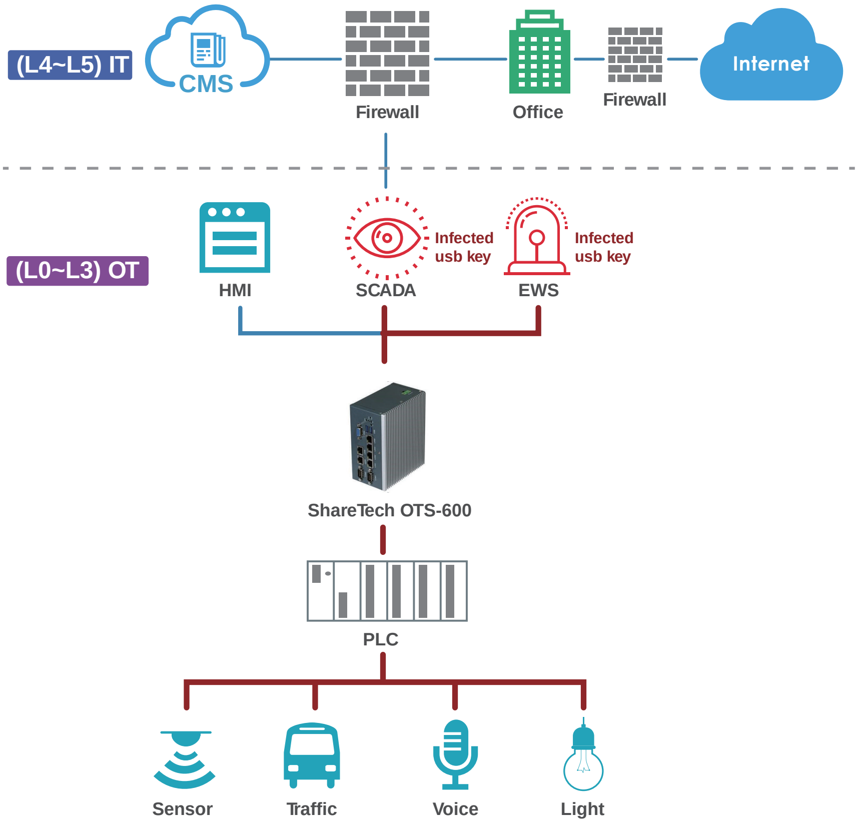
ShareTech OT

OTS-600



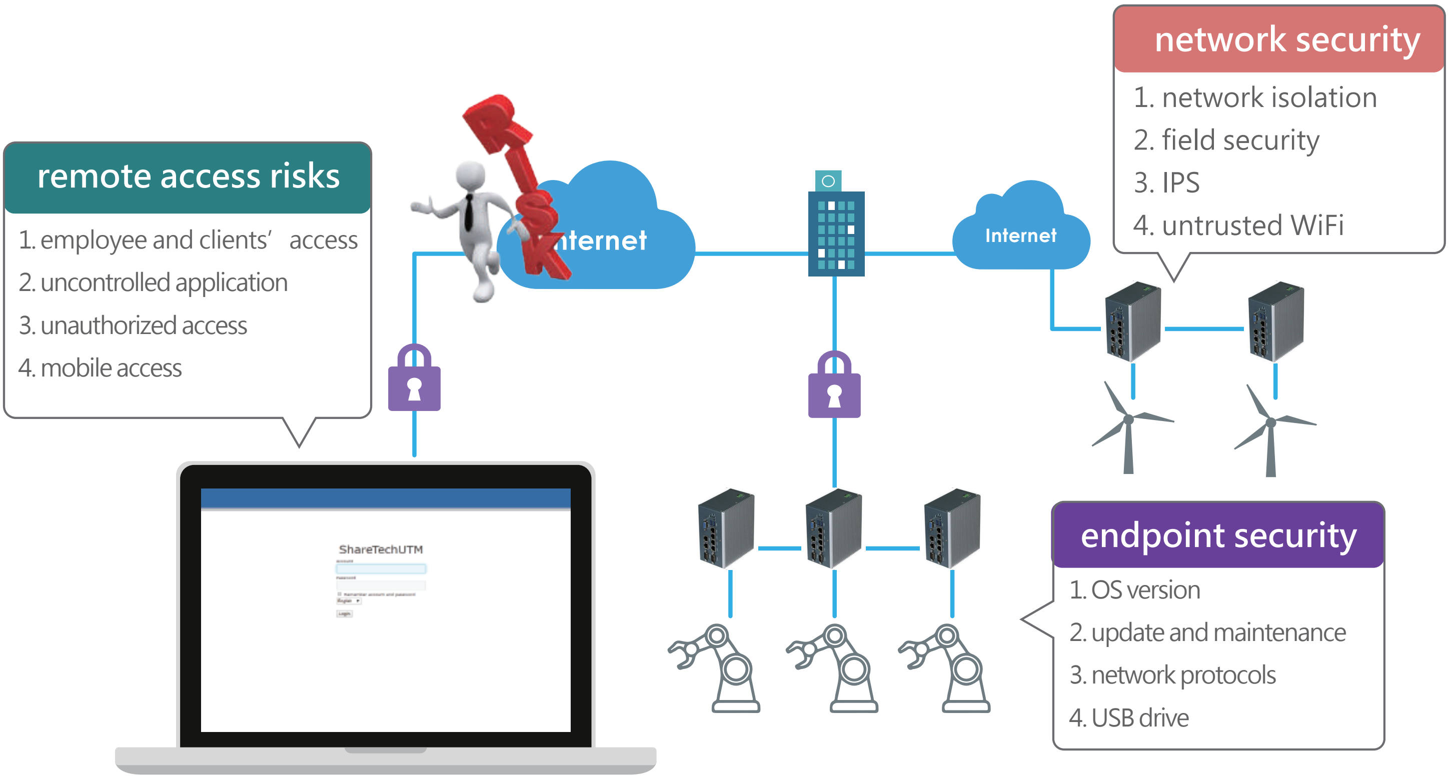
The security features of traditional IT solutions are designed primarily for business network operations. Suppose business-grade firewalls are placed within industrial networks that Industrial control systems (ICS) and SCADA are highly required, appliances are not suitable to operate in the harsh industrial environments.

To cooperate with programmable logic controllers (PLC), RTU, and other automatic controller devices, ShareTech has launched the first OT security series for OT environments (extreme environments of high temperature and humid ambient). OTS-600 is an integrated OT security appliance maintaining ICS, healthcare, and infrastructure secure and stable.

OTS-600, a fanless desktop that supports LAN bypass function, can be integrated sustainability into business networks. It supports ICS protocols and delivers specialized threat protection such as deep packet inspection (DPI), allowlist, accountability, encrypted traffic inspection, virtual patch, OPC intrusion prevention, and authentication to control industrial networks against malicious attacks.

Vulnerability in the OT Environments

- Grey area in the OT environments: Unknown devices and connections
- Insecure identification: Defects from software design and implementation
- Insecure protocols: Data not encrypted
- Devices with inadequate security: Protection not available
- Insecure third-party libraries: supply chain attack and infection



remote access risks

1. employee and clients' access
2. uncontrolled application
3. unauthorized access
4. mobile access

network security

1. network isolation
2. field security
3. IPS
4. untrusted WiFi

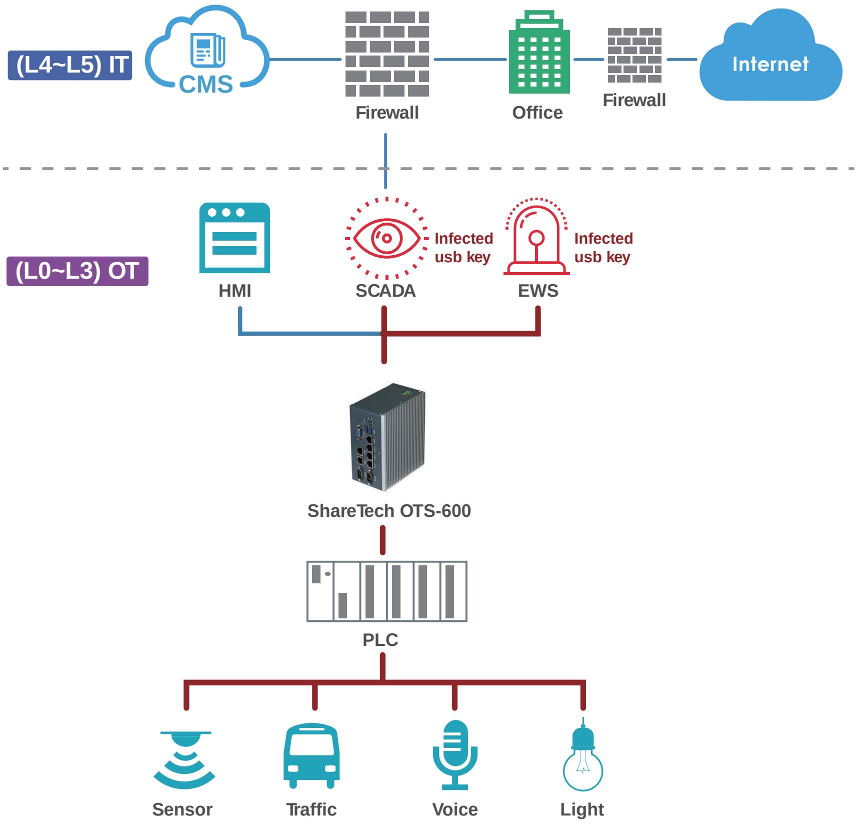
endpoint security

1. OS version
2. update and maintenance
3. network protocols
4. USB drive

ShareTech OTS-600 Features

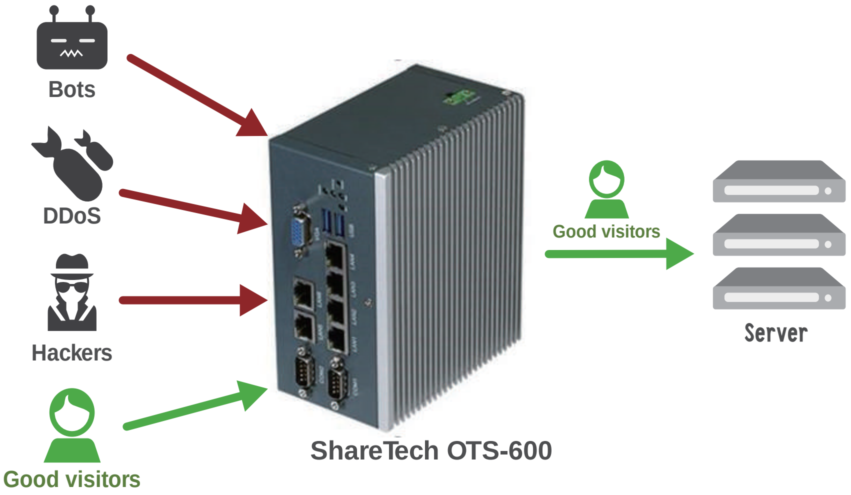
Physical and Virtual Isolation of Automation Network

Isolation plays an important role in industrial automation. The OTS Series can be the key component in hooking up the connected automation systems. An industrial firewall appliance can be installed in a one-node environment to control access to each automation system to block illegal connections and restrict access from the unprotected automation system. Furthermore, internal network security can be fortified by using virtually isolation segments and restricted ports.



Reduce Vulnerabilities of Industrial Automation

Removable media and devices such as USB, floppy drives, and devices could give attackers a path to access ICS/SCADA systems. Other than standard operating procedures might be changed, important data could be stolen or compromised. Unlike IT, many industrial control systems run 24/7, and nobody in their right mind would interrupt production in order to install a security patch or new firmware version. Built-in virtual patching is supported to act as a safety measure against threats that exploit known and unknown vulnerabilities.



Monitor Automation and Execute Virus and Vulnerabilities

A stable industrial-grade automation environment relies on full-stack monitoring for abnormal network behaviors and attacks, real-time vulnerability execution, and complete loggings. The OTS Series can analyze network traffics and scan industrial networks for viruses, malware, trojan, and automated vulnerabilities. Therefore, exceeded values over the threshold, encrypted malware traffics, abnormal commands, Trojan, and viruses can all be blocked in time. In addition, alerts/notifications for abnormal behaviors will be logged for future investigation.

Infection Control and Isolation

Attacking could have run rampant on the internal company network; therefore, defending a company intranet from intruders is a round-the-clock endeavor. Switches can be integrated into the ShareTech OTS Series. Co-Defense is a mechanism that immediately shuts down switch ports of infected areas when malware attacks occur. By isolating the infected production line, the spread of malicious attacks can be reduced. Moreover, manufacturing performance in other production lines can be properly maintained.

Supported Industrial Protocols

Common industrial protocols are supported such as EtherCAT making use of TCP/UDP 34980 and Ethernet/IP making use of TCP/44818 and UDP/2222. Related ports will be open individually and automatically once protocols were chosen by administrators. A significant disruption in production can cause revenue loss in businesses. The OTS Series can filter and further analyzed data packets. Thus, packets with suspicious values will be blocked, preventing industrial robotic arms from operating non-standard procedures.

OPC Intrusion Prevention

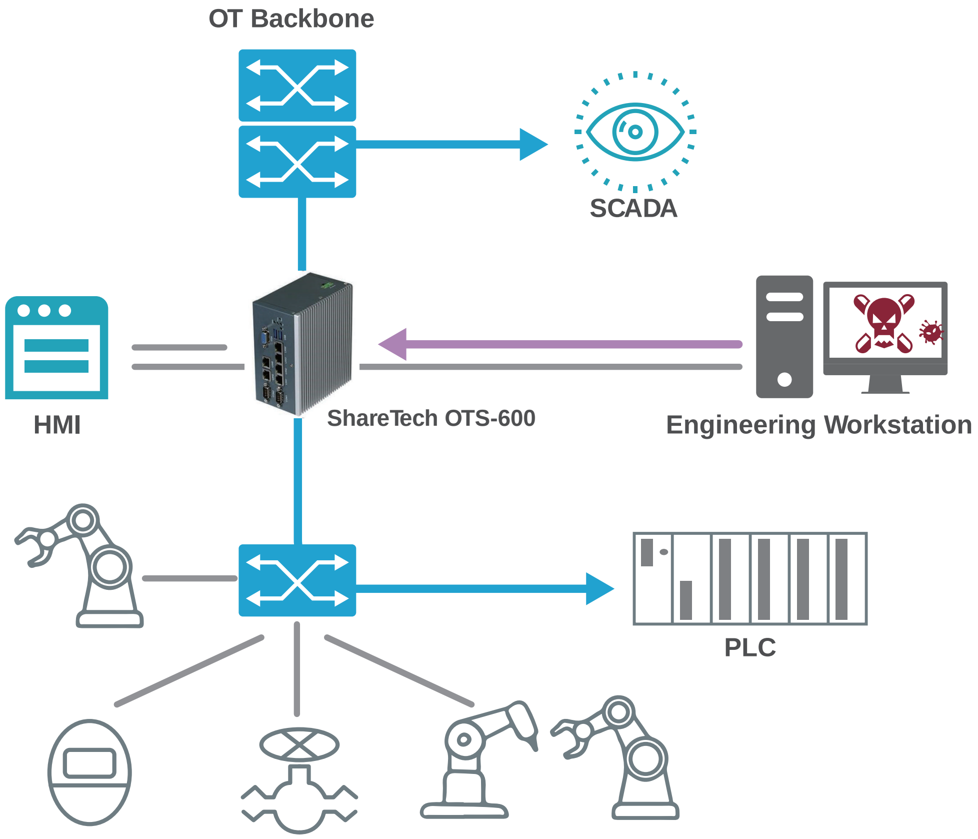
All the packets are collected from both IT and OT networks and Deep packet inspection (DPI) technology is taken to verify and analyze. According to these abnormal traffics, ShareTech OT security devices will generate related logs. Through these logs, administrators can easily make all the information of the events under control and can follow up afterward.

Authentication & Access Management

Authentication usually acts as the gateway to allow access to valuable data only to those who are approved by the organization, and it is as well as important in an OT environment. To have a timely response, some units will choose to use remote login protocols (SSH/Telnet/Web). Thus, access management should be taken to prevent hackers from accessing and exploiting important data. The OTS Series supports Host, Active Directory, POP3, and Radius so that administrators can keep the company's network resources safe and running efficiently through identity verification, authentication, and identity access management.

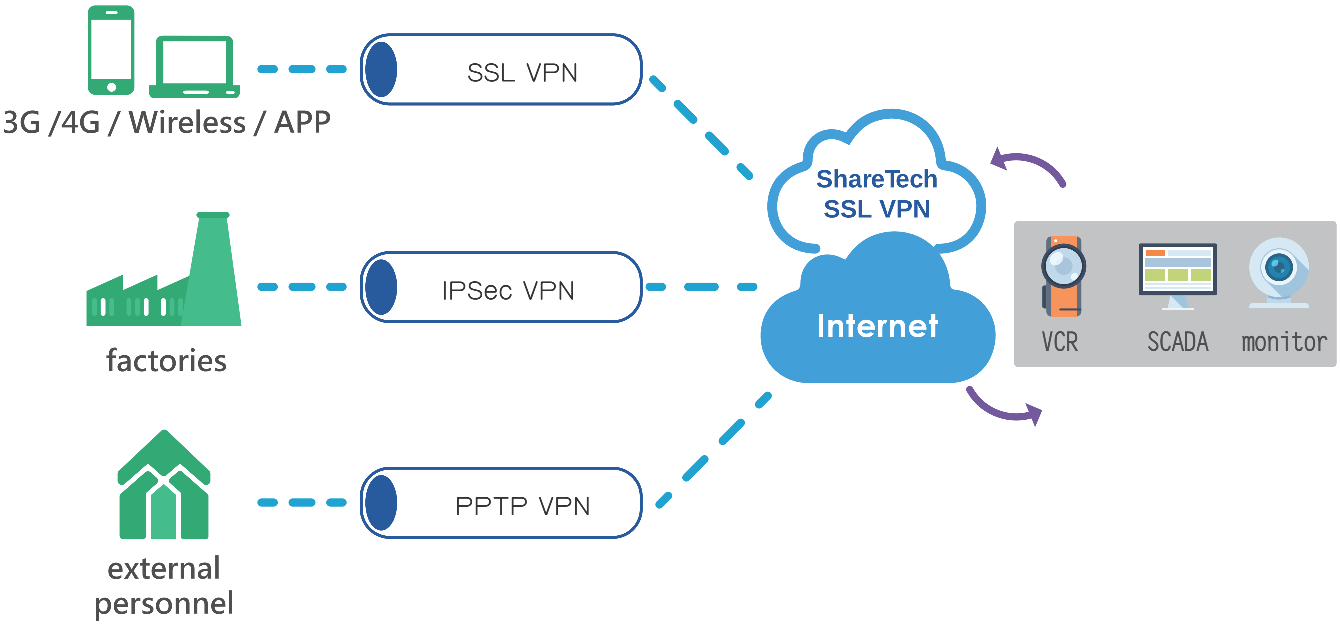
Application Allowlisting

Since various types of malware spread tremendously fast across networks, an updated blacklisting might not be reliable enough. Fortunately, most OT environments are relatively static so an allowlist approach can work properly. Administrators can decide which known applications can be allowed. Conversely, other unknown activities will be blocked or restricted to prevent them from opening up and spreading within a system.



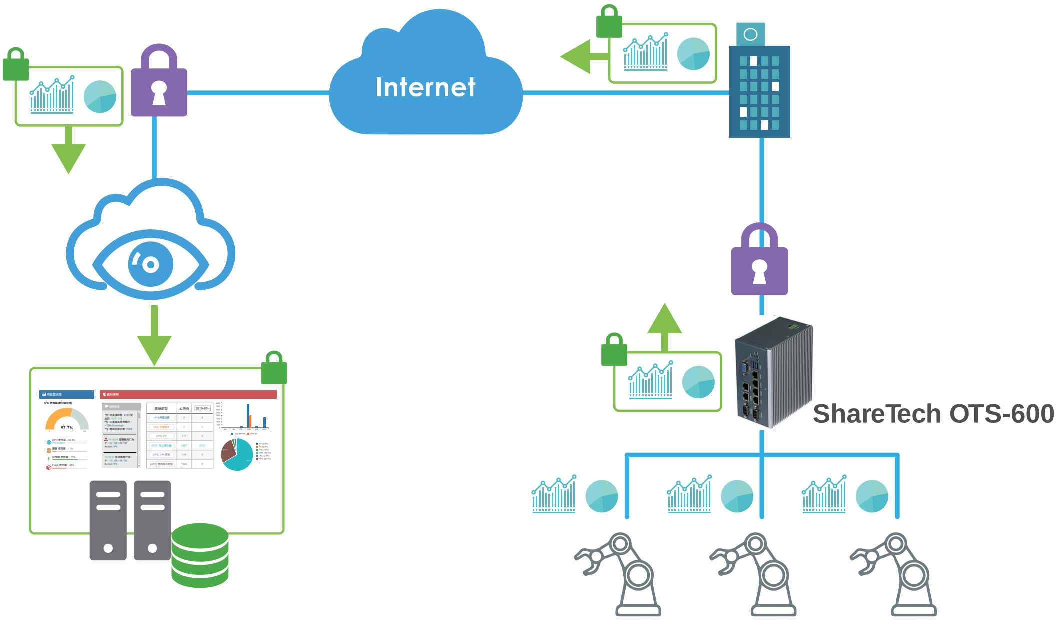
VPN

Industrial cooperation may at times rely on encrypted and secure remote access for remote maintenance. The ShareTech OTS Series can process queries from unidirectional devices in edge networks and support remote-access VPNs such as IPSec, PPTP, L2TP, and SSL VPN connections. The VPN services will be controlled and logged for any future potential investigations.



Dashboard

From the data of both IT and OT devices, ShareTech OT security devices analyze and generate a dashboard. This can help administrators easily understand the network security condition of the factory. If a cybersecurity incident happens, the dashboard will demonstrate the process and results. Besides, the dashboard will also show the operating situation of the devices and make the potential risk stand out.



Disaster Recovery

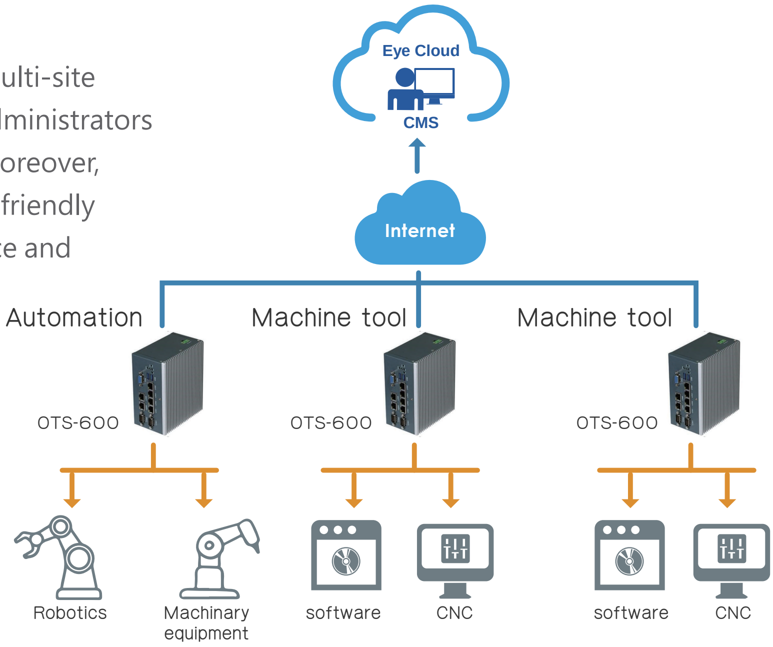
When an appliance cannot operate properly during security incidents, LAN bypass is supported to create a fault-tolerant link that enables the operation of the network in an open mode. If an appliance truly malfunctions, administrators can have the configuration files back in another appliance with USB instant recovery. By simply plugging in a USB drive to the USB port, configuration files will be imported automatically in a few minutes.

Support 3G / 4G USB

With a USB dongle, a maximum of 3 WAN links can be configured. A secure 3G/4G backup connection and uninterrupted WAN connectivity can be added to industrial firewalls.

Central Management (CMS and Eye Cloud)

Central management system (CMS) designed for multi-site network security appliances deployments allows administrators to remotely restart, reboot, and monitor devices. Moreover, Eye Cloud, a cloud service platform, provides users friendly interface to support instant equipment maintenance and management.



Features

Interfaces

- GE RJ45 Ports: 6
- RS-232 Com Port: 2
- VGA Port: 1
- USB3.0 Port: 2
- Bypass: 1 pair

Performance

- Firewall Throughput: 1.8 Gbps
- VPN Throughput: 200 Mbps (IPsec AES)
- OPC Throughput: 480Mbps
- Anti-Virus Throughput: 350Mbps
- Max. Sessions: 200,000
- Supported Protocols: Modbus, DNP3, IEC-104, EtherNet/IP, LanWorks, IEC-61850, BACNet, AXView2.0

Mount

- Din Rail and Wall mount

Height x Width x Length

- 126 x 74.5 x 146 (mm)

Power Consumption

- 2-Pin Terminal Block +9~36VDC

Operating Environment

- Operating Temperature: -40-75°C
- Operating Humidity: 10%-80%