Accelerating Network Transformation

Modernizing the Communications Networks Used by Power Utilities

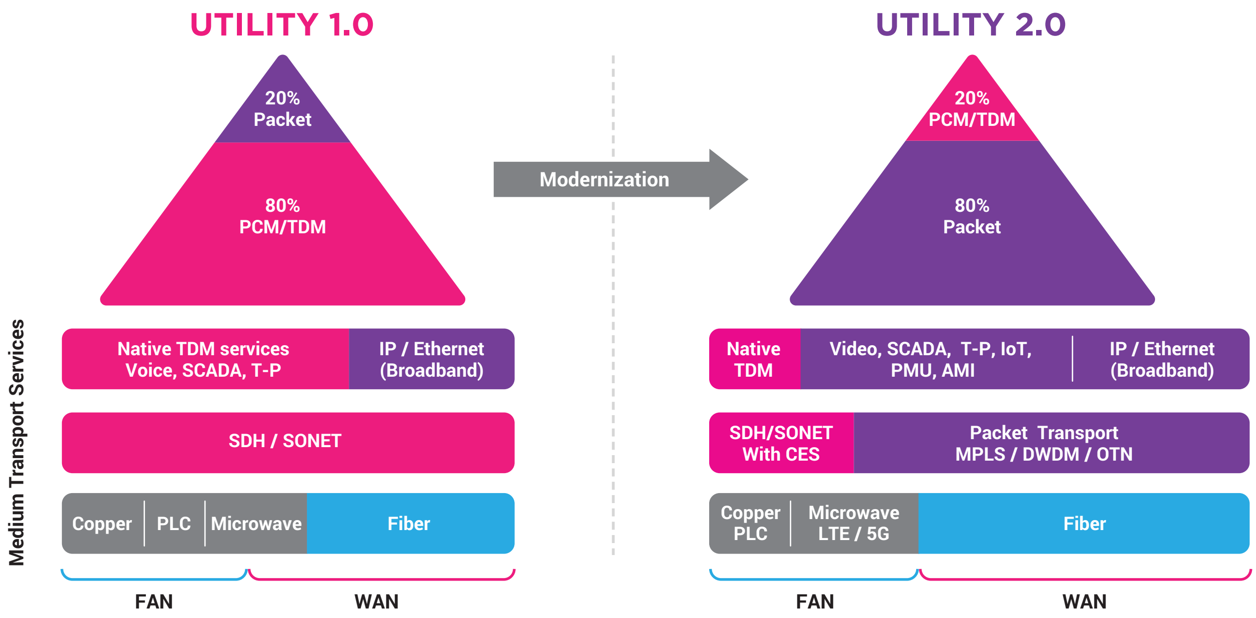
Solution Overview

Contents

1 Why Modernize the OT Communications Network

Power utilities urgently need to modernize to meet the 3Ds of Digitalization, Decentralization, and Decarbonization, transforming into what is being called Utility 2.0. To achieve this, they must evolve into a "Smart Utility" encompassing Smart Grid, Smart Meters, Smart Energy, and Smart Security. This transformation requires Operational Technology (OT) to provide vastly increased amounts of real-time information about the performance of the power network. To achieve this, we see mass rollout of new, packet based, smart devices such as sensors, actuators, Intelligent Electronic Devices (IEDs), and CCTV and to support the widespread deployment of these new "smart devices," the OT communications network must also be modernized.

The Field Area Network (FAN) needs to be expanded to reach all new devices. The existing FAN network is based on point-to-multipoint radio and wireless mesh networks (both narrowband and broadband) such as LoRa, as well wireline networks such as PLC, OPGW, ADSL, and GPON wireline networks. This network will be supplemented and eventually replaced by new wireless technologies.



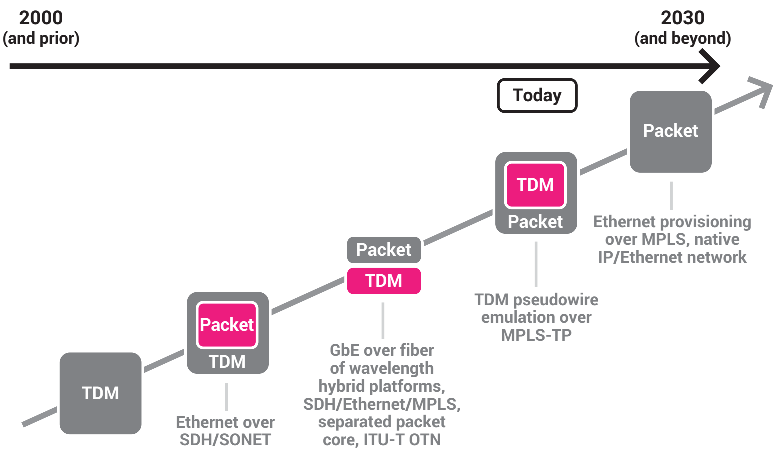
The Wide Area Network (WAN) in Utility 1.0 uses an SDH/SONET transport network to provide deterministic performance, extensive OAM capabilities, and high reliability. However, SDH/SONET was not designed to support the packet-based services and devices or the bandwidth needs of a power utility evolving to become a Smart Utility 2.0. A modern Packet Transport Network (PTN) is required to support these new services and devices, meet the bandwidth requirements, and support all the various FAN network topologies.

Fortunately, migration to packet transport using Circuit Emulation Services (CES) in conjunction with MPLS-TP is well-proven and provides the low latency, high availability, and determinism required for mission-critical OT applications and services.

In the rest of this document, we will focus on how the legacy SDH/SONET transport network can be migrated into a Packet Transport Network (PTN).

1.1 Evolving Approach to Supporting Packet

Over the past two decades, we have witnessed a gradual evolution in the communications infrastructure used in the OT network. At the beginning of the millennium, the introduction of packet services marked the start of 2nd Generation SDH/SONET and packet services were mapped onto the SDH/SONET network using Ethernet over SDH/SONET (EoS). By 2010, IP and Ethernet had become more widespread, and utilities began to see the benefits of transporting packet services natively with MPLS. This led to the introduction of hybrid platforms capable of supporting SDH/SONET/Ethernet/MPLS natively.



Today, we see the growing need to retire the SDH/SONET transport network and move all the OT services onto a packet transport network (PTN) capable of supporting both modern packet services as well as legacy PCM/SDH/SONET services. In the PTN, legacy services are mapped into packets by using standardized circuit emulation technology (CES/CEP), deterministic packet transport techniques such as MPLS-TP are used to ensure OT services are transported across the network to meet their stringent performance requirements.

1.2 A Packet Transport Network for Power Utilities

To achieve seamless migration, a modern Packet Transport Network (PTN) used by the OT network in critical industries must seamlessly support both legacy and modern packet-based services and applications for the subsystems it supports, such as SCADA, substations, CCTV, and Integrated Control Systems (ICS). To achieve this, the PTN must support multiple packet networking techniques, such as MEF 3.0, L2 VPNs, L3 VPNs, and EVPN and it must seamlessly integrate both packet and optical transport layers to meet the performance and bandwidth requirements imposed by a modernized OT network.

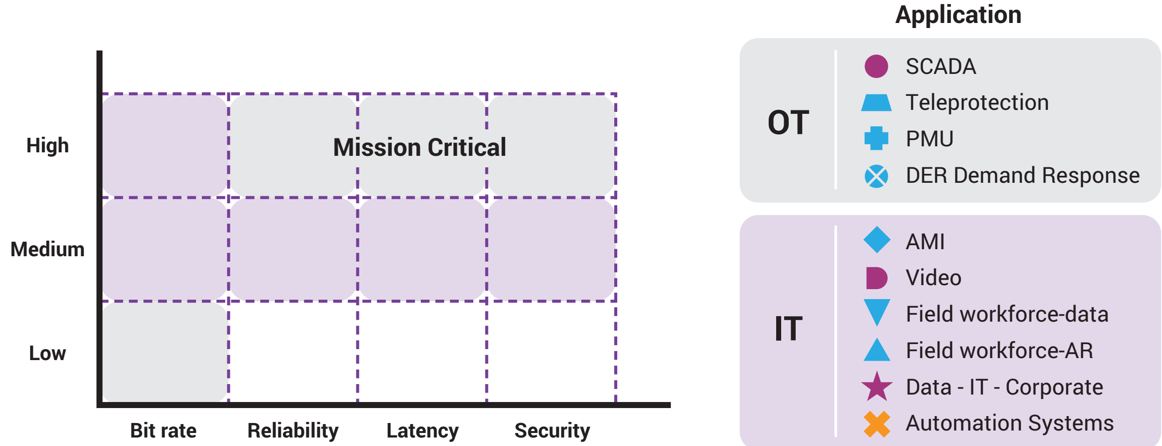
Power utilities have fundamental requirements that go beyond those of a standard PTN, these include:

- **Evolution to a Packet Transport Network**
  - **Risk-free migration:** This requires the right technology and processes and the ability to tailor the migration approach and timeline to meet specific operational and business needs
  - **Support for legacy devices:** Allow graceful migration by providing continued support for legacy devices alongside new ones on the same network.
  - **Guaranteed Network Performance:** Provide deterministic low latency, low jitter, bi-directional traffic paths, guaranteed restoration paths, and availability.
  - **Simplified Operations:** Ensure network performance meets operational requirements.
- **Support for Power Utility Evolution:**
  - **Continuous Network Evolution:** Able to support new services and technologies as they are introduced.
  - **IT/OT convergence:** Meet the service requirements of both IT and OT networks while segregating IT services from OT services.
  - **UTelco Evolution:** Provide the multitenancy capabilities to allow operators to offer “telco services” either as bandwidth wholesalers to Service Providers, or even as Service Providers themselves.

2 Choosing the Right Packet Transport Network Technologies

The power utility must consider its current and future business and operational needs when selecting the technology they require for their Packet Transport network (PTN), for example both IT/OT integration and UTelco evolution have a large impact on the technology required.

Operational Technology (OT) and Information Technology (IT) applications in power utilities mandate distinct performance requirements from their transport networks. Many OT applications are mission-critical and require strict performance guarantees for latency, jitter, reliability, and security, necessitating deterministic packet transport. Whereas the IT network applications and UTelco services can range from business-critical to best-effort and require modern, dynamic, IP/MPLS technologies.



2.1 Packet Technologies

2.1.1 IP/MPLS for IT Applications and UTelco Services

IP/MPLS was introduced to simplify the routing of IP traffic across the network. It routes traffic based on a Label Switched Path (LSP), which is built and calculated by label distribution protocols (LDP) such as MPLS-LDP, BGP, or RSVP-TE. Recently, segment routing (SR) has emerged as an alternative to LDP for identifying LSPs.

IP/MPLS offers several benefits:

- **Standardized services:** IP/MPLS supports many service types such as corporate voice, broadband, operational voice, video, SCADA, telemetry, using L2 VPNs, L3 VPNs and MEF services, including point-to-point (E-LINE), point-to multipoint (E-TREE), and multipoint-to-multipoint (E-LAN) on a single converged network.
- **Quality of Service (QoS):** IP/MPLS can assign QoS parameters, such as frame delay, jitter, and packet loss to each service-type transported.
- **Reliability:** IP/MPLS has a set of mechanisms to help minimize packet loss and ensure high-service reliability. IP MPLS can distribute traffic across LSPs to provide superior load balancing, this reduces congestion and improves network predictability. MPLS Fast Reroute (FRR) enables service restoration with SONET/SDH-like protection times of less than 50ms, although it cannot be guaranteed for all network topologies and conditions.

- **Service management:** Service management allows network operators to roll out, maintain, and troubleshoot their services in a cost-effective and timely manner. MPLS OAM tools complement the Ethernet link OAM (IEEE 802.3ah) and service management OAM (IEEE 802.1ag and ITU-T Y.1731) tools to create a multilayer OAM solution.
- **Scalability:** IP/MPLS supports a high number of service instances by supporting multiple services on each LSP. Bandwidth provisioning for each service is tailored to the needs of the customer at each site. MPLS-enabled services scale geographically, because they can be provisioned over multiple MPLS-based carrier networks. New options, such as pseudowire switching, help scale Ethernet services over several networks.
- **Support for multiple topologies:** IP/MPLS supports all network topologies, like mesh, ring, hub, star, dual homing.
- **RSVP-TE:** Supports bandwidth allocation and the reservation of resources across the network. RSVP-TE consumes lots of CPU resources and is complex to operate.
- **SR-TE:** Provides a simple, automated, and scalable architecture to engineer traffic flows in a network. It imposes a segment list consisting of a series of Node-SIDs and/or Adj-SIDs at the ingress router, to provide a traffic engineering capability (SR-TE) that is highly scalable. Uses a SR Path Computation Element (SR PCE) to compute a constraint based end-to-end path.

2.1.2 Deterministic Packet Transport for Mission-Critical OT Applications

MPLS-TP was specifically created and standardized to provide the deterministic behavior required to replace SDH/SONET networks. It is strictly connection-oriented and uses a Network Management System (NMS) instead of IP forwarding or a control plane. To achieve this, MPLS-TP takes IP/MPLS and adds connection-oriented capabilities to meet the deterministic behavior provided by SDH/SONET networks. It also removes some complex IP/MPLS functionalities that are not relevant to, or inhibit, deterministic packet transport.

With MPLS-TP, power utilities have the deterministic packet transport they need to support their OT applications:

- **Full control:** MPLS-TP management “looks and feels” like SONET/SDH, making migration from TDM to Packet less complex. A centralized NMS is used to route the traffic, ensuring it meets the strict Service Level Agreements (SLAs) required in the OT network. Separating the data plane and the control plane increases network resilience and security.
- **Pre-planned Protection Paths:** For applications such as SCADA and teleprotection, sub-50ms protection switching to a protection path with the same latency, jitter, and round-trip delay as the working path is mandatory. This is achieved by using pre-planned protection paths, this is similar to SDH/SONET.
- **Bi-directional Data Paths:** MPLS-TP uses the same data-plane mechanism as IP/MPLS. However, it employs bidirectional Pseudowires (PWs) and Label Switching Paths (LSPs) instead of the unidirectional PWs and LSPs used in IP/MPLS.
- **Mission-critical class OAM:** MPLS-TP supports extensive Operation, Administration, and Maintenance (OAM) capabilities, similar to those in SDH/SONET. These include enhanced Fault Management, Performance Monitoring, and in-band PW/LSP/Section OAM levels. The OAM functions are an integral part of the MPLS-TP data plane and are independent of the control plane. Therefore, troubleshooting in an MPLS-TP network is fast and easy to perform.

2.2 Optical Networking Technology

As power utilities evolve, they are introducing smart grids, deploying advanced metering infrastructure (AMI), implementing end-to-end asset management, and adopting bandwidth-intensive applications like video surveillance, augmented reality and artificial intelligence (AI). These modernized applications are driving an exponential increase in the bandwidth required to run the OT networks. Additionally, architectures are changing to allow this data to be stored and analyzed in real-time, with power utilities using data centers supported by low-latency communication systems to achieve real-time management of their OT infrastructure.

Many utilities currently rely on leased lines or first-generation optical networks. However, neither of these approaches can scale economically to meet the power utilities' modernization needs. Leased lines incur high monthly costs which continue to rise as new interfaces and increased traffic are added, and the utility has no control over their data communications network. First-generation optical networking systems cannot support new service interfaces or increased traffic without major upgrades, and they were not designed for this purpose. Upgrading these systems is essentially throwing good money at unsatisfactory band-aid solutions.

Often, the best approach is to introduce a brand-new optical networking system that can quickly pay for itself through facility consolidation and operational efficiency. Additionally, for power utilities aiming to become UTelcos, an optical infrastructure is a key asset which can be leveraged for wholesaling capacity, providing managed wavelengths, or serving as the bandwidth foundation for broadband backhaul and 5G xHaul.

An optical solution suitable for power utilities must be mission-critical grade and offer multiple degrees of flexibility and programmability, this includes:

- **Spectrum:** Support the flexibility offered by FlexGrid.
- **Line rates:** Software-controllable modulation schemes, baud rate, and flexible grid channel width optimized to the line rate and distance — from 50G to 600G, with 50G increments.
- **Client interfaces:** Support multiple types of client interfaces, extending to 400GbE for the most data-intensive applications, including long-haul and metro applications.

- **ROADMs:** An extensive ROADM portfolio enabling end-to-end, all-optical routing and automated wavelength restoration (WSON).
- **OTN switching:** Provides an optional layer of flexibility for rapid provisioning, wavelength grooming, and automated service restoration (ASON).
- **Alien Wavelength Support:** Allows other vendor optical wavelengths to be transported.
- **Layer 1 encryption:** Available to secure mission-critical OT communication traffic as required, can also be offered as a value-added service if operating as a Utelco.

2.3 Network Timing Considerations

In general, power utility OT networks are managed by controlling the 50Hz frequency, requiring a high degree of accuracy achievable only with a precise time reference. For instance, identifying fault locations is done by analyzing timestamped measurement values, preferably with accuracy at the 100ns level. As the timing becomes less accurate, it becomes harder to pinpoint fault locations.

The traditional approach in power industries for achieving a high degree of timing accuracy is to deploy timing networks which are separated from the data communications network. For example, the IRIG B protocol uses coaxial cables to carry timing signals directly between the IRIG B clocks. However, as OT networks become increasingly complex and interconnected, the need for precise time synchronization across the entire network has significantly increased. The IEEE 1588 Precise Time Protocol (PTP) has been standardized to provide this increased level of synchronization. It addresses the Ethernet latency and jitter issues in packet networks by time stamping the packets. With this timestamping approach 1588 PTP can achieve an unprecedented level of accuracy, between 10ns and 100ns.

Some grid applications, such as RTU and relays, require synchronization of the time-of-day (TOD) across devices. Other applications require precise frequency alignment between devices, known as syntonization. IEEE 1588 also provides the best solution for both scenarios.

2.4 Network Management

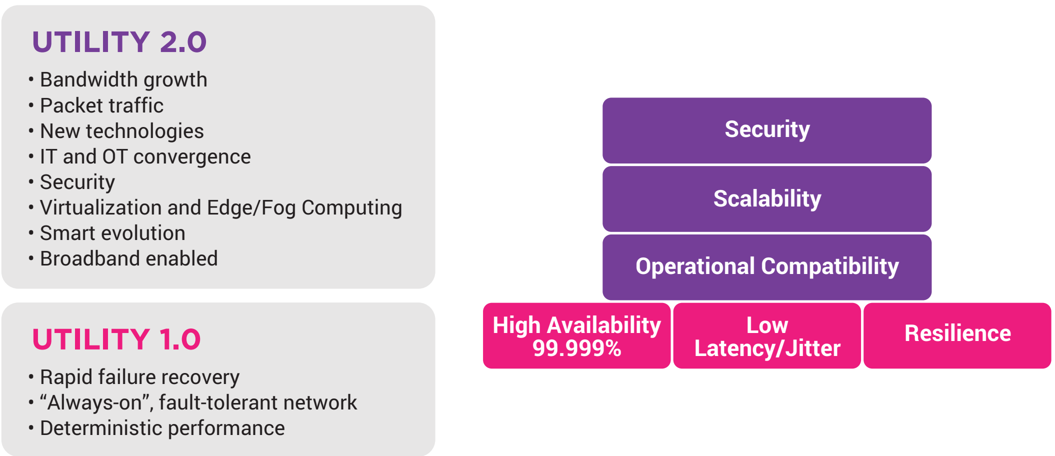
Today's IT and OT networks are increasingly complex, requiring network operators to simply operations with intuitive Network Management Systems (NMSs) able to provide end-to-end management of the network. Power utilities require a network management systems able to:

- Reduce or even eliminate manual provisioning errors
- Provide alarm management and fault localization
- Provide network performance monitoring with threshold crossing alerts (TCAs)
- Provide network health monitoring ASON, WSON, and MPLS LSP
- Support network restoration schemes, such as
- Provide multi-layer management across Packet and Optical layers
- Provide simple integration into the wider OSS/BSS ecosystems used by power utilities
- Provide geographic redundancy of the management system itself

In addition to the basic NMS functions above, advanced network analytics are key to providing the power utility with precise, real-time information about the status of their network. Analytics capabilities should include monitoring and reporting on network utilization, SLA compliance and flag potential problems before they affect services.

3 Risk-Free Migration Strategy

Modernizing the communication network is a major investment with potential risks. It is therefore essential to have a modernization strategy, approach and architecture before starting any modernization project. This strategy should address the business, operational and architectural needs, looking at the short, medium, and long-term goals and defining the timelines for each.



A network transformation strategy must identify how the utility will modernize, providing a phased migration roadmap, defining network investment and skills development. This migration roadmap must identify the operational compatibility required, defining how the new technology will be introduced alongside the existing technology and how the operations of the modernized network can continue to be evolved to meet evolving operational and business requirements. It must show both the functional and geographic scalability required to meet the ever-expanding number of network devices and associated FAN and the ability to scale to meet future operational or business requirements. Finally, it must identify how network security and integrity can be maintained and enhanced during and after the migration. This approach ensures the delivery of required capabilities at each step of the roadmap, while providing the framework for the operations staff to adjust to new requirements and technologies.

3.1 Operational Compatibility

Ultimately any migration will result in a packet transport network (PTN) comprising of a packet layer seamlessly integrated with an optical transport capability (this could be just optical pluggables in the packet transport devices OR more likely a separate Optical Transport Layer), The operational compatibility required during the migration is dependent on the migration approach and timeline. There are three main migration approaches used for migration:

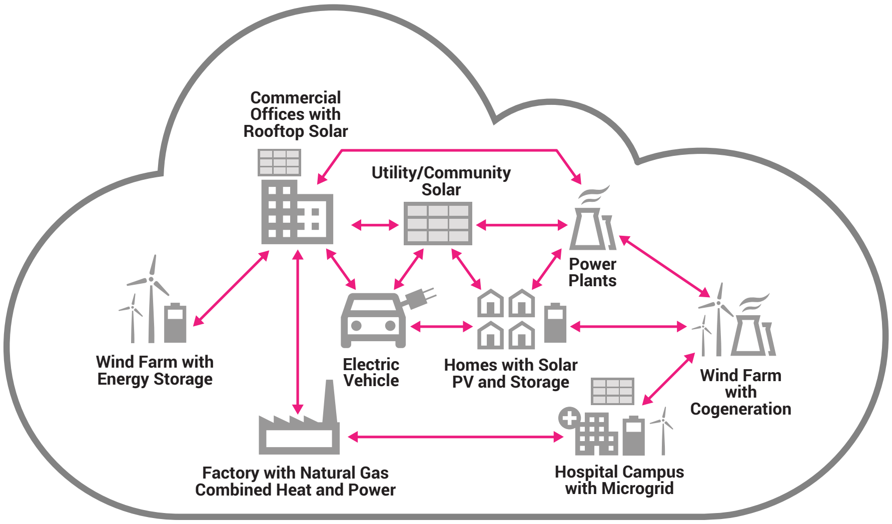
- **Full Migration (PTN Migration)** involves building a packet transport network (PTN) alongside the existing SDH SONET network. New packet-based services/applications are supported on the PTN, and legacy services/applications are migrated onto the PTN using circuit emulation. Once all legacy services/applications have been migrated the SDH/SONET network can be retired
- **Phased IP Approach (IP Overlay)**, involves building a packet transport network (PTN) alongside the existing SDH/SONET network to support new packet-based services/applications. The SDH/SONET network can only be retired when all legacy services/applications have been phased out or a full migration process run.

- **Phased Optical Approach (OTN Overlay)**, involves building a DWDM OTN network as an overlay to the existing SDH SONET network. High-order SDH/SONET tunnels/trails are migrated onto the new OTN, and packet aggregation elements are added to support new packet-based services/applications. Once all high-order tunnels/trails are migrated, the high-order SDH/SONET network can be retired. The low-order SDH/SONET network remains in place until legacy services are phased out or a full migration process is run.

Any IT/OT and Utelco strategy will influence the speed at which a fully functional PTN is required and hence the migration strategy selected.

3.2 Scalability

As power utilities are evolving to meet the 3Ds of Digitalization, Decentralization, and Decarbonization, they are mass deploying new packet based, smart devices such as sensors, actuators, Intelligent Electronic Devices (IEDs), and CCTV to create the energy supercloud.



Not only is the number of devices increasing, but these new packet also based devices are driving the PTN to scale across multiple dimensions:

- **Geographic footprint:** Increasing further into the network with devices such as AMIs, EV charging stations and remote DER devices. To support this increased geographical footprint, it must be straightforward to support the FAN expansion to support these new devices.
- **Capacity:** New devices required by the modernized power utility such as surveillance cameras, synchro-phasers and smart meters means the PTN must seamlessly scale as new bandwidth hungry devices are added to the power utility OT network
- **Functionality:** DERs, AMI networks, EV charging stations, teleprotection, powerline monitoring systems, IT/OT convergence and Utelco evolution are driving the need for the PTN to evolve from a simple Layer 2 packet transport network to become a fully-fledged Packet transport network able to support a full range of Layer 2 and Layer 3 services.

3.3 Security

Cyber-attacks on power utilities have shown that it is possible to infiltrate OT systems via IT networks and gain control of critical systems such as SCADA. These attacks have also revealed that hackers can reside within the system for extended periods, remaining undetected while waiting for the optimal moment to launch an attack. It has become evident that legacy OT systems are particularly vulnerable, with recent high-profile attacks using highly sophisticated malware targeting specific SCADA RTUs and operational software.

To address these vulnerabilities, a robust cybersecurity approach is essential. This approach should employ a 'defense in depth' model, incorporating multiple layers of cybersecurity to provide overlapping protection:

- **Improved Asset Control:** Implement desktop hardening, antivirus software, and whitelisting to secure assets.
- **Enhanced Data Security:** Use encryption at all levels to protect data.
- **Advanced Cybersecurity Management Controls:** Utilize tools and processes to monitor systems and networks, ensuring continuous compliance with cybersecurity standards and addressing potential threats.
- **Substation Protection:** Deploy SCADA-aware Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
- **Application Security Mechanisms:** Provide security at the application layer with mechanisms such as firewalls, IDS IPS, Remote Access Services (RAS), and Network Address Translation (NAT).
- **User Access Controls:** Manage access to sensitive systems and data to ensure only authorized personnel have access.

A modern communications network brings a range of tools which help power utilities improve their cyber security and system integrity:

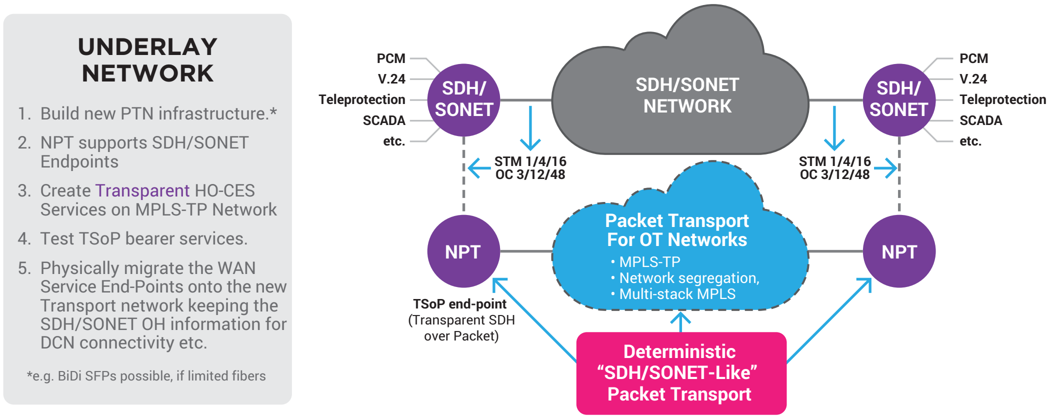
- **Secure communication links:** Transport Layer Security (TLS) cryptographic protocols protect intersystem links, ensuring privacy between the communicating entities. This includes links between network management and networking equipment, and remote databases. Additional capabilities are IP port blocking and requiring special authorization for remote sessions.
- **Hardened operating system:** Protect against misuse, including disabling unnecessary system services, added levels of user authorization.
- **Database security:** Securing local and remote access to management and control databases. This is achieved by using credentials which restrict user access to specified applications and operating system domains. For added security, aliasing is available, which hides the database connection string details from data- source definitions.
- **Geographic redundancy:** Solutions such as Remote Database Replication (RDR), provides disaster recovery backup recovery. RDR is configurable for a wide variety of topologies for different geographic infrastructure distribution and security needs.

- **Development security:** Selected vendors must adhere to secure software development lifecycle processes. This includes automatic static security code analysis on manufacturer in-house and 3rd-party software. This must also include analyzing any open-source components for possible security vulnerabilities.
- **Platform security:** Operates at a system level, independent of users and network operators. It hardens communication links and the underlying operation systems against improper use or hacking and ensures data integrity.
- **Encryption:** Can be applied at all layers of the network from Layer 1 to Layer 3. The range of encryption mechanisms available should be able to meet the needs defined in a risk vulnerability assessment. These can range from optical encryption and MACSec and should include advanced encryption key management capabilities such as QKD (Quantum Key Distribution)
- **Point of Access Security:** The network should provide a range of tools which allow it to be secured at the point where it connects to the Field Area Network. This includes Firewall and IDS/IPS, but power utilities should also consider SCADA Anomaly Detection (SAD) to ensure the SCADA network is operating as expected
- **Network Segregation:** The network should provide a range tools which allow the network to be segregated, this can include VPNs and network slicing techniques

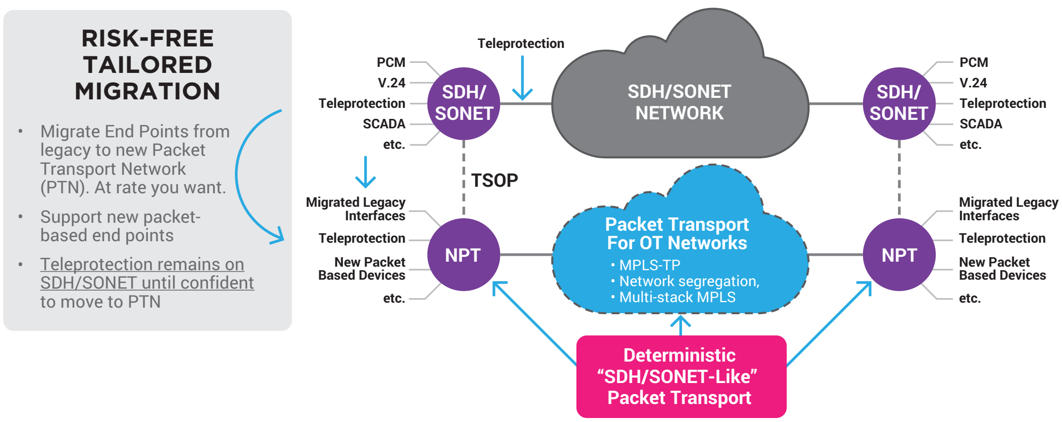
4 Risk-Free Migration

Power utilities require risk-free migration for migrating their legacy services onto the Packet Transport Network (PTN). A proven, phased approach is shown below.

Risk-free migration - STEP 1: Build Packet Transport Network



Risk-free migration - STEP 2: Move Client End-Points



4.1 Utelco Evolution

Power utilities have several unique capabilities that make evolving into a Utelco, offering telecom services, an interesting proposition.

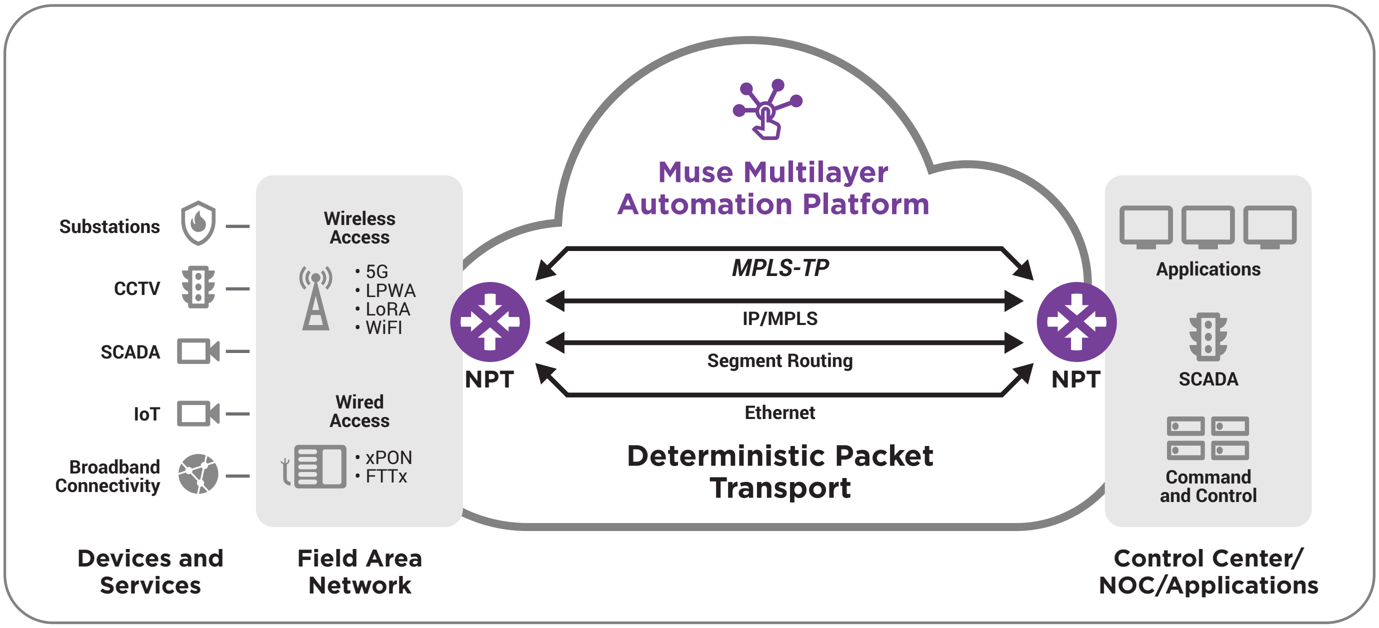
- **Rights of way:** They are authorized to lay fibers across the country.
- **Infrastructure:** The same infrastructure and equipment (fibers, towers, switches/routers, transmission equipment) that support the utility's operation, and which in many cases is underutilized, can be leveraged for developing a telecommunication business. Additionally, utilities have established B2B and B2C relationships and infrastructure for billing and customer service.
- **Knowledge:** The know-how and ability to build, operate, and maintain a telecom network is already in place, acquired while managing the network for the utility's internal services.
- **Finance:** The utility's parent company can finance the process of Utelco evolution.
- **Competitive landscape:** The status of the telecom services, the level of competition, geographical coverage, and existing room for an additional player also play a role. For example, 5G networks demand lots of fiber and network capacity and introduce new business models, applications, and revenue stream.

5 Ribbon's Solutions for Power Utilities

Ribbon is a global leader in providing critical industries with the field proven, tailored technology and processes they require to migrate their OT transport networks from SDH/SONET to PTN. Ribbon's PTN solution provides critical industries with the flexibility to evolve their transport networks to meet changing regulatory, operational, and business demands.

5.1 Key Elements of Ribbon's Solution for Power Utilities

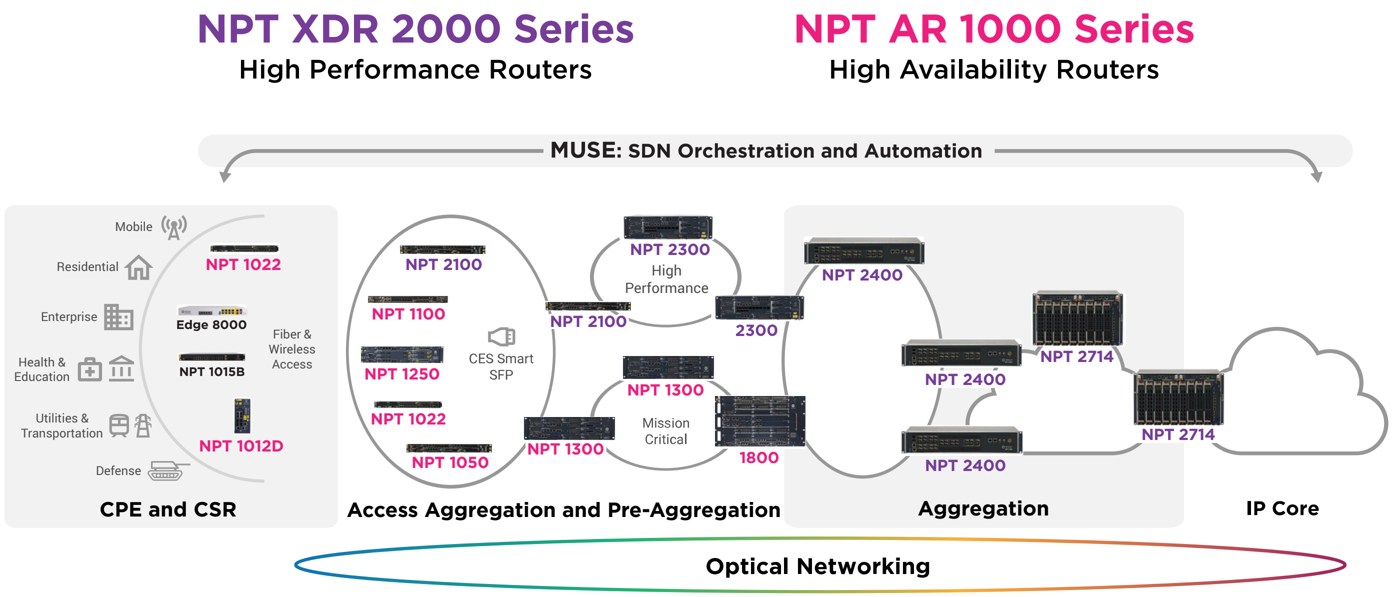
5.1.1 Ribbon's Multi-stack MPLS



Multi-stack MPLS provides critical industries with the comprehensive multi-protocol support they need for seamlessly integrating both new and legacy operational technology (OT) services and devices. Multi-stack MPLS provides critical infrastructures with the routing protocols they need to make IT/OT convergence and Utelco evolution straightforward:

- **MPLS-TP:** Essential for deterministic packet transport, MPLS-TP supports mission-critical OT services such as SCADA and teleprotection. In conjunction with Circuit Emulation (CES), it facilitates a smooth transition from SDH/SONET networks, as recognized in the Cigre Green Books. MPLS-TP also delivers all the OAM and centralized management capabilities provided by the legacy SDH/SONET networks.
- **SR-TE:** Provides deterministic transport in IP/MPLS networks, though it is not yet a widely field-proven technology for OT networks. Multi-stack MPLS allows critical infrastructures to evolve their MPLS-TP networks to SR-TE, if they decide required.
- **IP/MPLS:** Ideal for non-mission-critical services, such as IT networks and for critical infrastructure companies evolving into UTelcos.
- **Network Slicing:** With a toolkit of hard and soft slicing techniques, network slicing provides critical infrastructures with the strict segregation they require for IT/OT convergence. It also provides the multitenancy needed for critical infrastructure companies transitioning to UTelcos.
- **Future Evolution:** Ribbon's multi-stack MPLS simplifies the addition of new protocols as they become standardized, ensuring future readiness.

5.1.2 Ribbon’s NPT Access and Aggregation Routers



Modern Interface Support
- 10GE/25GE/100GE/400GE
- 10/100/1000 Base-T
- PoE+
- CWDM, DWDM
- 100G/200G/400G Coherent
- Timing: 1PPS, 10MHz, GNSS ANT, ToD and BITS (8273.2 Class C)
- FlexE

Legacy Interface Support
- FXO, FXS
- 2 wire, 4 wire, E&M
- V.24 Transparent, Synchronous Asynchronous (RS232)
- V.35/V.11, V.36/RS422/RS449
- C37.94
- 64K Codirectional
- Dry Contact
- CEP, SAToP, CESoPSN
- E1/T1, E3/DS3
- STM-1/OC-3, STM-4/OC-12, STM-16/OC-48, STM-16/OC-48

Ribbon NPT routers support all the packet transport needs of OT, IT, and UTelco networks, providing:

- Extensive support for the legacy PCM and SDH/SONET interfaces required by Critical Industries
- Support for the full range of modern interfaces used by in both the OT and IT networks
- Multi-service access routers able to support TDM, L2VPN, EVPN, L3VPNs
- High capacity/multi-tera core routers required in the Core of the network
- The advanced synchronization required in Critical Industries and to support 5G
- The network segregation technology required to support both IT/OT convergence and the multitenancy required in any evolution to Utelco
- Form factors which scale 8G to 14T
- High availability with fully redundant hardware form factors
- Support for redundant architectures such as dual-homing and LAG

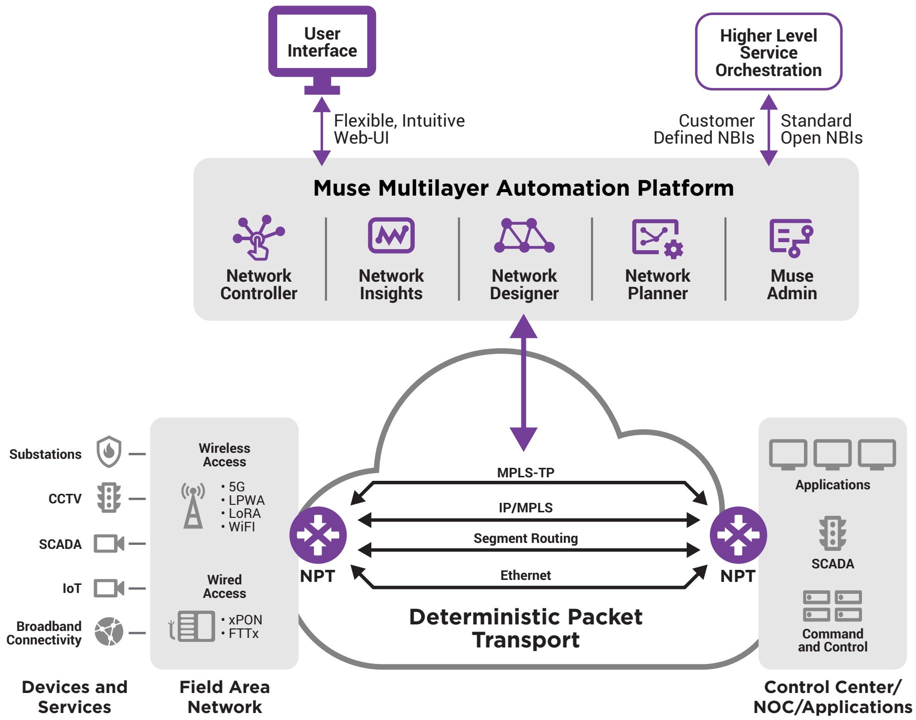
5.1.3 Apollo Optical Networking

Apollo is a cutting-edge optical networking system. Designed to meet the unique demands of critical industries, Apollo's pay-as-you-grow deployment model, high availability, and robust security offer the reliability and flexibility critical infrastructures require as they modernize their OT transport networks.

Key Features

- **Optical Encryption:** Apollo's optical encryption utilizes AES-256 encryption and adds no latency to the traffic. Notably, Apollo offers the unique capability to selectively encrypt or leave unencrypted individual services on the same wavelength, this provides utilities with complete control over their traffic.
- **Optical Failure Survivability:** Apollo provides sub-50ms protection switching. Survivability can be further enhanced by incorporating ROADMs to dynamically re-route wavelengths around network failures.
- **Layer 1 Multiservice Support:** Apollo supports Ethernet, Fibre Channel, legacy SDH/SONET, and various video interfaces.
- **Smooth Migration:** Entire networks can be seamlessly transitioned to an Apollo network within a few hours. If required, Apollo can also transport other vendor optical wavelengths as an alien wavelength.
- **Rapid Fault Localization:** Apollo, together with Muse, pinpoints fiber cuts to within a few meters. When paired with a GPS module, this feature enables critical infrastructures to dispatching repair crews to the precise fault location, minimizing truck rolls and accelerating maintenance activities.

5.1.4 Powerful SDN domain controller



COMMON CRITERIA
CERTIFIED
EAL2

Ribbon's Muse Multilayer Automation Platform provides the intuitive management and control which critical industries require to operate their Packet Transport network. Its multi-layer network visualization offers comprehensive lifecycle management capabilities such as planning, provisioning, alarm management, fiber health management, and performance monitoring. With these advanced tools, Muse eliminates manual provisioning errors, enables rapid and accurate fault localization to minimize maintenance truck-rolls, and ensures continuous network monitoring to meet all performance requirements. Using modern, industry-leading cloud-native techniques, Muse provides a powerful workflow engine, the ability to easily integrate into the wider OSS ecosystem, and a high-availability clustered deployment.

5.2 Security

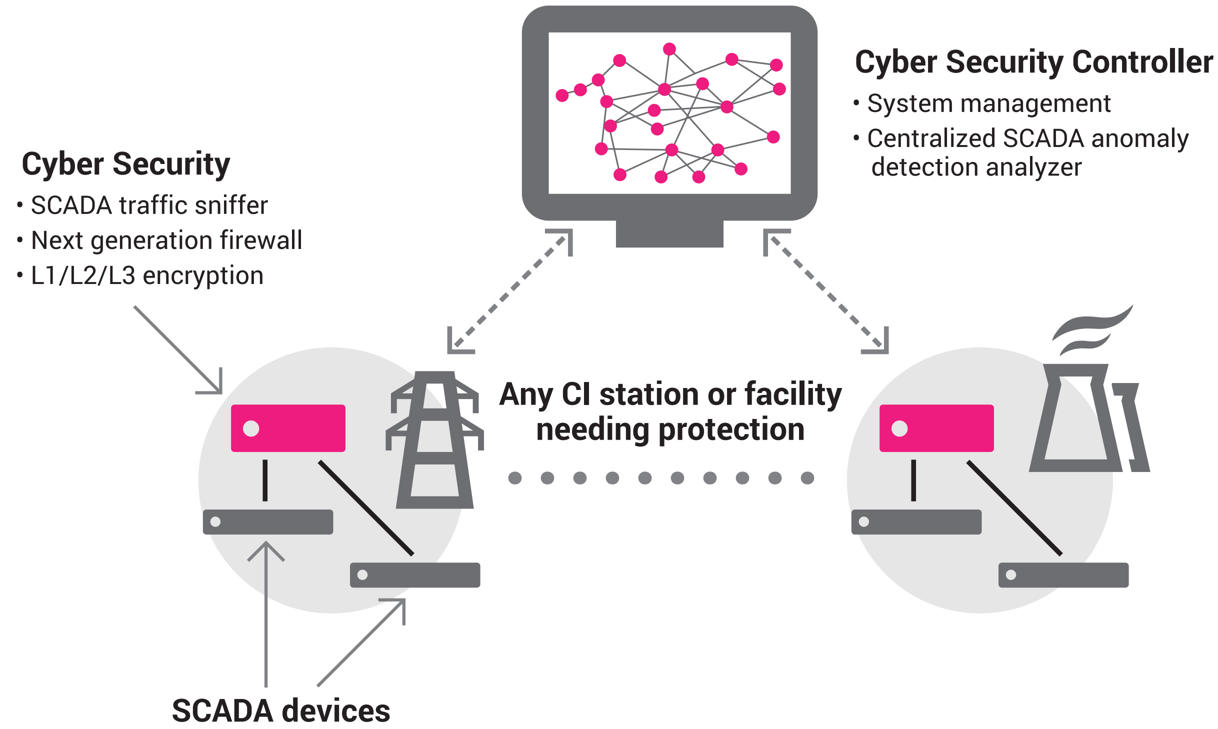
Ribbon's IP Optical PTN for power utilities is designed with multiple layers of security, extending from management systems to the network equipment itself:

- **User Security:** Ensures that only authorized users can access the Ribbon management and control systems by providing:
  - **Authorization and Authentication:** Centrally-administered RADIUS, TACACS+, Kerberos, or LDAP-based applications, with the option for two-factor authentication.
  - **User Profile Management:** Role-based access control (RBAC).
  - **Enhanced Security Items:** Features such as login attempt monitoring with lockouts, activity filtering, monitoring, and logging.

- **Platform Security:** Operates at a system level to harden communication links and underlying operating systems against improper use or hacking:
  - **Secure Communication Links:** Transport Layer Security (TLS) cryptographic protocols protect all intersystem links in Ribbon's IP Optical solutions.
  - **Hardened Operating Systems:** Methods include disabling unnecessary system services, adding levels of user authorizations, and implementing special measures like firewalls, IP tunneling, VPNs, RAS, and NAT.
  - **Database Security:** Access to management and control databases is secured both locally and remotely. For added security, aliasing is available.
  - **Geographic Redundancy:** Utilizes a field-proven Remote Database Replication (RDR) mechanism for flexible redundancy.
  - **Development Security:** Ribbon employs a secure Software Development Life Cycle process.

- **Networking Security:** Ensures that only authorized users can access the Ribbon management and control systems.
  - **Layer 1 Optical Encryption:** Provides AES256 encryption and is fully FIPS104-2 Level 2 certified.
  - **IP Routing and Packet Transport Network Security:** Includes Access Control Lists (ACL), MACsec encryption, VPN security, Port-based Network Access Control (PNAC), Broadcast Storm Control, and Dynamic ARP inspection.
  - **Security Isolation through Network Slicing:** Utilizes a toolkit of hard and soft slicing technologies.
  - **Comprehensive Security Ecosystem:** Employs best-in-class security capabilities such as SIEMS, IDS, IPS, and SCADA anomaly detection to build a comprehensive security ecosystem.

- **Power Company SCADA and OT Network Cyber Protection:** enables power companies to defend against various attack vectors on their OT and SCADA networks, including man-in-the-middle, lateral, and zero-day attacks. Economical run-time platforms, deployable at any CI facility, consolidate cybersecurity functions and prevent attacks before they can cause harm. These platforms and their functions are managed centrally, providing SOC personnel with early warnings of anomalies and impending attacks.

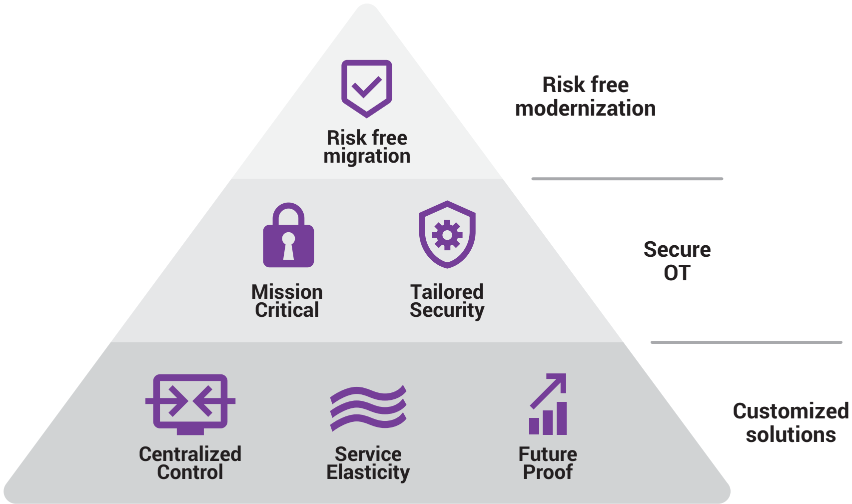


5.2.1 Integrated Solutions

Ribbon offers comprehensive turnkey services for power utilities, with the flexibility to integrate third-party capabilities into our IP Optical solutions:

- **Microwave Wireless:** Ribbon supports a variety of microwave systems, with management seamlessly integrated into our Muse SDN orchestrator.
- **Power Solution Packages:** Our solutions range from classic DC-power to full multi-source and backup solutions. Ribbon provides a series of building blocks to create tailored solutions that meet specific needs of power utilties, including custom-made power and telecommunications racks.
- **Full Site Management:** We offer complete site management for our equipment, including all the necessary sensors to ensure the site is secure, monitored, and climate-controlled.
- **Shelters and Cabinets:** Ribbon provides mission-critical grade shelters and street cabinets for situations where space is limited, or new site deployments are needed. These solutions include all site sensors, air conditioning, heat exchange, and power systems.

5.3 Proven Risk-Free Migration



Ribbon offers a comprehensive suite of field-proven products and processes, drawing on over 20 years of experience in helping customers evolve their networks. NPT's unique, multi-stack MPLS combined with Circuit Emulation (CES) capabilities and robust, customizable migration processes enable critical industries to confidently migrate their legacy SDH/SONET networks. The resulting packet transport network is agile enough to meet future needs while maintaining support for legacy interfaces as long as necessary. With a modern PTN in place, Ribbon's multi-stack MPLS facilitates continuous evolution, allowing the network to transition from simple Layer 2 and MEF services provided by MPLS-TP and Carrier Ethernet to newer services requiring SR-TE, EVPN, and Layer 3 VPN.

Contact Us Contact us to learn more about Ribbon solutions.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.