Situational Awareness of Maritime Cyberattacks& Data Protection

Isidoros Monogioudis, Hellenic American University

Agenda

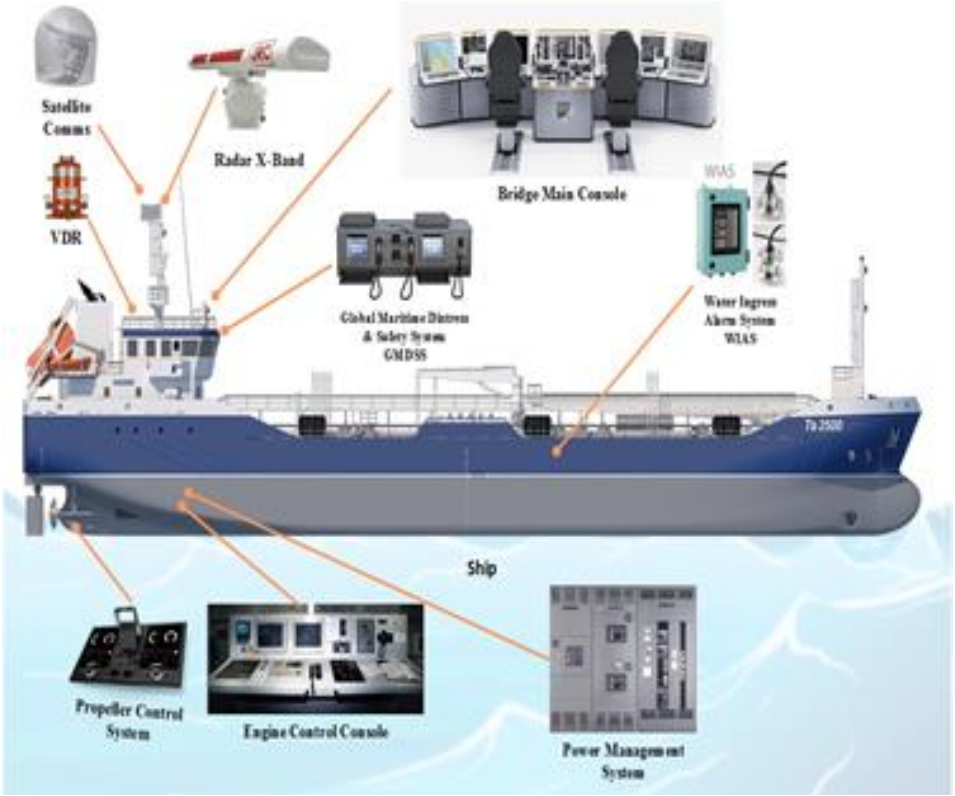
- Maritime digital environment
- Cyber Threat landscape
- Cyber situational awareness requirements
- Maritime cyber security situational awareness

Maritime digital environment

- Information Technology (IT)
  - Offices
  - Ports
  - Oil rigs
  - Navigation
  - Ships (partially)
- Operation Technology
  - Ships
  - Offices (for management)

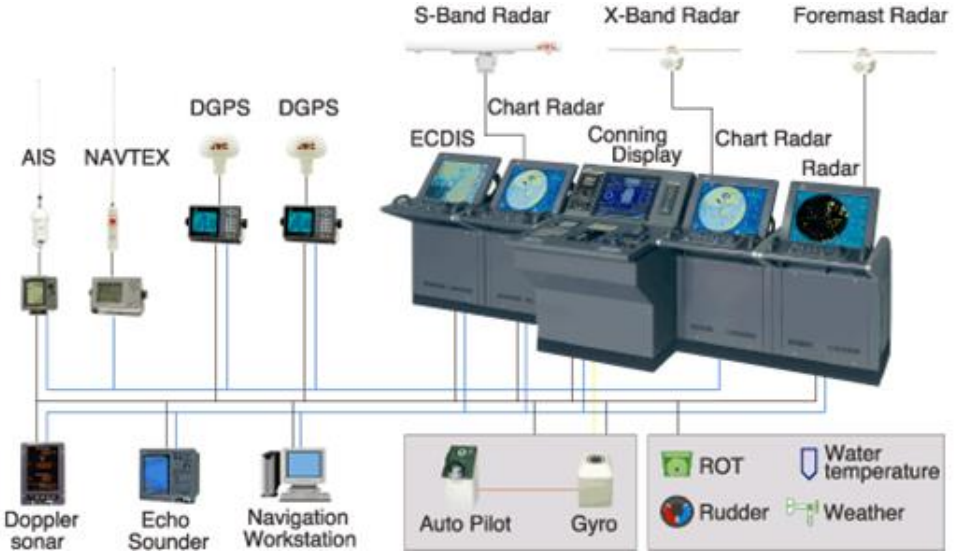
Maritime digital environment

- Operational Technology Challenges
  - Real-time
  - Strict access to OT
  - Control physical world
  - Response is time-critical
  - Fault tolerance is essential
  - Systems diversity
  - Software changes
  - Limited resources



Maritime digital environment

- OT Systems (1/2)
  - Vessel Integrated Navigation System (VINS)
  - Global Positioning System (GPS)
  - Satellite Communication System
  - Automatic Identification System (AIS)
  - Electronic Chart Display and Identification System (ECDIS)
  - Marine Radar Systems
  - Global Maritime Distress and Safety System
  - Voyage Data Recorders
  - Dynamic Positioning Systems



Maritime digital environment

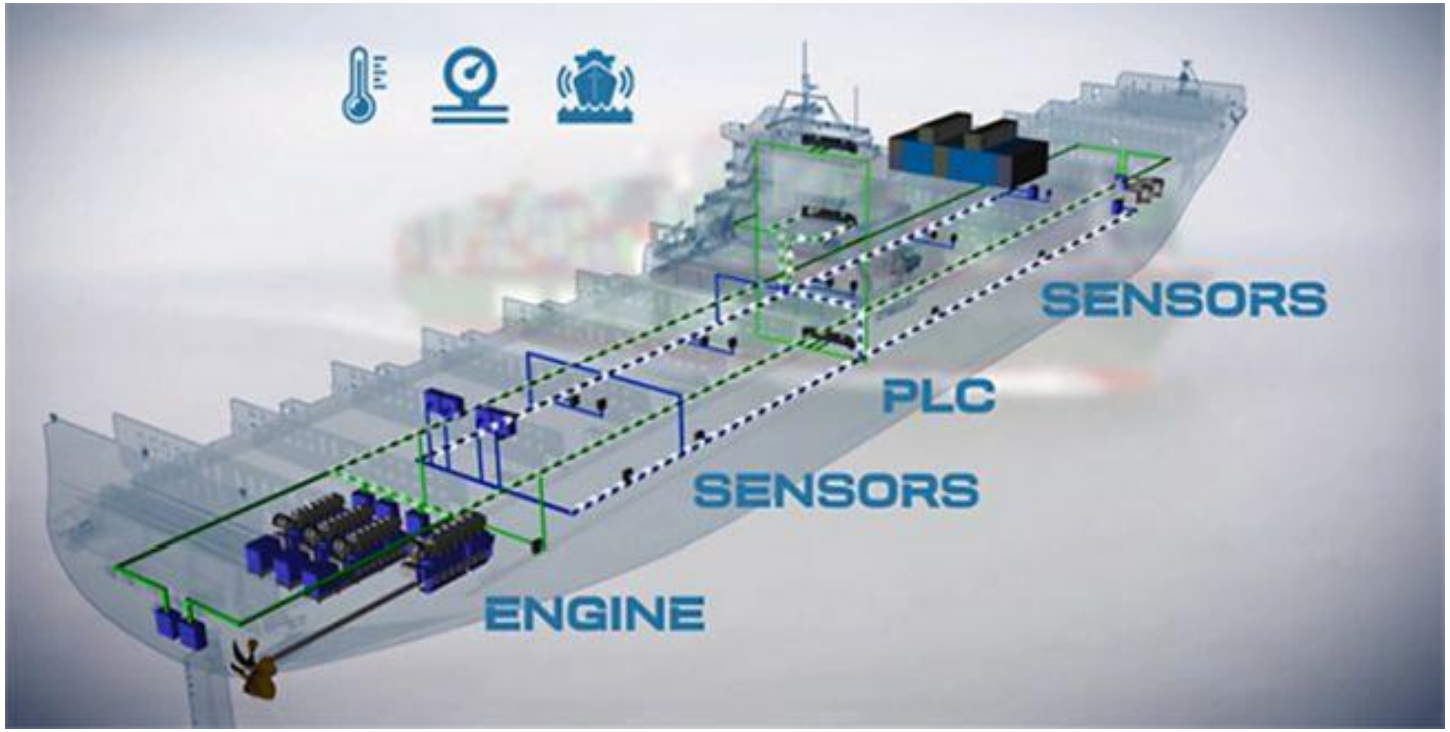
- OT Systems (2/2)
  - Engine Control Console
  - Main Switchboard
  - Alarm Monitoring and Control System
  - Power Management System
  - Ship Emergency Response System
  - Valve Remote Control System
  - Ballast Water Systems
  - Water Ingress Monitoring System

Maritime digital environment

- The future…MAS!
- Maritime Autonomous Systems
- Artificial Intelligence
- Internet of Things (IoT)
- Internet of Ships and Sea Services
- Smart Shipping

Cyber Threat landscape

- A completely digitalized shipping means great reliance on IT, software and communications systems



Cyber Threat landscape

- Cyber Safety Incident (BIMCO definition) is a result of:
  - a cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)
  - a failure occurring during software maintenance and patching
  - loss of or manipulation of external sensor data, critical for the operation of a ship – this includes but is not limited to Global Navigation Satellite Systems (GNSS).

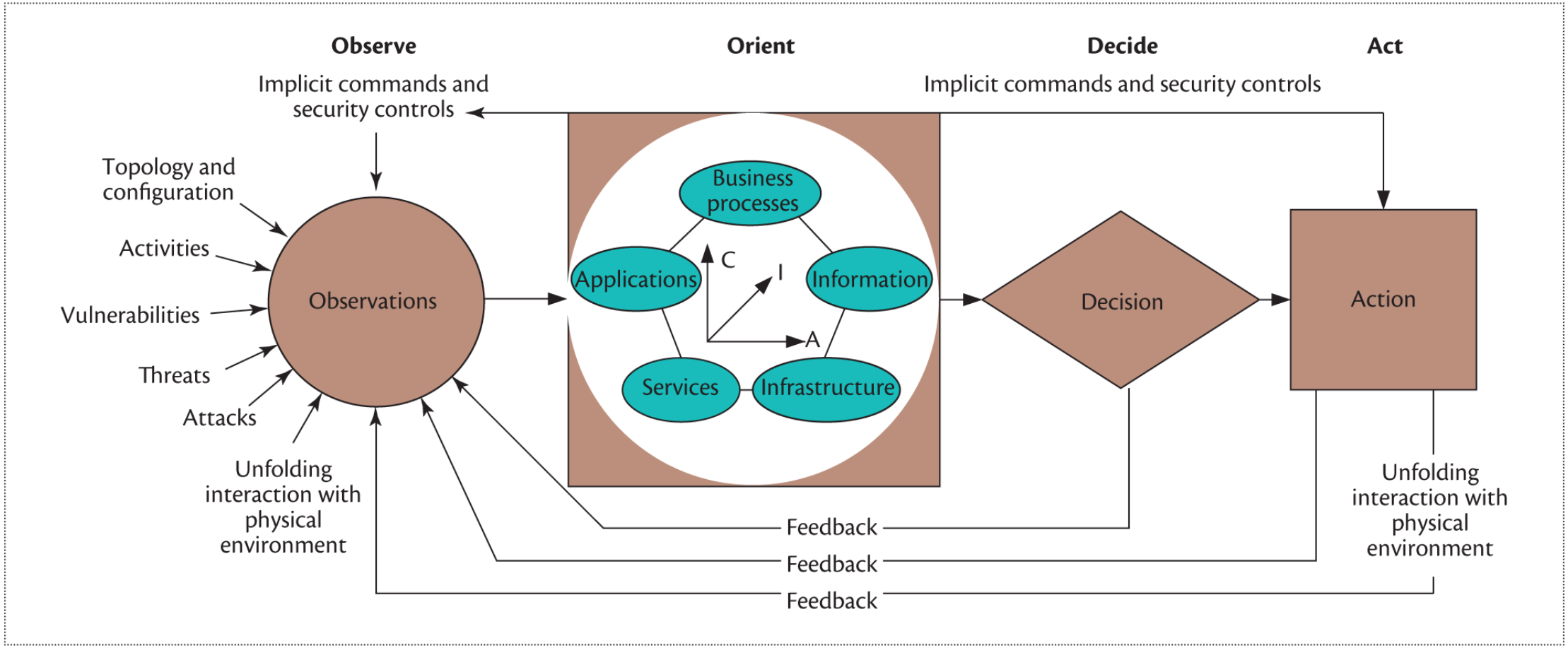
Cyber Threat landscape

- Threat Actors
  - Hacktivists
  - Criminals
  - Opportunists
  - State Sponsored Groups
  - Disgruntled employees

Cyber situational awareness requirements

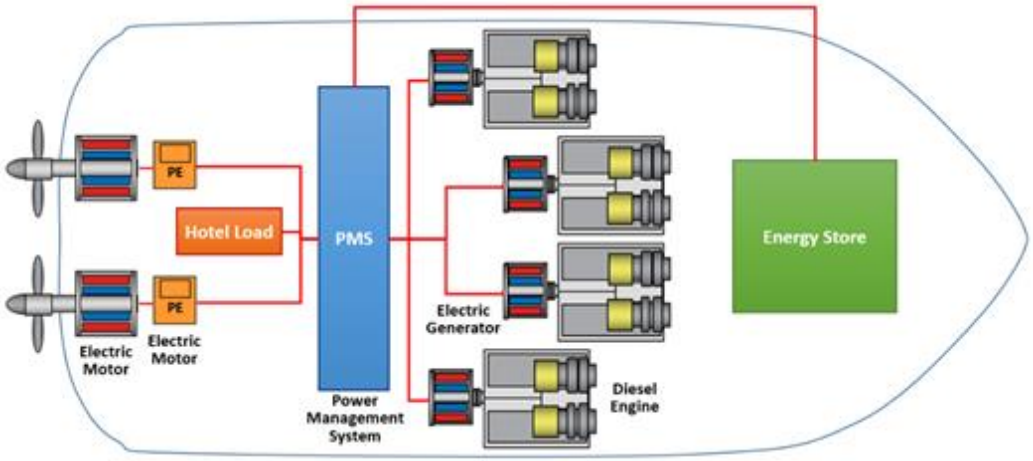
- What is it?
  - Collection, correlation and analysis of IT and OT data that can provide visibility and awareness of normal and abnormal behavior supporting the decision-making process for cyber risk management
- IT systems can be covered by already existing “land” cyber security technology
- Maritime specific OT systems are partially/limited covered by existing solutions
- Industrial – IoT security solutions seem to fit better but still need special tailoring

Cyber situational awareness requirements



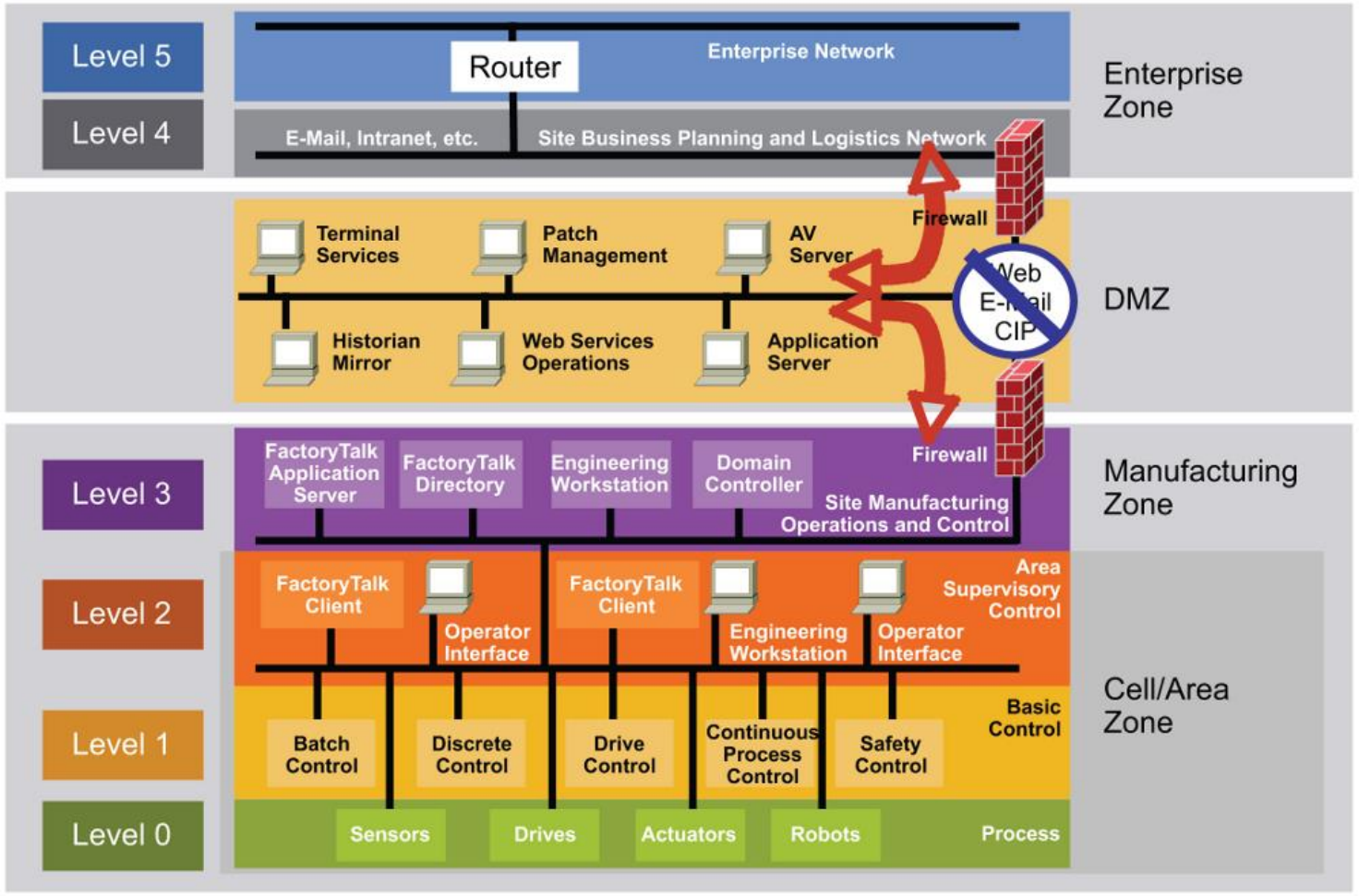
Maritime cyber situational awareness

- What OT we need to observe
  - Date and Time (SVDR)
  - Ship's Position (SVDR)
  - Speed and Heading (SVDR)
  - Radar Data (SVDR)
  - ECDIS Data (SVDR)
  - Watertight and Fire Door Status
  - Speed and Acceleration
  - Main Alarms
  - Power Management Systems
  - ….
  - Every OT device is a data source



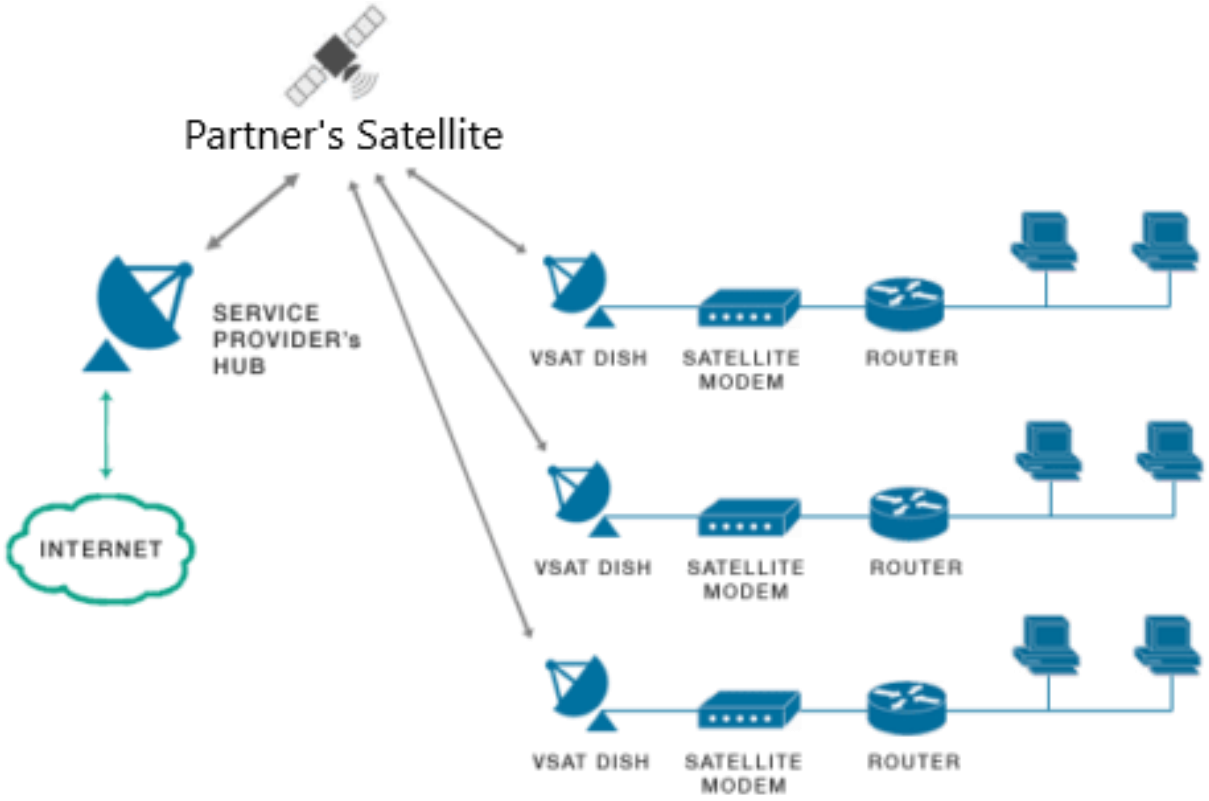
Maritime cyber situational awareness

- How OT data can be collected
- PURDUE Model



Maritime cyber situational awareness

- Data transfer to Central Platform
- VSAT
- Cloud
- Smartship project



Maritime cyber situational awareness

- Cyber Security Components
  - Real-time Asset management
  - Security configuration baseline
  - Failure detection
  - Continuous Vulnerability assessment
  - Data protection
  - Threat prevention
  - Incident detection and response
  - Risk mitigation
  - Operational resilience

Maritime cyber situational awareness

- Key Takeaways:
  - Digitalization and connectivity increases cyber exposure
  - Combination of IT and OT consists the Maritime cyber environment
  - Data collection from vessels remains a big challenge
  - VSAT and PURDUE model can enable the process
  - Big Data Analytics and AI will enhance efficiency
  - Advanced and contextual visibility can provide a high cyber security posture

Maritime cyber situational awareness