EdgeFirewall Datasheet

Aiming to create better and safer working environments and life experiences through the products we deliver.

AVCOMM Technologies, Inc

www.avcomm.us

Email: info@avcomm.us

Phone: (713) 933-4534

Address: 333 West Loop North, Suite 460
Houston, TX 77024
United States

EdgeFirewall

Product overview

Avcomm Industrial Firewall is a boundary isolation and Cybersecurity protection product designed and developed for the industrial control system environment. The product is based on the hardware architecture of the industrial-grade ARM multi-core processor chip and the intelligent industrial control Cybersecurity operating system (NS OS) with independent intellectual property rights, based on optimized The software and hardware architecture improves the processing capacity of packets, performs deep packet inspection (DPI, Deep Packet Inspection) of mainstream industrial protocols, and uses "whitelist + intelligent learning" technology to establish data acquisition communication and industrial control network inter-regional communication models to ensure that only Trusted traffic can be transmitted on the network to provide Cybersecurity guarantee for the interconnection between the industrial control network and the external network, and the network connection between the internal area of the industrial control network.

Product features

Accurate industrial protocol analysis and identification capabilities

Through the self-developed deep packet analysis engine, Avcomm industrial firewall can detect more than 100 industrial protocols, and can detect OPC, Modbus, IEC 60870-5-104, IEC 61850 MMS, Siemens S7, Ethernet/IP (CIP), Profinet, Fins and other mainstream industrial control protocols do in-depth message analysis to identify the effective content characteristics, payload and available matching information in the message, such as malware, specific instructions and application types, and achieve real-time analysis and accurate analysis of the industrial control protocol features Recognition.

Fine-grained instruction-level access control

Based on the precise identification capabilities of industrial protocols, industrial firewalls can not only implement traditional access control strategies based on multiple dimensions such as Cybersecurity domains, IP, MAC, time periods, services, and execution actions, but also support more than ten mainstream industrial control protocols such as OPC and Modbus TCP. It supports more than 1000 kinds of function code recognition and can achieve more fine control granularity at the instruction level or even the range level.

Industrial-grade hardware platform with high reliability and low latency

Avcomm industrial firewall adopts high-performance industrial-grade ARM multi-core processor chip and deep packet parsing engine, which combines software and hardware to provide high throughput and low latency processing capabilities. With deep packet inspection (DPI) enabled, the device is fully equipped with a strategy The delay is not higher than 200us. The hardware platform design of the product follows the industrial control industry standards, adopts a fan-less design, redundant key components, software and hardware support bypass, and the hardware platform achieves industrial level 3 or above B quality, and the minimum power consumption of the whole machine is only 7W, which can meet the low power consumption in an industrial environment. It meets the requirements of power consumption, wide temperature, dust-proof, moisture-proof and high reliability, and supports multiple installation methods such as rail-mounted, wall-mounted, and cabinet installation.

Tel: 713-933-4534 **Web: www.avcomm.us** **Email: info@avcomm.us**

Specifications

Industrial Protocol depth analysis

- 100+ general protocol and industrial protocol identification
- Support mainstream industrial control protocols such as OPC, Modbus, IEC 60870-5-104, IEC 61850 MMS, Siemens S7, etc.
- Support more than 1000 protocol function code recognition
- Support the customization of industrial control protocol analysis without secondary development

OPC protocol analysis

- Support OPC dynamic port recognition
- Support OPC DA, XML-DA operation, support OPC read-only
- Support OPC range control
- Support the OPC 3.0 specification issued by the OPC Foundation;

Modbus TCP protocol analysis

- Support Modbus TCP protocol syntax check, Reset and connection tracking, etc.
- Support Modbus TCP CP protocol whitelist, support read and write operations, point table, value field control

Security strategy

- Based on the division of Cybersecurity domains, support Cybersecurity policies based on Cybersecurity domains
- Support access control rules based on source IP, source MAC, destination IP, destination MAC, protocol (TCP/IP)
- Support access control strategy of industrial protocol whitelist
- Support self-learning to create whitelist rules, and the learning time can be adjusted
- Support IP/MAC address binding rules
- Support ACL time period control, ACL compilation, fast ACL search

Routing function

- Support static routing function, 1000 routing tables
- Configuration supports 8 IP addresses/interfaces
- Support ARP proxy

Deployment mode

- Transparent mode, routing mode

IP/MAC address binding

- Intelligent auxiliary generation of learning rules
- Support binding rule import and export

Ethernet/IP(CIP) protocol analysis

- Support Ethernet/IP (CIP) protocol syntax check and packet loss Reset, support Ethernet/IP (CIP) protocol self-defined parameter configuration
- Support CIP data sheet, PCCC control.

Log management

- Support access policy log, whitelist log, blacklist log
- Support proprietary tools to view, retrieve, backup, and audit logs
- Support log backup
- Supports statistics log in the form of histogram

Unified management

- Only trusted hosts that pass IP authentication and IP+MAC binding can access the current device system
- Support mandatory password strength
- Support decentralized and hierarchical management
- Support report function, users can view event, log and audit statistical data through the report, support report download
- Support automatic upgrade of Cybersecurity products
- Support the policy configuration and delivery of Cybersecurity devices

Topology management

- Support editing and displaying system topology
- Support automatic discovery of firewall devices
- Support firewall device status display

Unknown device detection

- Support rapid detection of unknown device detection

Operating mode

- Learning mode, warning mode, protection mode

Siemens S7 protocol analysis

- Support distinguishing and controlling Siemens S7 read and write operations
- Support Siemens S7 version number, register area, DB area code, point type, value range, transmission layer protocol field control

Real time monitoring

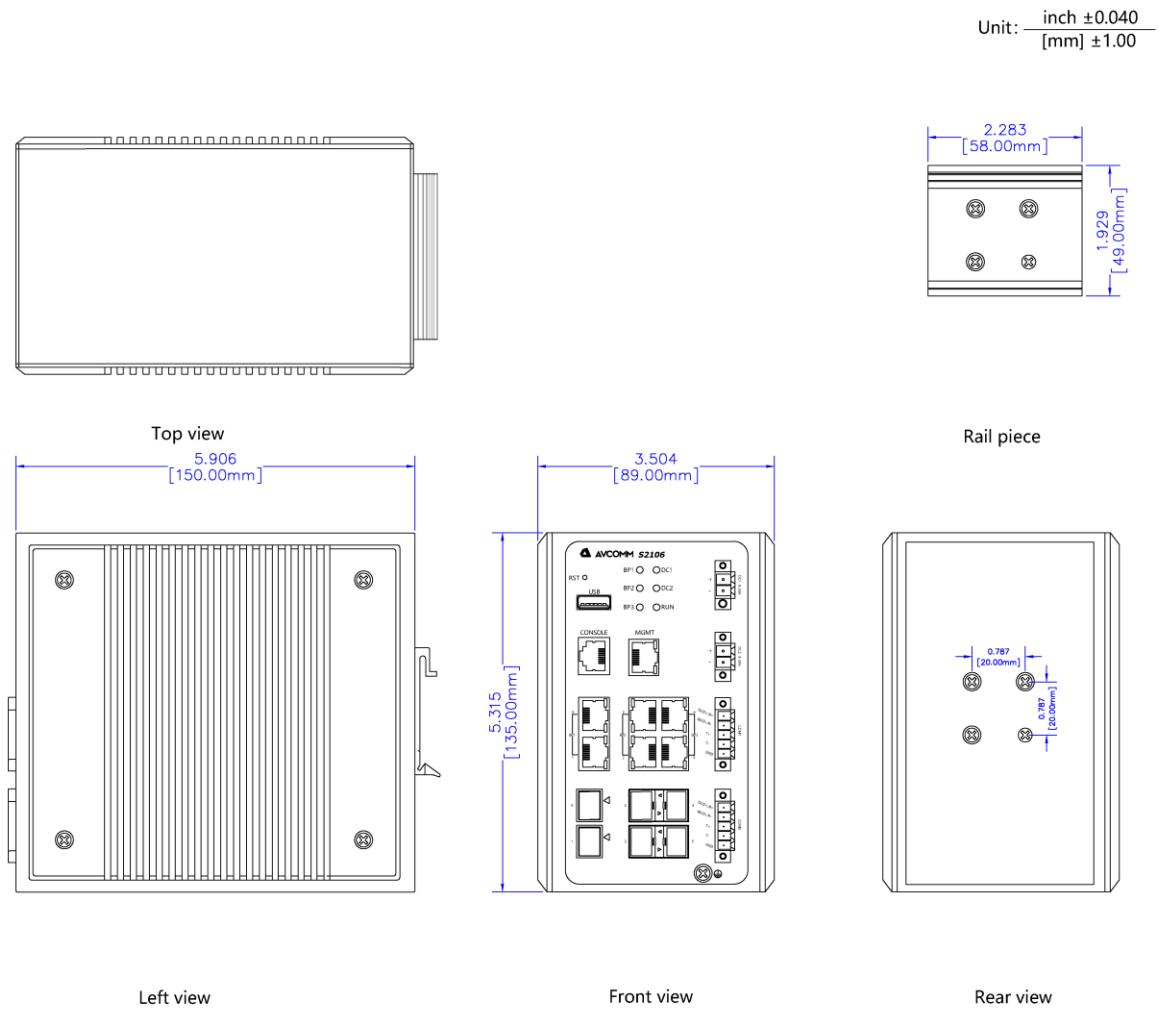
- Support real-time monitoring of equipment status
- Support real-time monitoring of alarm events, and support event export function
- Support log monitoring function

Hardware Index

Index item	S2106	S2112	S2124
Business port	6 gigabit Combo port	8 gigabit ports + 4 gigabit Combo port	16 gigabit ports + 6 gigabit Combo port + 2 10-gigabit SFP+ port
Bypass	3 RJ45 interface	6 RJ45 interface	11 RJ45 interface
Out-of-band management port	1 10/100/1000M adaptive RJ45 port	1 10/100/1000M adaptive RJ45 port	1 10/100/1000M adaptive RJ45 port
Console port	1 RS232 to RJ45 interface	1 RS232 to RJ45 interface	1 RS232 to RJ45 interface
HA port	/	1 10/100/1000M adaptive RJ45 port	1 10/100/1000M adaptive RJ45 port
Serial interface	2 RS485/422/232 Three in one serial port	2 RS485/422/232 Three in one serial port	2 个 RS485/422/232 Three in one serial port
USB interface	1 USB 2.0	1 USB 3.0	1 USB 3.0
Working environment	Temperature: -40 ~ 75℃ Humidity: 5%-95%, no condensation	Temperature: -10 ~ 60℃ Humidity: 5%-95% without condensation	Temperature: -10 ~ 60℃ Humidity: 5%-95% without condensation
Storage environment	Temperature: -40 ~ 85℃ Humidity: 5%-95% without condensation	Temperature: -40 ~ 85℃ Humidity: 5%-95% without condensation	Temperature: -40 ~ 85℃ Humidity: 5%-95% without condensation
MTBF	>250000 hours	>250000 hours	>250000 hours
Power	9-36VDC，Redundant power supply	100-240V AC，Redundant power supply	100-240V AC，Redundant power supply
Highest power	Typical power consumption 14.5W, Max 25W	Typical power consumption 26W, Max 46W	Typical power consumption 29W, Max 50W
Dimensions (width * depth * height)	89x150x135mm	440*400*44mm	440*400*44mm
Installation method	35mm Standard DIN rail snap connection	Standard rack mounting	Standard rack mounting

Installation dimensions

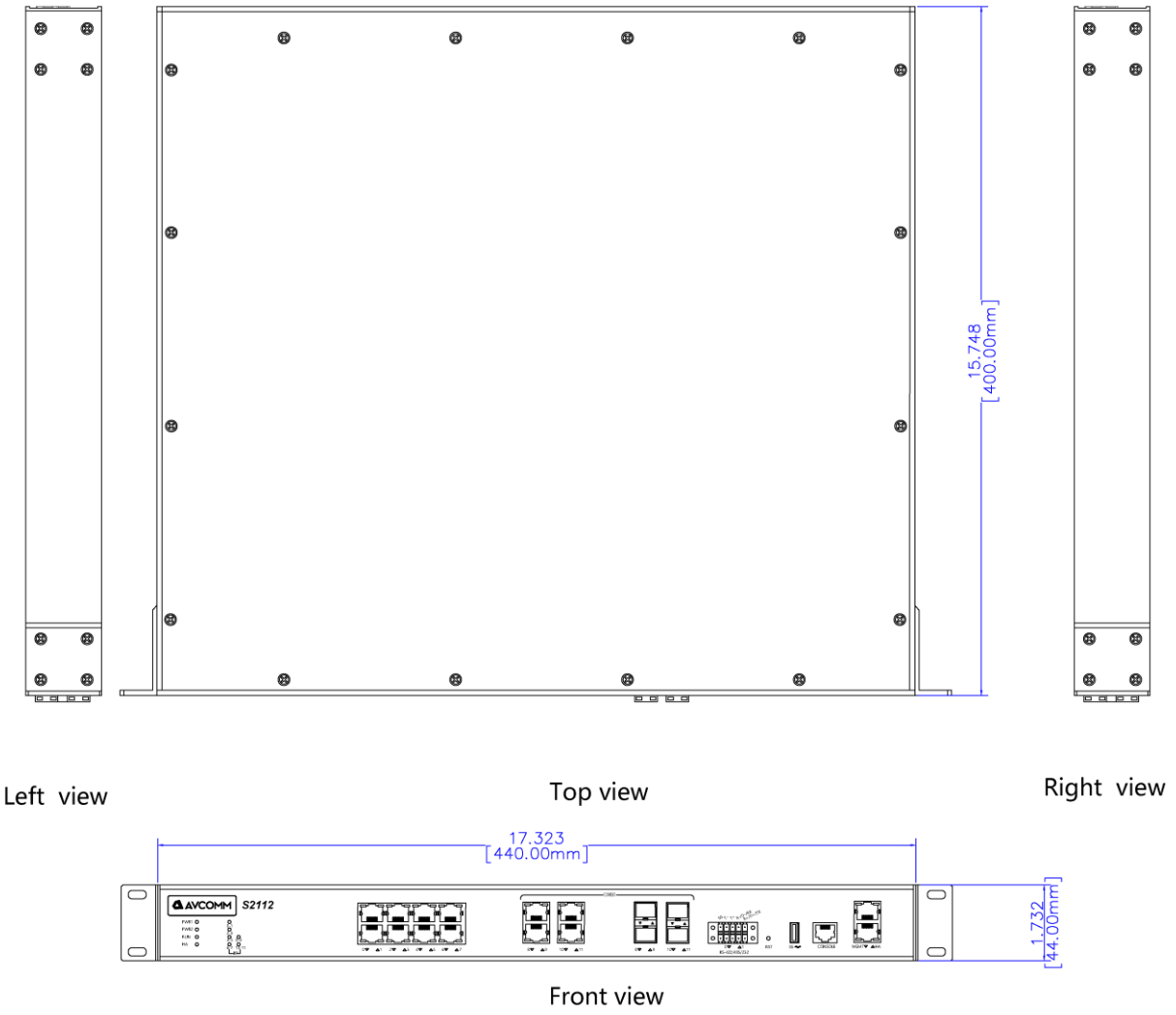
S2106



Installation dimensions

S2112

Unit: inch ±0.040 / [mm] ±1.00



Left view

Top view

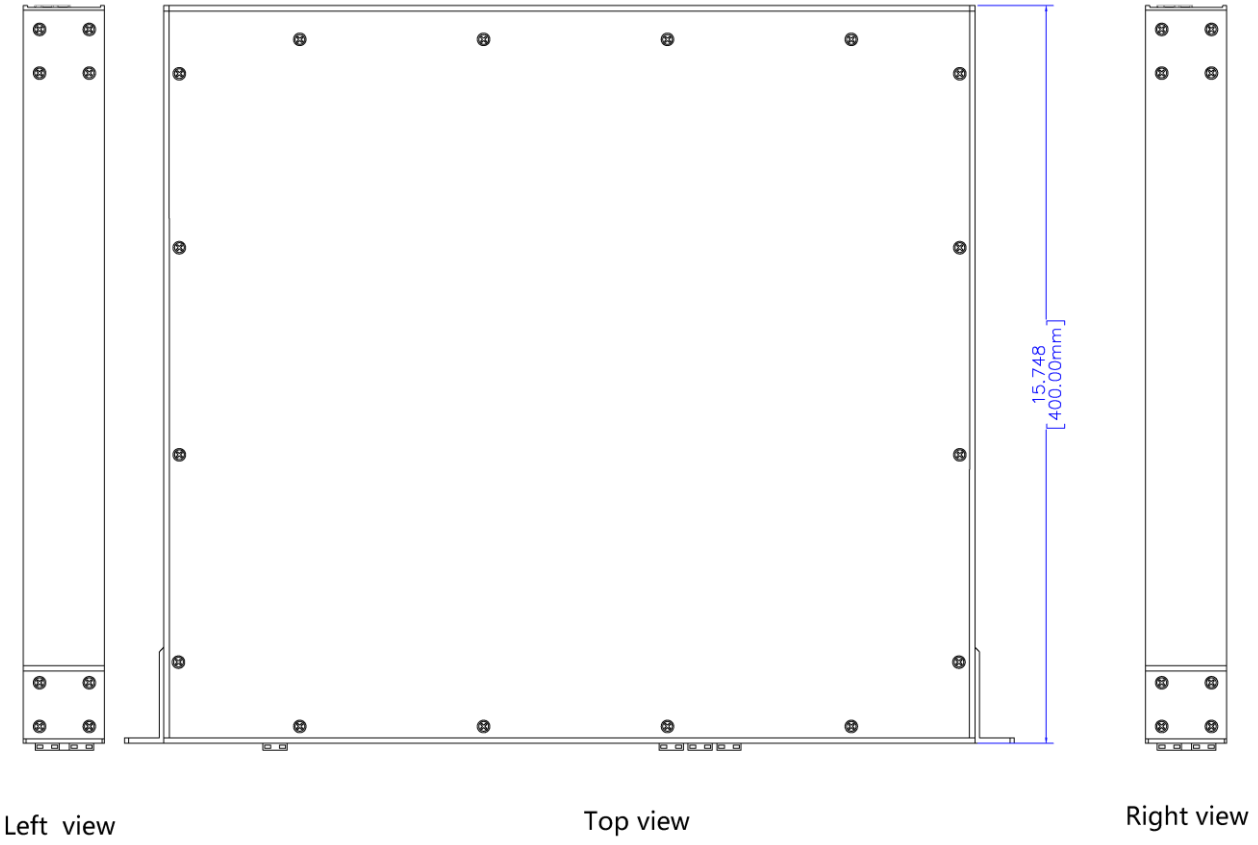
Right view

Front view

Installation dimensions

S2124

Unit: inch ±0.040 [mm] ±1.00



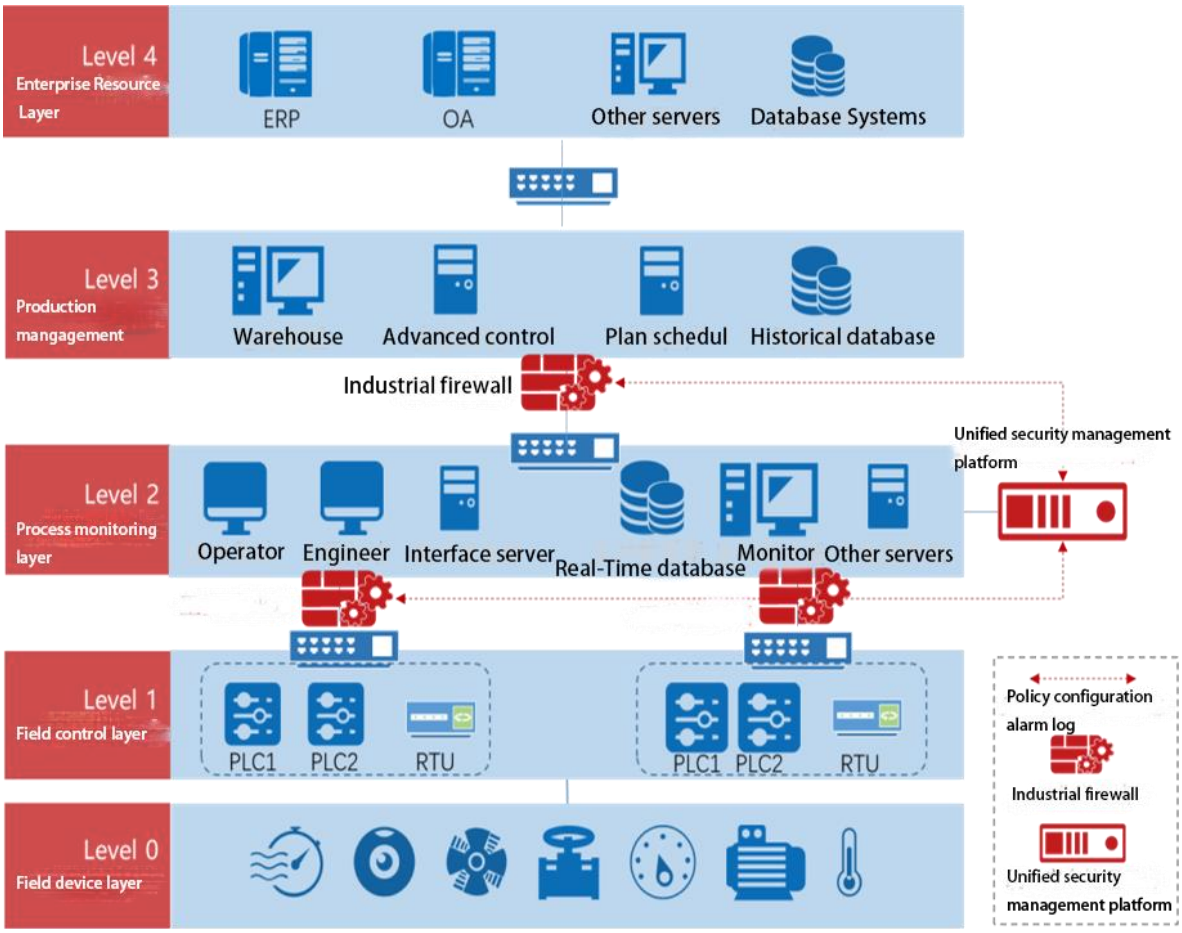
Left view

Top view

Right view

Front view

Application Scenarios



Process monitoring layer device access control

- It is deployed in series between the production execution layer and the process monitoring layer
- Session state detection and packet filtering detection mechanisms are adopted to limit unauthorized access to the process monitoring layer
- Automatically learning the communication relationship between networks, modeling normal communication behavior, abnormal communication behavior will be intercepted
- Establish the device whitelist baseline, real-time detection of device access behavior, the discovery of unknown device access will generate alarm

Field control layer equipment command level protection

- It is deployed in series between the process monitoring layer and the field control layer
- Based on the deep analysis of industrial control protocol, it can intercept and warn illegal operation instructions
- Based on the communication records of industrial control protocol, it automatically learns the business communication logic relationship, operation function code and parameters, etc., and forms the normal communication behavior model
- Packet filtering log, industrial protocol filtering log and other Cybersecurity event logs are recorded and reported to the unified Cybersecurity management platform