Alcatel-Lucent Enterprise Oil and Gas Solution Guide

Solution guide
Oil and Gas

Alcatel·Lucent
Enterprise

Table of Contents

Figures

About this document

Purpose

This guide presents Alcatel-Lucent Enterprise solutions for Oil and Gas industry customers. This guide will present the use cases, business drivers, technical requirements, and solution overview along with the Alcatel-Lucent Enterprise value proposition for each solution set.

Audience

This guide is intended for Alcatel-Lucent Enterprise Business Partner sales and pre-sales staff as well as customers.

Scope

This document will not provide in-depth product specifications as these are already provided in datasheets. This document is split into individual modules for each solution set so the reader can focus on the section most relevant to them.

The Oil and Gas supply chain

The oil and gas industry is comprised of three segments: Upstream, Midstream and Downstream.

Upstream, sometimes refered to as Exploration and Production (E&P), handles the drilling of oil and gas wells and exploration of resevoirs, both onshore and offshore.

Midstream deals with transporting the raw material from wells to refineries, storing, and further processing. It include pipelines, shipping, trucks and storage facilities.

Downstream is responsible for removing impurities and refining the raw material into the final products, and commercially distributing the products for public use. These include oils, jet fuel, gasoline, natural gas and other products.

Figure 1 - Oil and gas segments

Upstream

Upstream or Exploration and Production (E&P) is the segment handling drilling of oil and gas wells and exploration of reservoirs both, onshore and offshore

Midstream

Midstream segment deals with transporting the raw material from wells and refineries, storing, and further processing. This includes pipelines, shipping, trucks, and storage facilities

Downstream

Downstream segment deals with removing impurities and refining the raw material into the final products, and commercially distributing the products for public use. These include oils, jet fuel, gasoline, natural gas, and other products

Industry challenges and requirements

The oil and gas industry faces with many challenges. Due to increasing demand for energy supplies, oil and gas companies are required to explore, drill and extract oil, and gas from untapped reserves in remote and harsh environments. This should be done efficiently in order to maintain safety and security, regulatory compliance and ensure smooth operational workflows.

Mission-critical communications network

The oil and gas industry requires a mission-critical network that must provide the ability to deliver communications when conventional networks cannot meet the demand. The network must maintain operation under fault conditions to ensure mission-critical communications.

Physical safety and security

Workers in the industry are exposed to harsh and hazardous environments, not including natural disasters which can be a huge risk. This risk can be reduced by facilitating better video surveillance, tracking of employee and sensors, better emergency and alarm response and monitoring real-time data to protect resources.

Cybersecurity

Energy and utility is among the most targeted industries. They face significant threats from disruption, sabotage and terrorism. The digitalisation of the industry, while it provides many benefits, it has further increased the risk. Strengthening the security and resiliency of the infrastructure is necessary.

Standards and regulations

The energy industry is heavily regulated, and companies need to be complaint to ensure better efficiency, employee safety and to implement sustainable practices.

Mobility

Digitalisation of the industry is pushing companies to meet the expectations of being connected from anywhere. Worker mobility is essential to allow access to data on demand and allow critical infrastructure monitoring.

Resiliency

The ability for the infrastructure to adapt to a change in conditions and recover is a requirement for mission-critical networks. The communications network should minimise failover time and provide minimal services disruption.

Latency and jitter

Increased latency and jitter in data networks in mission-critical networks can limit productivity and increase response time to incidents. Even if sensor and device data is accurately measured, the data required to make quick decisions might be delayed in reaching the field operation workers. Reducing latency can identify risks early and provide accurate data to manage issues faster.

Environmental hardening

Industrial-grade, highly secure and intelligent infrastructure is required for superior performance in mission-critical applications running in harsh environments with shock, vibration and/or extreme temperatures.

Simplicity

Operational simplicity is required to allow full visibility of the infrastructure and to enable the operational support team to quickly analyse and troubleshoot any faults.

Scalability

The constant evolution and digitalisation of the oil and gas industry requires a massively scalable infrastructure.

OT and IT convergence

Gartner defines Operational Technology (OT) as hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.[1] OT networks usually include Industrial Control Systems (ICS) like Distributed Control Systems (DCS), and Supervisory Control And Data Acquisition (SCADA) systems.

OT-IT covergence refers to the integration of OT, which is used to control and monitor industrial processes, with IT, which is used to manage and process data using applications such as enterprise resource planning software and data analytics platforms. In recent years, this has become increasingly relevant with the digitalisation of industrial processes.

Traditionally, these networks did not require OT security since they were not connected to the Internet. However, with the increase demand for mobility and digitalisation of the industry, further convergence between the enterprise network and the operational network is increasing. This increases security risks and further expands the attack surface for bad actors.

1 https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

The convergence of OT-IT systems will help address industry challenges:

- It will allow for the seamless integration of processes and workflows which can ensure standardisation, interoperability and compatibility of processes
- Cost optimisation can be acheieved by facilitating sharing of data between IT and OT which can prevent errors
- Operational efficiency can be increased by enabling faster decision-making with real-time monitoring and emergency response

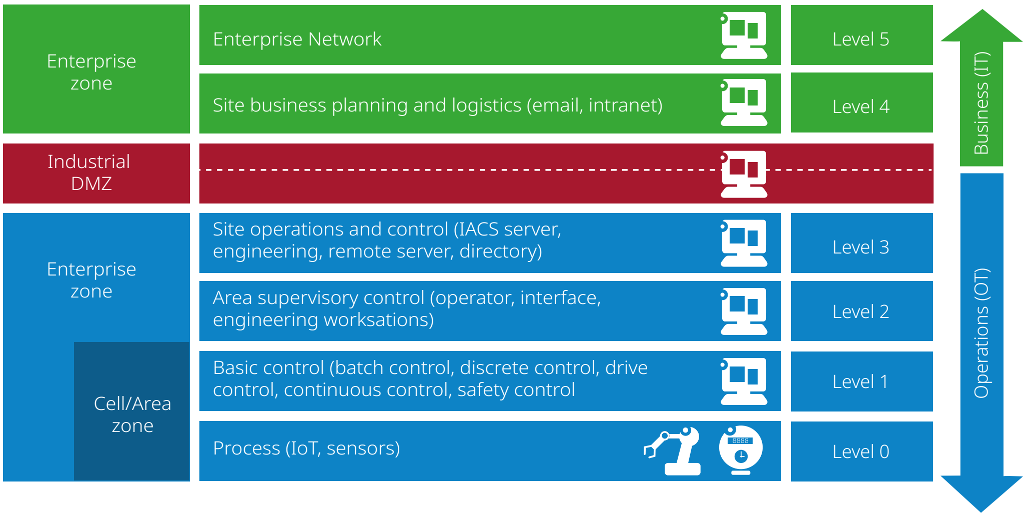
ALE's vision for the Oil and Gas industry

Alcatel-Lucent Enterprise's vision is to support the Oil and Gas industry's move from a connected industry to a smart and safe industry. This can be achieved by:

1. Enhancing safety and security by improving emergency management, alarm and notification services and context-aware communications, and by owning a resilient infrastructure.
2. Increasing operational efficiency by boosting employee productivity, allowing mobility and collaboration, and by securely onboarding Internet of Things (IoT) devices with automation.
3. Improving customer engagement with digital engagement and customer support, enhanced business applications with rich communication, and by interacting with Artificial Intelligence (AI) and Bots.

Oil and Gas reference architecture

Figure 2 - Purdue Enterprise Reference Architecture (PERA)



The Purdue Model, created by the Purdue University, has been widely adopted and was created to define best practices between industrial control systems (OT) and business networks (IT). This reference model is also part of the IEC-62443 standard defined by the International Electrotechnical Commission (IEC). This model provides segmentation at different levels, or zones, where each of them are responsible for a certain function or process. There are six network levels in the hierarchy:

Level 5 – Enterprise network

This level includes the enterprise network and is comprised of corporate-level services supporting individual business units. They include services such as e-mail, Human Resources Management System (HRMS), and other business applications. These services are usually hosted in data centres (DCs) in a different location or co-located.

Level 4 – Business network

This level consists of the access network connecting to local users. Business workstation, IP Telephony, printers, and other peripherals are located at this level. It is the last level where direct Internet access should be allowed. Network communications can be best effort delivery with normal reliability and resiliency.

OT-IT Boundary – Industrial DMZ

Sometimes refered to as Level 3.5, this is the boundary where the industrial DMZ (iDMZ) is located. It is the buffer zone where the highest security should be implemented to segment IT and OT communication. External access should be very restricted for remote access for troubleshooting and monitoring purposes.

Level 3 – Site Operation and Control (Supervisory)

This level is where the monitoring, supervising and operational support for an entire site or region is located. Alarm servers, Industrial Automation and Control System (IACS) servers, Human-Machine Interfaces (HMIs), Historians, and management servers are located at this level of the hierarchy. Domain services such as DHCP, AD, DNS and time servers are located at this level. There is a high requirement for real-time communications with high reliability and resiliency at this level.

Cell Area/Zone

A cell/area zone is a functional area within a plant or facility and it includes the remaining Levels 0-2. These levels have a critical requirement for real-time communications, reliability and very low latency.

Level 2 – Local Operation and Control (Supervisory)

The scope of this level includes monitoring and supervisory control of a single process, cell, or line. Processes are usually isolated from one another and grouped by function, type, or risk. These include engineering workstations, HMIs, control room, and other systems.

Level 1 – Local (basic) Controllers

Often combined with Level 0, this level consists of controllers that communicate with Level 0 related instrumentation such as process sensors and actuators. DCS, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs) and control processors exist in this level.

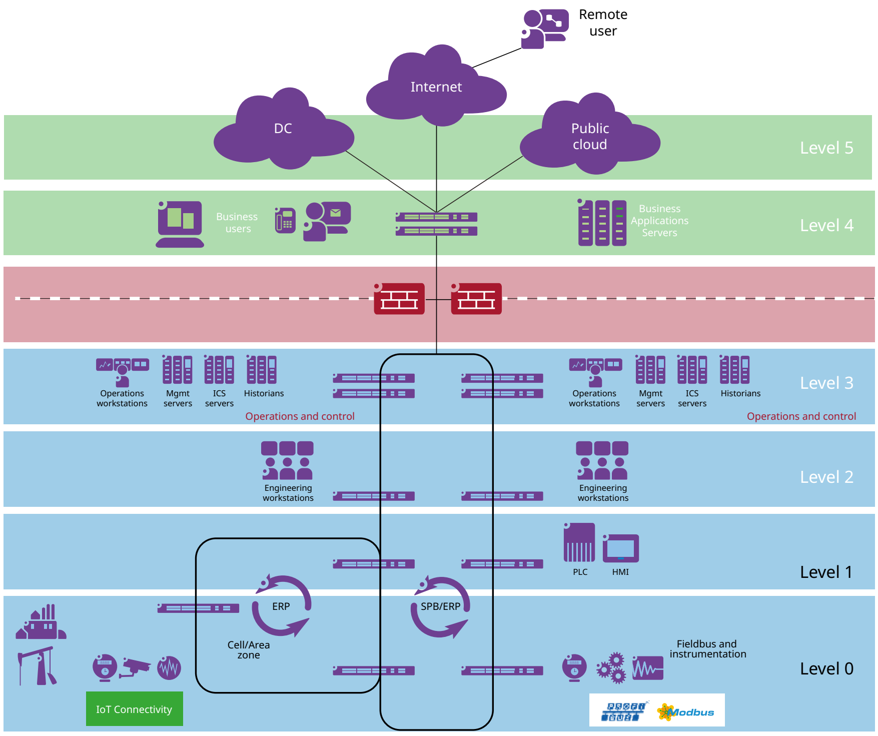
Level 0 – Physical Process/Field Devices

This level defines actual physical processes such as basic sensors and actuators, Intelligent Electronic Devices (IEDs), Industrial IoT (IIoT) devices and other field instrumentation.

Solution overview

This document highlights the architecture proposed for the industrial and enterprise zones. You may refer to the Data Centre Solution Guide referenced in the Related Documents section for further details on our Data Centre architecture solutions.

Figure 3 - Industrial Automation Network Reference Architecture



In industrial networks, the backbone network is commonly connected in a ring topology, while a star topology is used in the access layer. Site attachment can be designed as Layer 2 or Layer 3. We will discuss the backbone layer architecture considerations for both classifications and later on discuss the access layer or site attachment. The architecture shown above uses two key technologies which support a dynamic and resilient network, Shortest Path Bridging (SPB) and G.8032v2 ring topology with Ethernet Ring Protection (ERP).

Why Use SPB?

SPB MAC-in-MAC (SPB-M), defined by the Institute of Electrical and Electronics Engineers (IEEE) in the specification IEEE 802.1aq, is a standards-based technology. SPB overcomes Spanning Tree Protocol (STP) limitation such as unused links, sub-optimal paths and slow convergence. It creates loop-free topology without blocking links and offers faster convergence and path optimisation. Benefits include:

- Less complex network: Dynamically build and maintain the network topology between nodes. SPB also uses a single control-plane protocol (IS-IS).
- Efficient operations: Load share and use all available physical connections making more bandwidth available
- Operations, Administration and Maintenance (OAM) support for monitoring and troubleshooting
- Improved performance: Seamless, sub-second network changes with a multi-path fabric for traffic distribution
- Reduce potential for human error: Automatic configuration to prevent human errors

SPB allows for micro-segmentation and a virtualised environment for increased security.

Alcatel-Lucent Enterprise hardened switches are the industry's only hardened switches that support SPB-M, which is ideally suited to the substation environment. SPB-M provides a resilient network that is easily provisioned, can expand quickly, and reliably carries critical data to where it needs to go on a predictable, consistent basis. The network can quickly heal itself and keep vital substation power-systems connected.

Low-latency and jitter is achieved using the SPB Protocol. Latency, jitter and packet loss Service Assurance Agent (SAA) tests are automatically set-up between all Backbone Edge Bridge (BEB) nodes and Backbone Core Bridge (BCB) nodes and across all Backbone VLANs (BVLANs). SPB support for multiple trees and multiple active paths unlocks utilisation of bandwidth in optimal paths that would otherwise be wasted, increasing throughput and reducing latency. Furthermore, in an SPB network, traffic is classified at the Service Access Point (SAP) and the classification does not change as traffic traverses the backbone and until it exits through another SAP at the destination BEB.

For more details, please refer to the SPB Architecture Guide referenced in the Related Documents section.

Why Use ERP and MRP technology?

Ring topologies are commonly used for industrial automation networks due to low latency, fast convergence times and long-distance wiring requirements. Following are two types of technologies that support ring topologies and provide protection mechanisms: ERP and Media Redundancy Protocol (MRP).

ERP

ERP is used in networks providing fast sub-second convergence. It enables rapid convergence times, typically less than 50 milliseconds, in the event of a link or node failure in a ring network. It does so by dynamically re-routing traffic through backup links, which helps to maintain network uptime and availability. It is designed for networks with physical layer ring or interconnected rings structures and provides a protected single path of communication between any two nodes in the network.

ERP is defined in the ITU-T G.8032 standard and is used to protect against network failures and minimise service disruptions.

Please refer to the ERP Application Note referenced in the Related Documents section for more details.

MRP

MRP may also be used in cases where interoperability is required with other vendors. MRP is a standard-based recovery protocol described in the IEC 62439-2 standard, applicable to high-availability automation networks with ring topologies. Its main functionality is to react deterministically, with predictable recovery mechanisms and recovery times, in the event of a single switch or link failure in networks. As a standards-based protocol, with interoperability among different vendors running MRP, it should allow for a smooth expansion of the existing network or a straightforward replacement of the incumbent vendor.

The MRP protocol defines predictable mechanisms of network recovery by assigning different "roles" and related functionalities to the switches in the ring. The Media Redundancy Manager (MRM) role is assumed by a single switch in the ring. Its tasks are to observe the ring topology by sending MRP test frames at a configured time period in both directions of the ring. It also controls the ring topology by keeping one ring port in forwarding while the other ring port is in blocked state if MRP test frames are received by another ring port. Keeping one ring port of MRM in blocked state for data plane frames prevents the formation of a Layer 2 loop in the ring. All other switches in the ring will assume a Media Redundancy Client (MRC) role. The main tasks of MRCs, in addition to forwarding MRP test frames sent by MRM, are to detect link changes on its own ring ports and to signal those changes towards the MRM. In the event that there is no link or switch failure in the network, the ring is closed.

Backbone design

ERP-based architecture

One of the options to implement in your backbone is a Layer 2 ring design with ERPv2 as shown in **Figures 4** and **5** below. Routing will be performed on the nodes used for Operations and Control, or in the firewall with a Virtual Router Redundancy Protocol (VRRP) for redundancy.

Figure 4 - ERP-based Backbone Design - Operations and Control Zone Routing

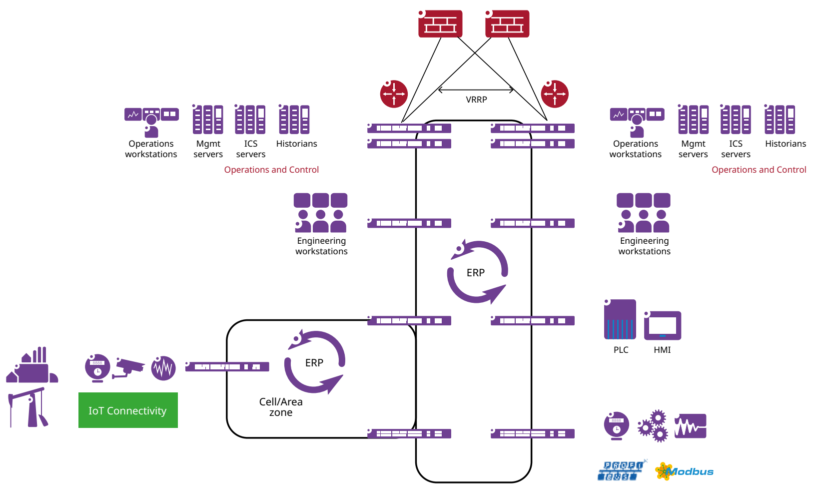
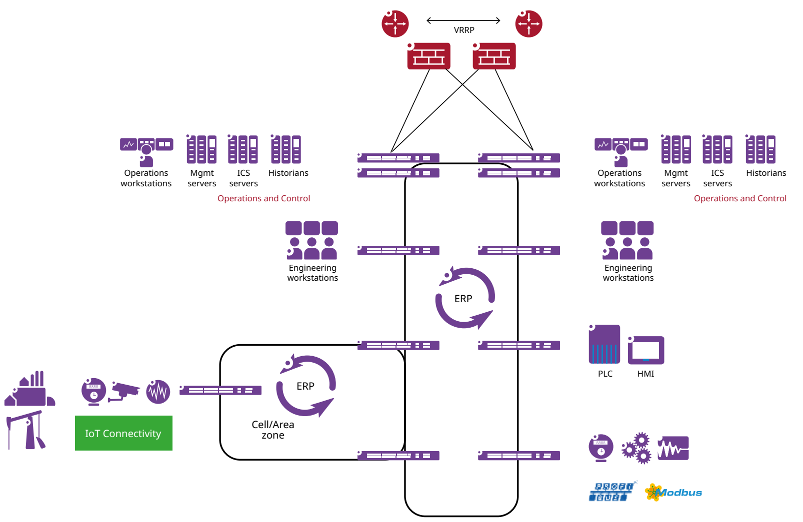


Figure 5 - ERP-based Backbone Design - iDMZ Firewall Routing



Advantages of this design include:

- Cost: Lower cost switches that do not require advanced routing capabilities can be deployed in the ring network and only the Operations and Control switches will require high-switching throughput and advanced routing.
- Rapid convergence time: Typically less than 50 milliseconds, in the event of a link or node failure in a ring network without dependance on another protocol for signalling

Disadvantages include:

- Non-scalable: This design increases the bridging domain which increases the failure domain and is therefore not scalable. A simple broadcast storm will cause network outages.
- Non-efficient use of under-utilised links
- Non-service oriented architecture

The above disadvantages can be solved by using SPB in your network and limiting VLAN and Service ID (ISID) sharing across hierarchical levels.

SPB-based Architecture – L2VPN

Figure 6 - SPB L2VPN Backbone Design - Operations and Control Zone Routing

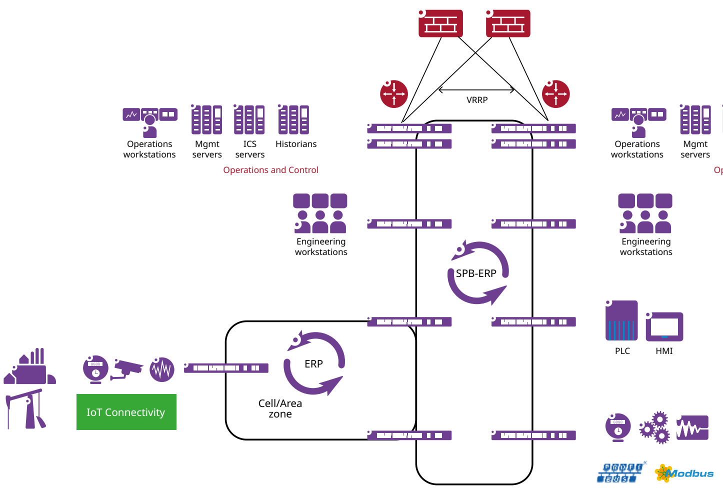
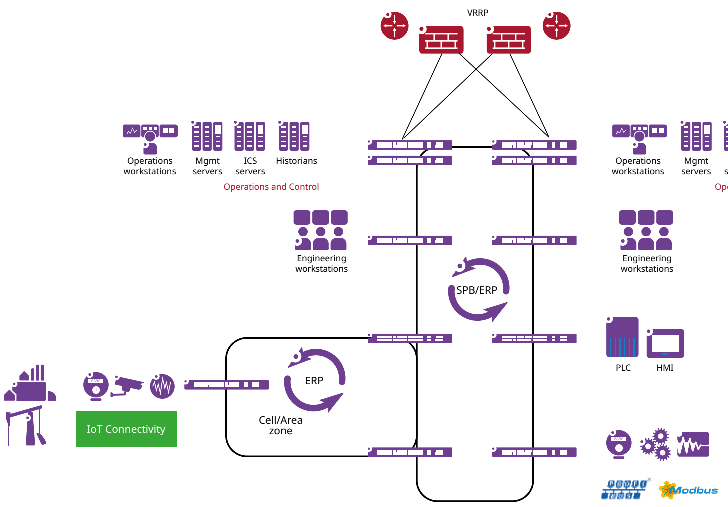


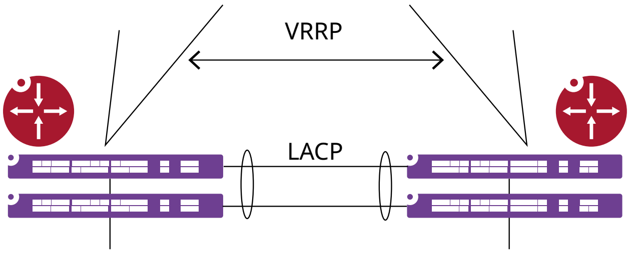
Figure 7 - SPB L2VPN Backbone Design - iDMZ Firewall Routing



In **Figures 6** and **Figure 7**, SPB is used as backbone network protocol. In an L2VPN architecture, no routing is performed at the cell/area zone level or at the point of attachment to the backbone, the BEB. Site VLANs (CVLANs) will be mapped to ISIDs at the site BEBs through SAPs. The default gateway of Customer VLANs (CVLANs) and inter-VLAN routing will be performed at the Firewall or the Operation and Control nodes with VRRP load-balancing by splitting the subnets between both of them. There will be two VRRP groups and the priority for each group will be set such that each switch is a master of one group. This will evenly balance traffic across BVLANs and VRRP groups. Dynamic User Network Profile (UNP) and SAPs will be configured on BEB nodes as per the different CVLAN. To provide the necessary micro-segmentation, VLANs can be segregated at each level of the Purdue hierarchical model as discussed in the Oil and Gas Reference Architecture section.

Virtual Chassis

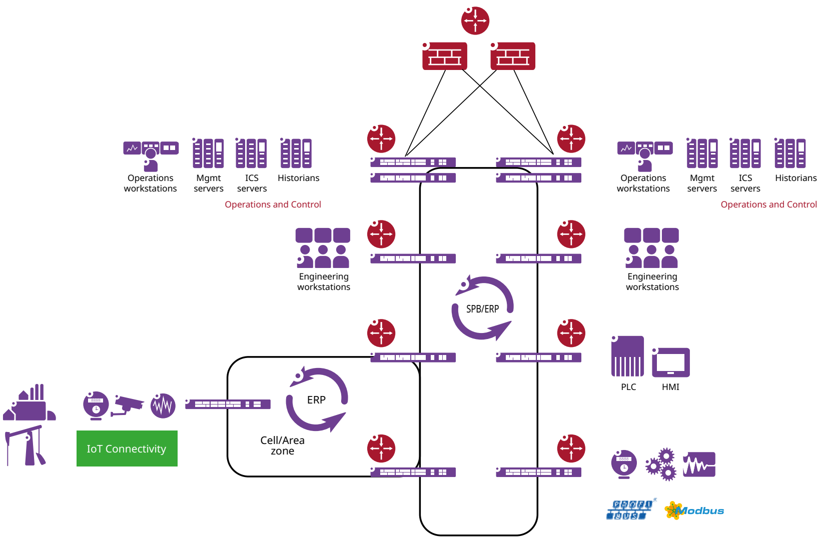
Figure 8 - Virtual Chassis Operations and Control Nodes



The Virtual Chassis (VC) feature can be used for redundancy at the Operation and Control nodes to provide a single logical entity of multiple switches with a single control and management plane. The ERP Ring between Operation and Control zones can be connected with redundant links and a Link Aggregation (LAG) protocol, such as Link Aggregation Control Protocol (LACP), can be configured or can be connected with a single link.

SPB-based architecture – L3VPN

Figure 9 - SPB L3VPN Backbone Design



In an L3VPN architecture, routing is performed on each site BEB with different sites using different subnets with the BEB configured as the site's default gateway. Inter-subnet routing is required to connect the sites. By leveraging the existing SPB control plane IS-IS instance, site routes are exported to the SPB IS-IS instance, associated to the ISID, and bound to the WAN IP as a gateway address.

In terms of data plane traffic, SPB bridges traffic from ingress BEB to egress BEB along the shortest path.

Shared services such as DHCP, DNS; and DC services can be implemented through Virtual Routing and Forwarding (VRF) leaking.

Please refer to the SPB Architecture Guide referenced in the Related Documents section for more details.

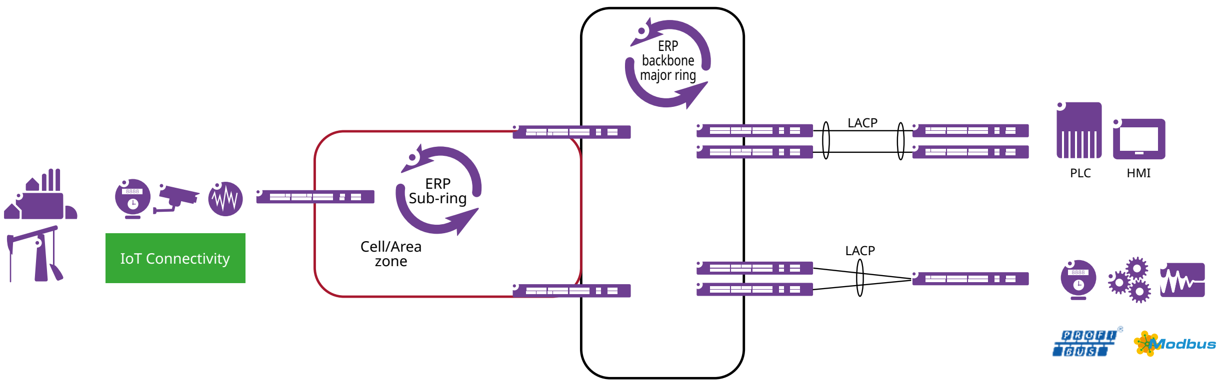
Site attachment

The access layer is where the endpoint devices will connect to the network. Segmentation, Quality of Service (QoS), and policy enforcement should be done at this layer. Segmentation allows for smaller bridging and failure domains and limits Broadcast, Multicast, and Unknown Unicast (BUM) traffic to each segment. The site or cell/area zone can be connected in a Link Aggregate using LACP or in a multi-ring design with ERPv2.

LAG and VC

LACP aggregates one or more Ethernet interfaces to form a logical point-to-point link to increase bandwidth and availability. It provides network redundancy by load-balancing traffic across all available links. The VC could be configured on the cell-area zone or not, however if using LACP, the VC should be configured in the backbone. This allows the backbone switches to have a centralised control and forwarding plane.

Figure 10 - Site attachment options



ERP Multi-ring design

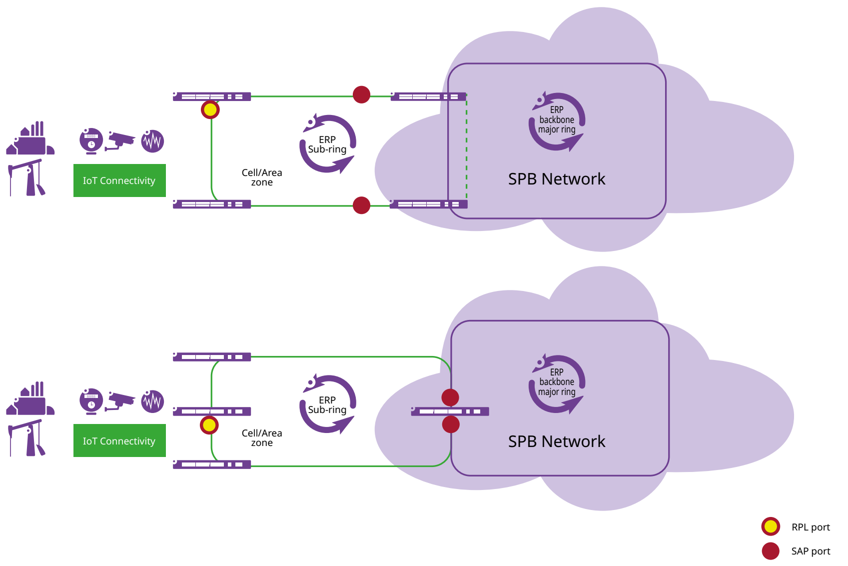
If we are using an ERP-based backbone architecture shown earlier, then configuring a sub-ring at the site attachement is supported. This is called a multi-ring design. The sub-ring is connected to the Major Ring at the interconnection nodes. The sub-ring is controlled by its own ERP instance with its own Ring Protection Link (RPL) and Ring Automatic Protection Switching (R-APS) channels are not shared across ring interconnections. The major ring however controls the full physical ring.

Please refer to the ERP Application Note referenced in the Related Documents section for further details.

ERP and SPB interworking

In the event you are using an SPB-based backbone architecture, the sub-ring can be attached to two BEBs through SAP ports. We can provide seamless connectivity between the ERP ring and the SPB backbone. The ring is closed through the SPB backbone and R-APS Protocol Data Units (PDUs) will be tunneled through the SPB backbone to other BEBs connecting the ISID. An ERP control VLAN is created on the site and an ISID is created to transport it across the SPB backbone. The SPB Service associated with the ERP Service VLAN must be configured in the Control BVLAN. The RPL port should not be configured in the ERP BEB. SPB BEBs will participate in both SPB and ERP protocol exchanges and will trigger an RPL port-down or port-up when a link failure is detected.

Figure 11 - ERP/SPB interworking



There are two topologies supported as shown in **Figure 11**. ERP rings can connect to the SPB network through a single BEB or through separate BEBs.

Centralised operations and management

Operations and Control Zone

The Operations and Control Zone or Control Room Operations is the primary centralised location where all aspects of the ICS are supervised and controlled and responses to incidents are coordinated. The Operations and Control Zone manages the multiple complex processes involved in each of the industrial segments. Multi-disciplinary teams as well as various systems, applications, databases and interfaces with third-parties such as emergency responders can also be found in the Operations and Control Zone. A Backup Operations and Control Zone can be setup to host redundant infrastructure and resources such that it can replace the Operations and Control Zone in the event of a disaster or during maintenance. The Operations and Control Zone and the Backup Operations and Control Zone can operate in active/active or active/standby mode.

Since the Operations and Control Zone and the Backup Operations and Control Zone are connected as part of the same ring topology, they will benefit from fast convergence with ERPv2.

Management

Management of the network nodes can be done in several ways depending on the architecture.

ERP-only:

- Out-Of-Band Management (OOBM) with Ethernet Management Port (EMP) Ports
- OOBM with VLAN port
- In-band Management with Management IP Interface

SPB L2VPN/L3VPN:

- OOBM with EMP Ports
- OOBM with Management IP Interface
- In-band Management with Management IP Interface on the Control BVLAN
- Dedicated Management SPB Service and VRF Instance

It is always recommended to use OOBM, and in case in-band management is used, then a dedicated management VRF and service should be created different from customer or service traffic.

Alcatel-Lucent OmniVista 2500 Network Management System

The Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) provides a comprehensive and powerful network management tool. You'll benefit from a full set of components for infrastructure and device configuration, monitoring, backup, scheduling, security, alerts, quarantine, troubleshooting, downtime resolution, and overall management. Along with making day-to-day network operations more efficient, OmniVista provides all the network management tools and reports you need to track and achieve your business goals.

The SPB network can also be easily managed from OmniVista. OmniVista allows detection and configuration of:

- SPB links
- BEB and BCB devices in the SPB network
- SPB Services and SPB access interface
- SPB SAP and SPB Service Distribution Point (SDP)
- Layer 2 switches/access points (APs) connected to the SAP

Please refer to OmniVista 2500 NMS datasheet referenced in the Related Documents section for more details on OmniVista 2500.

Operations, Administration and Maintenance Tools

Ethernet Operations, Administration, and Maintenance (OAM) can provide the detection, resiliency, and monitoring capability for end-to-end service guarantee in your mission-critical network. Service OAM (IEEE 802.1ag and ITU-T Y.1731) and Link OAM (IEEE 802.3ah EFM Link OAM) can be used to troubleshoot and monitor services or individual links to ensure the network is running efficiently and at an optimal level.

Additionally, the Service Assurance Agent (SAA) tool, enables customers to assure new business-critical applications, as well as services that use data, voice and video. Use SAAs to verify service guarantees, increase network reliability by validating network performance, proactively identify network issues and increase Return on Investment (ROI) by easing the deployment of new services. The SAA feature uses active monitoring to generate traffic in a continuous, reliable and predictable manner, thus enabling network performance and health measurement.

Please refer to the Alcatel-Lucent OmniSwitch® Network Configuration Guide referenced in the Related Documents section for further details.

Automation

The Alcatel-Lucent Enterprise Autonomous Network architecture operates from the network edge to the core.

Unified edge: Users, devices, and IoT can connect to the Local Area Network (LAN) and/or Wireless Local Area Network (WLAN) with a consistent connection experience and performance capabilities. Switching from fixed LAN to wireless LAN with the same device is simple and secure.

Unified fabric: LAN, WLAN, core/data centre, and soon, a branch portfolio with cloud management and embedded security.

Network services automation: This is the key layer in the autonomous network that enables network automation through programmability, provisioning, analytics, the Rainbow™ by Alcatel-Lucent Enterprise workflow engine, as well as third-party integration.

Security

Alcatel-Lucent Enterprise follows two approaches to securing mission-critical infrastructure: Privacy by Design, and a Multi-Layered Approach.

Privacy by Design

Alcatel-Lucent Enterprise offers a four-step Privacy by Design approach, that provides a foundation to build and maintain an efficient and legally-compliant digital infrastructure. The Privacy by Design approach allows you to control the data, devices and shared online services.

The Privacy by Design steps are:

1. Build a trusted infrastructure

   The zero trust approach prevents non-secured devices and content from entering your system. When building your infrastructure, you need to ensure the foundation is secured. A trusted technical partner can accompany you during and after implementation to ensure continuous security. Please refer to the Zero Trust Architecture ebook referenced in the Related Documents section.
2. Study the impact on the company and its ecosystem

   Organisations must be ready to respond to data requirements and requests for data reports. You must control and know your data cartography and processing.
3. Adopt the latest digital trust standards

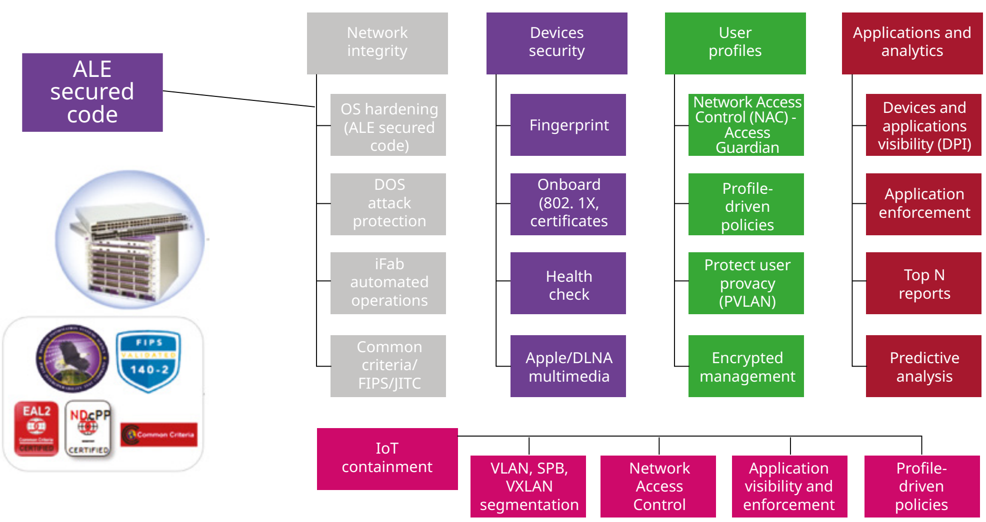
   After building and studying the infrastructure, addressing regulations standards is mandatory for compliancy, which can increase your client and employee trust in you.
4. Combine key factors for a successful implementation

   The last step is the definition of rules, further analysis and archiving. Once you are compliant with the regulations and standards you can maintain compliancy throughout the long-term with built-in security and flexible models.

Multi-Layered security

The OmniSwitch implements a Multi-Layered Security approach to secure the data, control and management plane of the switch. The following sections covered the various security implementations:

Figure 12 - ALE Multi-Layered Security approach



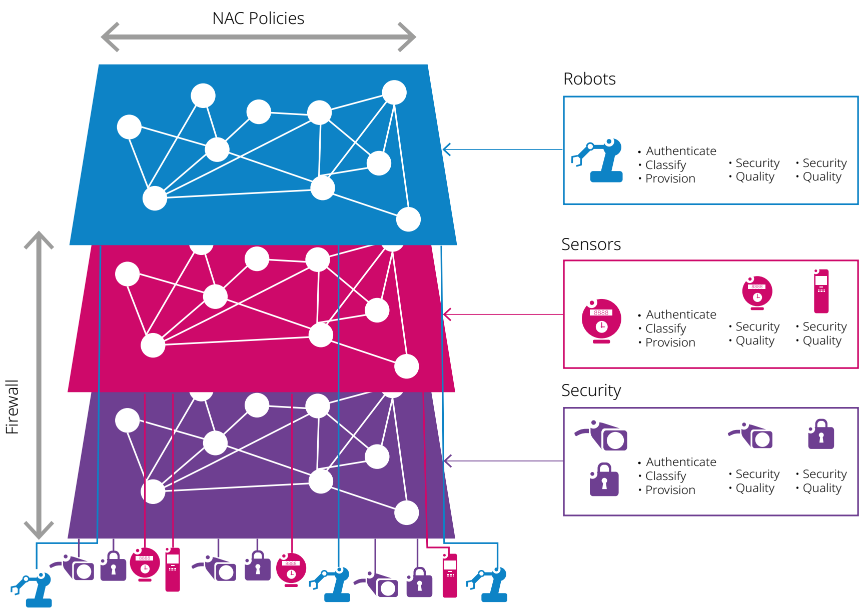
Following are a few best practices and recommendations to follow to secure your network infrastructure:

1. Update Alcatel-Lucent OmniSwitch and Alcatel-Lucent OmniAccess® Stellar APs regularly to ensure the latest vulnerabilities are patched and mitigated.
2. Avoid using insecure protocols in your network.
3. Ensure the switch code is protected by using ALE Secure Diversified Code.
4. Implement micro-segmentation and zero-trust strategies in your network and authorise Network Admission Control (NAC) policies.
5. Enable integrity and confidentiality in your network.

Please refer to the ALE Layered Approach and the Network Infrastructure Solutions Security Best practices documents referenced in the Related Documents section for further details.

Micro-segmentation

Figure 13 - Micro-segmentation



In the ALE IoT segmentation solution, IoT devices are grouped into different containers: Robots, sensors and security, among others. This containerisation increases security because a container is isolated from other containers, and devices in different containers can only communicate through a firewall. In addition, devices are mapped to containers according to the device type using authentication (MAC or certificate-based 802.1x). Once the device type and container are determined, the device is bound to a UNP which also restricts communication with other devices, even if in the same container, and apply fine-grained QoS policies to the device. In short, SPB creates a service-oriented secured network.

Another benefit of using SPB in the backbone network is that it is inherently more secure as the SPB nodes do not route IP traffic, they bridge it. This protects the network from IP-based attacks such as port-scans, spoofing, Denial-of-Service (DoS) attacks and others.

ALE compliancy and certifications

Alcatel-Lucent Enterprise solutions have extensive certification which validates our technology and services safety and security. Following are a number of certification bodies that have certified the ALE switching portfolio:

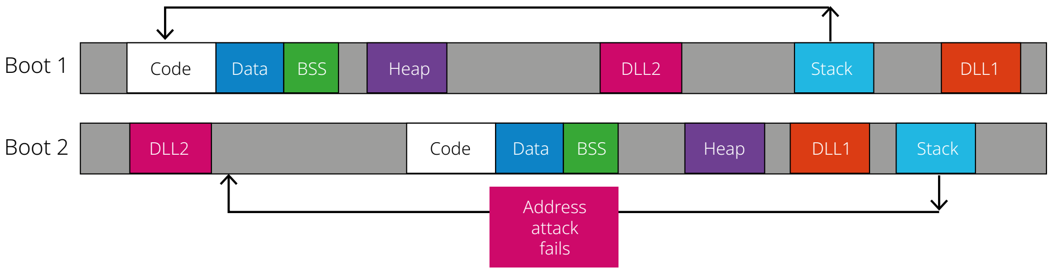
Common Crtiteria (CC): This certification provides assurance that the specification, implementation and evaluation process for software or IT product security has been conducted in a rigorous, standard and repeatable manner at a level that is equivalent with the target environment for use.

Joint Interoperability Test Command (JITC): JITC is the US Department of Defense's Joint Interoperability Certifier and only non-Service Operational Test Agency for Information Technology (IT) / National Security Systems (NSS). JITC provides risk based Test Evaluation and Certification services, as well as tools and environments to ensure Joint Warfighting IT capabilities are interoperable and support mission needs.

Federal Information Processing Standards (FIPS): FIPS are standards and guidelines for federal computer systems that are developed by the National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the federal government, many in the private sector voluntarily use these standards.

ALE Secured Diversified Code

Figure 14 - ALE Secured Diversified Code



Alcatel-Lucent Enterprise Secure Diversified Code technology uses a proactive security approach through Independent verification and validation (IV&V) and operational vulnerability scanning and analysis of switch software within the network equipment portfolio. It reviews the source code for:

- Equipment software vulnerabilities
- System exploits
- Embedded malware
- Back-door in software

The independent verification and validation works on identifying potential threats that may not be discovered during the internal Software Quality Assurance (SQA) testing.

ALE provides IV&V on external interfaces which connect to the software, including:

- HTTPS Interface
- Login Interface
- Network Time Protocol (NTP) Interface
- Command Line Interface (CLI)
- IP Port Usage
- Simple Network Management Protocol (SNMP) Interface
- Data Packet Interface

This identifies any security vulnerabilities in the software by a third-party to ensure network infrastructure integrity.

In addition to IV&V, ALE software diversification rearranges the memory map of the executable program so that various instances of the same software, while functionally identical, are arranged differently in memory. The Address System Layout Randomisation (ASLR) is a standard feature in the ALE switching portfolio. ASLR results in a unique memory layout of the software being run, each time the OmniSwitch reboots, to impede or prevent software exploitation.

MACsec

MACsec is an IEEE 802.1AE standard that provides security with encryption and authentication of Ethernet links between directly connected nodes. MACsec-enabled links are secured by matching security keys which are periodically refreshed. This provides confidentiality and integrity of data, preventing attacks such as:

- DoS
- Man-in-The-Middle (MiTM)
- Playback
- Wire-tapping
- Masquerading

Because MACsec operates at the MAC layer, it transparently secures all upper layer traffic transiting through MACsec-enabled links. This includes both application-layer data, as well as control-plane and management-plane communications. In addition, unlike IPSec, MACsec is implemented in hardware at wire-speed and does not introduce additional latency or bandwidth limitations.

MACsec can be configured between the ERP ring nodes at the backbone and access layers to provide the required confidentiality and integrity.

Please refer to the OmniSwitch AOS Network Configuration Guide referenced in the Related Documents section for more details on how to configure MACsec on your network.

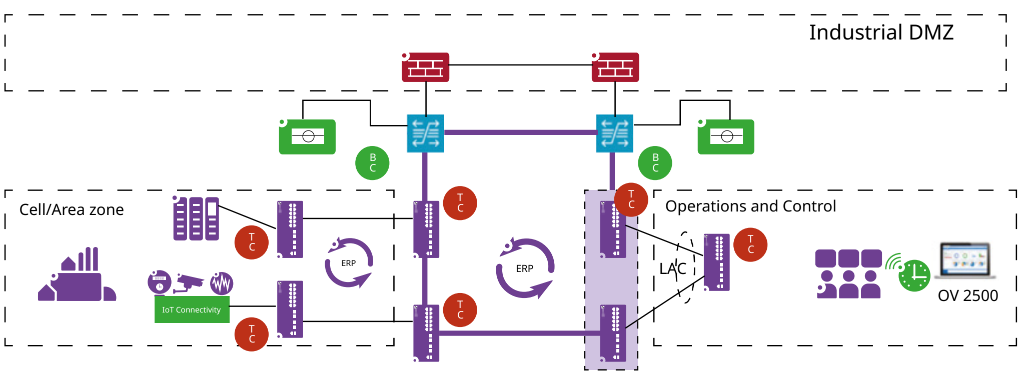
IEEE1588 – Precision Time Protocol

Accurate and precise timing is vital in mission-critical networks such as industrial plants and electric power utilities. They must synchronise time to ensure devices have accurate clocks, with accuracy measured in nanoseconds, for system control and consistent operation of automation systems. Incorrect timing can cause disasters in use cases such as motion control systems.

One of the protocols used to provide clock synchronisation of other network elements in the packet-based networked systems is defined by IEEE 1588-2019. It is the IEEE Standard for a Precision Clock Synchronisation Protocol for Networked Measurement and Control Systems also known as the Precision Time Protocol (PTP).

PTP enables system-wide synchronisation accurancy in the sub-microsecond range and supports redundancy and security.

Figure 15 - PTP architecture



Please refer to the PTP Application Note referenced in the Related Documents section for more details.

IEC 61850 messages

Alcatel-Lucent Operating System (AOS) can provide prioritisation of different types of messages as per the IEC 61850 standard, which defines communications protocols for IEDs at electric substations. Different message types are supported including Generic Object Oriented System Event (GOOSE) messages, Manufacturing Message Specification (MMS) messages, Sampled Values (SV) messages, and more. IEC 61850 messages can be prioritised based on applying a specific QoS priority to different message types.

Please refer to the OmniSwitch AOS Network Configuration Guide referenced in the Related Documents section for more details.

Conclusion

Alcatel-Lucent Enterprise offers a comprehensive set of solutions for the oil and gas industry to address their challenges, accelerate digitalisation across segments, optimise operations and increase productivity to meet the energy market's ever-increasing demands. Alcatel-Lucent Enterprise multi-layered security protects the mission-critical infrastructure from cyberthreats.

Appendix

Acronyms

AD	Active Directory
AI	Artificial Intelligence
AOS	Alcatel-Lucent Operating System
AP	Access Point
ASLR	Address System Layout Randomisation
BCB	Backbone Core Bridge
BEB	Backbone Edge Bridge
BUM	Broadcast, Multicast and Unknown Unicast
BVLAN	Backbone VLAN
CC	Common Criteria
CLI	Command Line Interface
CVLAN	Customer VLAN
DC	Data Centre
DCS	Distributed Control Systems
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DoS	Denial-of-Service attack
E&P	Exploration and Production
EFM	Ethernet in the First Mile
EMP	Ethernet Management Port

ERP	Ethernet Ring Protection
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GOOSE	Generic Object Oriented System Event
HMI	Human-Machine Interface
HRMS	Human Resources Management System
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
IDMZ	Industrial De-Militarized Zone
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
ISID	Service ID
IT	Information Technology
ITU-T	The International Telecommunication Union Telecommunication Standardisation Sector
IV&V	Independent Verification and Validation
JITC	Joint Interoperability Test Command
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation
LAN	Local Area Network
MAC	Media Access Control
MACSec	Media Access Control Security
MiTM	Man-in-The-Middle attack
MMS	Manufacturing Message Specification
MRC	Media Redundancy Client
MRM	Media Redundancy Manager

MRP	Media Redundancy Protocol
NAC	Network Admission Control
NIST	National Institute of Standards and Technology
NMS	Network Management System
NSS	National Security Systems
NTP	Network Time Protocol
OAM	Operations, Administration, and Maintenance
OOBM	Out-Of-Band Management
OT	Operational Technology
PDU	Protocol Data Unit
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller
PTP	Precision Time Protocol
QoS	Quality of Service
R-APS	Ring Automatic Protection Switching
ROI	Return On Investment
RPL	Ring Protection Link
RTU	Remote Terminal Unit
SAA	Service Assurance Agent
SAP	Service Access Point
SCADA	Supervisory Control And Data Acquisition
SDP	Service Distribution Point
SNMP	Simple Network Management Protocol
SPB	Shortest Path Bridging
SQA	Software Quality Assurance
STP	Spanning-Tree Protocol
SV	Sampled Values
UNP	User Network Profile
VC	Virtual Chassis
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VPN	Virtual Private Network

VRRP Virtual Router Redundancy Protocol

WAN Wide Area Network

WLAN Wireless Local Area Network

Related documents

[1] Industrial Automation Solution Guide

[2] Data Center Solution Guide - https://www.al-enterprise.com/-/media/assets/internet1ccc/documents/data-centre-reference-design-solution-guide-en.pdf

[3] PTP Application Note - https://www.al-enterprise.com/-/media/assets/internet/documents/precision-time-protocol-application-note-en.pdf

[4] ERP Application Note - https://www.al-enterprise.com/-/media/assets/internet/documents/ethernet-ring-protection-switching-application-note-en.pdf

[5] SPB Architecture Guide - https://www.al-enterprise.com/-/media/assets/internet/documents/spb-architecture-tech-brief-en.pdf

[6] Zero-trust Architecture eBook - https://www.al-enterprise.com/-/media/assets/internet/documents/zero-trust-architecture-ebook-en.pdf

[7] Network Infrastructure Solutions Security Best practices - https://www.al-enterprise.com/-/media/assets/internet/documents/network-infrastructure-solution-security-tech-brief-en.pdf

[8] ALE Layered Approach to Security - https://www.al-enterprise.com/-/media/assets/internet/documents/ale-layered-approach-to-security-transportation-tech-brief-en.pdf

[9] OmniVista 2500 NMS Datasheet - https://www.al-enterprise.com/-/media/assets/internet/documents/omnivista-2500-nms-datasheet-en.pdf

[10] OmniSwitch AOS Network Configuration Guide

Alcatel·Lucent Enterprise