BLUE Lightning AMPEX

Protect the Process

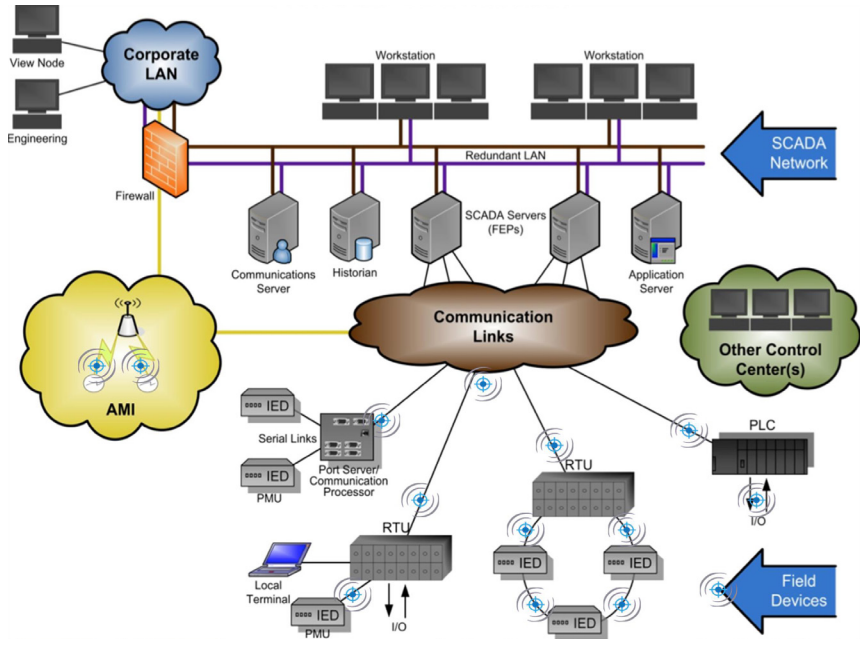
BLUE Lightning is highly scalable and flexible architecture engineered to support changing needs. From monitoring all SCADA network traffic within the control network security perimeter, to enabling detection of insider threat attacks, or spoofing attacks. BLUE Lightning protects against any attacks that may have circumvented perimeter defenses.

Features

- Gain unmatched in-depth network situational awareness of your entire control system process
- Protection at the lowest level of a control system network
- Not a signature based security solution
- Firewall technology built into each SNIEPR Sensor provides Micro Firewalls deep in network
- SIEM agnostic allows for decisive action when vulnerabilities and threats are identified
- Improve situational awareness and reduce total cost of ownership with multiple applications on a single platform
- Network behavioral monitoring and intrusion detection
- Decreased maintenance cost by detecting variables indicating equipment anomalies
- Scalable for any size network

BLUE Lightning detects intrusions, malware, and network abnormalities at the physical layer in real-time. This means it can defend against spoofing attacks – even if the malware has successfully attacked and gained control of a programmable logic controller (PLC) or remote terminal unit (RTU).

BLUE Lightning can be deployed either in line with the customer's network or in an out of band configuration both of which reach deep inside the control network, and continually monitor the information directly from local devices. The sensor scans the protocol with various algorithms to correlate the information, then forwards alerts using a secure communication channel to its controller which streams the information to any Security Information and Event Management (SIEM) system.



Where BLUE Lightning is Deployed on a Control System Environment

Additionally, BLUE Lightning offers independence from your control system provider. It can be implemented into a control system provider's PLCs, RTUs, data concentrators, and other industrial control systems devices. However, it doesn't have to be – implementing BLUE Lightning in parallel avoids a wholesale replacement of SCADA components.

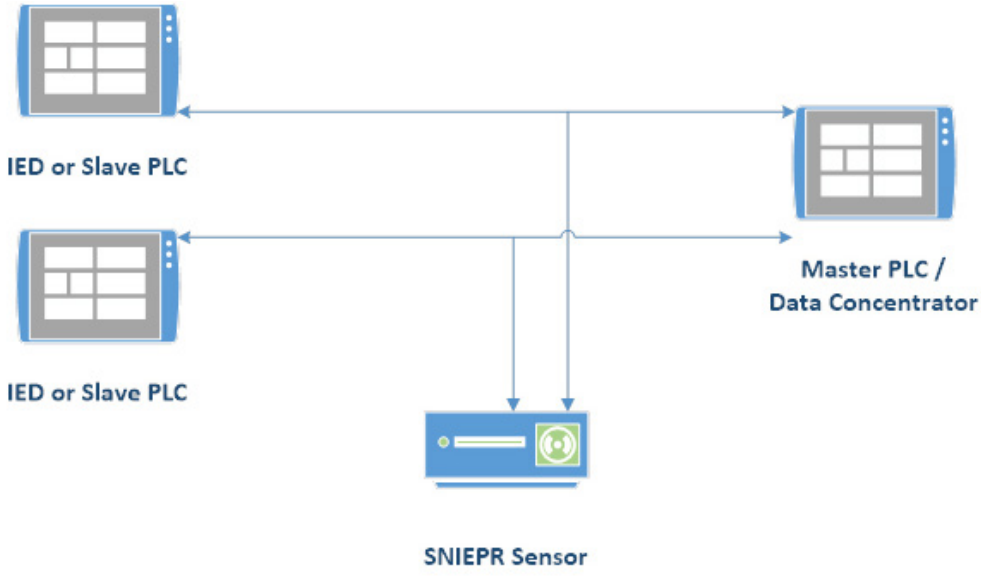
Small, low power, and sufficiently rugged for harsh outdoor extremes of temperature, BLUE Lightning fits into any control architecture – no rework of effectively operating industrial control systems is ever necessary. Likewise, as the control system evolves and matures, BLUE Lightning continues to operate and delivers first line control over your operation's data security at its lowest digital level – below your SIEM, below your routers, below your processing, and separate from traditional log reviews, which can be manipulated.

Endpoint Cyber Security for Industrial Controls and Critical Infrastructure

BLUE Lightning utilizes a patented algorithm for endpoint protection to deliver effective, high-confidence detection. It detects any and all extraordinary traffic on the network before any malware can mask it.

This technology scans and monitors industry standard protocols used by process control systems such as Modbus, DNP3, BACNet, and GOOSE, and generates alarms that are saved to the sensor monitor for diagnosis and action.

Where SNIEPR Sensor is Located



What are the applications for BLUE Lightning?

- ICS Asset Management
- Situational Awareness
- Multi-zone Mesh Protection
- Secondary Data Integrity
- Partnerships & Technology

Ampex Data Systems Corporation, A Delta Information Systems company
26460 Corporate Ave., Hayward, CA 94545, USA
Tokyo Office
www.ampex.com **1-650-367-2011** **sales@ampex.com** +81-3-6433-9081 info@ampex.co.jp

Ampex is a US Owned and Operated; AS9100/ISO 9001 certified small business.