Microwaves&RF

MEIR BARTUR, CEO, Optical Zonu, www.opticalzonu.com

How to Supervise and Monitor RF-over-Fiber Links

Even as RF over fiber (RFoF) technology provides secure, resilient, long-distance data transmission, it's a technology that's short on standards. Learn how to get the most out of RFoF links on a network-wide basis through effective supervision and monitoring.

As telecommunication networks become more advanced at an ever-greater scale, the supervision and monitoring of equipment is vital for optimizing performance, detecting and resolving faults promptly, and ensuring proactive maintenance. In response, digital networks have built a significant and standardized infrastructure around industry-based protocols called Simple Network Management Protocol (SNMP) that enables network-wide supervision.

However, unlike other equipment in a telecommunication network, RF-over-fiber (RFoF) links aren't standardized. RFoF is a technique of converting RF into lightwaves for secure, resilient, long-distance data transmission *(Fig. 1)*.

RFoF links can build upon the basic infrastructure, but they require special attention during implementation across various use cases. Effective supervision also supports cost management by identifying inefficiencies and guiding informed decisions about upgrades or modifications, ultimately ensuring the seamless operation and longevity of those networks.

It's imperative that network managers have the appropriate capabilities to allow for easy supervision and monitoring at all levels. When working with RFoF equipment, these critical capabilities must be built from the ground up with the connectors to enable such monitoring and control.

The Layers of RFoF Supervision and Monitoring

A telecommunications network is a complex system of hardware with different levels of supervision and monitoring. Ideally, operators want a proper setup *(Fig. 2)* for every network component at all levels, which is easier said than done.

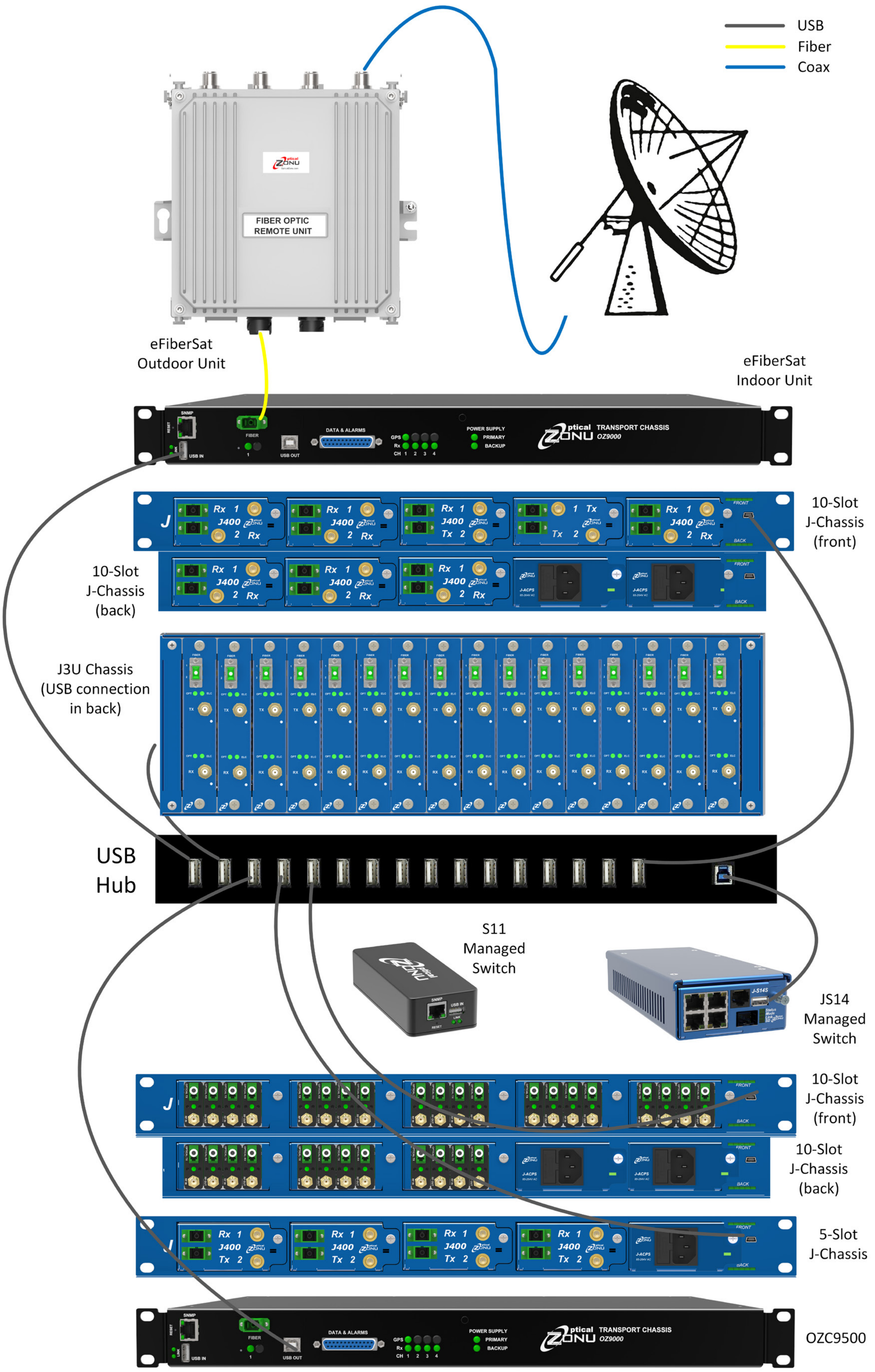
The different levels include:

- *Internal architecture:* The goal is to ensure all components and subassemblies are built with access to all key physical parameters and warning/alarm levels, and they're interconnected so that a single point interface per box can access all of the information and control all relevant parameters.
- *Device-level ("box") monitoring:* These are monitoring capabilities embedded into the hardware devices themselves, observable to any end-user at the proximity of the hardware, such as alarms, beepers, lights, and so on.
- *Local access:* Local access refers to the ports on the devices (i.e., "box") themselves that can directly connect to a computer, such as a USB, and open a web or graphical user interface from within the telecommunication room.
- *Remote connectivity:* Operators must have the ability to diagnose device performance, view alerts, and deal with other issues from a remote location. This can be done using private network connectivity or SNMP.

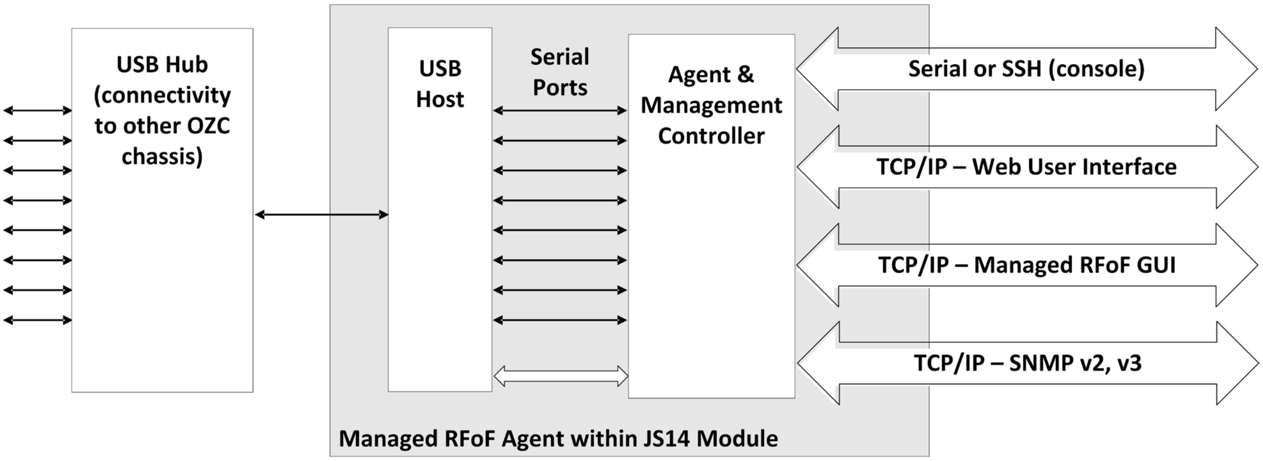
The Requirements for Effective RFoF Supervision and Monitoring

Across the different layers of supervision and maintenance, network operators should desire a few crucial capabilities while monitoring their networks at little cost to the organization. Because the C-suite of an organization doesn't always appreciate the bells and whistles of their network infrastructure, low cost becomes key. Such capabilities include:

- *Real-time status:* This entails the ability to receive immediate and up-to-the-moment information about the operational condition and performance of networks and devices. It involves continuously monitoring various parameters and metrics in real-time, granting operators and administrators instant visibility into the health and functionality of the network.
- *Preventative warnings:* Operators should receive proactive alerts and notifications generated by monitoring systems to signal potential issues or irregularities in the telecommunication network or devices, whether it's a capacity planning, threshold, maintenance alert, or oth-



1. Shown is an example of standard RFoF infrastructure for proper supervision and monitoring.


USB Hub (connectivity to other OZC chassis)
USB Host
Serial Ports
Agent & Management Controller
Serial or SSH (console)
TCP/IP – Web User Interface
TCP/IP – Managed RFoF GUI
TCP/IP – SNMP v2, v3
Managed RFoF Agent within JS14 Module

2. This depicts an RFoF supervision and monitoring workflow setup for network operators.

ers. These preemptively address problems before they escalate into critical issues, helping telecom operators or administrators take corrective actions in a timely manner.

- *Troubleshooting:* Systematic process of identifying, isolating, and resolving issues or problems within a computer network to restore normal network operation and minimize downtime. Network monitoring plays a crucial role in this process by providing real-time data, alerts, and insights that aid in diagnosing and resolving problems efficiently.

Implementing Supervision and Maintenance of RFoF Links

Because RFoF is typically deployed across complex networks delivering bidirectional RF signal flow to multiple points via star or star-ring hybrid configurations, "best practice" design must be implemented across the network-management architecture. It's equally important to ensure the supervision and maintenance capabilities of these devices are simplified without a compromise to the data availability and control features. Below are the key points to building such a system.

Internal subassemblies must gather all relevant information, enable control, and be centrally accessible

It's critical to build a bus configuration where all internal modules (whether plug-in or built-in) are reporting and being controlled via a unified structure. This is because obtaining isolated data from each separate module prevents operators from seeing the bigger picture of their network. It's also painstakingly tedious.

Devices should have USB (or equivalent) access

On the device layer ("box"), every RFoF network device, receiver, transmitter, and switch should be equipped with built-in USB connectivity that can access all of the internal data sources and control registers. Multiple boxes can be linked via a USB hub that's connected via a single USB connector to a management agent. The agent should also have a web server interface (Web-UI), full SNMP compatibility, and an internal engine for its specialized graphic user interface (GUI). This gives operators remote access to a chart-based view of various diagnostics or of physical alarm behaviors as they appear *(Fig. 3)*.

Devices should not use an IP address per device ("box")

In digital networks, every switch has an SNMP connector that enables computers to connect to the device from the internet, locally or remotely. However, this is extremely limiting for RFoF operation managers who are unable to see alerts and diagnostics across every link because source and destination aren't collocated in one place. Therefore, each one has a unique IP address.

Addressing this problem typically requires the tedious task of configuring each component to a single IP address, which can sometimes total in the hundreds depending on network size. Also, each must be mapped to a specific link. Some RFoF products instead consolidate the diagnostics and alert data for multiple transmitters, RF optic amplifiers, detectors, and other sources onto a single IP address via a communication bus so that managers can collect, view, and control all of the data in one place.

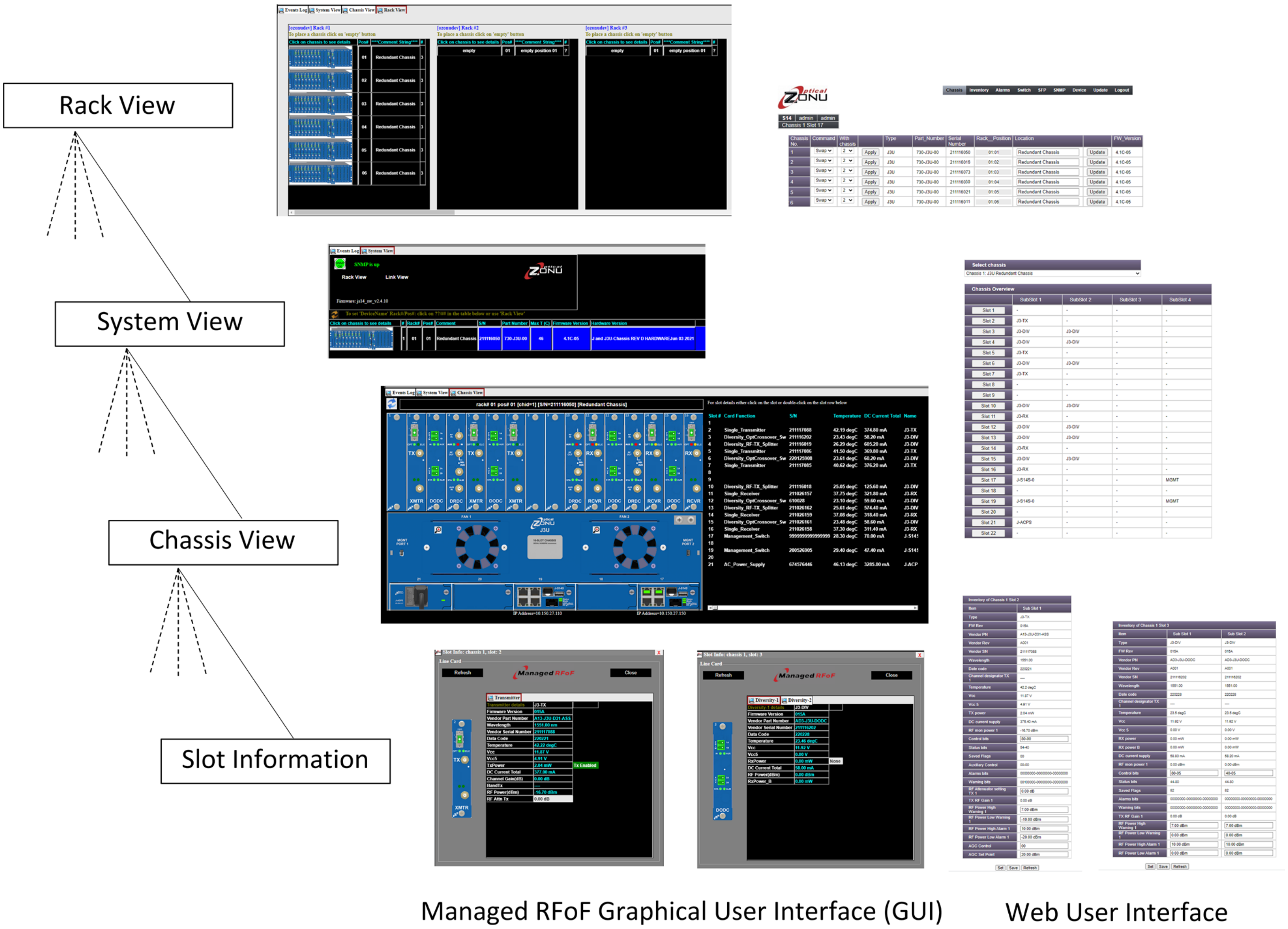
Devices must be equipped with fiber fault detection

Aspects of RFoF that not everyone is ready to address are breaks, cracks, disconnections, or other damage to the fiber lines themselves. Therefore, it's important that RFoF devices used in the network come embedded with optical time-domain reflectometer (OTDR) fiber fault detection. It can send high optical power pulses to detect any disruptions with the fiber, accurate to a few meters, for quick remediation of the issue.

While some OTDRs are handheld and pluggable, there are significant benefits to having a pluggable module that can be placed in networks as they grow, or retroactively in existing networks.

Create a network management system (NMS)

Even if all network devices are funneled to a communication bus and monitored via a single IP for a specific location, there's a need to view multiple links to multiple locations, which necessitates multiple IP addresses. For example, a



3. Here's an operator's view of a RFoF graphic user interface (GUI) and web server interface (Web-UI).

network manager overseeing a global network of data centers requires something even better to collectively manage RFoF over multiple distant locations.

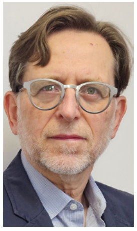
It's important to have a cloud-based network-management system capable of recognizing all products, enable mapping, and provide drill-down capability to individual sub-slots. That way managers can look at multiple systems and devices simultaneously and see what's going on in large deployments. In a wireless network environment, for example, a manager remotely adjusts gains to achieve the ideal level of RF signal amplification between the two ends.

Ask the Right Questions About RFoF Supervision

Oftentimes, the main reason network managers don't have proper supervision and maintenance of their telecommunications network is a lack of understanding about what's available to them and how simple it can be when asking the right questions of their OEM or integrator. By having the different layers and capabilities of supervision and maintenance on standardized components, as well as non-standardized components like RFoF, network operators can ensure that their telecommunications networks have the proper oversight.

Meir Bartur, Ph.D, is the President & CEO of the Optical Zonu Corporation. Dr. Bartur has over 30 years of experience in leadership, product development, and technology innovation. As a Senior Member of the IEEE and recognized leader in the development of low-cost fiber-optic

solutions for FTTx, he contributed to the IEEE ITU PON standards.



Before founding Optical Zonu, Dr. Bartur directed Advanced Product Development and Strategic Technology for access transceivers at MRV Communications (MRVC), as well as business relations with its major clients. Prior to that, he held posts as VP of Engineering & Technology at SSDI (Solid State Devices Inc.), VP of Engineering at MEC (Molecular Electronics Corp), and Systems Engineering Captain in the Israeli Air Force.