Cynalytica

Safely and securely monitor your onshore and onboard operations' serial-connected Industrial Control Systems (ICS)

Eliminate SCADA's blind spot with the SerialGuard AnalytICS Platform

The SerialGuard AnalytICS Platform helps you apply zero-trust security to maritime serial networks by introducing secure real-time monitoring and intrusion detection to serial-connected ICS. The scalable platform acts as an all-in-one operational health monitor and serial network security solution that provides:

Zero-Trust Security

True Visibility & Monitoring
Directly monitors communications to and from OT operation and navigation systems in real-time to improve situational awareness and help combat stealthy spoofing/false feedback attacks.

Intrusion Detection
Alerts on anomalies indicative of misconfigurations, unauthorized commands and malicious cyber attacks.

Integration with SIEMs
Seamlessly integrates with SIEMs (e.g. Splunk, Elk, etc.) for optimized visibility, enhanced event correlation, and effective SOAR execution.

ICS Health Monitoring

Troubleshooting & Diagnostics
Helps quickly pinpoint operational faults to improve response times and ensure operational continuity.

Centralized Data Collection & Analysis
Centralizes serial data collection from multiple ICS devices and contextualizes the data for easy analysis.

Reliable Operational Datasets
Builds serial datasets for advanced digital strategies such as Asset Performance Management (APM), Overall Equipment Effectiveness (OEE), and Predictive Maintenance.

The SerialGuard AnalytICS Platform

Bringing True Visibility to Maritime Industrial Control Systems

ONBOARD

Validate vessel movement and enviromental conditions by securely monitoring NMEA 0183 and other serial-supported shipboard devices including:

- ✔ **Navigation Systems**
- ✔ **Propulsion Control**
- ✔ **Ballast Management Systems**
- ✔ **Manoeuvring**
- ✔ **Power Systems**
- ✔ **Thruster Control**
- ✔ **Water Ingress Detection Systems**
- ✔ **Vessel Safety Systems**

and many more...

ONSHORE

Verify the integrity of your onshore industrial processes by securely monitoring serial communications that control critical operations including:

- ✔ **Position, Navigation, and Timing (PNT)**
- ✔ **Traffic Management**
- ✔ **Cargo Handling**
- ✔ **Terminal Power Systems**
- ✔ **Terminal Safety Systems**
- ✔ **Fueling Systems**
- ✔ **Water Level Management Systems**
- ✔ **Building Management Systems**

and many more...

Secure and Scalable Technology

SerialGuard™

✔ **Passive**

✔ **Fail-Safe**

✔ **Full/Half Duplex Serial Monitoring**

✔ **RS-232/485/422 Protocol Monitoring**

✔ **Protocol Agnostic Support**

✔ **Deep Packet Inspection**

SerialGuard is a passive hardware sensor that installs seamlessly into supervisory control and data acquisition (SCADA) and NMEA-connected control systems. The SerialGuard sensor passively taps RS-232, RS-485/RS-422 serial interfaces to securely capture serial data. It then encapsulates the captured data into encrypted TCP data packets before securely transmitting them to the AnalytICS Engine for inspection.
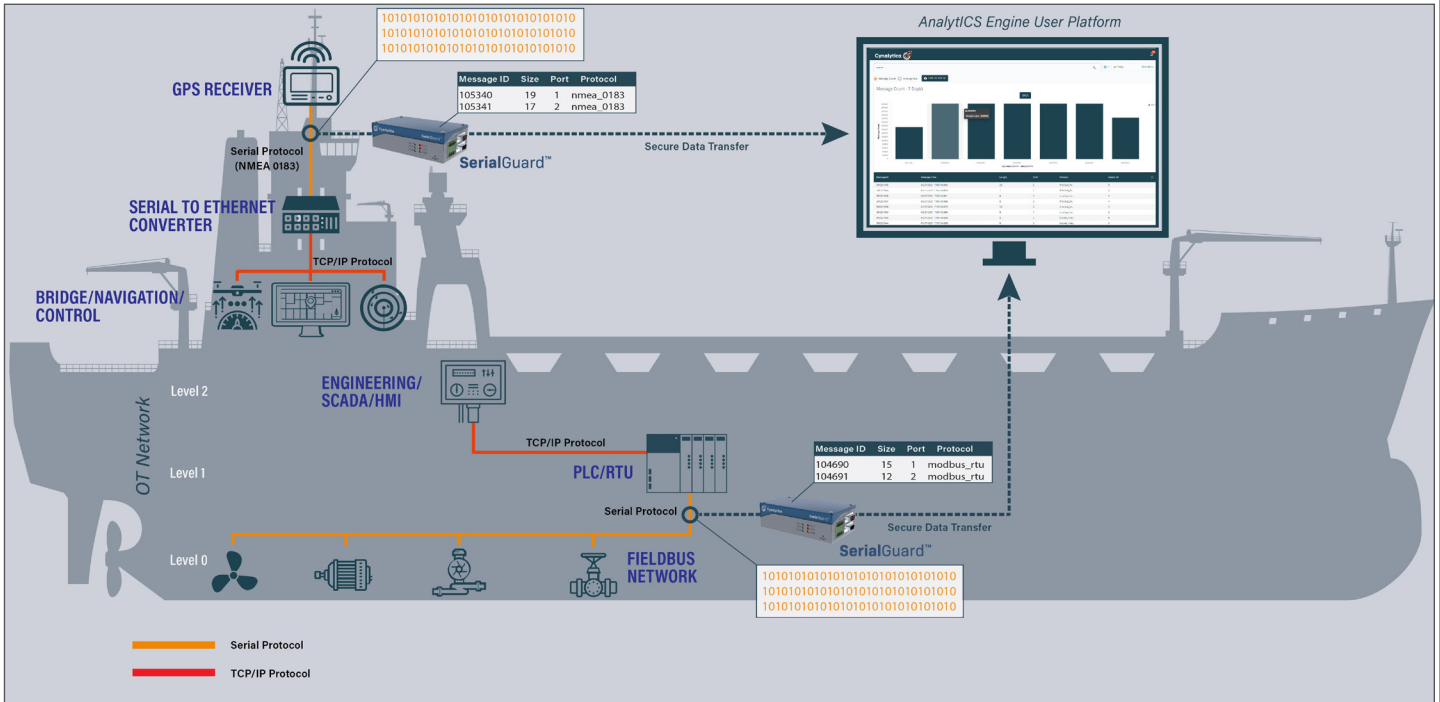
AnalytICS Engine
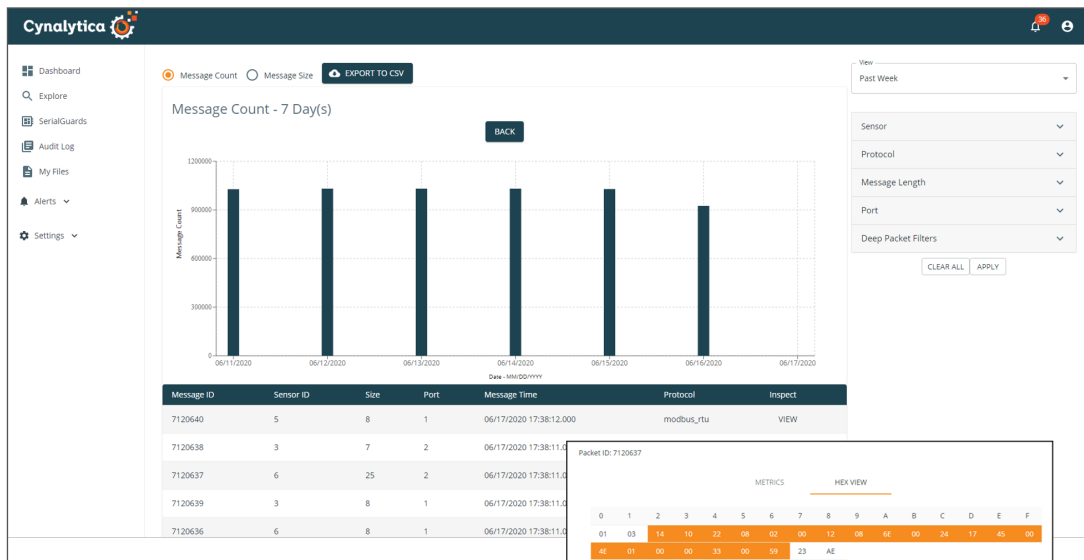
AnalytICS Engine, SerialGuard's supporting platform, operates as an intrusion detection system (IDS) and data validation tool. The software securely aggregates the serial data into easy-to-read visualizations, enabling you to baseline normal operations, analyze trends and create alerts on serial traffic behavior.

✔ **Enables Rule-Based Alerts**

✔ **Performs Deep Packet Inspections**

✔ **Understands Individual Serial Packets**

✔ **Integrates with 3rd Party SIEMs (e.g. Splunk, etc.)**

✔ **Manages SerialGuard Sensors Remotely**
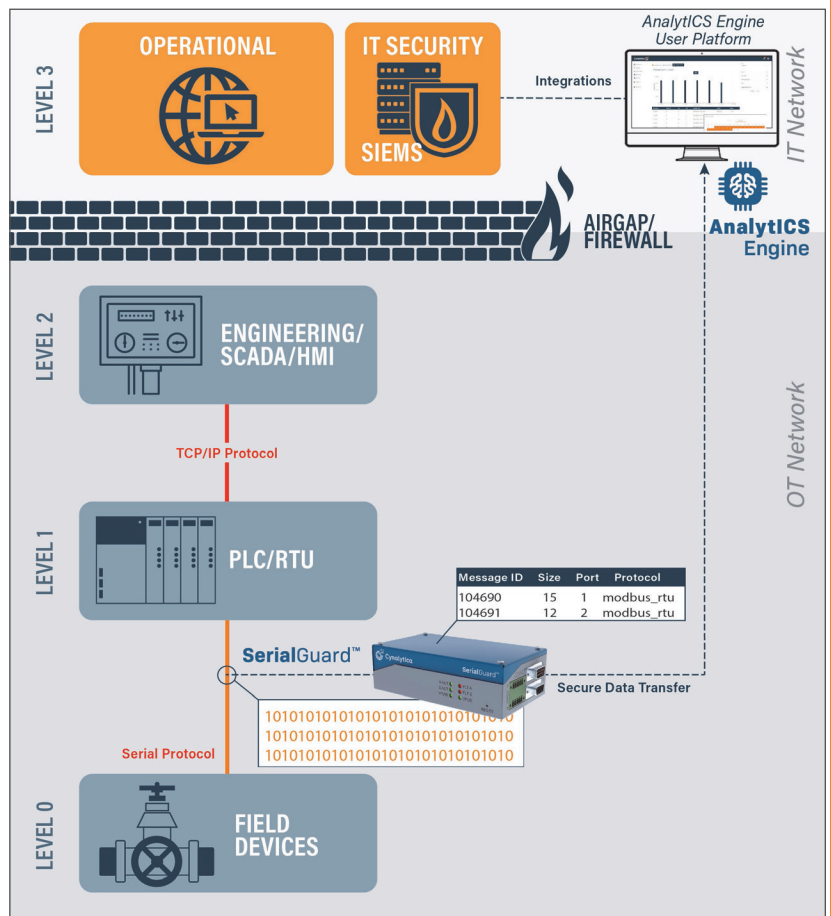
✔ **Features Easy-To-Read Data Visualizations**

Onboard Topology

✔ Monitors NMEA 0183 network traffic in real-time to help validate the integrity of essential marine electronics and to support vessel environment verification.

✔ Monitors serial communications within vessels' OT network environments to help ensure safety and availability of critical operational processes.

AnalytICS Engine User Platform

GPS RECEIVER

Message ID	Size	Port	Protocol
105340	19	1	nmea_0183
105341	17	2	nmea_0183

Serial Protocol (NMEA 0183)

SerialGuard™

Secure Data Transfer

SERIAL TO ETHERNET CONVERTER

TCP/IP Protocol

BRIDGE/NAVIGATION/ CONTROL

OT Network

Level 2

ENGINEERING/ SCADA/HMI

Level 1

TCP/IP Protocol

PLC/RTU

Serial Protocol

Message ID	Size	Port	Protocol
104690	15	1	modbus_rtu
104691	12	2	modbus_rtu

SerialGuard™

Secure Data Transfer

Level 0

FIELDBUS NETWORK

Serial Protocol
TCP/IP Protocol

Onshore Topology

✔ Monitors serial communications at the lowest level of the OT network, serving as the last line of truth in your defense against cyber intrusions.

✔ Supports ICS protocols such as Modbus RTU, DNP3, IEC-101, BACnet MS/TP and more.

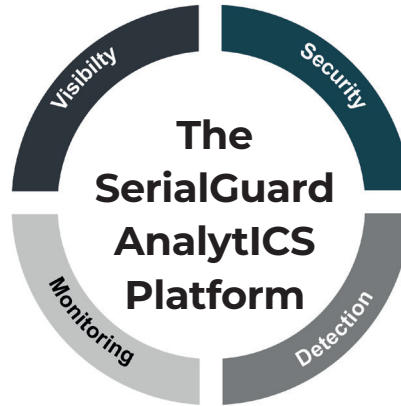✔ Easily deployed across small to complex ICS network environments.

AnalytICS Engine User Platform

LEVEL 3

OPERATIONAL

IT SECURITY

SIEMS

Integrations

IT Network

AIRGAP/ FIREWALL

AnalytICS Engine

OT Network

LEVEL 2

ENGINEERING/ SCADA/HMI

TCP/IP Protocol

LEVEL 1

PLC/RTU

Message ID	Size	Port	Protocol
104690	15	1	modbus_rtu
104691	12	2	modbus_rtu

SerialGuard™

Secure Data Transfer

Serial Protocol

LEVEL 0

FIELD DEVICES

Key Features

Visibility
- Supports RS-232, RS-485/422
- Provides full/half duplex monitoring
- Real-time operating system

Security
- Fully Passive
- Fail-Safe
- Encapsulates tapped serial data in encrypted TCP data packets

The SerialGuard AnalytICS Platform

Visibilty · Security · Detection · Monitoring

Monitoring
- Deep packet inspection for NMEA 0183*, Modbus_RTU, DNP3 and more...
- Normalizes serial data for effortless baselining
- UI offers deep insights into asset behavioral patterns and events

Detection
- Monitors level 0/1 communications to detect cyber-physical attacks and events
- Provides rule-based anomaly alerts
- Integrates alerts with SIEMs (e.g. Splunk, Elk, etc.)

Contact the Cynalytica team for a full list of supported NMEA 0183 sentences

Benefits

✔ Enables OT operators to securely monitor multiple devices from a centralized location.

✔ Provides accurate situational awareness into the operational health and cybersecurity posture of legacy infrastructure.

✔ Decreases the need for specialized personnel to carry out troubleshooting and diagnostics.

✔ Improves response times for increased uptime.

✔ Helps streamline IT/OT network security for improved cybersecurity posture.

Visit our website to request a demo or to order your Enterprise Starter Kit today!