Cynalytica

Eliminate SCADA'S Blind Spot with the SerialGuard AnalytICS Platform

Protect your utility's critical services by safely and securely monitoring your serial-connected Industrial Control Systems (ICS) at the cyber-physical level.

The SerialGuard AnalytICS Platform helps you adopt zero-trust security at levels 0/1 by introducing secure real-time monitoring and intrusion detection to serial-connected ICS such as PLCs, RTUs, pumps, mixers, clarifiers, flow restrictors, and many more. 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 field devices 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 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.

Key Features

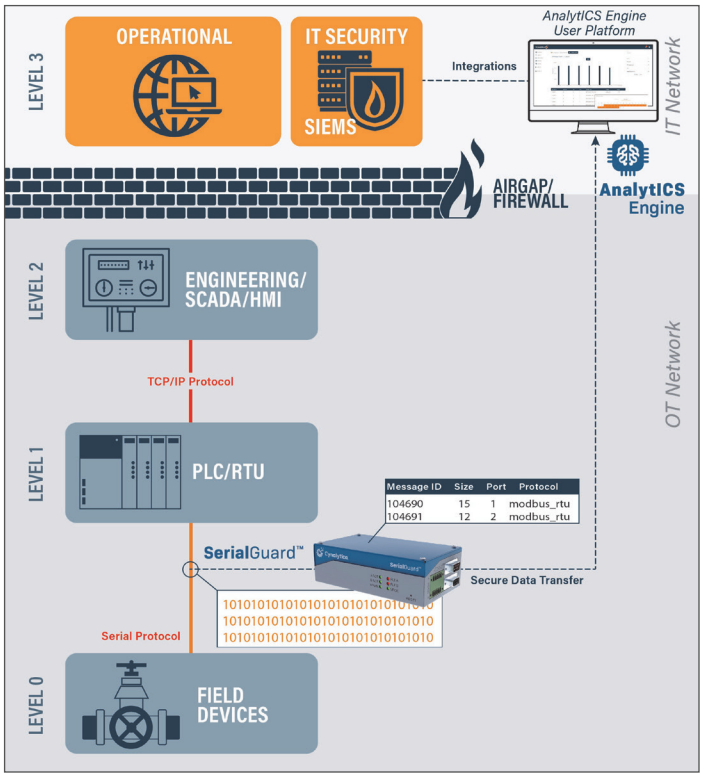
Visibility
- Supports RS-232, RS-485/422
- Provides full/half duplex monitoring
- Real-time operating system

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

Monitoring
- Deep packet inspection for DNP3, Modbus_rtu, Profibus, 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

Benefits

- Enables OT operators to securely monitor multiple field 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!