VESSEL INSIGHT

KONGSBERG

KOGNIFAI ECOSYSTEM

Cybersecurity

HIGHLIGHTS

- Security by design
- Defense in depth
- IoT Edge Security
- Secure communications
- Cloud security
- Monitoring & Event management

Security first

The Kognifai Ecosystem has been designed and developed with security in mind. The ecosystem has many technical barriers to guard against potential security threats as well as monitoring and intrusion capabilities, to detect and mitigate potential threats and vulnerabilities.

Defense in depth

The Kognifai Ecosystem uses several layers of measures and barriers to protect data and systems. This approach is also referred to as “defense in depth” and provides an effective defense against security threats. These layers cover the hardware and network onboard, data communication and the cloud infrastructure

Network security

KONGSBERG’s Global Secure Network (GSN) ensures a virtual private network (VPN) between a client’s vessels and the cloud systems. This network also provides onboard separation between control zone networks and data exchange zone (DXZ) components onboard the vessel.

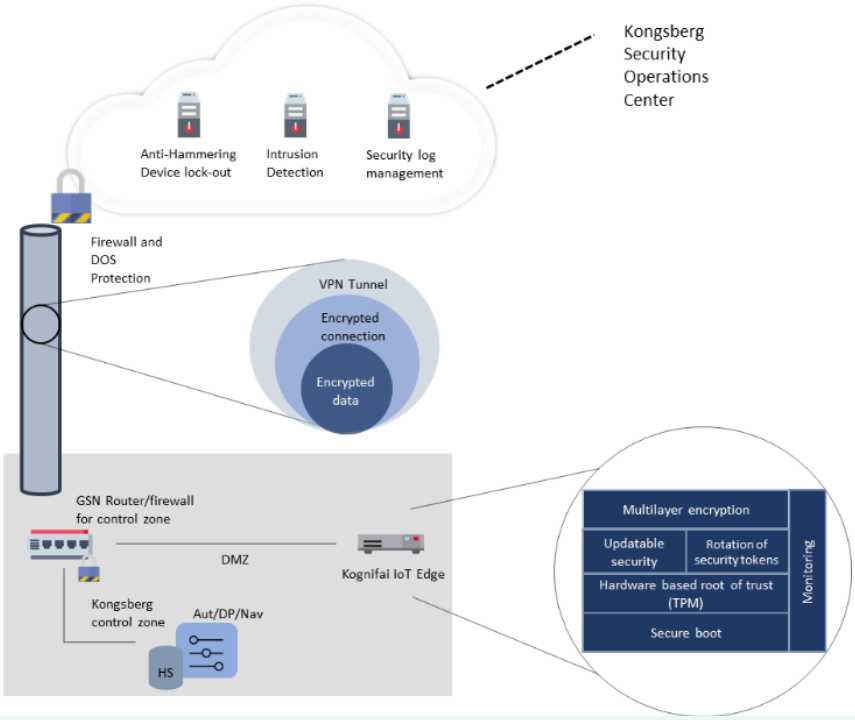
The Kognifai IoT Edge hardware is deployed in the data exchange zone (DXZ) which is established by the GSN router onboard the vessel. The setup enables data to be sent from control systems to the IoT Edge hardware while preventing the IoT Edge hardware to communicate directly with the control systems. The Global Secure Network (GSN) has been verified by Bureau Veritas - IEC 60945 Ed. 4.0 (2002) + /Corr.1 (2008), IEC 61162-460 Ed. 1.0 (2015) and DNV-GL - DNVGL-CP-0231 – Type approval – Security capabilities of control system components.

Secure Communication & Encryption

All connections between the edge and the cloud is run over encrypted channels. This encryption is in addition to the outer VPN security layer already provided by the Global Secure Network system. Both transmission of sensor data (AMQP over WebSockets /TLS) and device management (REST/TLS) are encrypted. The communication between the vessel the cloud is always initiated from the vessel. No ports are open for direct inbound access from the internet to the Kognifai IoT edge hardware.

Hardware based root of trust at the Edge

The Kognifai IoT Edge hardware supports hardware based root of trust. The trusted platform module (TPM) of the hardware is used to store the private/public key-pair. This ensures the confidentiality and integrity of the device's private key. The hardware based root of trust is used to authenticate the edge device with the cloud.



Security features

Global Secure Network	VPN Tunnel Firewall towards control zone Data encryption
Kognifai IoT Edge	Secure boot Hardware based root of trust (TPM) Daily rotation of security keys Encrypted communication Automatic transmission of security logs to cloud
Kognifai Cloud	Firewall /DDOS protection Intrusion detection Log analysis of edge & cloud devices Brute force attack protection Fine grained authorization OpenID and OAuth2.0 authentication Compartmentalized design to reduce attack surface
Monitoring & Event Management	Cloud services and network are monitored 24/7 to ensure high availability and detect cyber threats. The KONGSBERG Security Operations Center is responsible for triage and event coordination.

Kongsberg Digital
P.O. Box 1003
N-3601 Kongsberg, Norway

Phone: +47 32 28 82 00

kognifai@kdi.kongsberg.com