



工业防火墙 Datasheet

恩创致力于将先进的信息技术带入工业控制与工业信息领域。



安通恩创信息技术（北京）有限公司

www.avcomm.cn

电子邮箱: sales@n-tron.com.cn

电话: (010) - 82859971

地址: 北京市海淀区马甸东路19号金澳国际公寓3105

产品概述

恩创工业防火墙是针对工业控制系统环境设计开发的边界隔离和安全防护产品，产品基于工业级ARM多核处理器芯片的硬件架构和自主知识产权的智能工控安全操作系统（NS OS），基于优化的软硬件架构提高报文的处理能力，对主流工业协议进行深度报文解析（DPI, Deep Packet Inspection），运用“白名单+智能学习”技术建立数采通信及工控网络区域间通信模型，保证只有可信任的流量可以在网络上传输，为工控网络与外部网络互联、工控网络内部区域之间的网络连接提供安全保障。

产品特点

精准的工业协议分析识别能力

通过自主研发的深度数据包解析引擎，恩创工业防火墙能够检测出100多种工业协议，能够对 OPC、Modbus、IEC 60870-5-104、IEC 61850 MMS、Siemens S7、Ethernet/IP (CIP)、Profinet、Fins等主流工控协议做深度报文解析，识别报文中的有效内容特征、负载和可用匹配信息，如恶意软件、具体指令和应用程序类型，对工控协议特征做到实时解析和精准的识别。

细粒度指令级访问控制

基于工业协议的精准识别能力，工业防火墙不仅可以实现传统基于安全域、IP、MAC、时间段、服务、执行动作等多个维度的访问控制策略，对OPC、Modbus TCP等十余种主流工控协议支持超过1000种的功能码识别，可以做到指令级甚至值域级更精细控制粒度。

高可靠低时延的工业级硬件平台

恩创工业防火墙采用高性能工业级ARM多核处理器芯片和深度数据包解析引擎，软硬结合来提供高吞吐低时延的处理能力，开启深度报文检测（DPI）的情况下设备满配策略时延不高于200us。产品的硬件平台设计遵循工控行业标准，采用无风扇设计，关键部件冗余，软硬件支持bypass，硬件平台达到工业三级B以上品质，整机功耗最小仅7W，能够满足工业环境下低功耗、宽温、防尘、防潮及高可靠的使用要求，支持导轨式安装、壁挂式、机柜安装等多种安装方式。

功能规格

工业协议深度解析

- 100+通用协议和工业协议识别
- 支持OPC、Modbus、IEC 60870-5-104、IEC 61850 MMS、Siemens S7等主流工控协议
- 支持1000多种协议功能码识别
- 支持工控协议解析的自定义，无需二次开发

OPC协议解析

- 支持OPC动态端口识别
- 支持OPC DA, XML-DA操作, 支持OPC只读
- 支持OPC值域控制
- 支持OPC基金会发布的OPC 3.0规范;

ModBus TCP协议解析

- 支持Modbus TCP协议语法检查、Reset及连接跟踪等
- 支持Modbus TCP CP协议白名单, 支持读写操作、点表, 值域字段控制

Siemens S7协议解析

- 支持区分Siemens S7读写操作并加以控制
- 支持Siemens S7版本号、寄存器区、DB区区号、点类型、值范围、传输层协议字段控制

安全策略

- 基于划分安全域, 支持基于安全域的安全策略
- 支持基于源IP, 源MAC, 目的IP, 目的MAC, 协议 (TCP/IP) 访问控制规则
- 支持工业协议白名单的访问控制策略
- 支持自学习创建白名单规则, 学习时间可调节
- 支持IP/MAC地址绑定规则
- 支持ACL时间段控制、ACL编译, 快速ACL查找

路由功能

- 支持静态路由功能, 路由表条数1000条
- 配置支持8个IP地址/接口
- 支持ARP代理

IP/MAC地址绑定

- 智能辅助生成学习规则
- 支持绑定规则导入导出

部署模式

- 透明模式、路由模式

Ethernet/IP(CIP)协议解析

- 支持Ethernet/IP(CIP)协议语法检查及丢包 Reset, 支持Ethernet/IP(CIP)协议本身自定义的参数配置
- 支持CIP数据表、PCCC控制

日志管理

- 支持访问策略日志、白名单日志、黑名单日志
- 支持专有工具查看、检索、备份、审计日志
- 支持日志备份
- 支持直方图形式统计日志

未知设备检测

- 支持快速检测未知设备的检测

工作模式

- 学习模式、告警模式、防护模式

拓扑管理

- 支持编辑、显示系统拓扑
- 支持防火墙设备自动发现
- 支持防火墙设备状态显示

统一管理

- 通过IP认证、IP + MAC绑定的可信主机才能访问 目前设备系统
- 支持强制口令强度
- 支持分权分级管理
- 支持报表功能, 用户通过报表可查看事件、日志 和审计的统计数据, 支持报表下载
- 支持安全产品的自动升级
- 支持安全设备的策略配置和下发

自管理

- 自管理防火墙不需要搭配统一安全管理平台使用
- 支持和管理平台相同的功能配置

实时监控

- 支持设备状态实时监控
- 支持告警事件实时监控, 并支持事件导出功能
- 支持日志监控功能

硬件指标

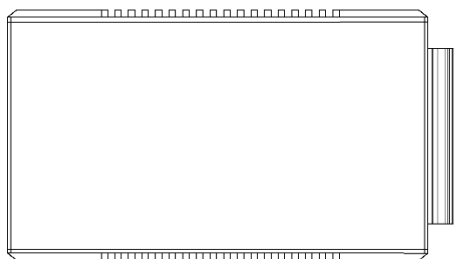


指标项	S2106	S2112	S2124
业务端口	6 个千兆光电互斥接口	8 个千兆电口+4 个千兆光电互斥接口	16 个千兆电口+6 个千兆光电互斥接口+2 个万兆 SFP+接口
Bypass	3 组 RJ45 接口	6 组 RJ45 接口	11 组 RJ45 接口
带外管理口	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口
console 口	1 个 RS232 转 RJ45 接口	1 个 RS232 转 RJ45 接口	1 个 RS232 转 RJ45 接口
HA 接口	/	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口
串行接口	2 个 RS485/422/232 三合一串口	2 个 RS485/422/232 三合一串口	2 个 RS485/422/232 三合一串口
USB 接口	1 端口 USB 3.0	1 端口 USB 3.0	1 端口 USB 3.0
工作环境	温度：-40~75℃ 湿度：5%-95% 无凝结	温度：-10~60℃ 湿度：5%-95% 无凝结	温度：-10~60℃ 湿度：5%-95% 无凝结
存储环境	温度：-40~85℃ 湿度：5%-95% 无凝结	温度：-40~85℃ 湿度：5%-95% 无凝结	温度：-40~85℃ 湿度：5%-95% 无凝结
MTBF	25 万小时	25 万小时	25 万小时
电源	9-36V DC, 冗余供电	100-240V AC, 冗余电源	100-240V AC, 冗余电源
最高功率	典型功耗14.5W, 最大功耗25W	典型功耗26W, 最大功耗46W	典型功耗29W, 最大功耗50W
尺寸 (宽*深*高)	89x150x135mm	440*400*44mm	440*400*44mm
安装方式	35mm DIN 导轨卡接安装 壁挂式安装	标准机架式安装	标准机架式安装

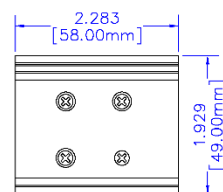
安装尺寸

S2106

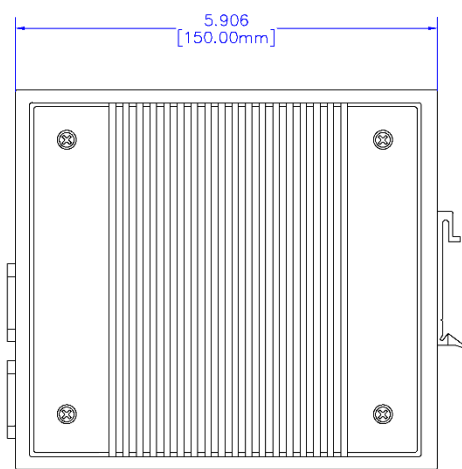
单位: $\frac{\text{inch} \pm 0.040}{[\text{mm}] \pm 1.00}$



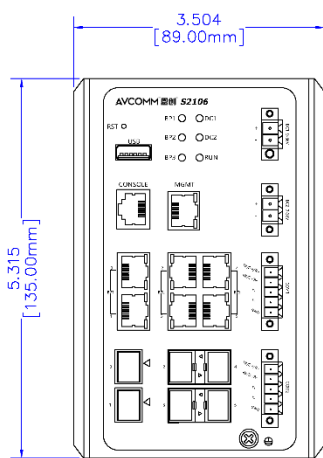
顶视图



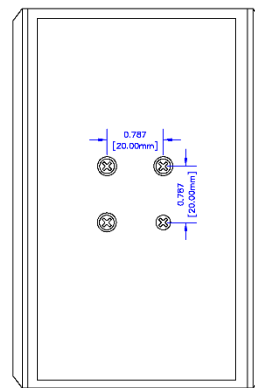
导轨片



左视图



前视图

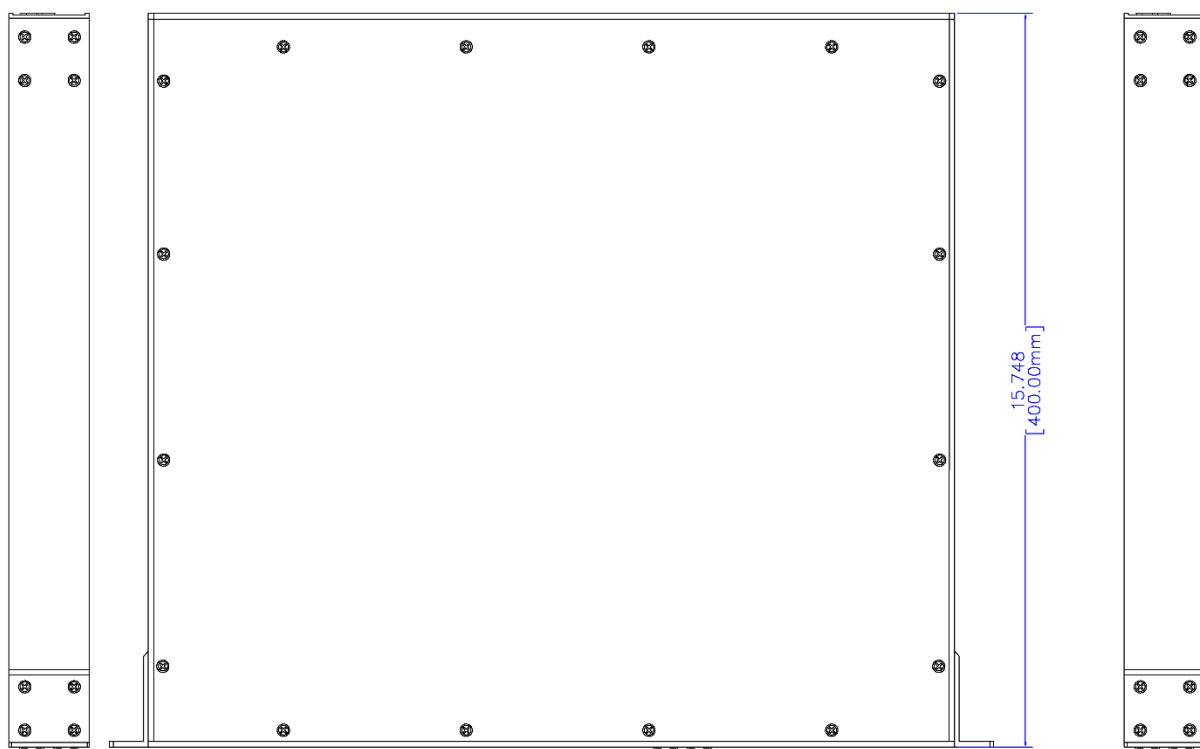


后视图

安装尺寸

S2112

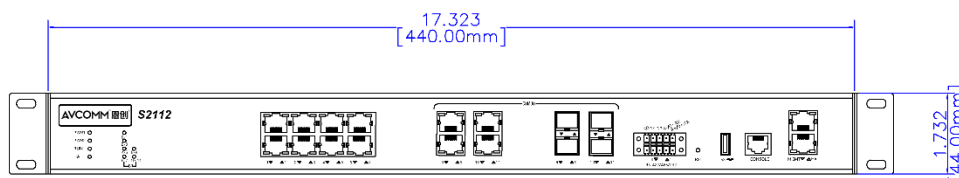
单位: $\frac{\text{inch} \pm 0.040}{[\text{mm}] \pm 1.00}$



左视图

俯视图

右视图

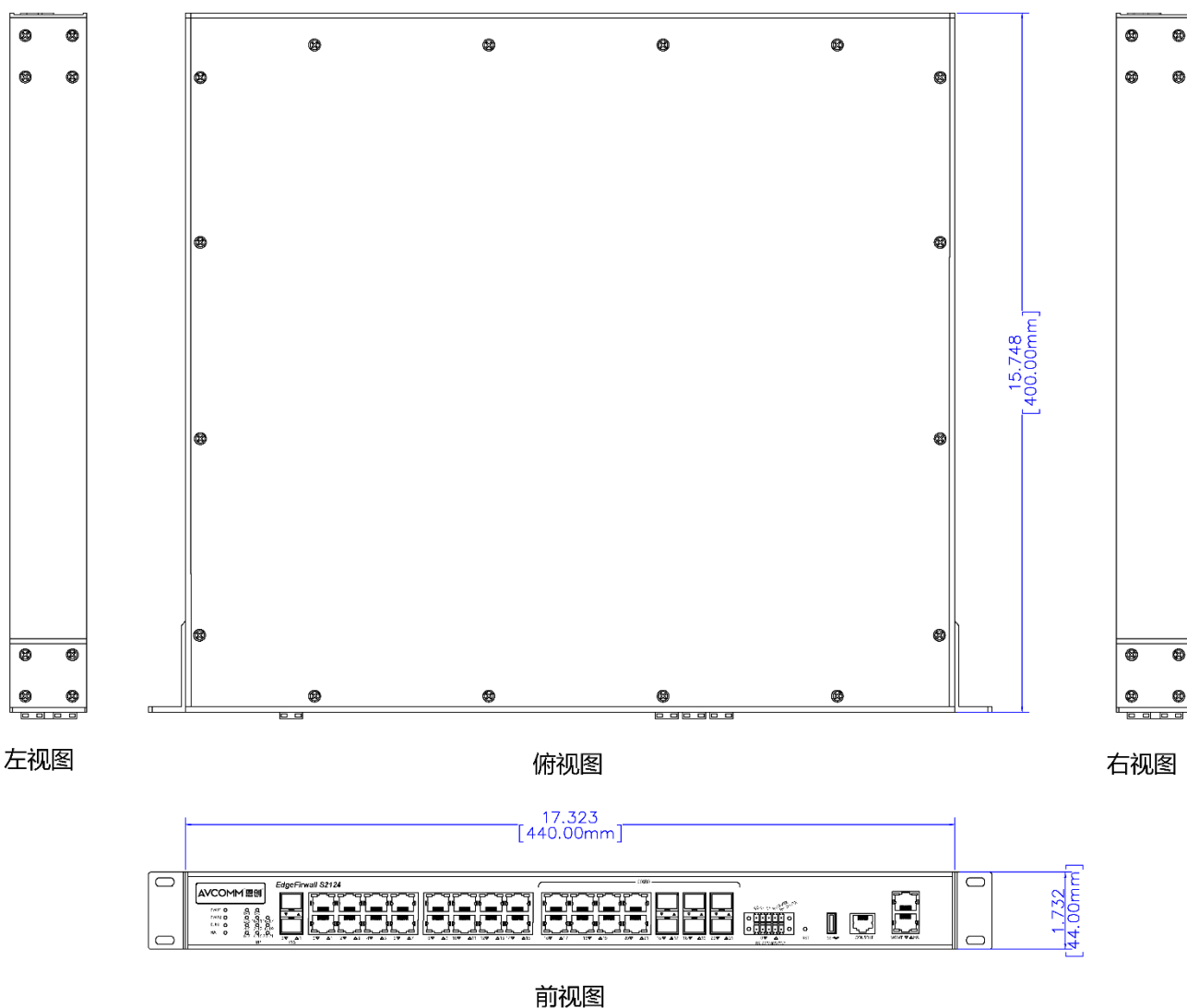


前视图

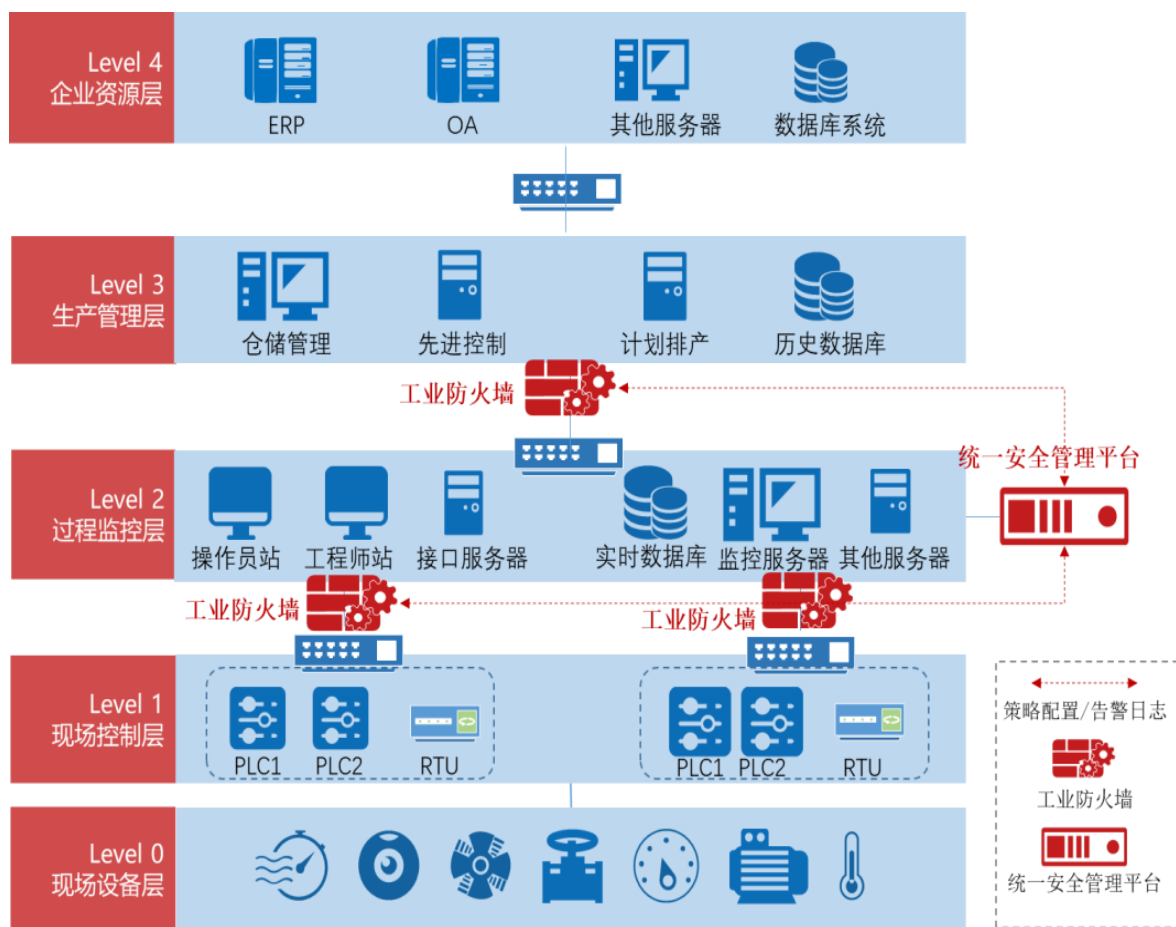
安装尺寸

S2124

单位: $\frac{\text{inch} \pm 0.040}{[\text{mm}] \pm 1.00}$



应用场景



过程监控层设备访问控制

- 以串联方式部署在生产执行层与过程监控层之间
- 采用会话状态检测、包过滤检测机制，限制对过程监控层的非授权访问行为
- 自动学习网络间通信关系，对正常通信行为建模，异常通信行为将被拦截
- 建立设备白名单基线，对设备接入行为实时检测，发现未知设备接入即产生告警

现场控制层设备指令级防护

- 以串联方式部署在过程监控层与现场控制层之间
- 基于工业控制协议的深度解析，实现对非法操作指令的拦截和告警
- 基于工业控制协议通信记录，自动学习业务通信逻辑关系、操作功能码和参数等，形成正常通信行为模型
- 对包过滤日志、工业协议过滤日志等安全事件日志进行记录，并上报至统一安全管理平台