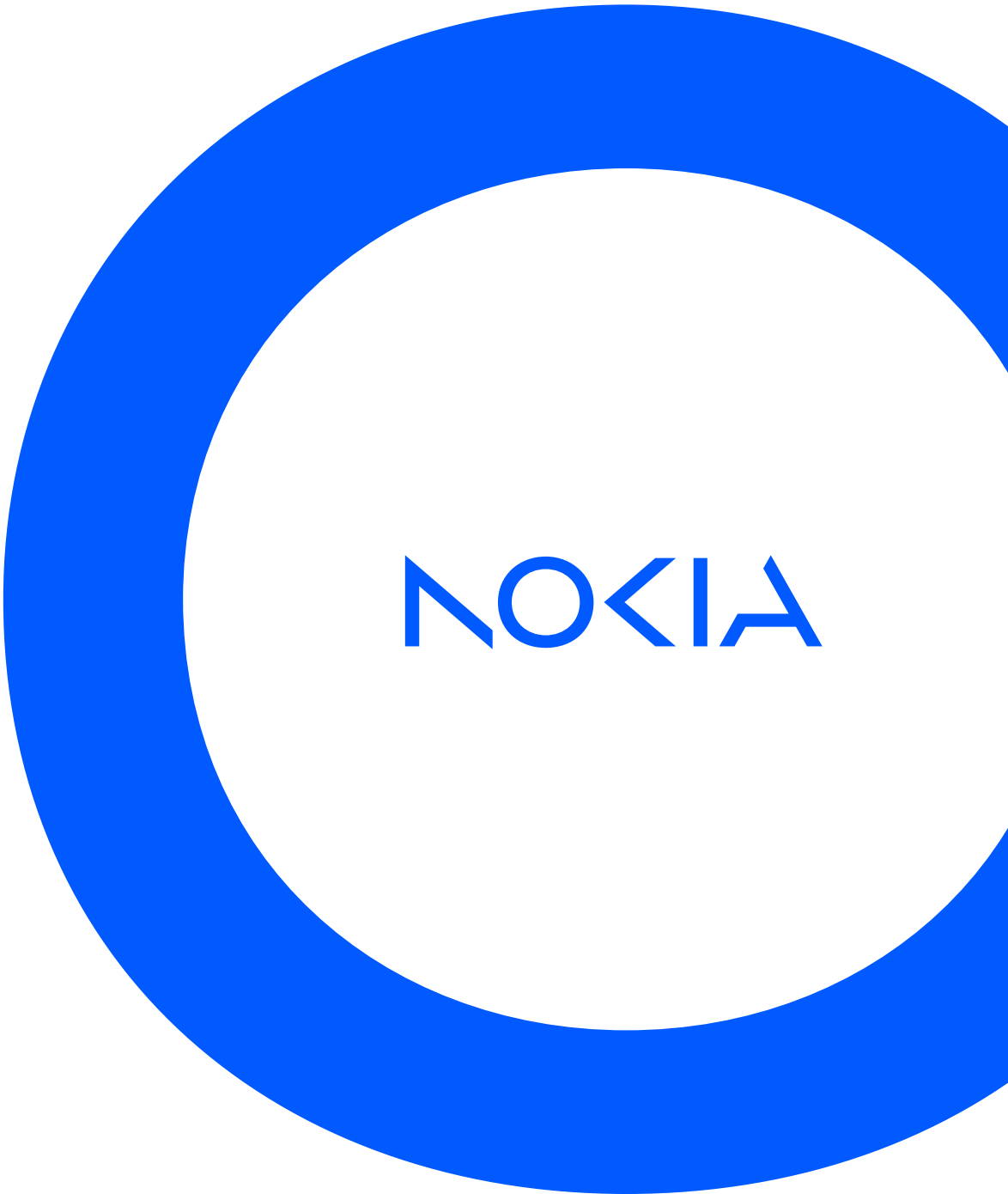
Transforming mission-critical networks

Migrating legacy SCADA traffic to IP/MPLS networks

Application note



Abstract

Our modern society is fully dependent on smooth and safe operations of critical infrastructures operated by power and water utilities, oil and gas industries as well as transportation authorities, all of which have operations that are usually widespread geographically. To ensure smooth and safe operations, they need to continually collect data from and monitor processes at all remote stations using supervisory control and data acquisition (SCADA) systems over mission-critical communications networks.

As operators of mission-critical networks rapidly adopt IP/MPLS as the communications technology of choice, there is a great need to continue to support existing deployed SCADA systems, which use low-speed serial and 4-wire analog interfaces. Furthermore, even though IP/MPLS is capable of reliably carrying TDM data transparently, advanced communications functionalities are required to accommodate the multipoint communications between SCADA servers and remote terminal units (RTUs).

Rising to this challenge, Nokia delivers a converged IP/MPLS critical communications solution with integrated multidrop bridging and raw socket transport capabilities, offering wide flexibility to migrate legacy SCADA traffic to an IP/MPLS network gracefully. This paper discusses how an IP/MPLS network, equipped with these capabilities, can be deployed to provide the essential communications for SCADA systems.

Contents

Introduction

Smooth and safe operations of critical infrastructures by power and water utilities, oil and gas industries as well as transportation authorities are pivotal to a functioning modern society. Because their infrastructure is usually widespread geographically and at times extends even to uninhabitable terrain, they need to continually acquire data from all remote locations to monitor and supervise industrial processes.

A supervisory control and data acquisition (SCADA) system allows operators to continually monitor and process status data in the field from an operations center. Also sometimes called "telecontrol equipment" in power utilities (as in the IEC 60870 suite), a SCADA system increases the efficiency and uptime of industrial processes and operations. SCADA data can also be integrated with new analytics applications.

Due to the long service life of a SCADA system (20 years or more), there are many legacy systems in active service today. The legacy systems communicate over TDM networks, using proprietary protocols in a multipoint fashion over low-speed serial interfaces, such as RS-232/V.24, RS-530/RS-422 and X.21, or 4-wire E&M analog interfaces.

Challenges for migrating legacy SCADA traffic to IP/MPLS networks

As TDM communications equipment and services are reaching end-of-life, mission-critical communications networks are rapidly being modernized to IP/MPLS networks. With an expected SCADA system service life of 20 years or more, it becomes crucial to gracefully migrate legacy SCADA traffic from TDM networks onto the new IP/MPLS networks with no performance degradation.

Three major hurdles stand between legacy SCADA systems and IP/MPLS migration:

- Connecting to legacy SCADA system communication interfaces
- Transporting multipoint traffic
- Securing SCADA communications.

This paper discusses how the Nokia IP/MPLS solution removes the hurdles, to enable operators evolving their networks to IP/MPLS while keeping existing SCADA systems with no disruption in operations.

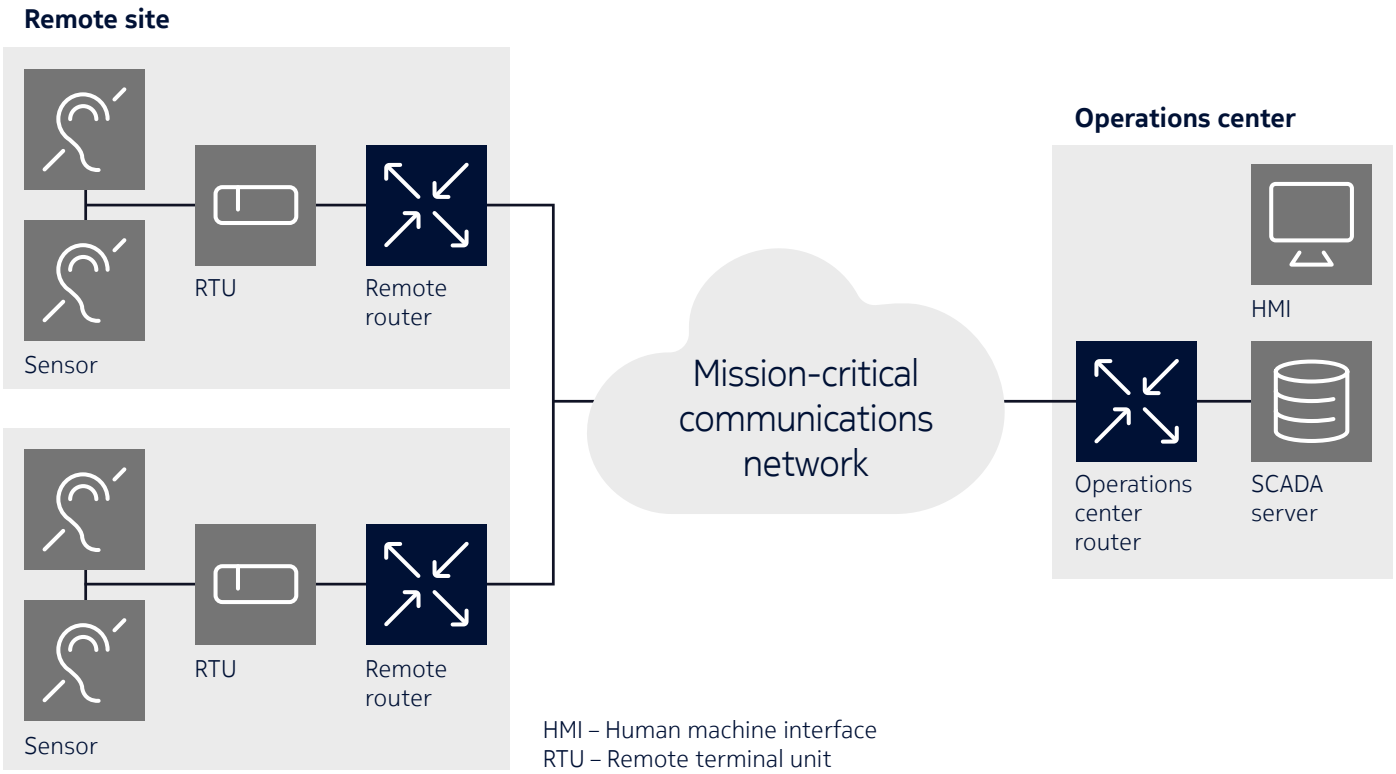
SCADA system overview

A typical SCADA system has four components (see Figure 1):

- **Sensors:** Devices in the field that monitor industrial processes and associated equipment.
- **RTUs:** Devices in the field that collect information from sensors and transmit that data to a SCADA server. RTUs are also known as slaves or intelligent electronic device (IEDs).
- **SCADA server (also called front end processor or FEP):** The heart of a SCADA system, located at the control or operations center, with which the user interacts, usually through a human–machine interface (HMI) on a computer. The server controls and communicates with tens, hundreds or even thousands of RTUs periodically. Due to a SCADA system's criticality to infrastructure operations, there is typically a pair of servers operating in hot backup/failover mode. The SCADA server is also known as the master.
- **Communications network:** Situated between the server and remote RTUs, the communications network provides reliable, secure communications between them. Because it carries information critical for safe and efficient operation of the industrial process, the communications network is considered a mission-critical network.

As explained earlier, legacy SCADA systems use either low-speed serial interfaces or 4-wire analog E&M interfaces. Therefore, it is imperative for the communications network to support these interfaces.

Figure 1. Nokia Mission-Critical Communications Networks Solution for Power Utilities



HMI – Human machine interface
RTU – Remote terminal unit

Communications between server and RTUs

There are three communication architectures:

- Centralized
- Distributed
- All-IP (typically found in newer SCADA systems)

In all three communication architectures, reliable and consistent high network performance is essential to ensure that industrial processes and equipment are monitored and controlled constantly. Moreover, secure communications are also crucial to ensure confidentiality, integrity and authenticity of SCADA traffic. Network communications failure or compromise will interrupt SCADA system operations, leading to industrial systems operational inefficiency and failure, and causing economic loss—and even loss of life.

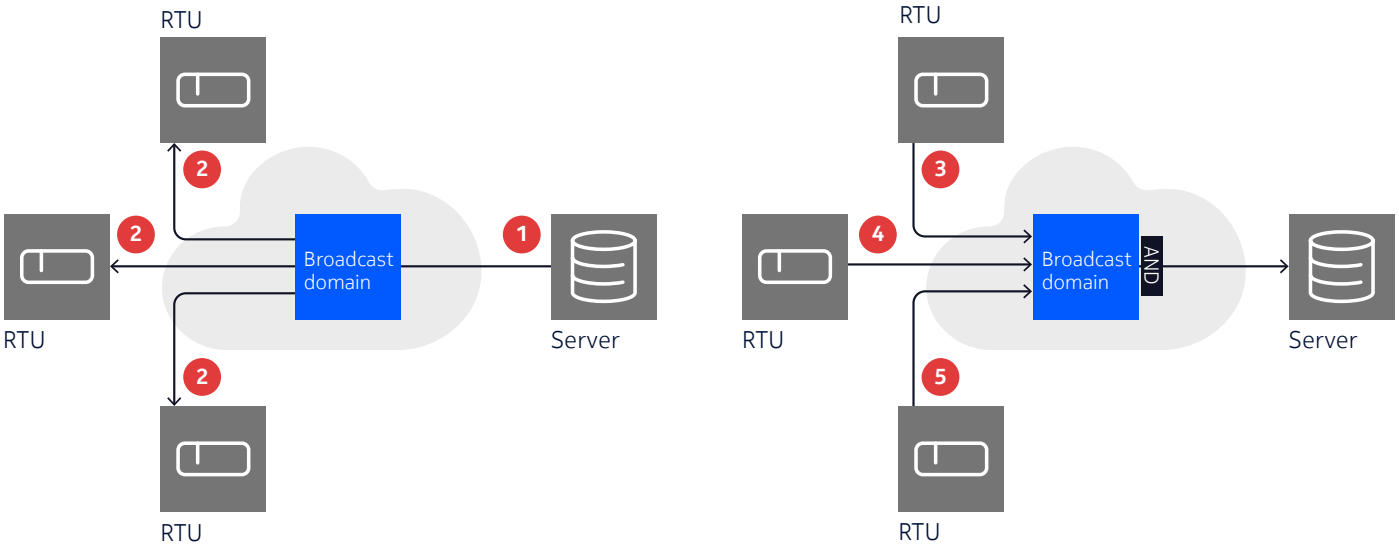
Each type of architecture is described in more detail in the following sections.

Centralized communications architecture

In a centralized communications architecture, the server is connected to the network communicating with all RTUs using one interface. The communications between the server and RTUs proceeds as follows:

1. The server sends a broadcast query message encoded with an RTU address to the network to query each RTU sequentially.
2. The network replicates the message and broadcasts it to every RTU.
3. Although the query message is received by all the RTUs, only the addressed RTU processes the query and responds with a unicast reply message. Due to the nature of TDM communications, when not queried, RTUs are sending idling zero bits constantly. Some RTUs also use RTS to signal the bridge to allow access. As a result, the broadcast bridge needs to have the capability to apply an AND logic to extract the reply message and forward to the server.
4. The server then queries another RTU with another broadcast message encoded with another RTU address,. The polled RTU responds as in Step 2.
5. These steps are repeated continually.

Figure 2. A centralized SCADA communications architecture

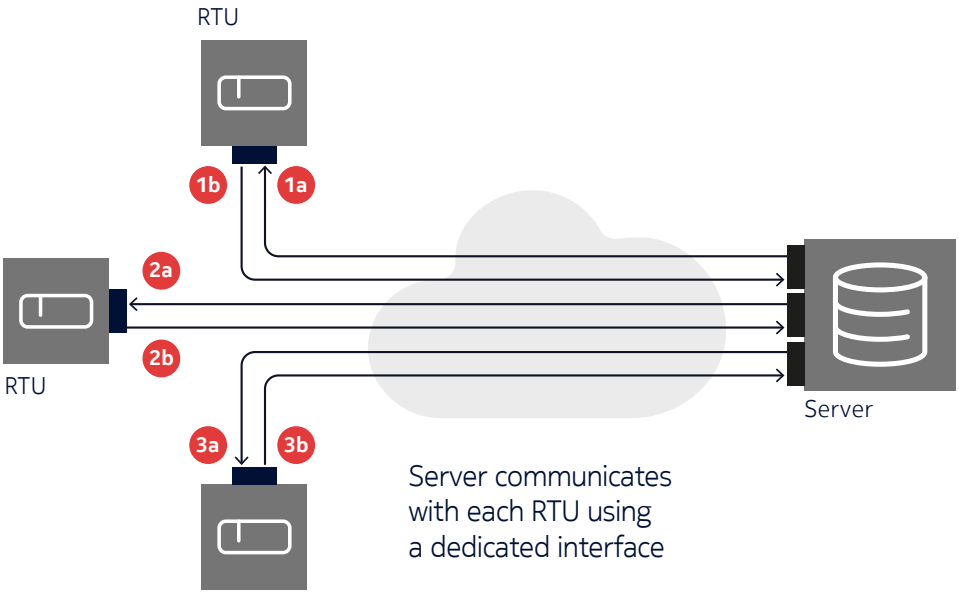


Distributed communications architecture

In a distributed communications architecture, the server communicates with each RTU using a separate, dedicated interface on the server, as follows:

1. The server sends a query message through a network connection to each individual RTU using a corresponding server interface (see 1a, 2a and 3a in Figure 3).
2. Upon receipt of the query message, the RTU responds with a unicast reply message (see 1b, 2b and 3c in Figure 3).

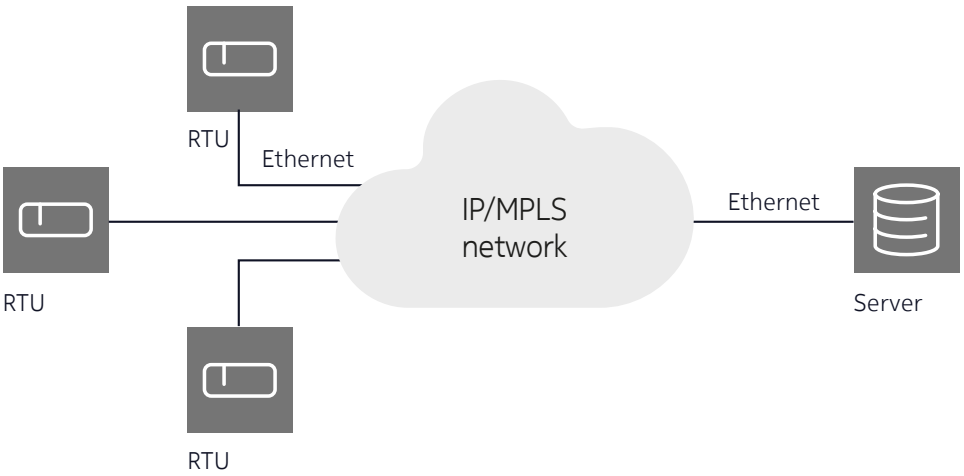
Figure 3. A distributed SCADA communications architecture



An all-IP communications architecture

All-IP is the prevalent communications architecture for newer SCADA systems. Both the server and RTU equipment are equipped with an IP/Ethernet-based communications interface. They communicate in TCP or UDP sessions encapsulated in IP packets (see Figure 4).

Figure 4. An all-IP SCADA communications architecture



The Nokia IP/MPLS converged network solution

Many operators of mission-critical networks have started to consider deploying, or have already deployed, converged networks to support all their applications: mission-critical applications such as SCADA, teleprotection and land mobile radio as well as non-mission-critical applications such as CCTV, telemetry and corporate data access. However, not all next-generation network solutions are appropriate. Although non-MPLS-based IP networks are widely used, particularly in the internet, they often lack the necessary deterministic quality of service (QoS) and traffic engineering capability as well as the required resiliency and operations, administration and maintenance (OAM) capability to support applications that require strict QoS and high availability. They also lack the flexibility to optimize the use of network resources and fast network fault recovery capability to ensure high availability. Accordingly, non-MPLS-based IP networks cannot be used as a converged network.

An IP/MPLS-based communications network has emerged as the prevalent choice due to its strong resiliency, robust QoS and versatile service capabilities.

By using a Nokia IP/MPLS network solution, operators get the best of both worlds—the versatility of an IP network and the predictability of a circuit-based network along with high capacity and support for packet-based traffic with high QoS. An IP/MPLS network enables the deployment of new IP/Ethernet applications and also supports existing TDM-based applications. Because IP/MPLS networks can continue to carry existing TDM services, operators can migrate TDM-based applications directly to IP/MPLS while enabling new IP/Ethernet-based applications.

A Nokia IP/MPLS network provides operators with the following features:

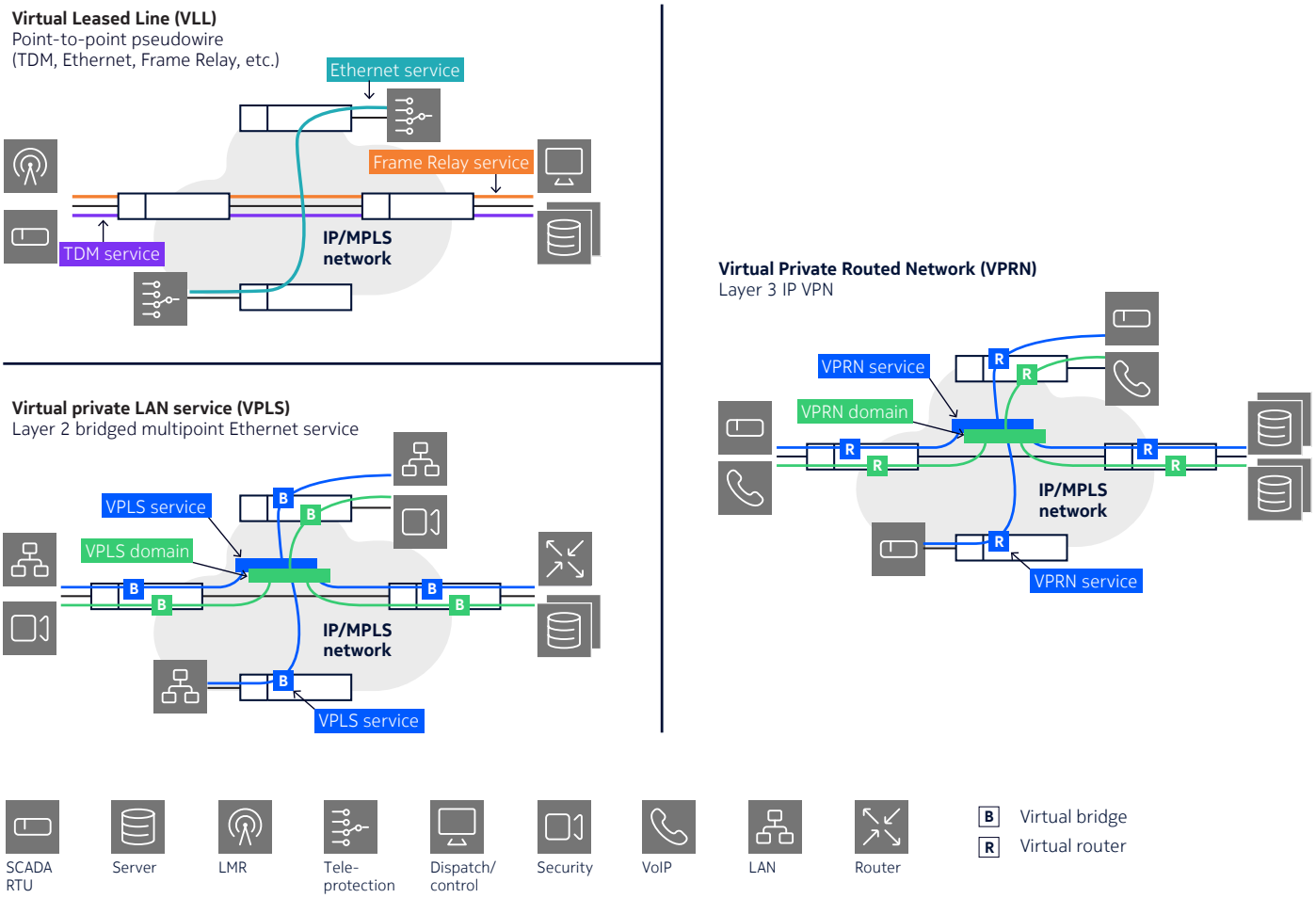
- Native support of a wide range of legacy interfaces, including RS232/V.24 and V.35 serial data, E&M, FXS and FXO analog voice, C37.94, G.703 co-directional and T1/E1
- MACsec[1] to safeguard all application traffic, including SCADA, teleprotection and control traffic such as IP routing and MPLS signaling protocols
- High scalability and robustness with full redundancy, rapid recovery mechanisms such as MPLS Fast Re-Route (FRR), and pseudowire redundancy
- Deterministic QoS to assure constant delay, delay asymmetry and jitter constantly
- Optimized network bandwidth usage and avoidance of common modes through traffic engineering.
- An extensive OAM suite for ongoing service and performance management
- Flexible network topology (linear, hub-and-spoke, multi-ring and mesh) atop versatile transport and access technology (fiber, microwave, copper and cellular/Wi-Fi)
- An advanced and scalable network services platform to optimize and automate provisioning and operations

1 To learn about MACsec, read the whitepaper Securing IEC 61850 communications

Many VPNs, one network

To support many applications over a converged network, a Nokia IP/MPLS network provides for the virtual isolation of various traffic types on a single infrastructure supporting many virtual private networks (VPNs) simultaneously. As shown in Figure 5, whether the network is a virtual leased line (VLL) of various types, a virtual private LAN service (VPLS) or a virtual private routed network (VPRN), deploying Nokia IP/MPLS allows full separation of control and data traffic in each VPN from other applications or operations in the network. The results are a fully secured environment, effective infrastructure sharing and optimal bandwidth allocation for all applications.

Figure 5. Nokia IP/MPLS-network



Nokia IP/MPLS solution components overview

The Nokia IP/MPLS solution provides a service-oriented approach that focuses on service scalability and quality as well as per-service OAM. A service-aware infrastructure enables the operator to tailor services such as mission-critical applications so that the network has the assured bandwidth to meet peak requirements. The Nokia service routers support IP routing and switching, which enables the network to support real-time Layer 2 and Layer 3 applications.

The Nokia converged IP/MPLS network leverages multiple state-of-the-art technologies. The network extends IP/MPLS capabilities from the core to access and includes the following main components:

- Nokia 7705 Service Aggregation Router (SAR)
- Nokia 7750 Service Router (SR)
- Nokia 7250 Interconnect Router (IXR)
- Nokia 7210 Service Access Switch (SAS)
- Nokia Wavenance microwave radio connecting MPLS nodes with microwave links
- Nokia 1830 Photonic Service Switch (PSS) as optical core underlying the IP/MPLS network
- Nokia Network Services Platform (NSP) as a unified network and services manager

The Nokia SCADA migration solution to IP/MPLS

While IP/MPLS networks already provide the necessary TDM adaptation, resiliency and QoS for reliable SCADA communications, advanced networking capabilities are required to support multipoint SCADA communications between the server and RTUs. Nokia offers deployment flexibility with two migration options: multidrop bridging and raw socket transport.

Multidrop bridging solution

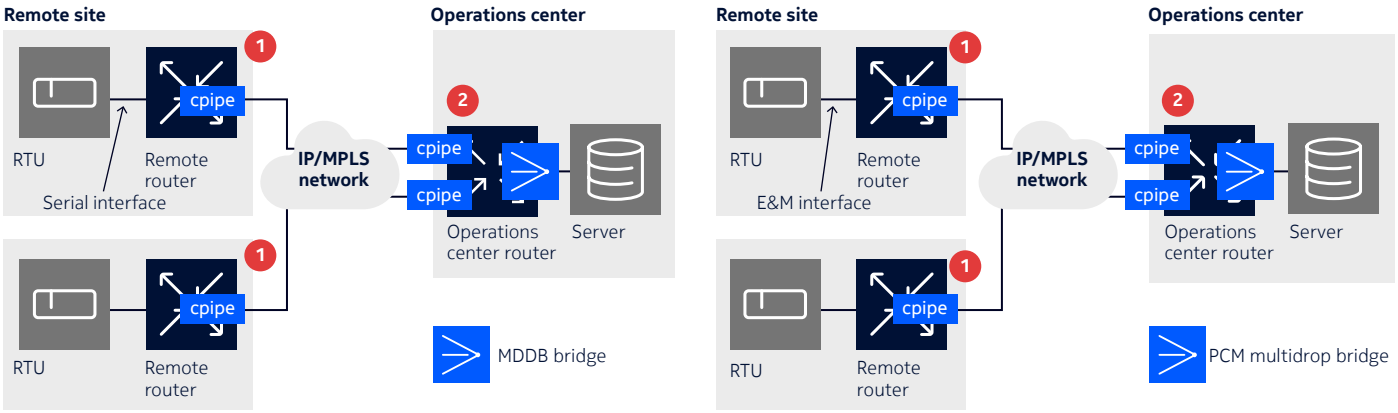
The multidrop bridging solution enables migration of traffic from legacy SCADA systems from a TDM network to an IP/MPLS network while allowing operators to retain legacy interfaces in RTUs and servers, thereby ensuring no discontinuity to SCADA operations. The solution is supported on the 7705 SAR and is ideal for migration of SCADA communications with a centralized architecture. There are two multidrop bridging variants:

- Multidrop data bridging (MDDB) for SCADA systems with RS-232/V.24 (asynchronous and synchronous modes), RS-530/422 and X.21 serial interfaces
- PCM multidrop bridging for SCADA systems with 4-wire analog E&M interface.

Solution architecture for centralized communications architecture

Figure 6 shows the architecture of the two 7705 SAR-based multidrop bridging solutions. The multidrop bridge is deployed centrally in an operations center router.

Figure 6. The two multidrop bridging variants: MDDB and PCM multidrop bridging



MDDB solution

PCM multidrop bridging solution

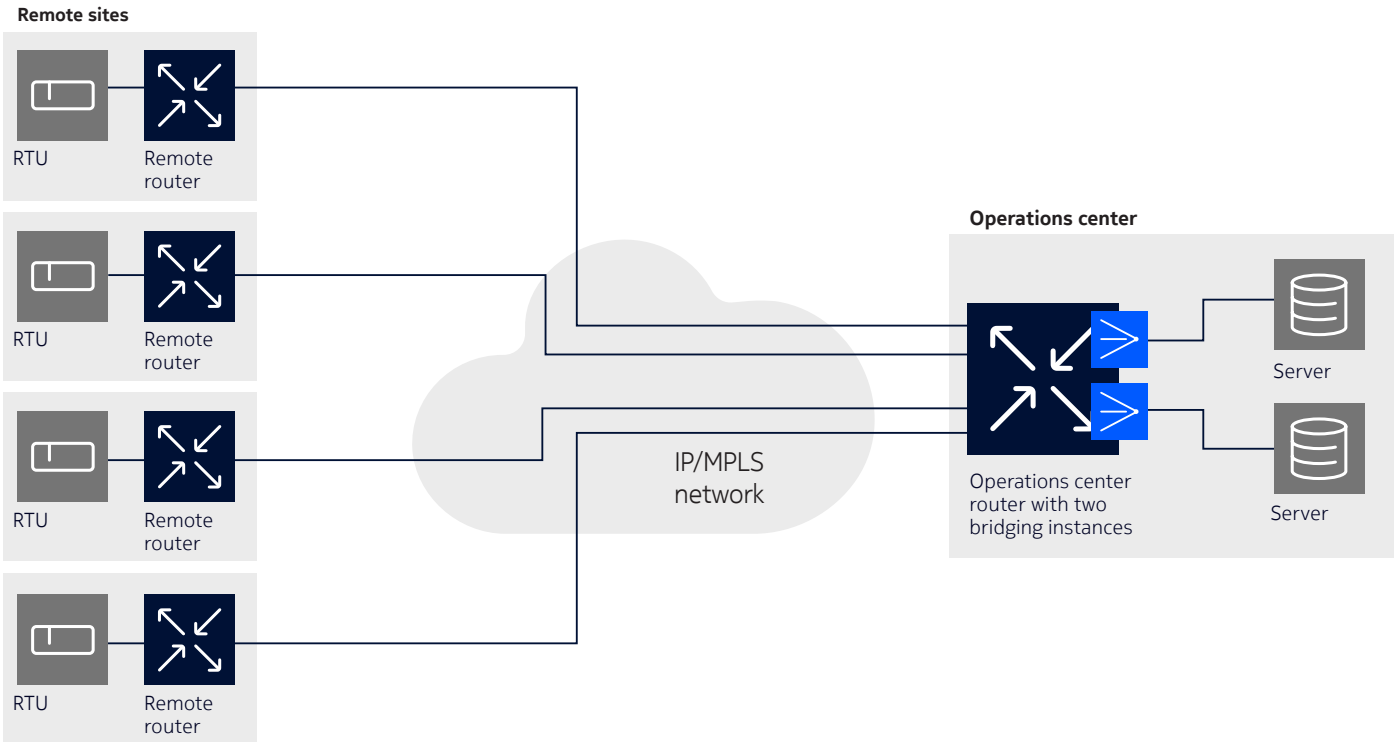
As shown in Figure 6, the solution provides two key functions in the communication between server and RTUs:

1. At remote sites, 7705 SARs use TDM pseudowires[2], also called cpipes, to packetize and transport traffic from RTUs across the IP/MPLS network toward the control center gateway router. Where a 4-wire E&M interface is used, the analog signal is digitized with pulse code modulation (PCM) technology before packetization. Both μ-law and A-law companding are supported. Because the serial interface speed usually ranges from 300 b/s to 19.2 kb/s, the traffic needs to first be rate-adapted to 64 kb/s. It is then packetized into an MPLS packet. The packet is carried over a pseudowire inside a label switched path (LSP) tunnel established by MPLS signaling, reaching the operations center.
2. At the operations center, a 7705 SAR acts as a multidrop bridge (MDDB for serial interface and PCM multidrop bridge for E&M interface). The multidrop bridge is implemented in a dedicated resource card called the Integrated Services Card (ISC). It receives all traffic from various RTUs through individual TDM pseudowires, filters out the idling traffic and sends the reply message to the SCADA server.

The server communicates with the RTU using the same steps in reverse order. The server sends traffic to the multidrop bridge, which broadcasts it over individual pseudowires to each RTU.

The ISC is a powerful resource card supporting either MDDB or PCM multidrop applications. Sixteen separate multidrop bridges (up to 30 ports/bridge) are available on the ISC with the flexibility of cascading multiple bridges to create a larger bridge or having multiple SCADA networks supported on one card (see Figure 7).

Figure 7. Two multidrop bridges to support two SCADA systems



2 The traffic from RTUs is transported across the IP/MPLS network using TDM pseudowire technology as described in IETF RFC 5086, Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN).

SCADA server redundancy protection

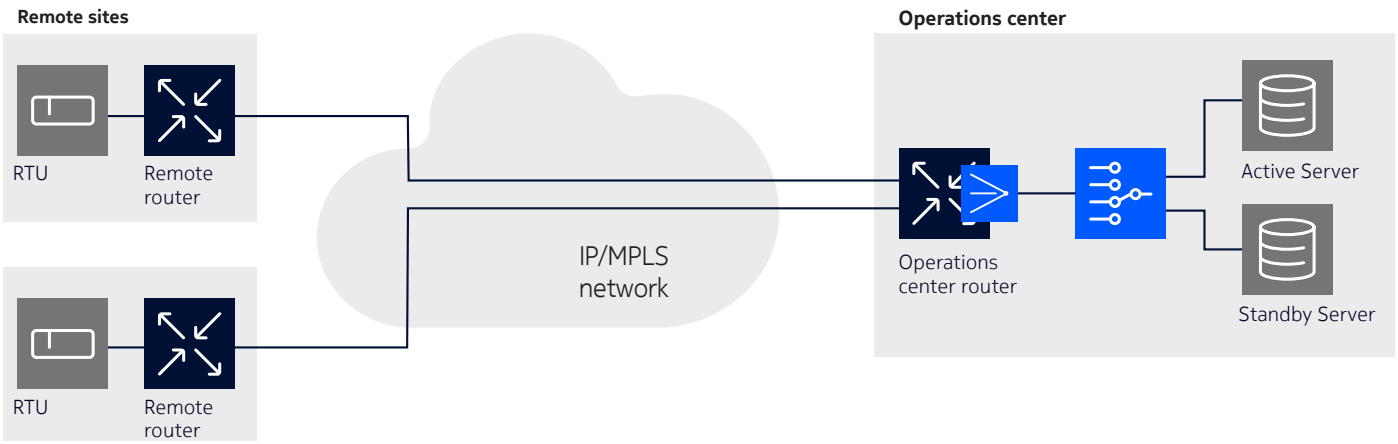
The server is critical to SCADA operation. If it fails, no field data or alarms can be recorded and processed. The operator would become blind to the condition and state of the industrial process in the critical infrastructure. This situation could potentially cause catastrophic damage, particularly if it lasts for a long time. Therefore, server redundancy protection is prevalently deployed to maximize uptime.

SCADA solutions support redundant servers with both an active and a standby server listening to replies from RTUs, but with only the active server transmitting queries. The Nokia multidrop bridging solution is designed to work with this server redundancy behavior. There are various protection models for network operators to choose from. Each model provides a different level of protection, requires a different amount of resources to implement, and often is dependent on the server functionality. Depending on the network's reliability and robustness requirements as well as other logistics constraints, an operator can choose accordingly.

Model 1: Active/standby server pair with an external A/B switch

Model 1 has one control center router with one MDDB and an A/B switch connected to active and standby SCADA servers to provide redundancy protection (see Figure 8). If the active server fails, the operator intervenes manually to activate the A/B switch to connect to the standby server.

Figure 8. Protection Model 1

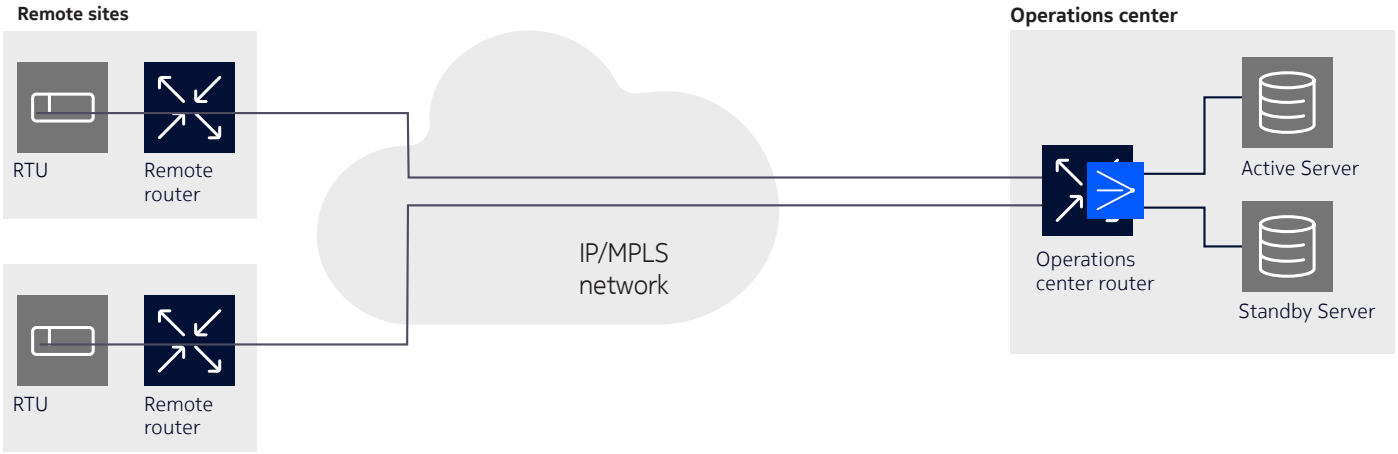


Model 2: Active/standby server pair with two interfaces over one multidrop bridge

Model 2 is similar to Model 1 except that instead of using an external A/B switch, each server connects to the multidrop bridge4 with its own interface (see Figure 9). The standby server interface can be configured to be in either warm or hot state. If configured for warm state, the standby server will receive the same traffic from the multidrop bridge as the active server. Data sent by the standby server will be dropped by the multidrop bridge. If the active server fails, the operator needs to intervene to toggle the standby server interface status to active using the Nokia NSP or a command line interface (CLI).

Dependent on SCADA system capability, hot state protection is possible. When configured for hot state, both the active and standby servers receive data from RTUs but only the active server transmits data. The standby server transmits only all ones. If the active server fails, the switchover is seamless because no operator intervention to toggle the interface status is required, as in the case of warm state protection. However, operators need to ensure that the standby server does not transmit when in standby mode.

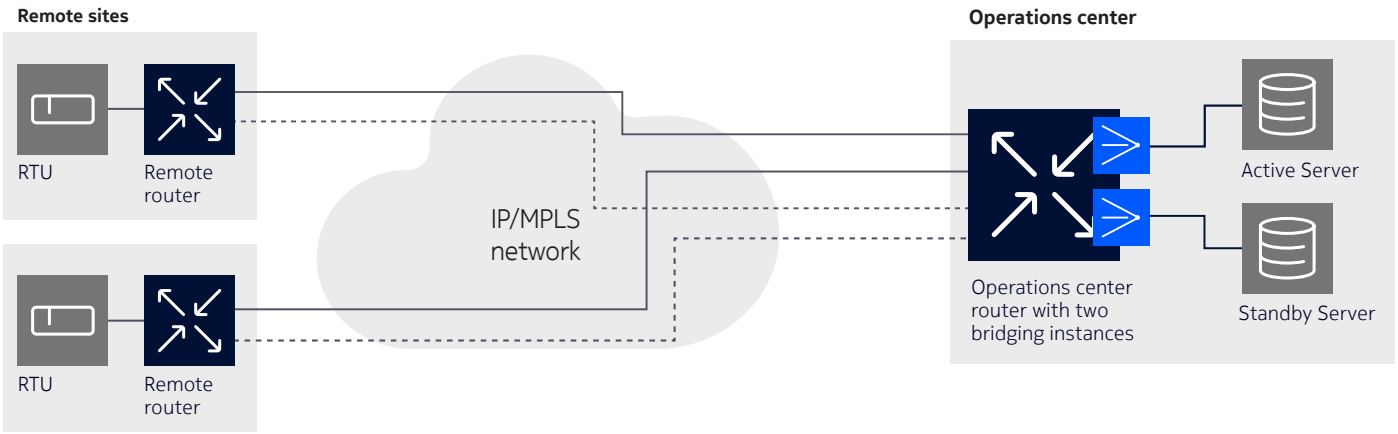
Figure 9. Protection Model 2



Model 3: Active/standby server pair with two multidrop bridges over one router

In Model 3, in addition to the two servers, there are two ISCs in the control center router, each running its own multidrop bridge instance (see Figure 10). The router is also typically equipped with redundant control and fabric complex and dual power feed to eliminate any single point of failure.

Figure 10. Protection Model 3



Model 4: Geo-redundant active/standby server and router pair

In Model 4, the two multidrop bridge instances run on two control center routers, each connecting to a different server (see Figure 11). The two routers and two servers can be located in the primary and back control centers to provide geo-redundancy, which is integral to protection from disaster, including fire and earthquake. No automatic redundancy/switchover between active and standby servers is possible as in models 1 and 2.

Figure 11. Protection Model 4

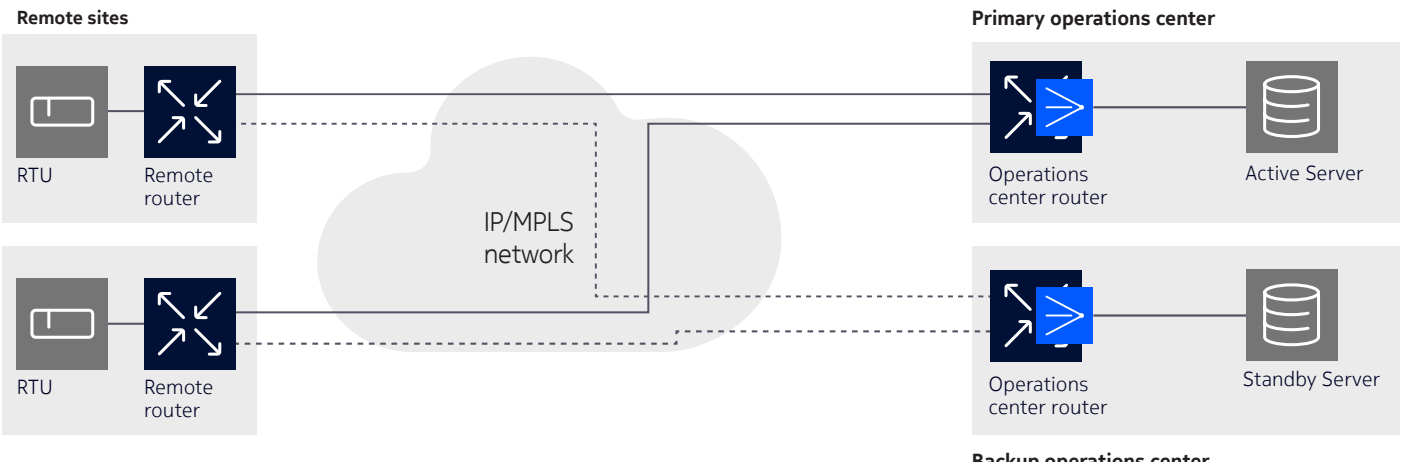


Table 1 provides a concise comparison of the four protection models. Each model has its own merits and associated costs. To choose the model that best suits their needs, operators should assess their reliability and robustness requirements.

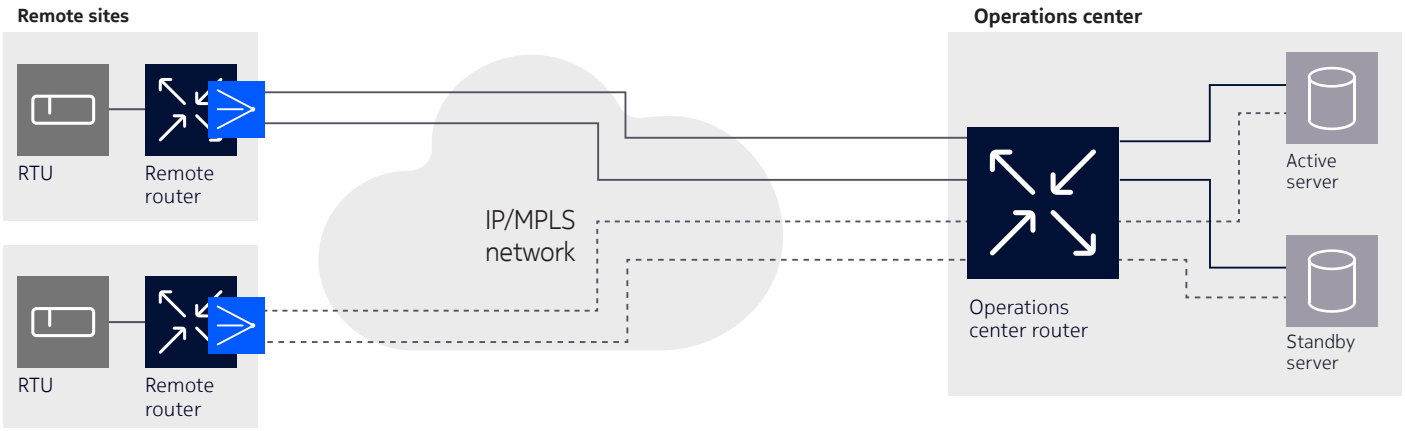
Table 1. Comparison of the four protection models

	Model 1	Model 2	Model 3	Model 4
Required equipment at operations center	2 x server 1 x A/B Switch 1 x 7705 SAR 1 x ISC	2 x server 1 x 7705 SAR 1 x ISC	2 x server 1 x 7705 SAR 2 x ISC	2 x server 2 x 7705 SAR 2 x ISC
Protected components	Server 7705 SAR Control/fabric/power	Server 7705 SAR Control/fabric/power	Server Whole 7705 SAR node	Operations center
Geo-redundancy protection	No	No	No	Yes

Migrating traffic from SCADA systems with distributed communications architecture

The multidrop bridging solutions can also be deployed to migrate traffic from a distributed communications architecture. The multidrop bridge, instead of being deployed in the central operations center router, is deployed at remote site routers, allowing each RTU to communicate with both active and standby SCADA server (see Figure 12). The ISC card can be used at each RTU location for maximum protection or can be used at an aggregation site subtending to other sites to optimize configurations.

Figure 12. Deploy multidrop bridging in a distributed communications architecture environment



Raw socket transport solution

There is another migration option that uses raw socket transport over serial data over IP. It is a technology that transports characters received from an asynchronous RS-232/V.24 interface by TCP or UDP sessions in IP packets. Raw sockets are ideal for migration of SCADA systems that utilize servers with IP/Ethernet interfaces where SCADA data are encapsulated over TCP or UDP, yet still have RTUs at remote sites with asynchronous RS-232/V.24 interfaces.

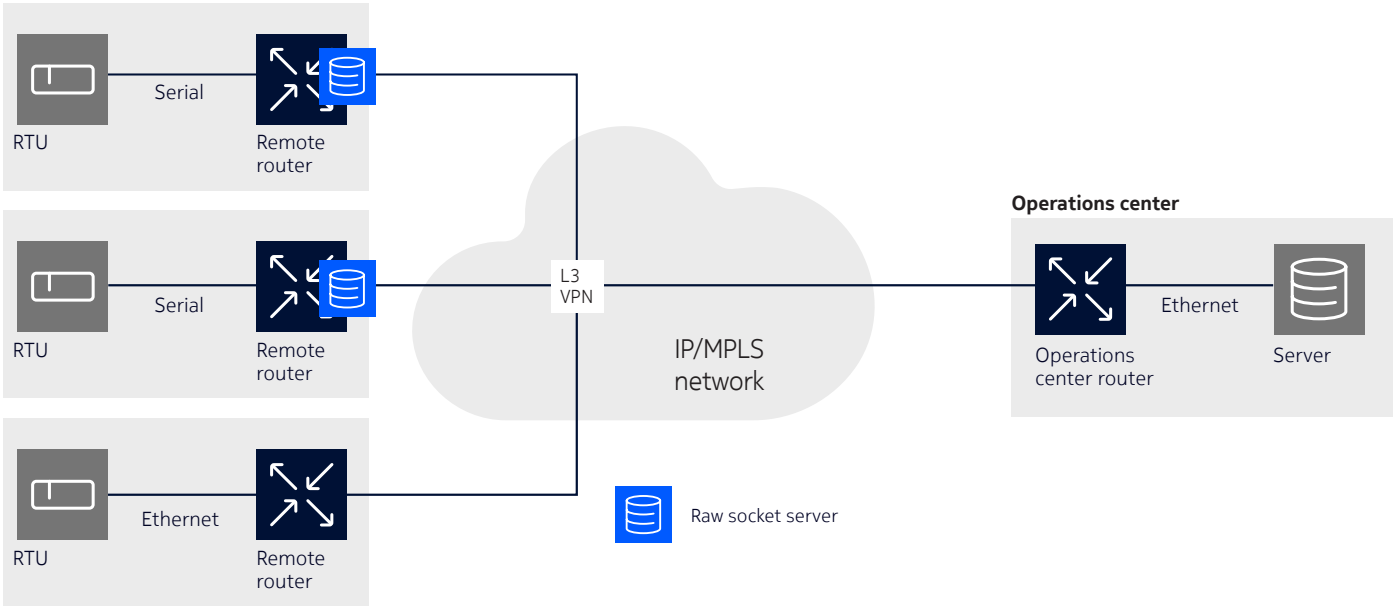
In this solution, a raw socket server implemented on the router at remote RTU sites listens for new TCP or UDP sessions initiated by the SCADA system in the operations center. After a session is established, SCADA data are transmitted over the TCP or UDP session and the remote router is responsible for de-encapsulating and encapsulating the raw serial data into and out of the TCP or UDP session. The IP packets carrying the SCADA data can be transported over a VPRN service from the operations center to the remote sites.

Some operators today have deployed terminal servers in remote sites to perform raw socket transport functions. However, those terminal servers are mostly unmanaged and not built for industrial use, thereby becoming a single point of failure in SCADA communications. The 7705 SAR, with an integrated raw socket server function, can carry SCADA protocol traffic without external unmanaged terminal servers, a more ideal grid modernization strategy that optimizes operations costs and increases reliability.

Raw socket transport solution architecture

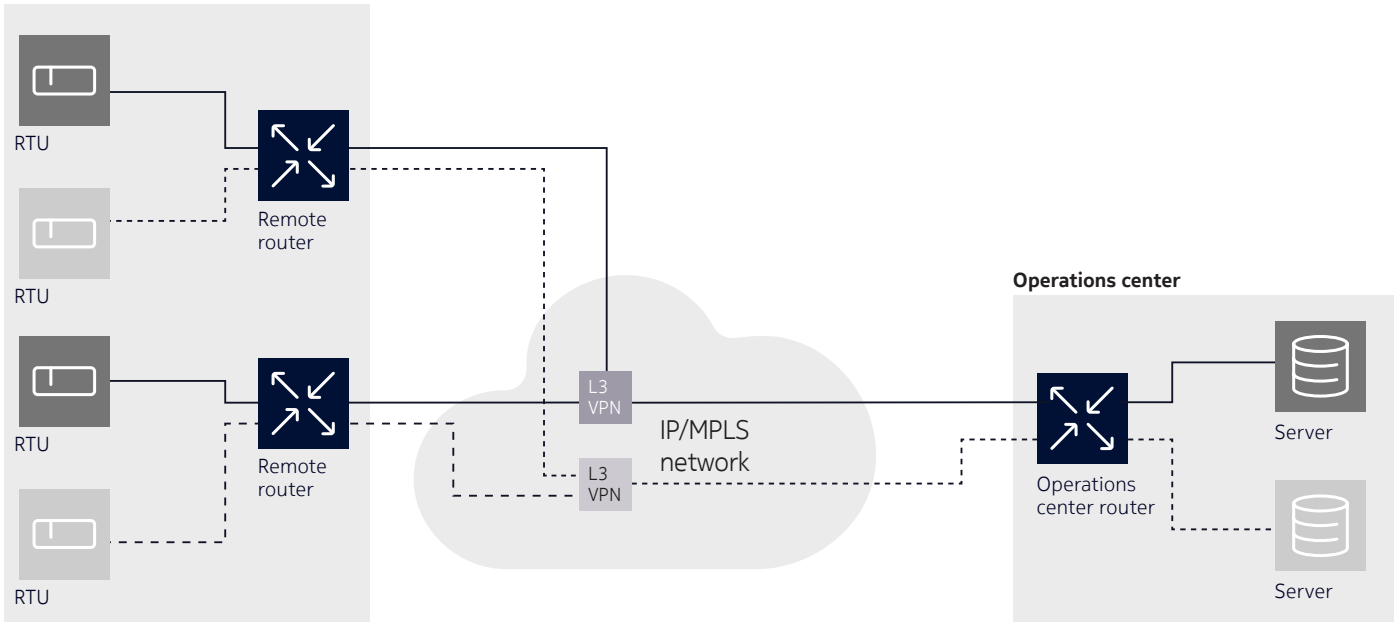
Figure 13 shows a SCADA system consisting of a SCADA server with a IP/Ethernet interface and three remote RTUs. Among the three RTUs, two are legacy ones with serial interface and one is new and equipped with an IP/Ethernet-based interface. The 7705 SAR remote router adapts serial traffic from the two legacy RTUs into TCP or UDP sessions over IP packets, and sends them to the server using a layer 3 MPLS service such as a VPRN or Internet Enhanced Services (IES) provided by the IP/MPLS network. The 7705 SAR can also connect the new IP/Ethernet-based RTU to the server using the same Layer 3 VPN or IES service.

Figure 13. SCADA communications over a layer 3 IP/MPLS VPN



Moreover, when new SCADA systems are deployed, the solution architecture can be extended with new L3 VPNs with complete traffic and routing segregation. Figure 14 illustrates a scenario where two L3 VPNs are provisioned to provide segregated communications to two SCADA systems.

Figure 14. Extending raw socket transport solution for multiple SCADA systems



SCADA server redundancy protection

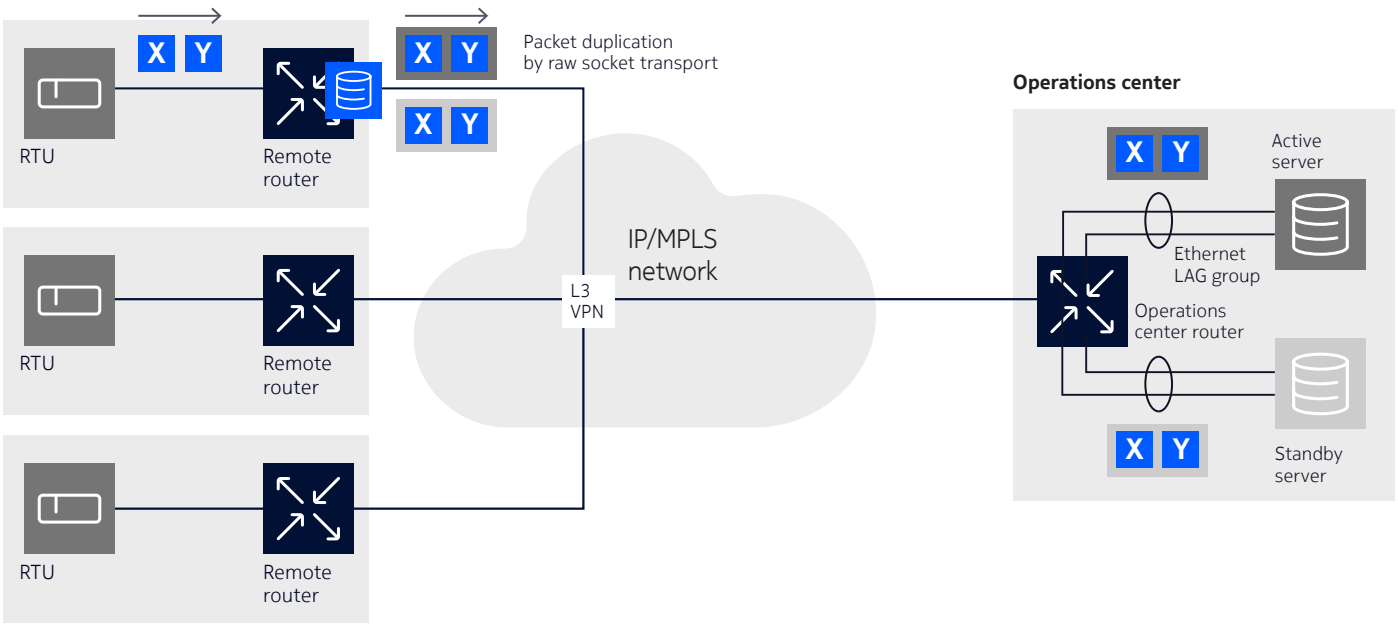
As described earlier in this paper, SCADA servers are critical to SCADA systems, which are at the heart of critical infrastructure operations. Consequently, redundancy protection is highly desirable to maximize infrastructure availability. The raw socket transport solution is designed to support server redundancy protection with various protection models, each offering a different level of protection and requiring a different amount of resources to implement.

Protection Model 1: Colocated active/standby server pair

Model 1 has one operations center router connected with an active/standby server pair (see Figure 15). To enhance resiliency, each Ethernet link to the servers can be configured as a IEEE 802.3ad link access group (LAG). Only the active server will communicate with RTUs. When a RTU replies, the raw socket transport function will duplicate and send the response message to both active and standby servers so that both servers are up to date with the collected field data to ensure no operation interruption in case of server switchover.

It should be noted that the operations router has full hot redundancy equipment protection, including control, switching fabric, line card, synchronization, power source and fan. Unless there is a major failure affecting a wide area in the building, SCADA system communications will not be disrupted.

Figure 15. Protection Model 1

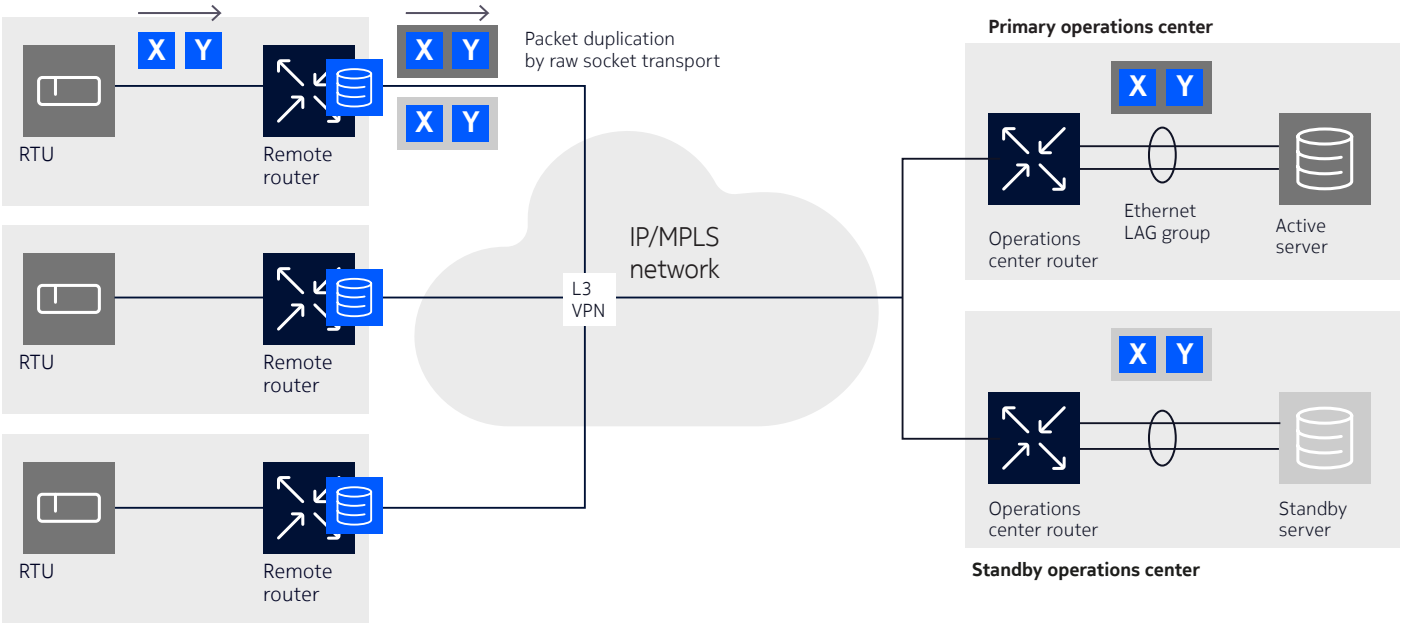


Protection Model 2: Active/standby server pair with geo-redundancy

Model 2 extends the scope of redundancy protection by locating the standby server in a standby operations center at a different geographic location (see Figure 16). With geo-redundancy, SCADA systems continue to operate despite a major disaster at the primary operations center.[5]

5 In particular, the use of LTE wireless routers among utilities has started to become prevalent in their field area networks (FANs). Please watch this video to find out more.

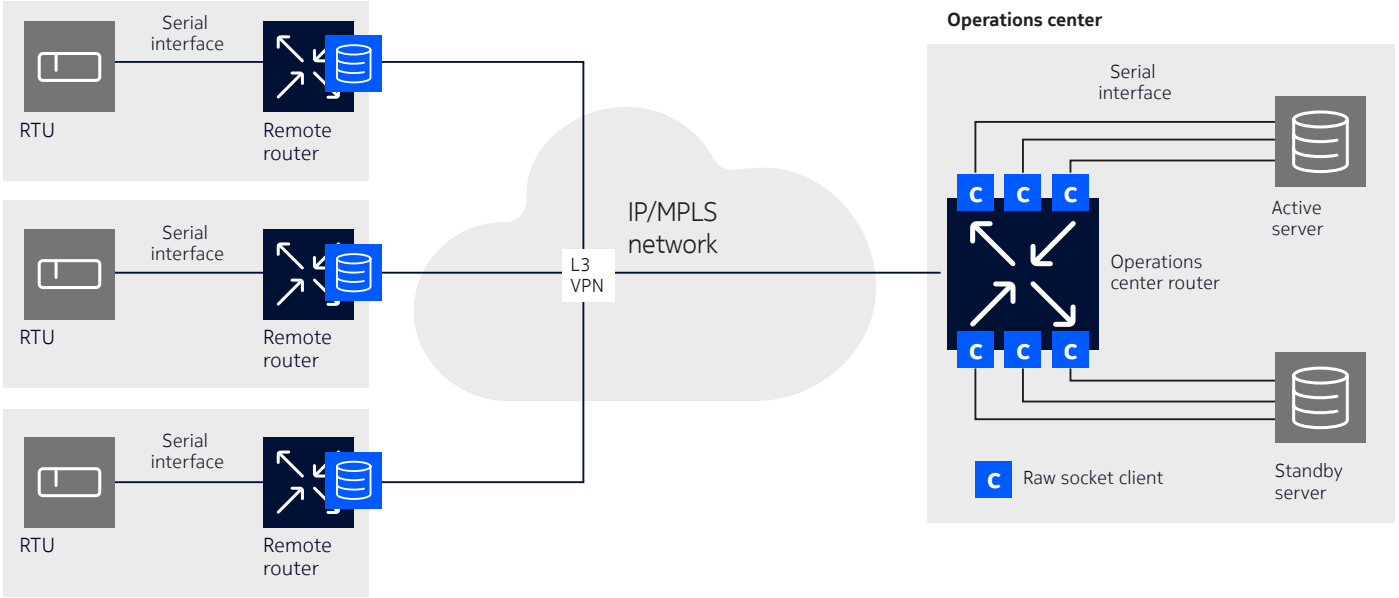
Figure 16. Protection Model 2



Migrating traffic from SCADA systems with distributed communications architecture

The raw socket transport solution is ideal to migrate SCADA traffic from a system with distributed communications architecture with high scalability efficiently, without resorting to special hardware. With asynchronous serial interfaces on both servers and RTUs, the 7705 SARs in remote sites and operations centers are configured with raw socket servers and clients, respectively (see Figure 17).

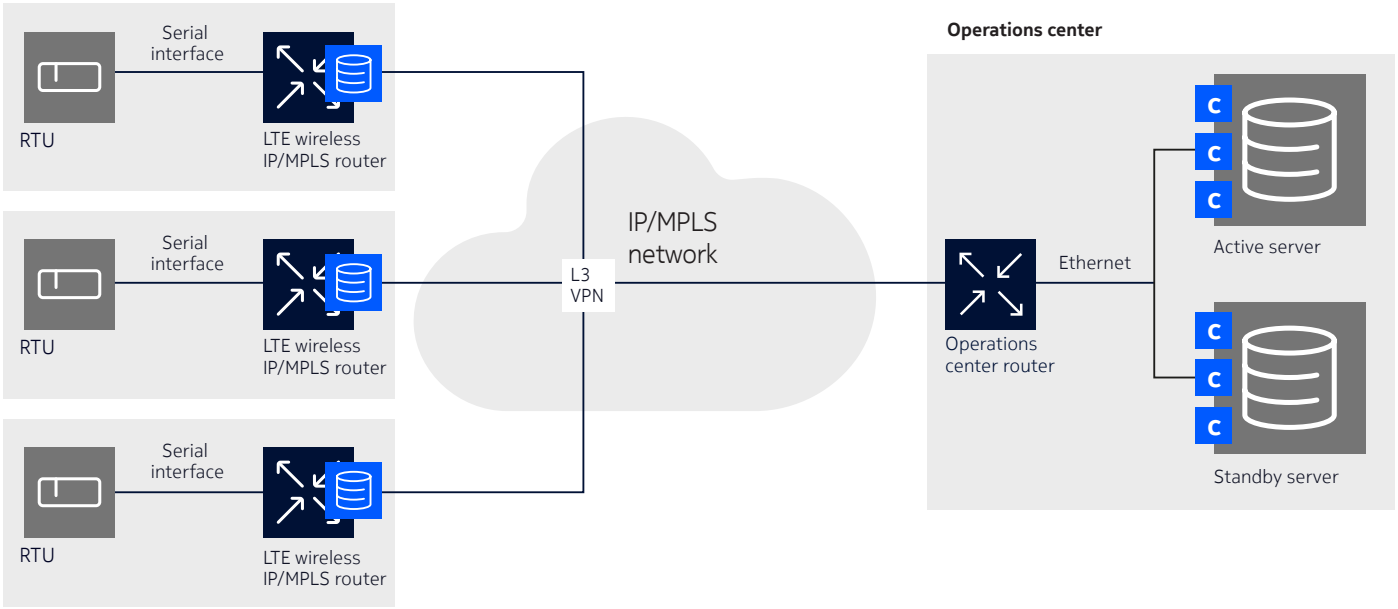
Figure 17. Deploying raw socket transport in a distributed communications architecture environment



Migrating traffic from SCADA systems deployed in the field

SCADA applications are commonly deployed in the field, e.g. along feeder circuits beyond low-voltage distribution substations or in oil, gas and mining fields. These locations do not usually have fixed network access to connect RTUs. The raw socket transport solution can be wirelessly extended to reach these locations with the use of LTE technology. Figure 18 depicts a scenario where a 7705 SAR with a LTE interface at remote site uses raw socket transport to carry SCADA traffic back to the operations center.

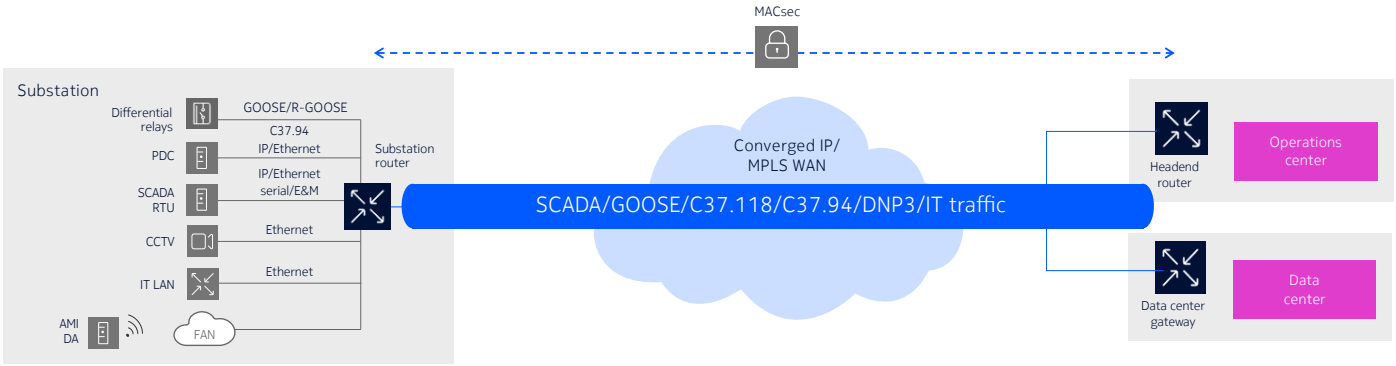
Figure 18. Combining LTE and raw socket transport for field SCADA traffic migration



Securing SCADA communications

An IP/MPLS network with label switched path tunneling and segregated VPN services is already inherently secure. But as the frequency and complexity of cyberattacks continues to rise, cyber security is a pressing concern, particularly for networks carrying critical applications. Encrypting traffic in networks is a key measure to protecting the confidentiality, integrity and authenticity of grid communications. MACsec, with its universal encryption capability protecting IP, non-IP and control traffic, is ideally suited to safeguard critical SCADA and other grid communications against current network threats and emerging quantum attacks (see Figure 19).

Figure 19. MACsec safeguards SCADA communications and more



Conclusion

Mission-critical infrastructure operators depend on reliable, secure transport of SCADA traffic to monitor, analyze, control and maintain the critical infrastructure every day. It is crucial that legacy SCADA system communications can be migrated to new packet networks gracefully with no compromise. The Nokia IP/MPLS communications network has the adaptability and versatility to reliably and securely carry legacy serial and 4W analog SCADA traffic as well as modern IP-based SCADA data and other new bandwidth-intensive applications. With a comprehensive and innovative product portfolio encompassing IP/MPLS, microwave, optical transmission, SDN, NFV and LTE, complemented by a full suite of professional services including audit, design and engineering practices, Nokia has the unique capability and flexibility to help operators of mission-critical networks upgrade their networks to cutting-edge IP/MPLS technology while retaining uncompromised support of legacy SCADA systems.

For more information about the Nokia solutions for industries and the public sector, please visit https://networks.nokia.com/industries.

Acronyms

HMI	human–machine interface
IP	Internet Protocol
LAN	local area network
LMR	land mobile radio
LTE	long term evolution
MDDB	multidrop data bridge
MPLS	Multiprotocol Label Switching
NFV	network functions virtualization
NGE	Network Group Encryption
OAM	operations, administration and maintenance
PCM	pulse code modulation
QoS	quality of service
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SDN	software-defined networking
TCP	Transmission Control Protocol
TDM	time division multiplexing
UDP	User Datagram Protocol
VLL	virtual leased line
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 1512700 (July) CID171892