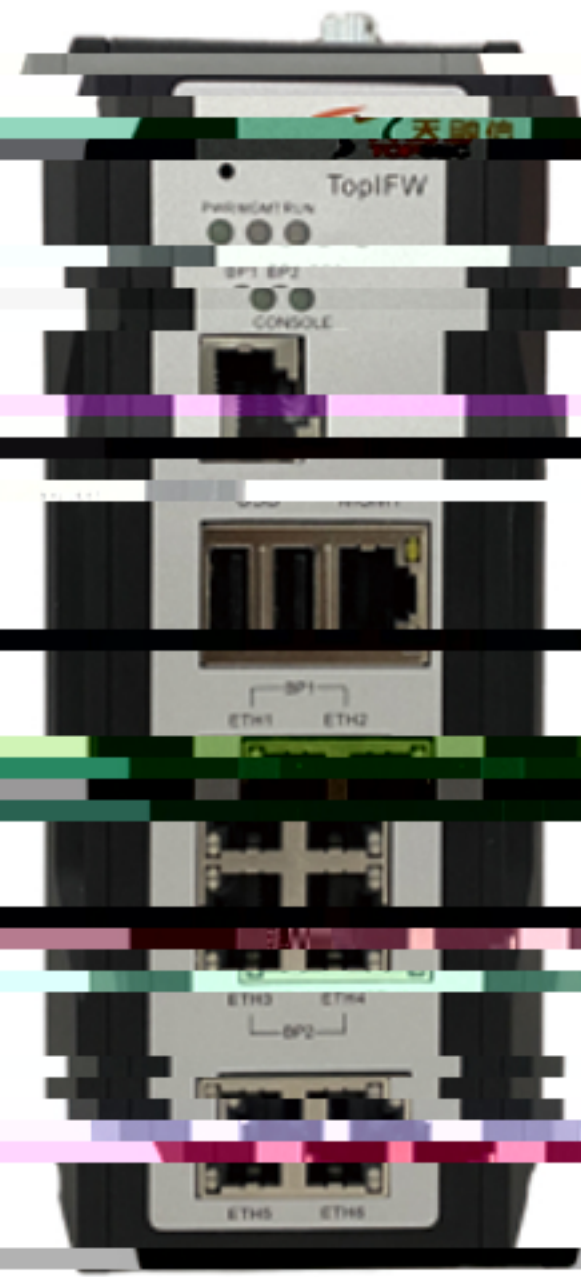


# 天融信工控防火墙系统TopFW(工控系列)

## 产品概述

天融信工控防火墙系统(TopFW)是面向工业互联网领域的安全防护类产品,主要应用于工业控制系统的网络边界、区域边界与重要设备前端的安全防护。系统采用独有的工业协议指令级“四维一体”深度防护技术,支持OPCDA、OPCUA、Modbus、S7、IEC104、DNP3、EIP、MMS、Proficnet、BACNET、FIN5等多种主流工业协议深度解析与指令级防护,并具备入侵防御、防病毒、IPV6、虚拟专网、负载均衡、流量管控、DOS攻击防护、ARP攻击防护等安全功能,可有效保障工控业务和系统自身双重安全。产品基于工业级安全硬件平台研发,具备低功耗、宽温、工业级接口、工业级接口、工业级接口等安全特性,适用于SCADA、DCS、PCS、PLC等工业监控系统以及现场控制设备安全防护,广泛应用于轨道交通、电力、冶金、煤炭、石油化工、市政、汽车、烟草、智能制造、核电军工等行业。



## 产品特点

### 深层次业务防护机制

天融信凭借在工控领域的技术积累,设计研发基于白名单的工业指令级“四维一体”深度防护技术,对工控协议的“完整性”、“功能码”、“地址范围”和“工艺参数范围”进行深度过滤和防护,及时发现可疑指令和恶意数据,从访问控制、业务行为、业务数据、业务认证工控网络和控制设备的安全运行。

### 全方位威胁感知能力

内置专业的工控攻击特征库,覆盖超过90%以上针对工业控制的入侵攻击和恶意代码感染等安全威胁,精准定位基于SCADA、PLC、DCS等工控业务场景的入侵攻击、恶意代码感染、病毒木马感染、拒绝服务攻击等安全威胁,及时发现并阻断攻击,防止安全威胁蔓延,保障工业控制系统稳定运行。

### 智能AI协议识别技术

内置智能AI协议识别引擎,支持30+工业协议的识别。采用单包特征识别、统计特征识别、多包特征识别、深度解析识别等多种识别技术对应用协议进行发现,能够全面满足工业企业用户对各类业务系统应用和协议的管控需求。

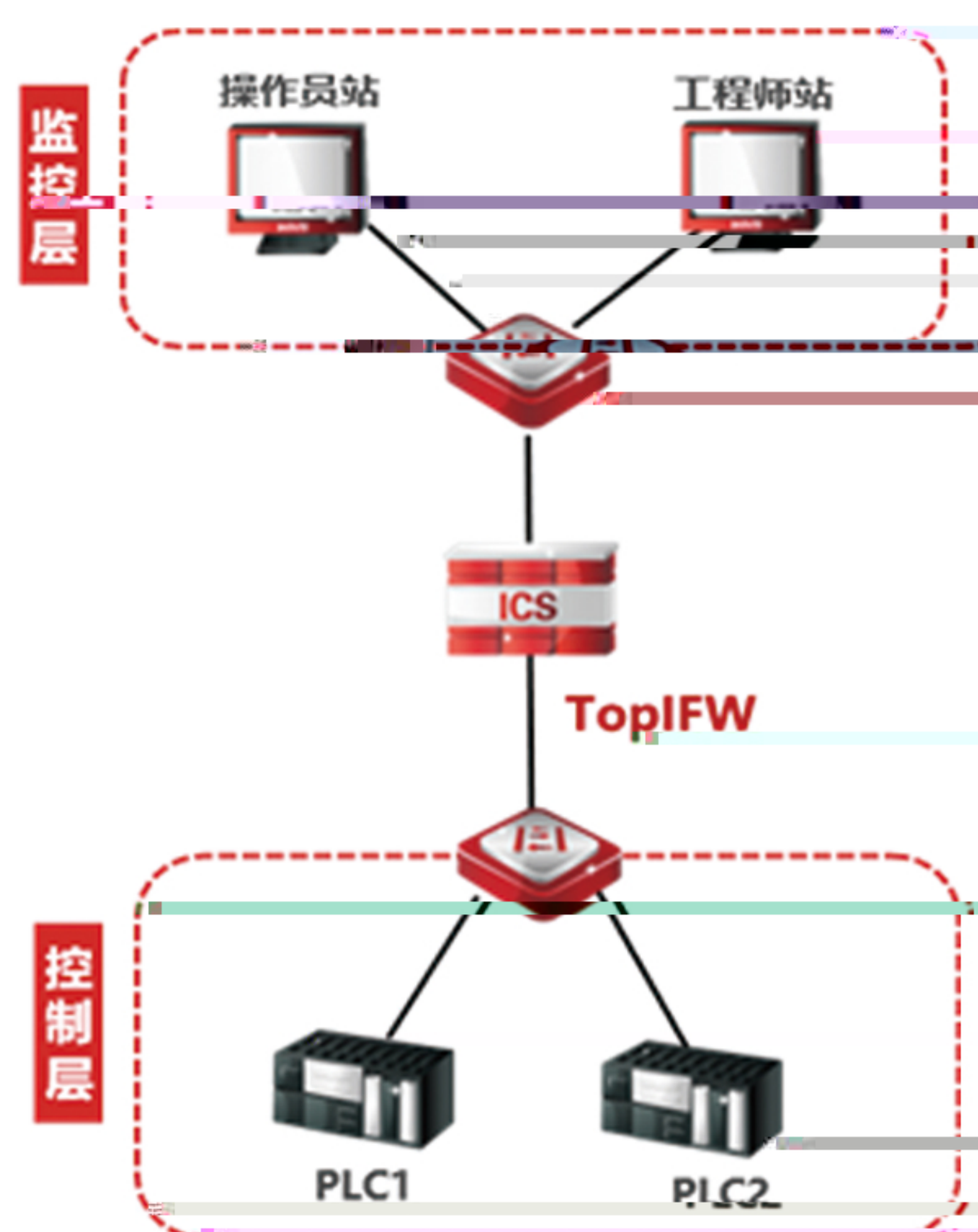
### 强大的网络适应能力

天融信根据新型工业互联网结构,基于通用网络功能,增加虚拟专网、IPV6、虚拟线、双机热备、链路聚合、负载均衡、流量管控等工业应用场景所需网络安全功能,适应日益复杂的工业互联网环境,降低用户其他方面的投资,满足工业互联网业务发展需求。

## 典型应用

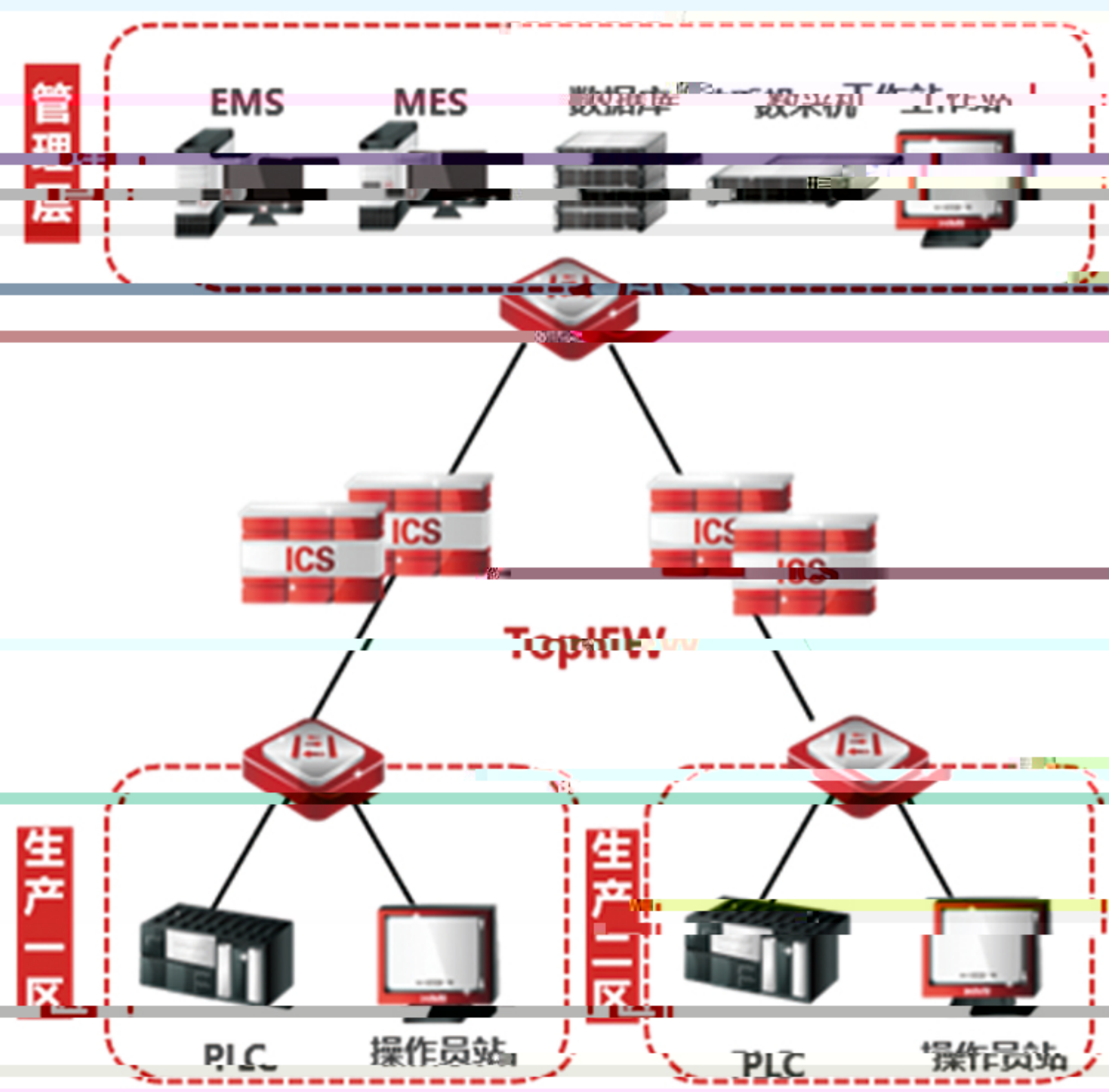
### 关键设备前端防护

TopIFW产品采用透明、路由或混合的工作方式，部署在逻辑控制设备前端，实现对关键设备的安全防护。通过基于网络层的防护策略，有效阻断非法主机与重要设备通信，结合工业协议深度控制策略，有效识别出非法指令与操作，避免因非法操作或误操作导致设备指令下发，保障控制装置或重要设备的安全。



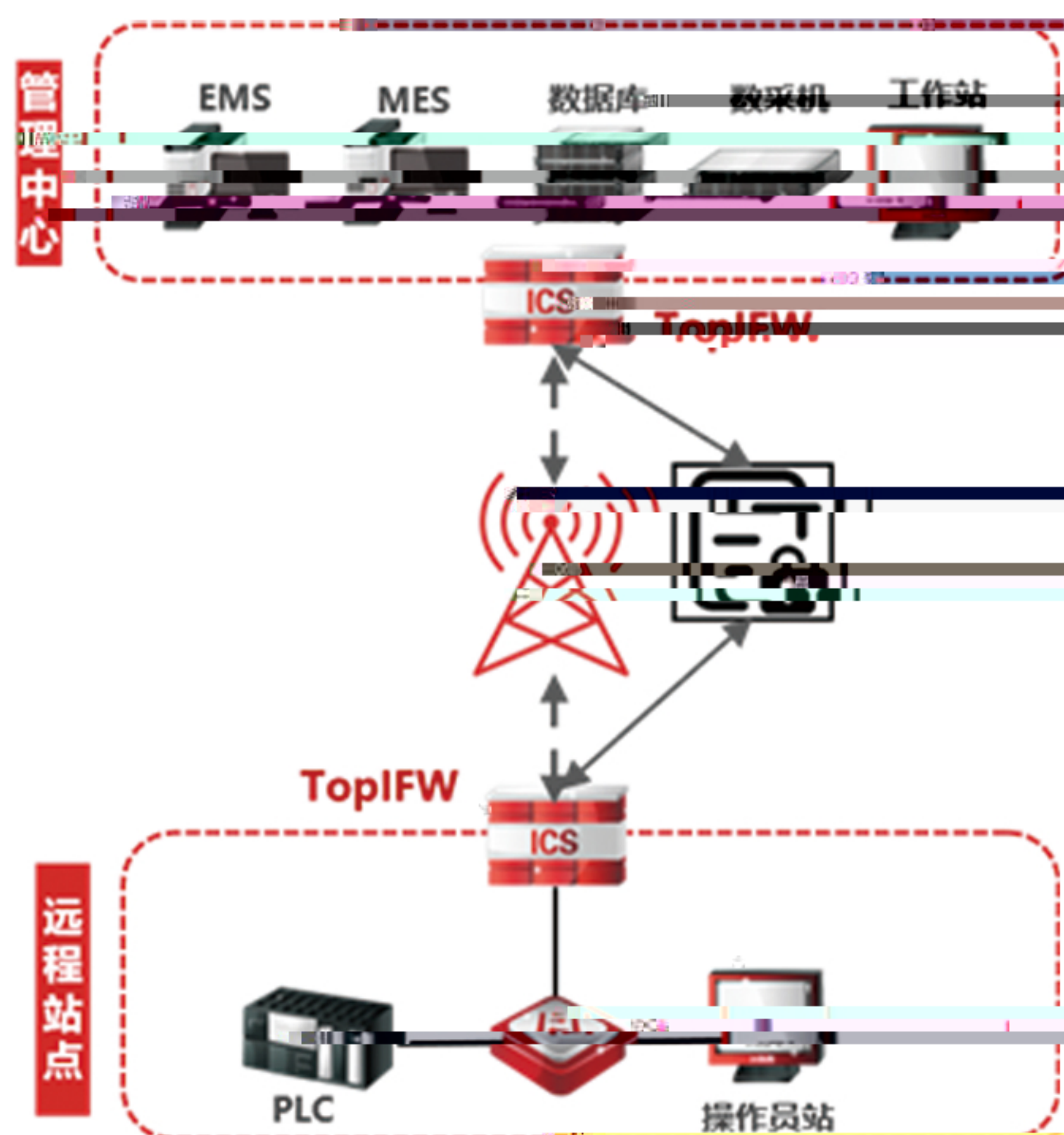
### 控制区域边界防护

TopIFW产品以透明、路由或混合的工作方式部署在逻辑控制区域的出口，实现不同逻辑控制区域之间的安全隔离。通过基于网络层的防护策略，有效阻断非法主机与重要设备通信，结合工业协议深度控制策略，有效识别出非法指令与操作，避免因非法操作或误操作导致设备指令下发，保障控制装置或重要设备的安全。同时，结合安全域之间的安全隔离策略，拒绝其他安全域的访问，同时支持多种攻击检测技术，可实现检测和抵御对过程监控网络的扫描或攻击，保障底层业务安全稳定。



### 远程站点安全防护

TopIFW产品支持IPSec VPN隧道接入技术，通过在远程站点区域部署工控防火墙设备，在两个VPN节点之间建立一个虚拟隧道通道。两个工控防火墙设备内部的工业网络，能够通过虚拟数据链路到达对方，基于特定的通信方之间在IP层通过加密与数据源验证等方式，来保证数据报文在网络上传输时的私有性、完整性、真实性和防重放，并可设置基于生产业务的安全防护策略，对交互的数据和指令信息进行细粒度安全管控，阻断外部入侵攻击威胁，保护工业数据的安全性。



### 生产区域边界防护

工控防火墙系统级TPA方式部署，其中一台处于业务处理状态，另一台处于备用状态，两台设备通过心跳线进行在线监测和数据同步，一旦业务设备出现故障或异常，备用设备将自动接管业务，从而保障生产业务的连续、可靠运行。

