AnalytICS Platform for ICS/SCADA & OT Monitoring

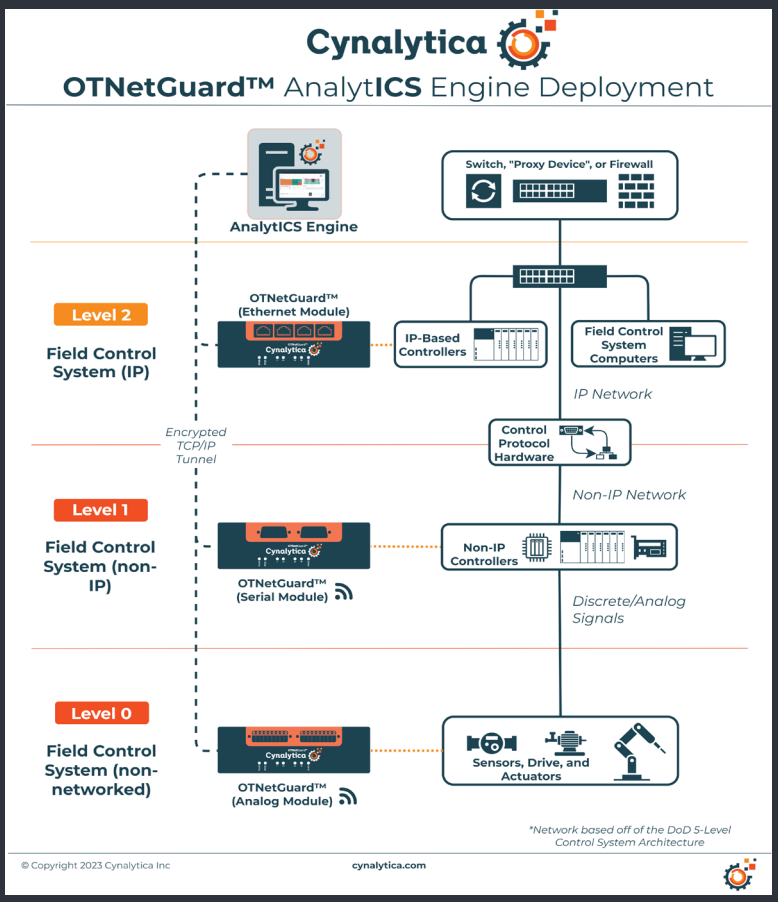
Enterprise-Scale Secure Data Visibilty and Situational Awareness for Industrial Control Systems (ICS) and OT Systems

Safeguarding Legacy and Modern Control Networks at Levels 0-2

The Cynalytica AnalytICS Platform is a high-performance operational health monitoring, analytics, and cyber-physical anomaly detection platform that brings safe and secure operational visibility to OT assets.

The AnalytICS platform helps operators monitor ICS/SCADA/OT communications (serial, analog, and IP) between field devices and controllers to provide the optimum viewpoint of industrial device behavior while supporting asset-owners in securely managing their digiral transformation efforts.

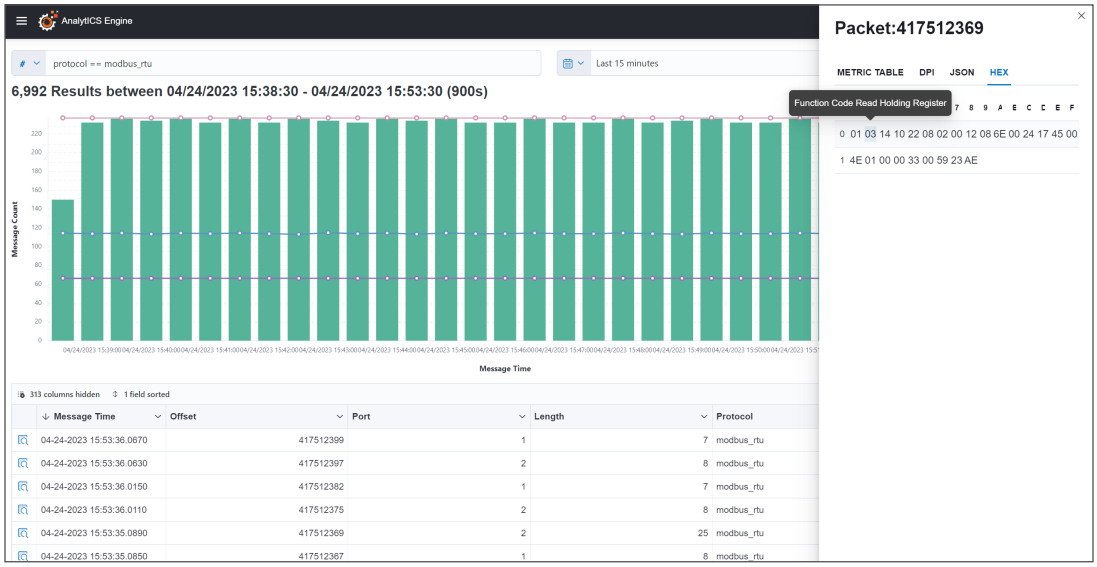
OTNetGuard™ and SerialGuard® are passive and fail-safe ICS/SCADA network taps. AnalytICS Engine is OTNetGuard and SerialGuard's supporting Enterprise Management and AnalytICS platform.



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® and OTNetGuard'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 all OT communications through encrypted communications.

- **Enables Rule-Based Alerts**
- **Performs Deep Packet Inspections**
- **Understands Individual OT Packets**
- **Integrates with Third Party SIEMs**
- **Remotely Manages Sensors**
- **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 OT communications data from SerialGuard and OTNetGuard sensors to provide optimum visibility of OT 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.

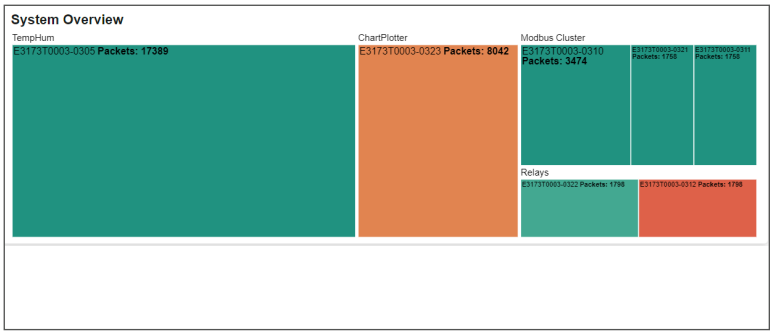
Highlights/Benefits

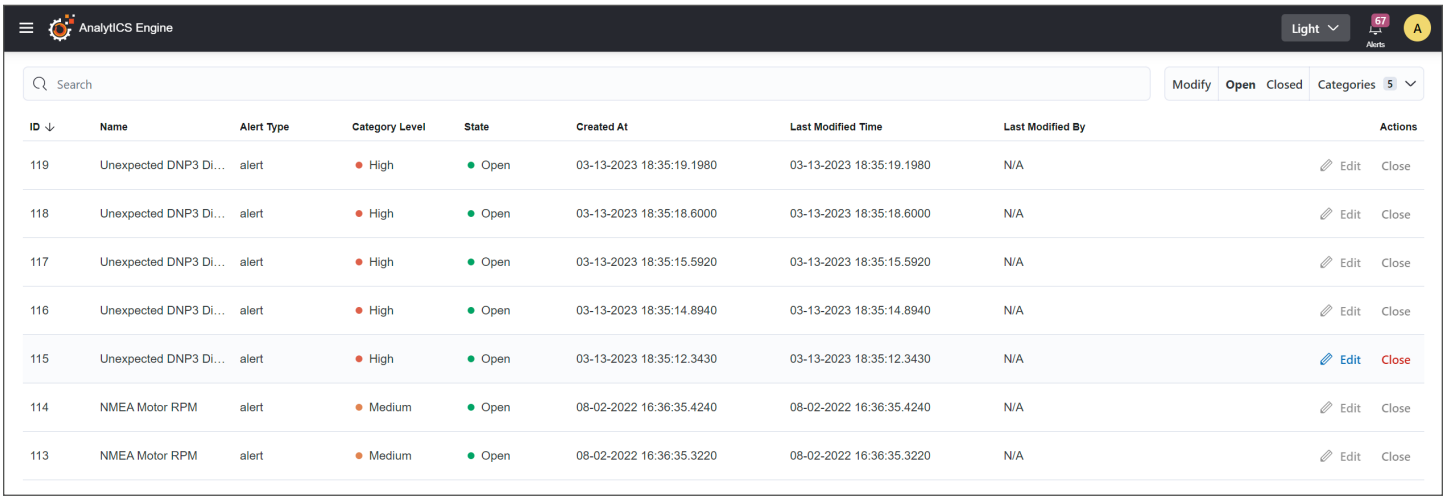
- Anomaly alerts significantly reduce Mean Time to Detect (MTTD) cybersecurity threats
- Validates data integrity of cyber-physical assets
- Enables operators to quickly detect and investigate configuration changes
- Saves time - configures and manages sensors from a centralized location
- Organizes data into easy-to-read graphics for efficient ICS health monitoring
- Gives a deeper insight into 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 sensors
- Encryption and authentication with role-based access control
- OT 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

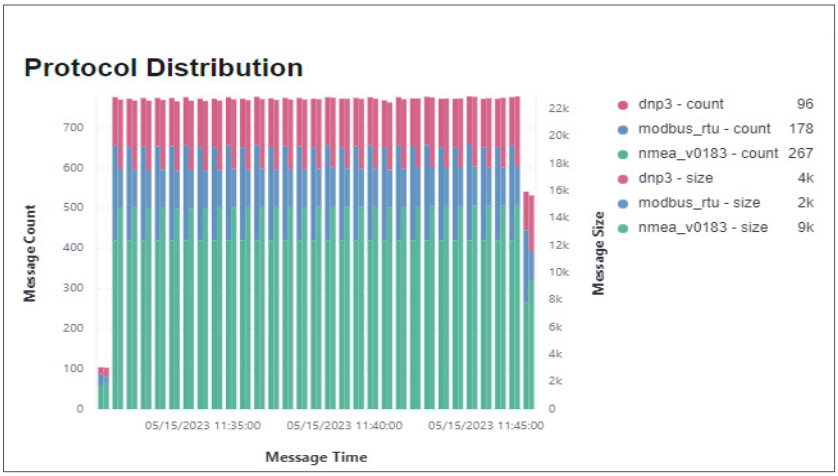




Powerful Data Visualization & Analytical Tools

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

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



Industry Integrations

The Cynalytica AnalytICS Platform can be deployed across all industry verticals that utilize ICS 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

Improves Operational Health and Cybersecurity Posture

Helps ICS Operators to:

- ✔ Verify Operational State of OT Systems
- ✔ Detect Cyber-Physical Anomalies & Attacks
- ✔ Discover Device Misconfigurations
- ✔ Prevent Network Downtime

CyRenQL™

The Evolutionary High Performance Integrated Query Programming Tool for IP and non-IP ICS/SCADA and OT Environments

The Cynalytica Query Language - CyRenQL

CyRenQL is a language designed to provide users the ability to create alerts, integrations, and other triggers from datasets in the AnalytICS Engine. It includes various components that allow for specific filtering to get a result set from a query.

- ✔ **Evaluate large & complex datasets across different protocol layers with easy to implement logic**
- ✔ **Create helpers to allow for optimizing logic**
- ✔ **Reusable and extensible logic**
- ✔ **Process high throughputs of data**
- ✔ **Integrate with SIEM and SOAR Platforms through pipelines**

Technical Features

- Supports JSONPath for advanced queries on datasets
- Ability to run analysis on any Key Value Pair (KVP) structured data (e.g., JSON, XML, YAML, TOML)
- LSP (Language Server Protocol) support - making IntelliSense available on any IDE that supports LSP
- Send result datasets over various outputs such as:
  - HTTP(s) endpoints in either JSON or XML
  - Syslog-NG
  - stdout
  - AnalytICS Engine alerts
  - Splunk HTTP Event Collector (HEC) via the Cynalytica ICS Monitoring Add-On for Splunk

OTNetGuard™

Next-Generation Monitoring for Industrial Serial Communications, Analog Signals, and TCP/IP for ICS/SCDA and OT Environments

Passive and Fail-Safe Tap With Out-of-Band Monitoring For ICS

Serial

TCP/IP

Analog
(4-20mA shown)

1 SFP+ Input
2 Modular Data Capture Platform (RS-232 Shown)
3 RJ-45 PoE+ Port
4 SIM Card and SD Card Slot
5 Groud Pin/Reset Button
6 24V AC/DC Power Input
7 Power and Activity LEDs
8 SMA Connector for Wi-Fi/Cellular
9 DIN Rail Clip (back of unit)

Features and Benefits

FEATURE	BENEFITS
Passive	System does not actively participate in the communication process or alter the content of the data being transmitted.
Fail-Safe	Designed to ensure that critical information is transmitted and received reliably and accurately, even in the event of a communication failure or interruption.
Cynalytica AnalytICS Engine Support	Encrypted communication backhaul, deep packet inspection (DPI), analytics, alerting and easy integrations with third-party SIEM and SOAR platforms.
Modular Data Capture Platform	Customer physical layer modules designed to support a wide range of OT network communications such as analog, discrete, and digital signals.
Wireless Backhaul	Optional module(s) for Wi-Fi and 5G Cellular connections that allow for deployment into remotely-connected environments.
SFP Support	Supports 1 Gbps Ethernet Copper of Fiber Channel.
Protocol Agnostic Support	Systems can communicate with different types of devices and systems, regardless of the communication protocol they use.
Full/Half-Duplex Monitoring	Supports simultaneously monitoring of both Tx/Rx channels.
Power Over Ethernet or 24VAC/DC	Simplified installation, flexibility in installation location, enhanced reliability, and lower cost.
LED Indicators	Facilitates quick diagnostics and communication activity for troubleshooting.
Web GUI	Quick setup and configuration without the need for command line access.
Secure Access	VPN, firewall, logging, and authorization.
DIN-Rail Mount Clip	Safe, reliable, and flexible mounting solution.
Manufactured in the USA	Designed, engineered, and manufactured in the USA.

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 and Fail-Safe**
- **Encrypted Communications**
- **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.

About Cynalytica

Cynalytica is a leading provider of industrial cybersecurity solutions, helping organizations to protect their critical infrastructure systems from cyberattacks while providing visibility and unique situational awareness to cyber-physical assets. With a range of innovative technologies, Cynalytica is committed to providing comprehensive, effective, and secure solutions for OT and ICS/SCADA systems. 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.