Cynalytica

SerialGuard™

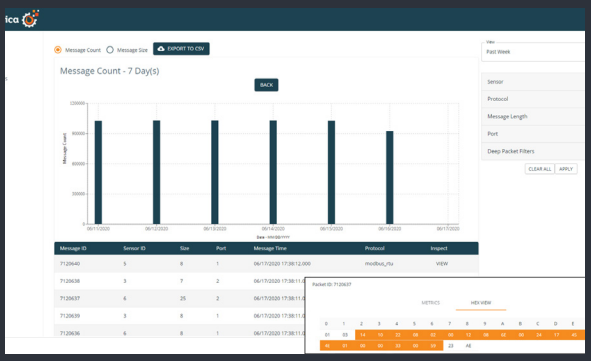
Introducing a New Level of Security to ICS Networks

Designed for Industrial Control Systems, SerialGuard™ is a high-performance, fully passive, serial packet sniffer that enables secure visibility within vulnerable legacy networks. The fail-safe sensor passively monitors Level 0 and Level 1 serial communications between field devices and controllers and with the Cynalytica AnalytICS Engine Platform can reveal and help alert traffic anomalies that are indicative of a cyber-attack, physical-attack, or system misconfiguration.

Enables ICS Operators to Detect Modern Cyberattack Techniques

SerialGuard installs in-line between field devices and controllers, enabling ICS operators to detect modern and commonly employed cyberattack techniques:

- **Man-in-the-Middle Attacks:**
  Captures interceptions and alterations of serial communications between field devices and controllers which go otherwise undetected.
- **Unauthorized Commands:**
  Captures messages that instruct field devices to perform outside their expected functionality.
- **Reconnaissance:**
  Enables operators to detect suspicious probes through the captured data packages.
- **Insider Threats:**
  Captures all communications between field devices and controllers, enabling operators to detect unauthorized commands by malicious insiders.



Safeguarding Legacy Control Networks at Level 0-1

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. 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*

Industry Integrations

SerialGuard 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.

FEATURES	BENEFITS
Passive	Cannot write to the serial line; therefore, it will not introduce a new attack vector to the OT Network.
Fail-Safe	Will not disrupt operations or flow of serial communications in the unlikely event of power failure.
Supports RS-232/485/422	Can be integrated with a significant number of industrial control systems.
Full/Half Duplex Serial Monitoring	Can support monitoring of both RX/TX channels.
Protocol Agnostic Support for Various Legacy Serial Networks	Configurable to accurately frame all the bytes into messages even if the serial protocol of captured data is unknown.
Deep Packet Inspection	MODBUS, DNP3, IEC-101 and more.
Real-Time Operating System	Guarantees the accurate capture of every byte with nanosecond resolution.
Encapsulates serial data in encrypted TCP data packets*	Secures data packages before forwarding them to Cynalytica's AnalytICS Engine or third party network security tools in order to ensure data integrity.
Power over Ethernet or 24V	Powered by ICS standard power supply options. Has minimal electrical wiring and low power consumption.
LED indicators	Illustrates the rate of the serial data flowing through the device. Also facilitates quick troubleshooting.
DIN-Rail Mounting bracket	Easily mounted on a DIN-Rail - an apparatus typically found on industrial controllers.
Quick Installation	Can be installed within minutes.
Graphical User Interface	Enables simple setup and monitoring.
Manufactured in the USA	Built in our ISO9001:2015 and AS9100D certified factory in the United States using J-STD-001 and IPC-A-610 standards.

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.