# Binary Armor®

## ELECTRIC GRID CYBERSECURITY

Sierra Nevada Corporation delivers a versatile Cybersecurity Solution for deployment throughout the electrical grid

## A Multi-Function Solution for Flexible Deployment Scenarios:

The patented, certified Binary Armor® end-point protection and network awareness device is a multi-function solution deployed in electrical utility networks today - in part because of its capabilities, and in part because of its versatility. Binary Armor can be deployed on the main substation data line for complete substation data control and protection. It is installed today within substations to protect Intelligent Electronic Devices (IEDs) such as Remote Terminal Units (RTU) and reclosers. Binary Armor can also be deployed very close to the distribution edge in automated metering solutions. For the best results, Binary Armor can be deployed throughout the distribution grid for synchronized, inter-operable, layered security and grid intelligence.

## Use Case: Securing the Substation's Main Data Line

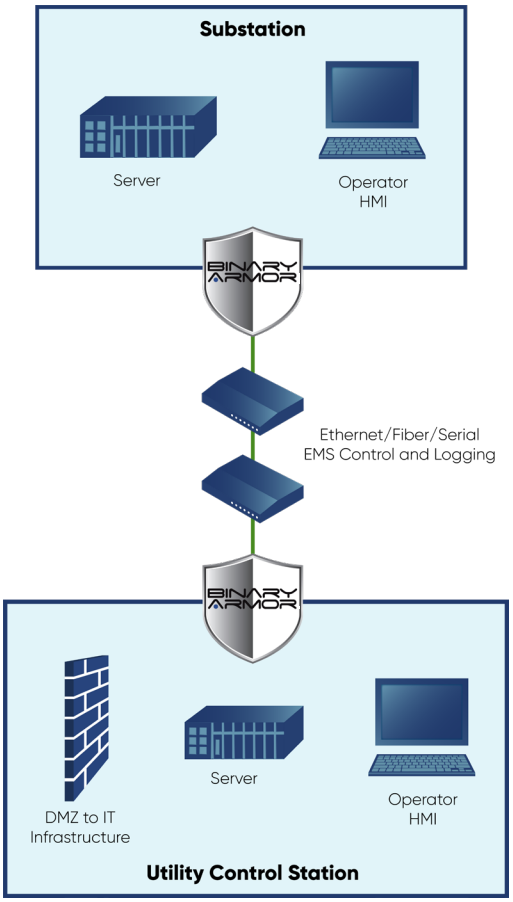


Figure 1

- **Capabilities -** The Binary Armor deep content inspection capability examines every byte of every message going to and from a substation, and so can force a 'select before operation' and block 'direct operates' on DNP3, for example. Binary Armor can handle >500Mbps throughput with virtually no latency. It supports dozens of active sessions at any point in time including SCADA traffic, update protocols, one-way streaming data outputs like C37.118 for synchro-phasors (PMUs) on transmission lines, and more. Plus, Binary Armor can establish a TLS 1.2 tunnel between the substation and the utility control center to protect the confidentiality and integrity of data in transit. The Binary Armor data handling capabilities ensure that the device will never become a choke point on the main data line. **See Figure 1.**
- **Benefits -** Employing Binary Armor on a substation's main data line enables evaluation of all data at the byte level. This robust protocol and message enforcement capability protects each system and device within the substation. The ability of Binary Armor to protect numerous substation devices with next-generation cybersecurity protection means the utility doesn't have to engage numerous OEMs and request security feature updates on many IEDs in a substation.

sales@binaryarmor.com | binaryarmor.com

## Use Case: Distribution Network Awareness and Reporting

- **Capabilities -** Distribution networks often have hundreds of wired and wireless devices reporting status and activity into the utility control center. Binary Armor, sitting in line with groups of small IEDs, serves as a network sensor as well as a network protector. Each Binary Armor unit monitors, logs, and reports every message passing through, or attempting to pass through, the device. Each device reports an alert when any malformed, invalid, or non-compliant message is encountered and blocked. DNP3 and Syslog messages from numerous Binary Armor devices can be aggregated at a single Binary Armor Master and Log Server in a utility control center as shown in **Figure 2**. The Binary Armor Master could then provide log inputs to the IT firewall/DMZ for delivery, evaluation, and response by utility control center operators.

- **Benefits -** Utility operators may not be aware that sensors have been overtaken by malware and are generating misleading or malicious status reports. Binary Armor, acting as a network sensor, will detect, block, and report malformed or malicious data traffic anywhere in the distributed grid network. Central access to all alerts and logs at the utility control center reduces response time to incidents, and aids in network triage and forensics. The Binary Armor control application can be configured to send key, personnel email/SMS notifications in the event of both security and operational incidents, even if they are off-site.

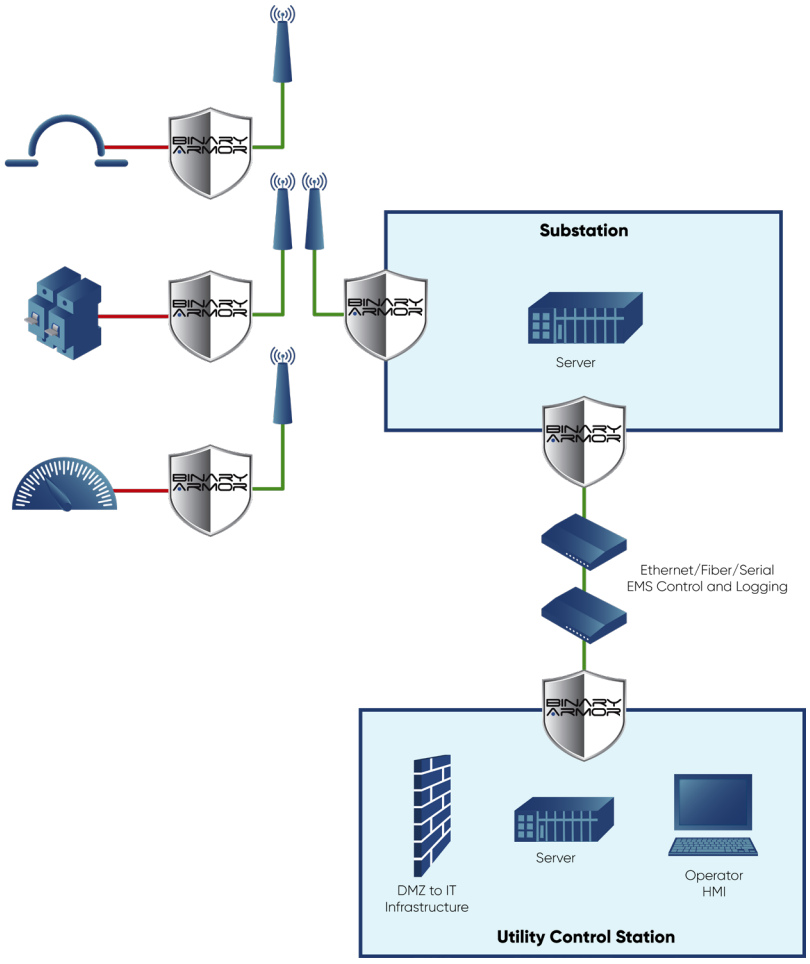


Figure 2

## Use Case: Securing Wireless Mesh Systems for Distributed Automation

- **Capabilities -** Many wireless grid devices lack adequate security controls to protect equipment and data. For example, some wireless modems/radios and wireless meters still use outdated AES-128 encryption, expose crypto keys, or otherwise improperly implement encryption. Binary Armor can secure wireless links between each subsystem and substation **(Figure 3)** through its FIPS 140-2 certified encryption implementation. In practice, each substation would maintain a Binary Armor Master device and Log Server for management of secure Binary Armor communications to downstream devices. Additionally, the Binary Armor GPIO ports can integrate local I/O-based alarms and deliver them to the substation RTU for delivery and alerting the emergency management system at utility control station. In case of emergency, technicians can be dispatched to the substation for local management and incident response.

- **Benefits -** Binary Armor has FIPS 140-2 certified encryption, which ensures that the device's encryption module has been implemented properly so the security promised by TLS 1.2 encryption will actually be delivered. Moreover, Binary Armor can inspect all incoming and outgoing message traffic transiting through the radio, and block non-conforming messages before they are delivered to other points in the network. Binary Armor implements best practice, layered security to any IP-based radio system without modifying the radio or wireless device itself. Integrating Binary Armor edge reporting and alerting does not require modification to main control/substation comms.

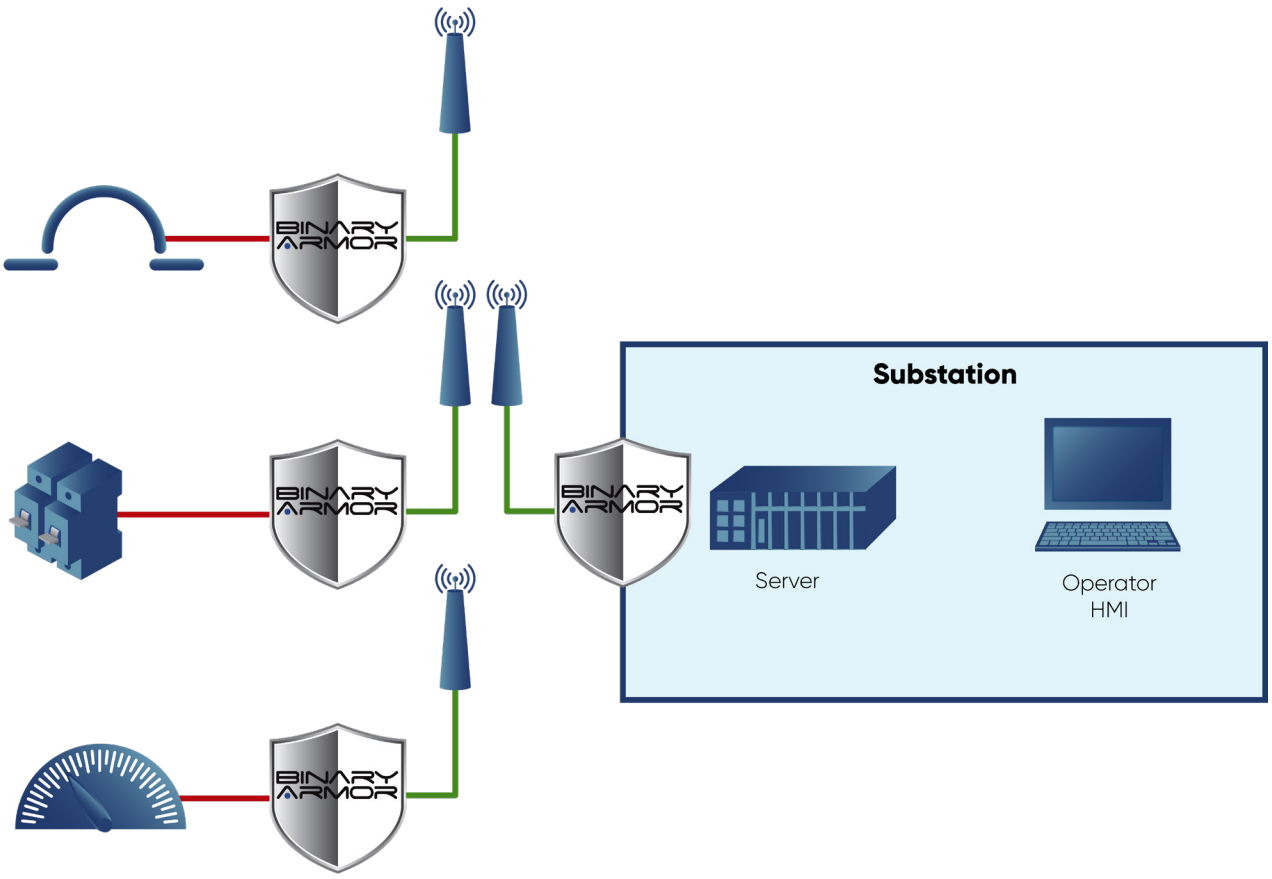


Figure 3

## Use Case: Substation to Substation Interconnection for Rapid Fault Location, Isolation and Recovery

- **Capabilities -** Continuous, uninterrupted electricity delivery is the goal of every electrical utility and the demand of every electricity consumer. Unfortunately, equipment failures happen despite the best efforts of engineers and operators. Digital Fault Location, Isolation, and Recovery (FLISR) systems are being deployed to detect and route around interruption-causing failures until repairs can be made. FLISR systems can be automated or semi-automated, but in most cases rely upon a central coordinating mechanism for response. Engineers understand that reporting substation faults back to a control center incurs a time penalty and can slow responses considerably. A common remedy is to interconnect substation Remote Terminal Units **(Figure 4)**, which allows the RTUs themselves to coordinate automated recovery actions much faster than a centrally managed response. While RTU-to-RTU interconnection can speed automated recovery, the interconnection itself opens another cyber vulnerability that could allow malware to move laterally from substation to substation and affect the entire automated response system.

- **Benefits -** Binary Armor can be placed on the substation to substation interconnection line(s) to prevent east-to-west malware movement and isolate malware to a single substation.

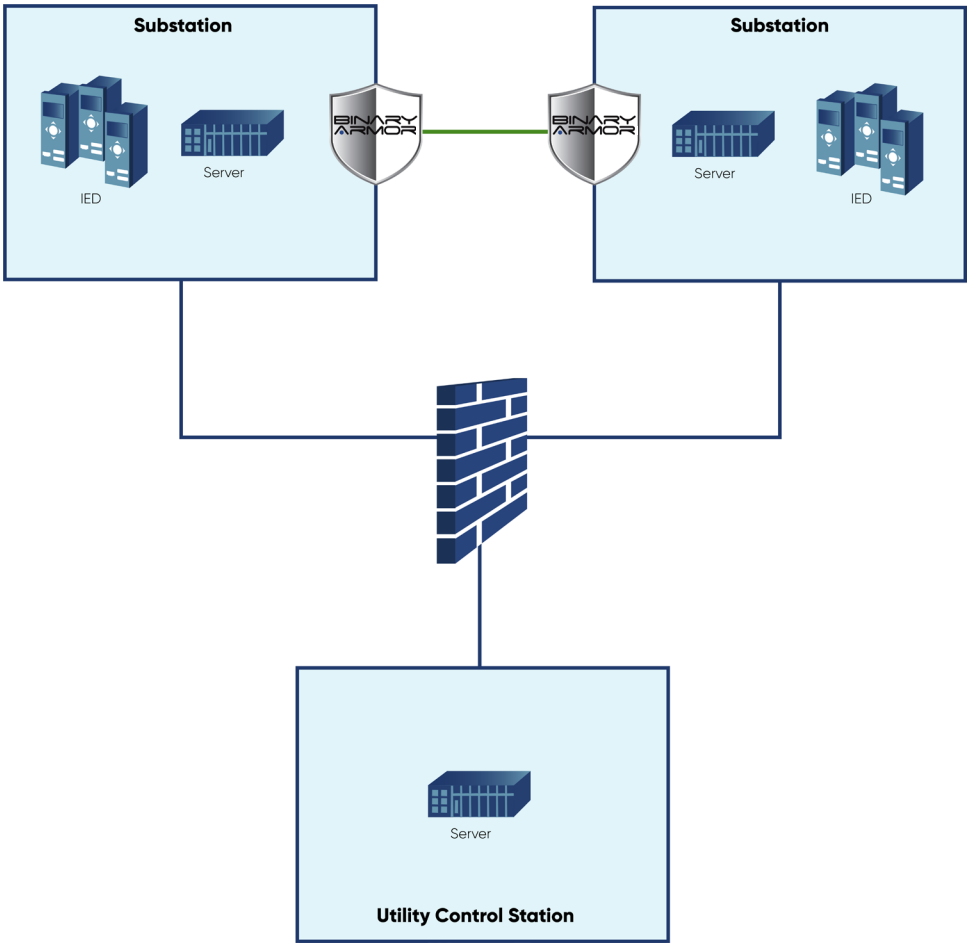


Figure 4

## Use Case: Core-to-Edge Distribution Grid Security

- **Capabilities -** Binary Armor can be deployed at numerous critical nodes throughout the distribution grid network **(Figure 5)** to provide end-to-end security. Deployed in this manner, Binary Armor will provide in-band data validation and workflow enforcement from the control center through substations out to edge wireless sensors. What is more, Binary Armor can create segmented security enclaves. Binary Armor devices deployed throughout the network create a de facto distributed, intelligent sensor network. Additionally, the encryption capability can augment out-of-band radio links for maintenance-related communications that are secure but don't consume operational bandwidth.

- **Benefits -** Deploying Binary Armor devices throughout the distribution grid enables cybersecurity professionals to orchestrate and control global and local security policies on numerous multi-function devices that seamlessly integrate and inter-operate together. Beyond that, the Binary Armor global and local security policies create an organic, synergistic, edge-to-core Quality of Service (QoS), and thus ensure anomalies like packet storms are blocked and dropped so important network traffic is uninterrupted. Equally important, the intelligent sensor grid created by deploying several Binary Armors delivers real-time, network-wide insight into grid behavior for comprehensive situational awareness and emergency response. Together, synchronized Binary Armors provide reliable, certified multi-layered security and segmentation that complies with NERC CIP and NIST 800 standards while delivering optimal operational performance and protection.

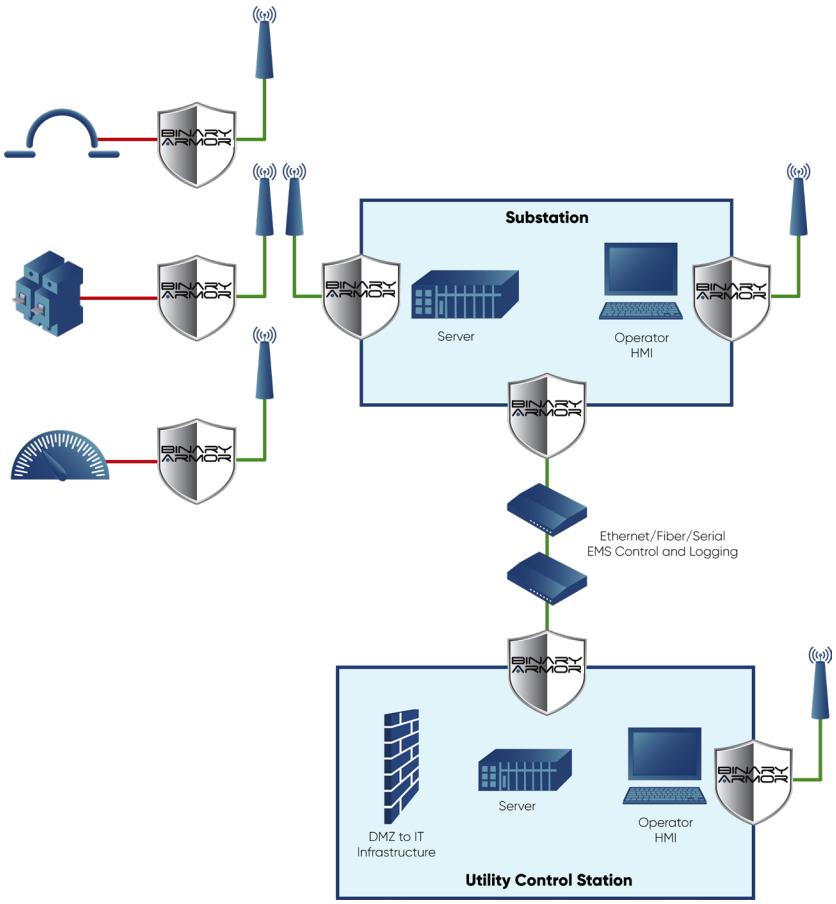


Figure 5

# Binary Armor®

ELECTRIC GRID CYBERSECURITY

## Use Case: Distributed Electrical Generation Security

- **Capabilities -** Distributed energy resources (DER) including solar, wind, remote conventional generators, and storage systems, promise diversification and resilience benefits to the grid. On the other hand, each DER increases the grid cyber-attack surface. DER nodes must only be connected to the grid with accompanying cybersecurity protection to avoid a glaring cyber vulnerability. Binary Armor, placed at the network interface between DER and the grid control system, can mediate all data flows and allow only known good data to traverse the network from one point to another.

- **Benefits -** Utilities can connect DER to their grid with confidence when connection is accompanied with the Binary Armor patented, certified cybersecurity protection. Control, status, and transaction-related messages can all be pre-defined and mediated through Binary Armor. Binary Armor also has several flexible operational modes that enable Binary Armor to adjust its protection profile to different approved traffic patterns as communication requirements change. The Binary Armor adaptive operating modes, activated via two-factor authentication, enable the device's protection policy to be modified in near real-time so that the network itself remains available and protected in all situations.

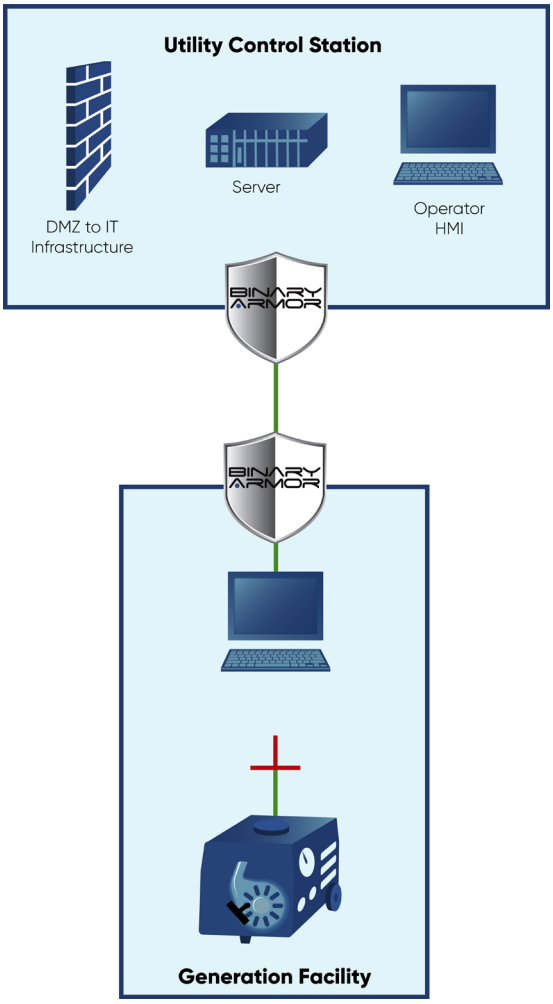


Figure 6

## Deploying Binary Armor

SNC's deeply experienced, industry-leading technical services team delivers best-in-class industrial control cybersecurity solutions to help you regain the upper hand against attacks from nation-states, terrorists, and cyber criminals. From cybersecurity site surveys to proof-of-concept pilot projects through full network deployments, SNC is your industrial cybersecurity partner.

For more information, contact us at: sales@binaryarmor.com