive Maintenance**: Detects trends before failure occurs, enabling preventative actions
- **Capacity and Asset Planning**: Understands link utilization and resource load to inform upgrades and refresh cycles
- **Documentation and Visualization**: Generates live topology maps and maintains device/configuration inventories

2. Cybersecurity Benefits

- **Defense-in-Depth**: Provides internal monitoring to complement perimeter controls
- **Anomaly Detection**: Alerts on rogue devices, port scans, unauthorized access attempts, or abnormal traffic patterns
- **Event Correlation**: Supports integration with Security Information and Event Management (SIEM) tools to unify operational and security visibility
- **Incident Response**: Expedites isolation of compromised devices or segments during an event
- **Compliance Support**: Assists with the North American Electric Reliability Corporation's Critical Infrastructure Protection and other regulatory audit requirements

3. Strategic and Cost-Effective Management

- **Reduced Downtime**: Minimizes time-to-resolution during faults or cyber incidents
- **Unified IT/OT Monitoring**: Supports the convergence of information technology and operational technology network operations
- **Future-Ready Infrastructure**: Enables smoother integration of distributed energy resources, substations, and smart grid components

---

SPaRC RECOMMENDATION

SPaRC recommends electric utilities and other infrastructure operators implement an NMS that supports open protocols such as SNMP, syslog, and flow-based telemetry (e.g., NetFlow, sFlow). Integration with timing and control system metrics (e.g., PTP offset and delay) can provide deeper insights.
When properly configured, an NMS helps ensure secure, resilient, and high-performing communications pathways—the foundation of modern grid operations.

NEXT IN THE SERIES Upcoming bulletins will provide implementation examples for configuring the NMS to do the following:

- Establish Internet Protocol Service Level Agreements to determine baseline performance
- Determine alerting strategies and dashboard design (NetFlow)
- Establish PTP synchronization performance metrics
- Establish primary and secondary configurations for failover
- Monitor unauthorized access attempts and abnormal port usage

For more information, visit https://securecomms.ornl.gov or contact SPaRC@ornl.gov.

The SPaRC (Secure Pathways for Resilient Communications) program is sponsored by the U.S. Department of Energy and executed through a multi-laboratory testbed to design, evaluate, and support next-generation secure grid communications.

The U.S. Department of Energy's SPaRC program is leading grid communications research and development through a multi-national lab virtual testbed, created to design, test, evaluate, and benchmark next-generation secure communications architectures and technologies. A secure communications system protects the end-to-end physical pathway that transports data from origin to destination. That pathway may involve different transmission methods, such as optical fiber, copper wire, and wireless technologies, and will transport a diversity of data, including grid state information and control messaging in a variety of analog and digital formats. Securing this end-to-end communications pathway, which is essential for reliable grid operations, involves preventing unauthorized access as well as monitoring traffic to identify anomalous activity without compromising the confidentiality, integrity, or availability of the data. Communications security methods complement the cybersecurity approaches used to protect data at the origin and destination. Key SPaRC activities include the grid communications test bed, next-generation communication experiments, and education and technical assistance. For more information see: https://securecomms.ornl.gov/