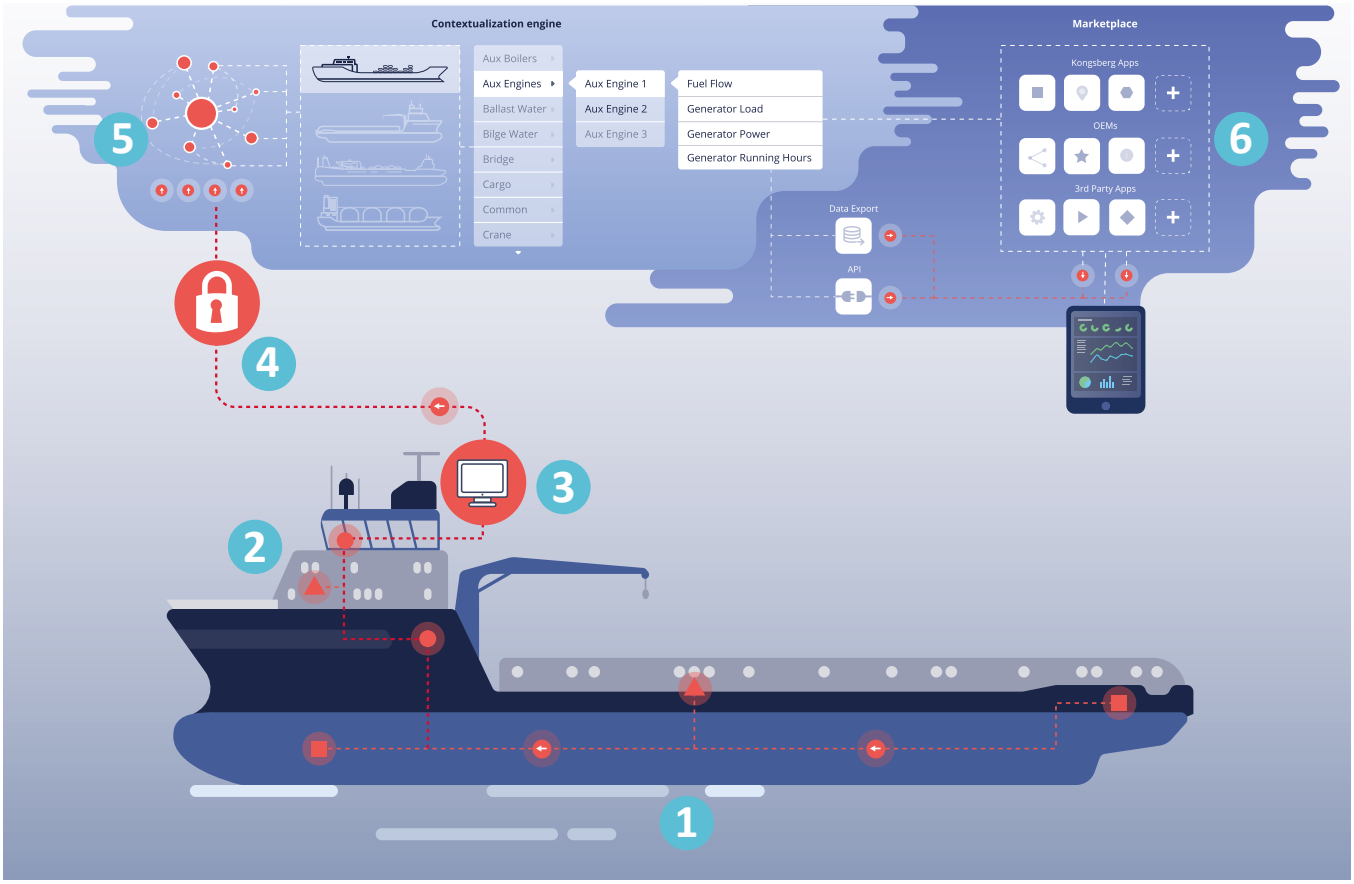
VESSEL INSIGHT

A SECURE SOLUTION FOR YOUR DIGITAL TRANSFORMATION!

KONGSBERG

We understand that keeping both data and your vessel secure is essential to your business. Delivering secure services is a continuous and highly complex activity. We take care of this complexity for you. Our layered security approach consists of physical security, Edge hardware, data communications, security by design development, monitoring and administrative controls. It covers infrastructure and devices on both the edge and in the cloud:



1 Physical barrier

The physical access to the equipment is the first barrier to threats along with the procedures and policies of the vessel.

2 Firewall

All network access points to the real-time components are protected by firewall or galvanic separation.

3 Edge Security

The edge is protected by certificates and encryption technologies, as well as encrypted data transfer in enclosed networks. Local user and endpoint access is securely managed and audited.

4 Global Secure Network

Once data is captured it is encrypted and sent to our cloud service using our Global Secure Network (GSN). This network is marine certified by DNV-GL and Bureau Veritas.

5 Cloud Security

Applications, APIs and data are protected by single sign on, two-factor authentication and customer integrated identity management, protected by azure cyber security services and KONGSBERG SOC. KONGSBERG is ISO27001 certified.

6 Marketplace / Partners

All applications are vetted before listing them on the marketplace. We review that the solutions are developed and maintained to ensure that your data is not misused.

HOW WE DEVELOP, DELIVER AND MANAGE MISSION CRITICAL SOLUTIONS

1 EDGE HARDWARE AND DATA COMMUNICATIONS

Vessel Insight Edge Hardware is responsible for capturing sensor data from your assets on the Edge. This hardware contains several security features including a unique identity to ensure the integrity of the data and detect device tampering. Once data is captured it is encrypted and send to our data centres using our Global Secure Network. This network is marine certified by DNV-GL and Bureau Veritas.

2 PHYSICAL SECURITY AND DATA LOCATION

Your data is stored in data centres which comply with the relevant regulations and have industry standard physical protection measures in place.

- Environmental control
- Redundant power supply
- 24/7 surveillance of premises
- Monitoring and traceability of physical access to premises

Vessel Insight data is currently stored exclusively in European data centers. For customer's subject to European legislation your personal data will always be stored in Europe.

3 MONITORING AND EVENT MANAGEMENT

Services are carefully monitored. This includes the continuous scanning for cyber threats and vulnerabilities. Data analytics and Denial-of-Service prevention are some to the measures taken to ensure reliable services. Our security operations centre (SOC), Cloud Operations and Cybersecurity specialists are key players in our approach. They are responsible for the triage, responding and learning from cyber security events. They provide development teams with practical guidelines and updated information on how to develop secure services and enable us to act and react to keep your data secure.

4 SECURE DEVELOPMENT

When delivering new features, services or making changes on Vessel Insight we follow our Software Development LifeCycle. This allows us to deliver high quality services and meet security requirements. Security requirements originate from a combination of legal, industry-specific regulations and practise as well as compliance requirements. These requirements are embedded and measured throughout the services lifecycle and include:

- Security audit and tests
- Security scanning and testing of source code (SAST)
- Manual Testing
- Penetration testing

Our services are tested to ensure resilience against threats as defined by OWASP10 and SANS25.

5 ADMINISTRATIVE CONTROLS

Our administrative controls cover the training, procedures and policies related to KONGSBERG employees and consultants. All work processes are defined in our Business Management System which is compliant with the ISO27001 standards and audited on a yearly basis.

Staff screening: All staff is screened as part of our hiring process to make sure we hire talent who fits the job and will take pride in providing world-class services to you as our customer.

Non-disclosure/confidentiality agreements: All members of staff and consultants have signed confidentiality agreements.

Training and awareness: Knowledge and expertise are crucial tools in providing state of the art solutions. KONGSBERG provides all staff with awareness courses on topics covering cybersecurity, privacy and other relevant aspects on a continuous basis. Development and Operation staff may receive more specific training depending on their role.

Access to data: Access to your data s limited to only a few people in our cloud operations and technical support departments.