



Protecting OT Networks Beyond the Reach of Traditional Information Technology Tools and Techniques with Binary Armor®

Sean Bayless, Systems Engineer, SNC Secure Cyber Solutions

INTRODUCTION

As Industrial Control Systems (ICS) have become increasingly connected, rules and regulations have been put in place to implement cybersecurity protections. Typically, since many of these systems have components such as servers, workstations and network switches, Information Technology (IT) personnel are often called in to help design and secure the systems. This results in the use of traditional IT tools and techniques such as firewalls, antivirus, Security Information and Event Management (SIEM) systems, Network Intrusion Detection Systems (NIDS), Network Performance Management (NPM) and Network Configuration Management (NCM) systems, and Host Intrusion Detection Systems (HIDS) to secure the devices. While these systems work up to a point in an ICS, they cannot always reach the endpoint devices – they assume the devices they monitor have standard operating systems (OS) such as Windows or Linux on which they can install agents that report back to central monitoring systems. They expect standard system logging (syslog) messages for event reporting and require potentially frequent updates to maintain these cybersecurity systems, so they remain current with the latest threats.

PROTECTING TO THE ENDPOINTS WITHIN AN ICS

SNC's Binary Armor® can help bridge the gap and bring cybersecurity to endpoint devices that may be less capable of being secured by traditional IT tools and techniques. The standard deployment for Binary Armor® is in-line in the network between the larger network and an endpoint as shown in Figure 1. Binary Armor® acts as a bump-in-the-wire device to monitor all network traffic traveling to and from the device being protected. It works by providing network segmentation, examining the full contents of the network traffic, parsing the message to compare against proper structure and customer-configurable rulesets, and (if it is allowed to pass) transmitting it out the other interface.

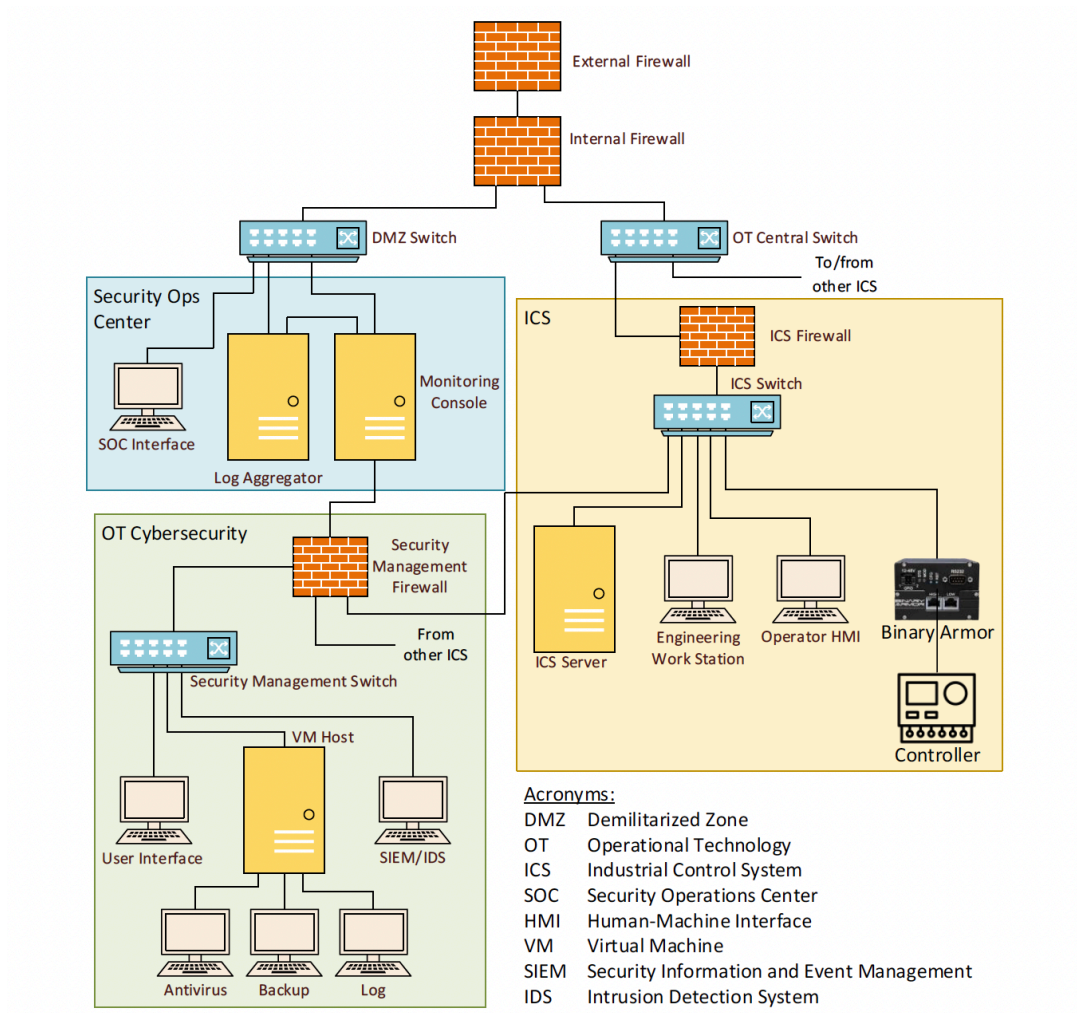


Figure 1: Example ICS Architecture with Binary Armor® Placement

Binary Armor® does not require installation of software on monitored devices, therefore it protects devices that do not have a standard OS or are purpose-built to complete only the tasks for which they are designed. This is a feature unique to Binary Armor® that allows utilities to protect ICS endpoints without requiring bulk modernization.

An example of this could be a digital valve controller. The controller is "smart" enough that it can report the position of its valve and take commands to open or close the valve. If the digital valve controller does not have a standard OS, it cannot have an agent installed that allows a traditional IT cybersecurity system to monitor its status. To infer status of the valve, the agent would have to be installed on the server with which the digital valve controller communicates. However, if the digital valve controller is compromised, it may report inaccurate information to its server, and the standard cybersecurity system may not be able to detect the faulty reporting.

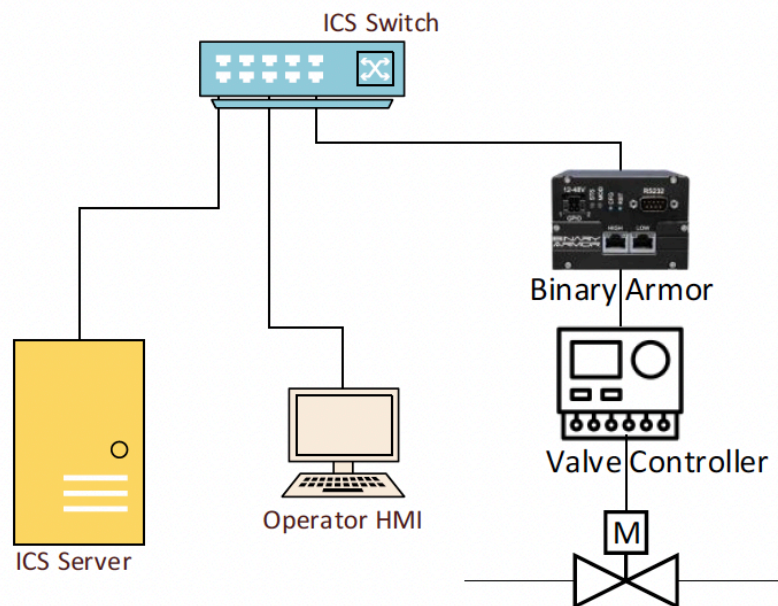


Figure 2: Binary Armor® Installed Between Server and Valve Controller

In this example, illustrated in Figure 2, Binary Armor® is installed in-line between the server and the digital valve controller. It can even be installed within a serial link for protocols using RS-232. As messages are sent from the server to operate the valve, they are verified first against the protocol being sent and then second, against a ruleset as configured by the operator of the device. This ruleset can have a rule such as: "the valve may not be opened past X percent." If a command is sent from the server that goes beyond the allowed range, Binary Armor® rejects the command, and the digital valve controller never receives it. The server may have this limit installed as well, but in the case that the server is compromised, Binary Armor® acts as a backup to prevent the potentially harmful command from being received by the digital valve controller.

As discussed above, Binary Armor® provides functional whitelisting and can parse many standard industrial protocols such as BACnet, DNP3 and Modbus so that it proactively prevents cybersecurity incidents from taking place. Only commands that have been deemed by the ICS owners as safe operational commands reach their destination. In the example illustrated in Figure 2, Binary Armor® stops the unsafe command to open a valve beyond its operational range and prevents the digital valve controller from a destructive action.

Conversely, traditional IT solutions, such as firewalls, can only verify the validity of the network packet containing the unsafe command, as opposed to its contents and rules, like what IPs and ports are allowed to communicate. The operator would see the status of the valve being opened too far after the fact, or a NIDS or HIDS would have to detect an intrusion through other methods and react via an alarm. However, by the time the action is detected as harmful to the ICS, it has already taken place and potential damage has already been done to equipment.

LOGS, ALARMS AND APP INTEGRATION

Binary Armor® keeps its own logs and alarms. These can be sent as standard syslog messages to any monitoring system configured to accept them. This allows Binary Armor® to act as a proxy for the endpoint device's status, as it monitors the entirety of traffic flowing to and from the endpoint. By integrating Binary Armor® logs into an existing security operations center, traditional IT solutions gain more insight into the systems they are protecting.

Binary Armor® also uses a form of representational state transfer application programming interface (REST API). If a cybersecurity monitoring system has software development kits (SDK) and their own API for developing displays, it is possible to create a link between Binary Armor® and the cybersecurity monitoring system. This means having control and display of Binary Armor® from within the cybersecurity monitoring system's screen instead of a separate administration tool. This makes it easy to manage and integrate Binary Armor® cyber defense into an existing architecture.

TLS ENCRYPTION AND TUNNELING

ICS faces another challenge as the growing number of network-connected devices allows systems to be linked through both local area network (LAN) or wide area network (WAN) for remote administration. Binary Armor® can be used to encrypt traffic for transmission over unsecure or public media, such as across telecommunications cables, fiber optics, or over cellular connections. Binary Armor® can add transport layer security (TLS) encryption at the boundaries of various network sites to further improve cyber defense and create a virtual private network (VPN) tunnel across the intervening media, signified by the yellow highlight in Figure 3. Even if the traffic is intercepted between company locations, the data is encrypted and safe from tampering or eavesdropping.

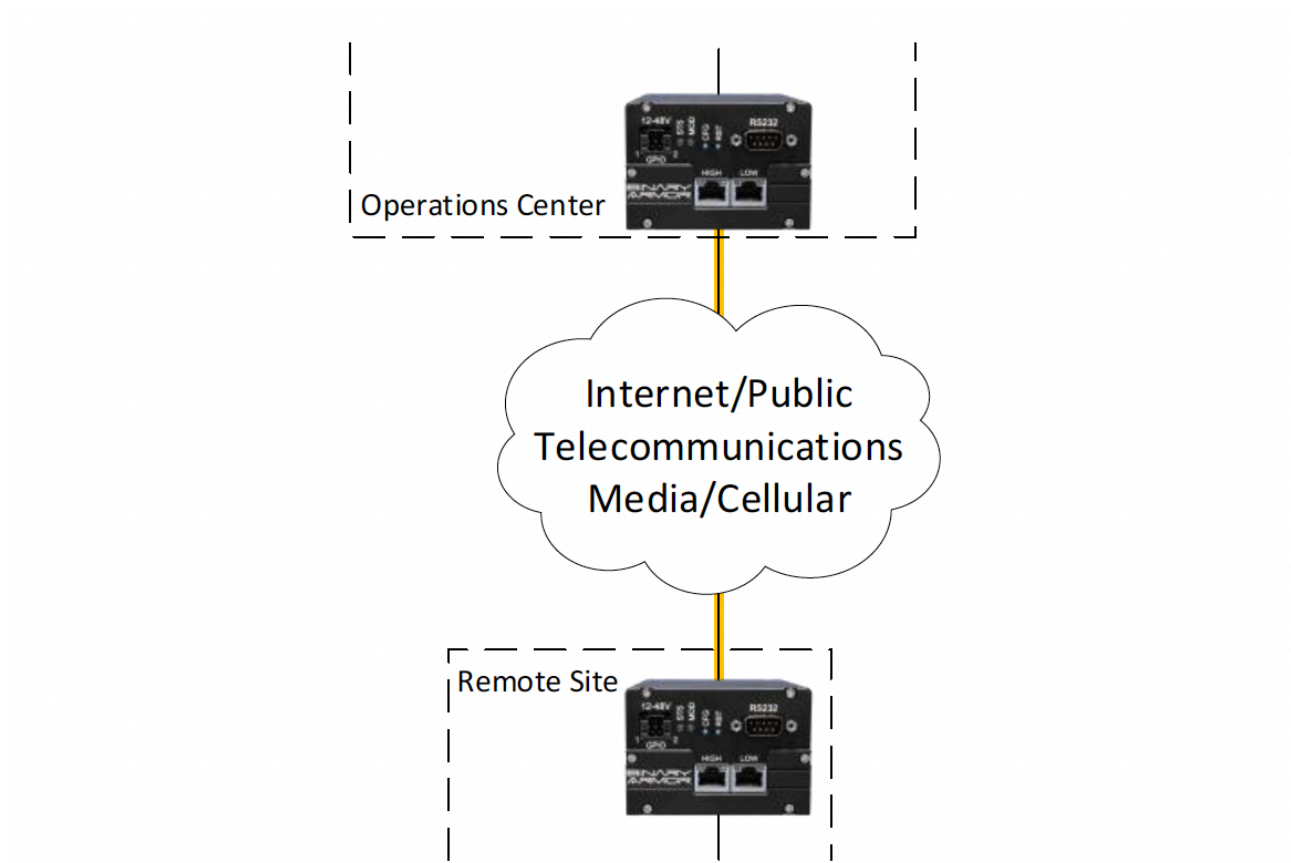


Figure 3: Binary Armor® Creating a VPN Tunnel with TLS Encryption

REMOTE ACCESS CONTROL

Windows has remote desktop which allows users to log into a server remotely to perform work. This allows users to avoid traveling to distant field sites. However, these same endpoints that do not have a standard OS are likely unable to have control over remote access. A user just logs in over the network, if that, and is given control of the device with very little oversight.

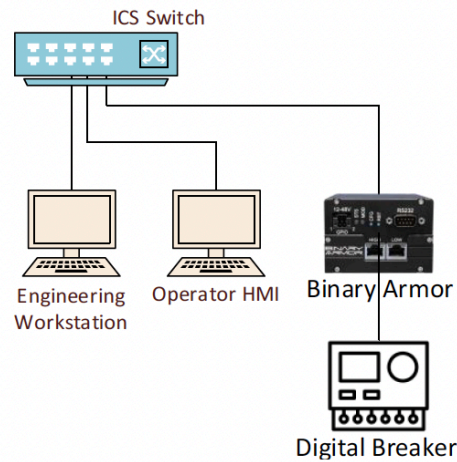


Figure 4: Binary Armor® Installed as Access Control for a Digital Breaker

Another application of Binary Armor® within an ICS is performing access control. Binary Armor® can be configured to not just monitor and take action based on traffic, but it can also act as a gatekeeper for remote access to a device. Binary Armor® can use "operational modes" to determine what direction traffic can flow, meaning that it can act as a unidirectional data diode providing read-only access to an endpoint and only, when necessary, allow write access. An example of this may be a digital electrical breaker as shown in Figure 4. A vast majority of the time, the breaker works on its own and may be able to provide telemetry and system status information in a read-only mode to a server and perhaps an engineering workstation. Generally, a few times a year, an engineer may need to have write access to adjust a setpoint or do some troubleshooting or install approved, periodic updates. Following site work control procedures, the engineer would then contact operations to request access much like they would for a physically restricted piece of equipment. The operator personnel would be able to change the operational mode within Binary Armor® to allow bi-directional traffic between the engineering workstation and the endpoint. The operator or security personnel would be able to watch the commands as they are sent from the engineering workstation to monitor for anomalous behavior, essentially performing the duty of a "digital security escort" much like a contractor may be required to be physically escorted on site to perform work. When the engineer has completed their work, the operator can return Binary Armor® to "read-only" mode. This means that remote access can be granted in the limited cases it is needed, as opposed to either being available all the time or not being available at all and requiring the engineer to go to the device locally.

CONTAINERIZED DEPLOYMENT

Finally, Binary Armor® is capable of being containerized as opposed to using its own hardware. It can be installed on a networking device or programmable logic controller (PLC) that is already existent in an ICS so that new hardware does not need to be installed. The same REST API as mentioned before would make it possible to control Binary Armor® through the host device's native interface if it has such API hooks.

CONNECT WITH US

ICS are becoming more and more connected, as is the rest of the world. Sensors and controllers are increasingly becoming part of the Industrial Internet of Things (IIoT) and are not designed to be installed standalone. Traditional IT tools and techniques can only see so far into networks because they require some sort of standard OS on the server they are monitoring. This is necessary for the installation of agents to report back to the cybersecurity systems. For endpoint devices that do not have a standard OS installed, Binary Armor® can monitor traffic to and from the devices to proactively ensure that only safe operational commands are passed through. Binary Armor® can also help facilitate safe remote configuration or operation of devices that need this functionality on a rare or limited basis and do not have the capabilities themselves.

Binary Armor® is just one part of a holistic solution that protects the entire ICS. IT tools and techniques still have their place looking for signatures of known exploits and watching for changes on the network, but those tools can and should be augmented by Binary Armor® to reach all the way to the endpoints.

✉ hello@binaryarmor.com

🌐 binaryarmor.com