Cynalytica

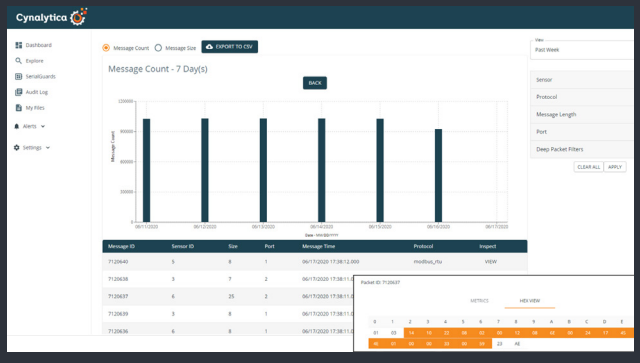
SerialGuard AnalytICS Platform

Enterprise-Scale Intrusion Detection and Data Visibilty for Legacy Industrial Control Systems (ICS)

Safeguarding Legacy Control Networks at Level 0-1

The SerialGuard AnalytICS Platform is a high-performance operational health monitoring and cyber intrusion detection platform that brings secure visibility to high-risk cyber-physical assets. The fully-passive platform monitors serial communications between field devices and controllers to provide the optimum viewpoint of serial device behavior while supporting legacy asset-owners to securely transition to Industry 4.0.

Improves Operational Health and Cybersecurity Posture



Helps ICS Operators to:

- **Verify Operational State of Legacy ICS**
- **Detect Cyber-Physical Attacks**
- **Discover Device Misconfigurations**
- **Prevent Network Downtime**

SerialGuard™

SerialGuard™ Monitors Critical Infrastructure's High-Risk Legacy Assets at the Lowest Level for Superior Data Integrity and Visibility

Passively Taps Level 0/1 ICS Serial Communications

- **Passive**
- **Fail-Safe**
- **Full/Half Duplex Serial Monitoring**
- **RS-232/485/422 Protocol Monitoring**
- **Protocol Agnostic Support**
- **Deep Packet Inspection**

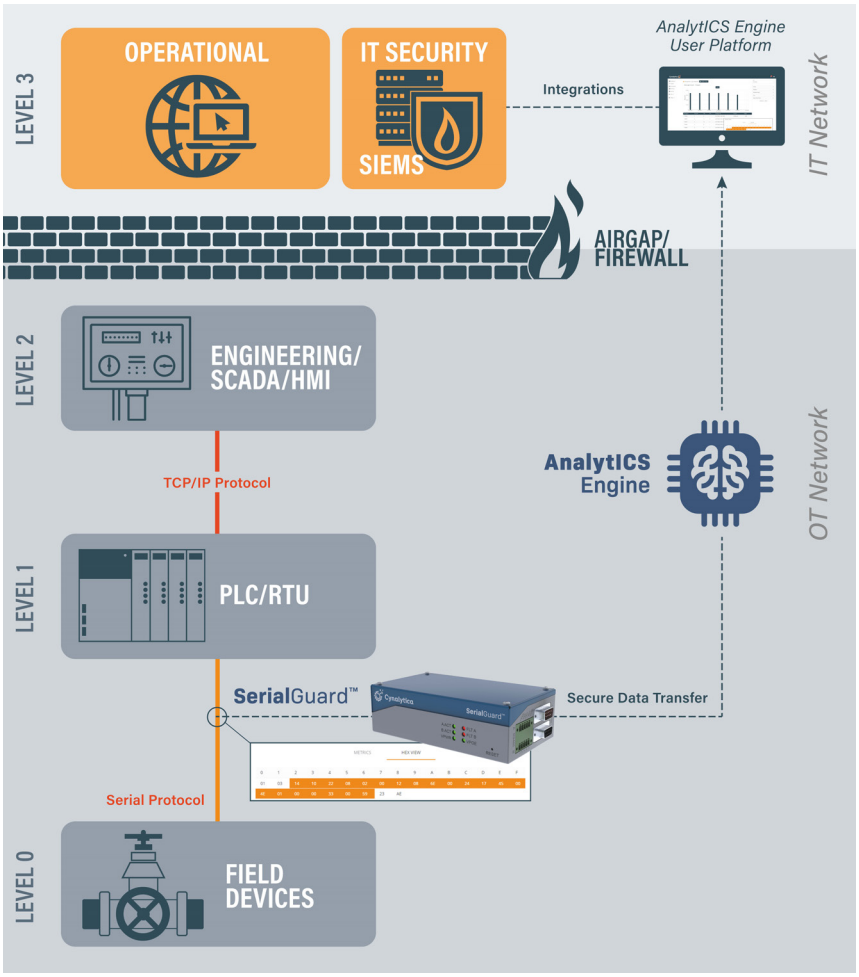
SerialGuard is a passive hardware sensor that installs seamlessly into supervisory control and data acquisition (SCADA) and other legacy control systems. The SerialGuard sensor provides Level 0 and Level 1 security monitoring for legacy industrial control systems that utilize RS-232, RS-485/RS-422 with serial communications protocols that are inherently vulnerable to cyberattacks.

Securely Captures Data

SerialGuard operates by passively capturing serial communications between field devices and controllers. It then encapsulates the captured serial communications data into an encrypted TCP data packet*, which is sent out over TCP/IP to the Cynalytica AnalytICS Engine.

Unlike commercial serial loggers, SerialGuard preserves the integrity of the signal on the serial bus. It will not inadvertently introduce a new attack vector to the OT network, nor will it disrupt operations or flow of serial communications in the unlikely event of power failure.

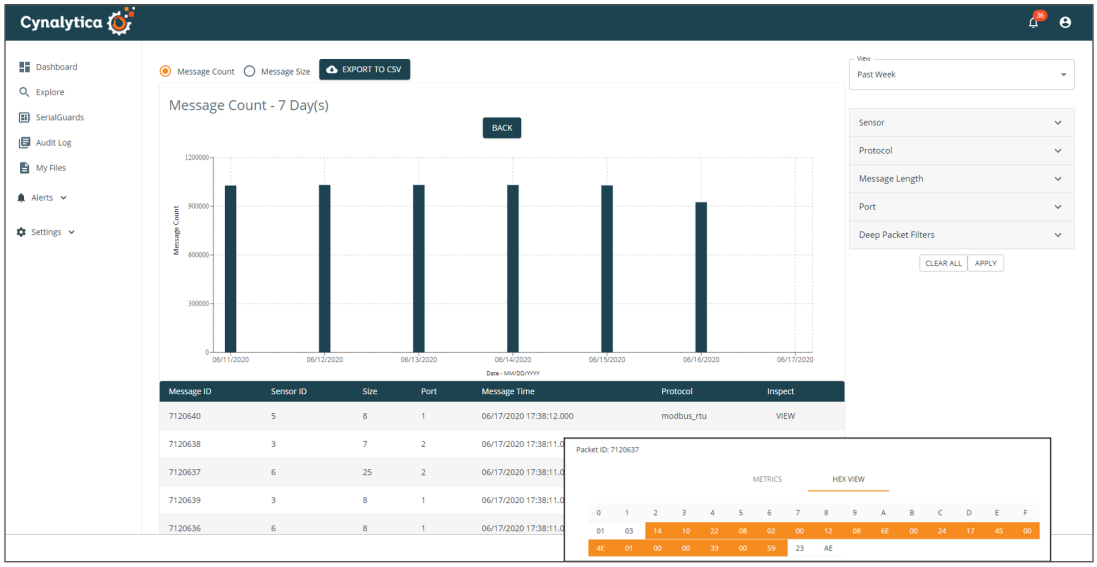
**SerialGuard can be configured to send unencrypted TCP data packets if required*



AnalytICS Engine

AnalytICS Engine Enables Rapid Detection of Cyber-Physical and Operational Incidents on Legacy ICS to Help Increase Asset Uptime and Avoid Asset Damage

Optimizes Visibility for Increased Anomaly Detection



AnalytICS Engine, SerialGuard's supporting platform, operates as an intrusion detection system (IDS) and data analytics tool. The software offers operators the ability to securely capture, baseline and analyze trends in serial communications through encrypted communications.

- **Enables Rule-Based Alerts**
- **Integrates with 3rd Party SIEMs**
- **Performs Deep Packet Inspections**
- **Remotely Manages SerialGuard Sensors**
- **Understands Individual Serial Packets**
- **Easy-To-Read Data Visualization**

AnalytICS Engine can be deployed on-premise or as a service and provides operators with an easy-to-use set of intuitive tools to monitor communications. Rulesets are flexible, ranging in complexity with the operators' needs that can flag anomalous activities on individual devices or across the network.

Our platform provides a scalable enterprise management tool incorporating serial communications data from SerialGuard sensors to provide optimum visibility of serial-based network traffic in Industrial Control Systems. AnalytICS Engine also seamlessly integrates with third party SIEMs to provide ICS/SCADA operators maximum visibility across their IT/OT networks.

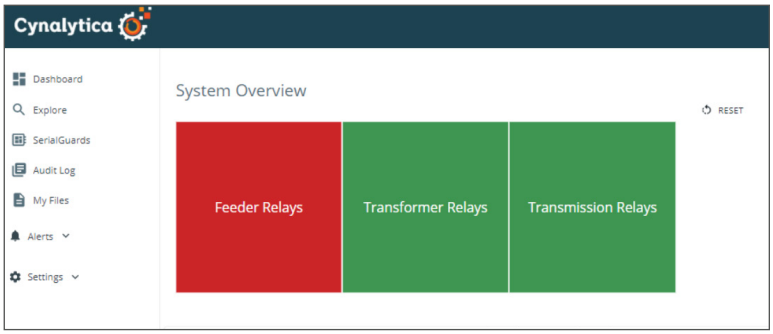
Highlights/Benefits

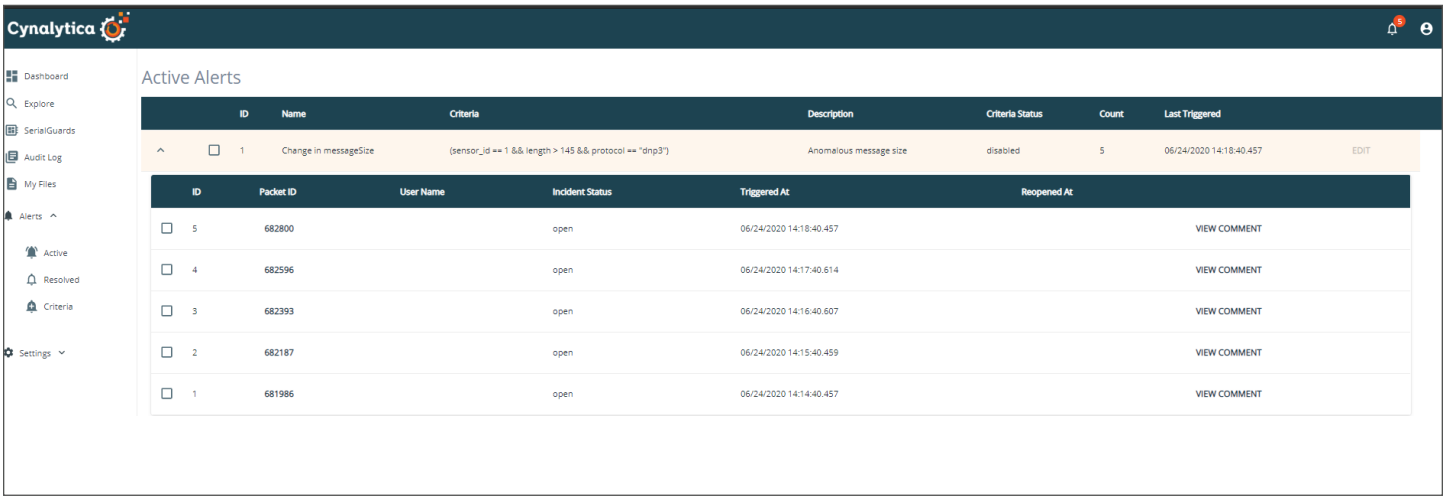
- Anomaly alerts significantly reduce Mean Time to Detect (MTTD) cybersecurity threats
- Validates data integrity of serial-connected cyber-physical assets
- Enables operators to quickly detect and investigate configuration changes
- Saves time - configures and manages SerialGuard devices from a centralized location
- Organizes data into easy-to-read graphics for efficient ICS health monitoring
- Gives a deeper insight into serial-based ICS traffic behavior
- Helps ICS operators and security teams to make quick, informed decisions

Management Features

AnalytICS Engine comes with built-in properties that perform device and data management tasks including:

- Remote configuration and management of SerialGuard devices
- Encryption and authentication with role-based access control
- Serial traffic alert monitoring
- Industrial system health monitoring
- Asset and cluster management
- Data historian and audit trails
- Protocol agnostic support
- Integration with commercial SIEMs
- Native support for Syslog, JSON and XML
- Data Export to CSV
- Large data storage

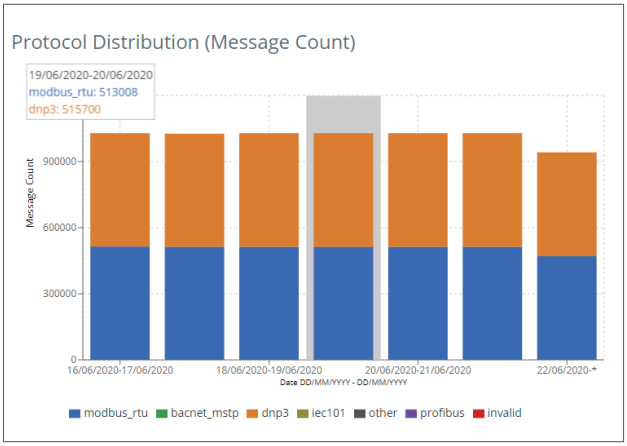




Powerful Data Visualization & Analytical Tools

AnalytICS Engine's powerful suite of data visualization and analytic tools help users understand the serial data sets and identify patterns with ease. Built-in capabilities include:

- **Visualization and statistical characterization of key serial traffic parameters, such as:**
  - Protocol density
  - Protocol distribution
  - Message size
  - Message count
- **Deep Packet Inspection of serial communications**
- **Rule-based anomaly detection**



Industry Integrations

The SerialGuard AnalytICS Platform can be deployed across all industry verticals that utilize legacy field devices, including many critical infrastructure sectors listed by the US Department of Homeland Security. Typical industry integrations include:

- Electrical power generation, distribution, and transmission facilities
- Refineries and other oil-and-gas production facilities
- Water infrastructure and gas transmission infrastructure
- Nuclear reactors, materials, and waste sectors
- Railway and mass rapid transit systems
- Chemical production plants
- Industrial and manufacturing plants

About Cynalytica

Cynalytica, Inc. combines a diverse set of industry expertise with decades of applied research and development experience to deliver pioneering cybersecurity and machine analytics technologies that help protect critical national infrastructure, securely enable Industry 4.0 and help industries accelerate their digital transformation objectives. The company employs innovative and novel techniques in machine learning, data analytics and high-performance computing combined with manufacturing capabilities to provide revolutionary threat detection solutions and analytics for industrial control systems and infrastructures.