Blueprint solutions for maritime vessels

White Paper
Blueprint solutions for maritime vessels

Alcatel·Lucent
Enterprise

Table of Contents

Introduction

As the maritime sector evolves to become more efficient and create a safer environment, new concepts and technologies are emerging every day. Digitalization within the maritime vessels sector extends beyond just the successful application of innovative technology – sustainability and safer shipping are of paramount importance. Smart shipping plays a crucial role in this area, including automating processes, preventive maintenance, and working more efficiently with the Internet of Things (IoT). Extensive automation requires a solid foundation to connect all systems, subsystems, and applications together seamlessly and simply. The building blocks essential to this undertaking will be described in the following sections.

Maritime vessels systems have traditionally been a mixture of different analogue and/or digital systems that operate independently of all other systems with little or no communications between systems. Alcatel-Lucent Enterprise's vision is based on experience gained through its eco-system of customers, System Integrators, and procurement agencies. We allocate resources to help improve legacy networks where budgets may be constrained, and where needed we build advanced, future-proof solutions. This enables a better experience and quality, increased productivity, as well as improved crew and passenger welfare. It also decreases IT workloads so they can focus on better workflow for optimum efficiency and availability.

Blueprint overview

Maritime vessels use data networks and voice/video communications for maritime and naval operations to monitor and control the ship, provide administration services, and to ensure safety and security for the ship and crew members.

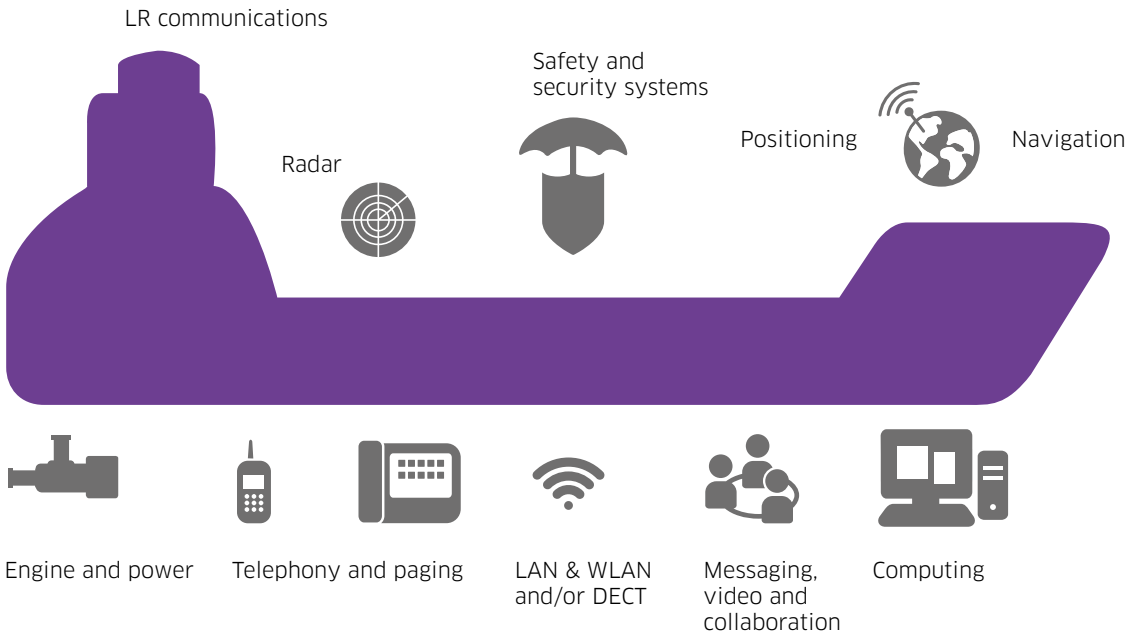
Onboard sea vessels there are a multitude of systems instrumental to support daily complex operations. These systems include:

- Safety and security
- Ship control
- Administration

Onboard systems

It is important to note that critical components of the communications system must be designed in such a way that any disruption does not directly lead to service interruption. Resilience and self-healing must be seriously considered when designing onboard networks and communications systems.

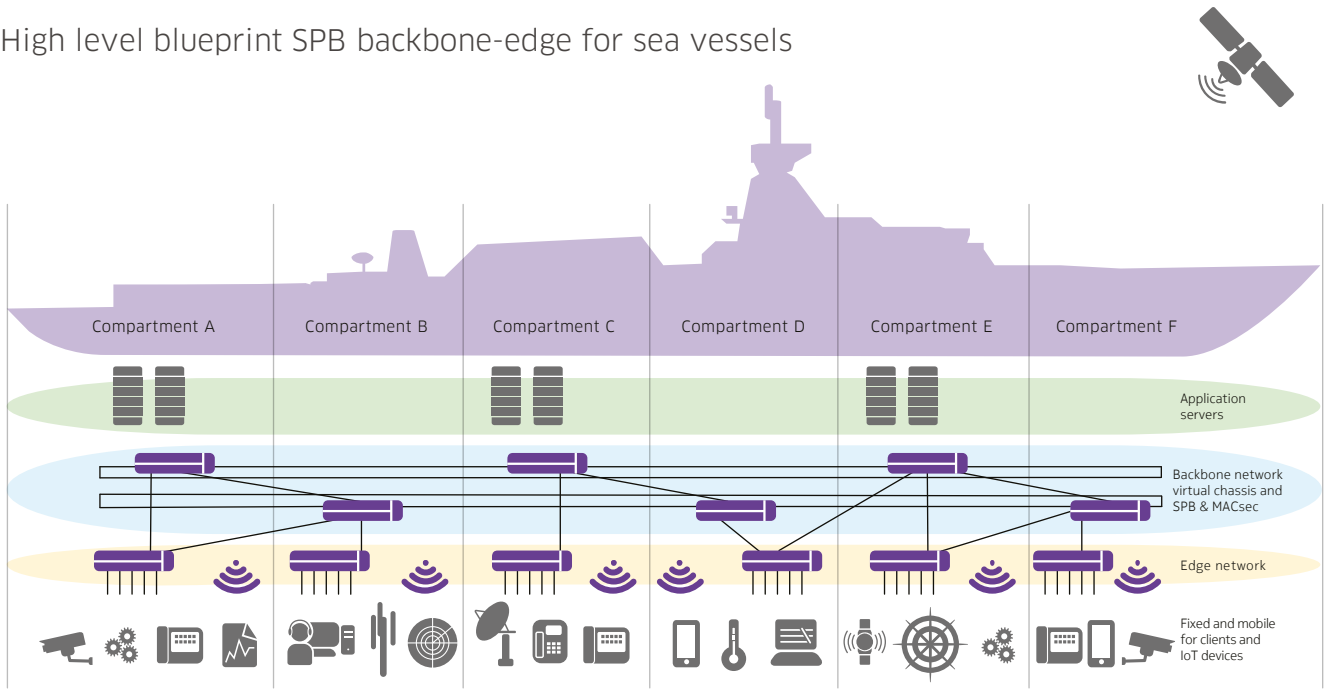
The diagram below provides a high-level overview of the critical communications systems:



Network design

The network diagram as shown below, represents a layered infrastructure adapted to the construction of a ship's hull, divided into watertight compartments to contain a breach of the hull that could affect the whole ship. The network must be extremely resilient to maintain services in emergency situations such as power failures, floods, or any other disaster. With multiple physical links and virtual capabilities, this network guarantees services for the unaffected compartments. In the event of physical link failures the network will automatically heal itself with fast-sub-second convergence time, using standard protocols to redefine network routes. This network supports services such as maintenance and operation, communications, back office, control center, and deck management, and among others, it has the automatic segmentation capability and security at the edge, including encryption and IoT containment.

High level blueprint SPB backbone-edge for sea vessels



IS-IS SPB and MACsec, two protocols combined to build a highly resilient, scalable and secured network

Maritime vessel communication specifics

Installing and using a network and communications system requires the following:

Maritime compliancy	• DNV-GL certifications • IEC 60945 certifications (Class A and B for ship deck and bridge applications)
Securing the installation (ISO 27001)	• Hardware, software, access control and monitoring
Communications between parties	• Network resilience and independencies between vessels compartments/segments • Network interoperability and open standards • Network security • Interfaces, bandwidth, traffic priority, encryption • Network updates • Long lifetime • Ease of operations and fast recovery in case of disaster
Powering the devices	• VDC, VAC, PoE variants
Recording the files	• Storage (24x7x365)
Analysing the data	• ICT team, access rules • IoT for preventive maintenance • Application monitoring and visibility for network analytics
Optional features	• Speakers, information panel (single pane of glass), Wi-Fi, µCell, analysis prediction and trends

Infrastructure fundamentals

Data network

The data network generally known as, Fully Integrated Information and Communication system (FICS), or Information, Communication and Command System (ICCS) is a converged network using IP over Ethernet. The main elements include:

- Utilization of open standards
- DNV-GL certified hardware
- IEC 60945 approved hardware
- SPB redundant and virtualized core network (containment of services)
- DNV-GL LAN access network SPB compliant for carrier grade mission critical network
- WLAN network based on latest Wi-Fi standards
- Servers and applications virtualization
- Network virtualization
- Advanced L3 routing capabilities/features wire-rate for any type of services
- ISS features (ACL, NAC, UNP)
- IoT filters and containment based on device finger printing
- Hardened code
- Unified NMS
- Controlled welfare

For operational reasons the network system must provide day-to-day (24x7x365) uninterrupted operations even in challenging conditions.

Voice components

Voice communication components required for intra-communication between the ship bridge and the crew and/or passengers:

- Voice exchange system (Analogue/Digital or IP terminals)
- Fixed telephony; either analogue, digital and/or IP
- Mobile telephony using DECT and/or Wi-Fi
- Rainbow™ by Alcatel-Lucent Enterprise application for crew if Wi-Fi or µCell systems allowed
- Handheld UHF/VHF/PMR
- Notification services
- Recording
- Controlled welfare

For security and safety reasons the voice system must provide day-to-day (24x7x365) operations and availability.

Power supplies

- Local source such as legacy VAC or VDC power plant or solar panels
- Remote source such as PoE and variants

Crew and passengers applications

- Welfare/Entertainment
- Internet
- Video/TV
- Wi-Fi
- Telephony
- Messaging

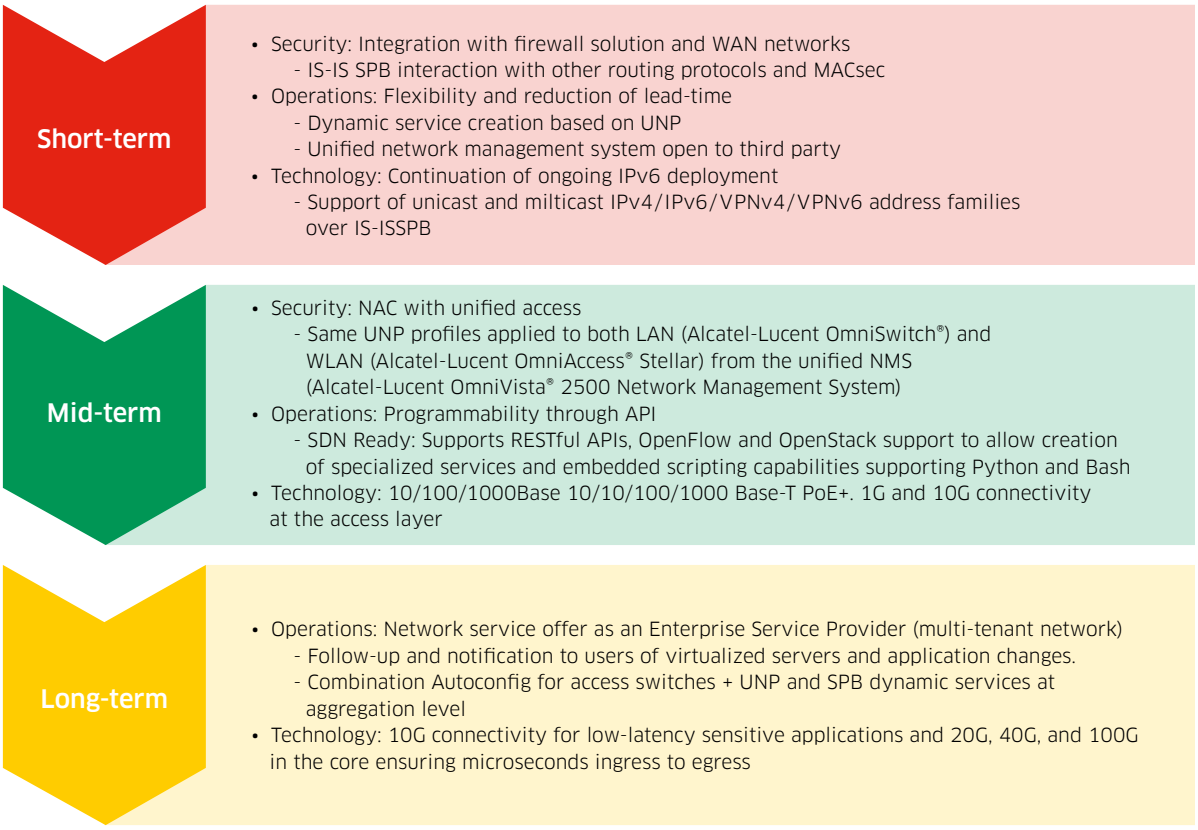
Safety and Security

- Ship Security Reporting System
- Automatic Identification System
- Global Maritime Distress Safety System
- Long Range Tracking and Identification System
- Vessel Monitoring System
- Automated Manifest System
- Automated Mutual Assistance Vessel Rescue System
- Vessel Management System
- RF and SatCom systems
- LAN infrastructure
- Handheld UHF/VHF/PMR

Administration

- Maritime applications
- Administration applications
- Mobile and fixed telephony
- RF and SatCom systems
- LAN infrastructure
- Logistics systems
- Notification system

ICT models for ships



Connected devices

In an Ethernet model, wired and/or wireless devices are always connected and powered, events or alerts are available immediately via the unified network management system. The system is centrally configurable to address a particular, predicted, emergent condition or provisioned to address a number of emergent needs.

In all cases a two-way communications are required for a better user experience. Due to the large number of devices and an increase in less qualified technologies (software openness, open hardware), the ICT team should ensure there are no issues or back door access from such devices.

Alcatel-Lucent Enterprise assists by containing those devices in limited and secured network segments with DoS mitigation and checking any abnormal traffic.

Mission-critical network design

A vessel's network must be designed to be resilient and meet the highest standards with no single points of failure. Typically, large sea vessels are comprised of seven compartments (for example ship haul segments). The data network must be designed to continue operation should one of these compartments fail. There are a number of mission-critical network technologies and designs available for use onboard sea vessels from SPB to ERP and MRP and virtualisation of the switching systems.

Ships do require a robust multi-service and fast convergence critical network technology. For this reason, Alcatel-Lucent Enterprise recommends Shortest Path Bridging (SPB) technology, which is robust, highly scalable and secure, and is designed to support multiple networks over the same physical infrastructure while keeping investment to a minimum. SPB is also highly capable of carrying multicast traffic for video and voice announcements, which are key to the vessel operation. SPB simplifies deployment and maintenance by automatically assigning services and devices to the correct network container. Creation of new services can be done instantly without having to redesign or re-configure the network. A second technology that can be deployed is Ethernet Ring Protection (ERP), which offers faster convergence times but is not as flexible as SPB, however, this technology may be easier to deploy depending on the fibre deployed in a ship.

Why choose Alcatel-Lucent Enterprise

- Proven track record (naval and commercial deployments)
- Purpose-built solutions and values, with carrier-class technology and performance
- Single vendor with maritime certified solutions for telephony, Ethernet switching and WLAN (Wi-Fi)
- PoE Models: 10, 24 or 48 auto-sensing Gigabit RJ45 access ports with 380w/780w PoE budget, IEEE 802.3af and IEEE 802.3at PoE compliant, with Dynamic PoE allocation (delivering only the amount of power needed by the powered devices)
- Well-known and interoperable voice system
- Rugged and industrial solutions DNV-GL and MIL-STD compliant
- Security: LAN and WLAN networks are secured with consistent policies for users and devices
- EAL2 voice and data compliancy
- Unified LAN and WLAN network management system
- Certified microcode for LAN switches
- CPaaS and UCaaS applications
- Ease of use

Considerations for selecting a solution

- Maritime standards compliancy
- Installation and configuration cost
- Time to configure a converged IP telephony, data and Wi-Fi solution
- Voice system openness
- Network openness and agility
- Network security

Conclusion

To address the needs of organizations that have limited staff and to avoid multiple expenditures, maritime vessel solutions must provide:

- Unified Access – with Adaptive Delivery of Network resources
- UCaaS for any conversation
- Application Visibility and Analytics
- Automated network configuration (iFab™, SPB, UNP™)
- Improved crew communication experience
- IoT containment
- Enhanced ISS with MACsec, Abnormal traffic detection, DoS, ACL, hardened µcode
- Maritime (DNV-GL) and technologies compliancy (IEEE, RFC)

ICT teams must prepare their infrastructures to support distributed devices anytime and anywhere in a secure manner.

Acronyms

AI	Artificial Intelligence
AIS	Automatic Identification System
AMS	Automated Manifest System
AMVER	Automated Mutual Assistance Vessel Rescue System
ECDIS	Electronic Chart Display and Information System
ENS	Emergencies Notification Services
FCAPS	Fault, configuration, accounting, performance and security
FE	Fast Ethernet
FICS	Fully Integrated Information and Communication system
GMDSS	Global Maritime Distress and Safety System
GE	Gigabit Ethernet
ICCS	Information, Communication and Command System
IMO	International Maritime Organization
ISP	Internet Services Provider
ISS	Information Security System
LRIT	Long Range Tracking and Identification System
MGig	Multi Gigabit Ethernet
PIDS	Passenger/Public Information Display System
PoE	Power over Ethernet
SOLAS	Safety of Life at Sea
SPB	Shortest Path bridging (IEEE 802.aq)
SRtP	Safe Return to Port
VAC	Voltage Alternative Current
VDC	Voltage Direct Current
VTMS	Vessel Traffic Management Services
VTS	Vessel Traffic Services

Alcatel·Lucent Enterprise