中数国科工业防火墙系统

产品白皮书

（中数国科技术集团有限公司）

北京市朝阳区外馆斜街泰利明苑写字楼 A 座

热线：13660007444

网址：cdtc@cdtc.com.cn

■ **版权声明**

产品营销部

2023 年 02 月 16 日

变更记录

序号	版本	变更记录	修改人/日期	检查人/日期	审批人/日期

目录

一、 前言

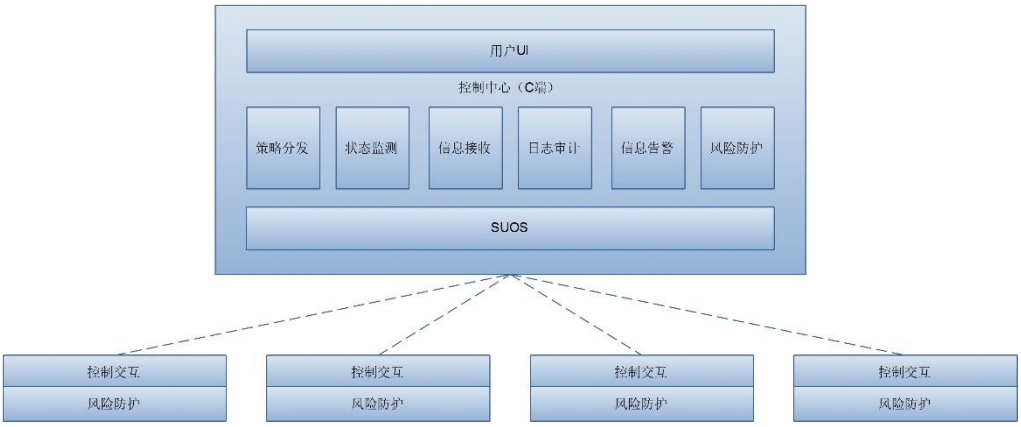
我国工控领域的安全可靠性问题不容忽视，工业控制系统的复杂化、信息化和通用化加速了系统的安全隐患，潜在的更大威胁是我国工业控制产业综合竞争力不强，嵌入式软件、总线协议、工控软件等核心技术受制于国外，缺乏自主的通信安全、信息安全、安全可靠性测试的标准。

同时 GB/T 22239-2019 信息安全技术网络安全等级保护基本要求中等级保护对象明确指出工业控制系统（ICS）内部应根据业务特点划分为不同的安全领域，安全域之间应采用隔离手段，通讯传输使用广域网进行控制指令或者相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输，与企业其他系统之间部署访问控制设备，配置访问控制策略。

二、 产品概述

面对市场现状和 GB/T 22239-2019 等级保护 2.0 要求，结合工业控制系统（ICS）防护痛点，中数国科集团有限公司推出中数国科工业防火墙系统。

针对工业控制系统的生产控制区（I 区）与生产监控区（II 区)之间的潜在安全风险，中数国科工业防火墙（简称：IAF）基于应用白名单策略、信令控制、参数控制、内容过滤、智能识别等技术手段，实现对生产控制区做整体的通信安全防护。



三、 产品功能

中数国科工业防火墙系统（以下简称 IAF）的核心功能是针对工业网络应用提供防护功能，主要体现在以下几个方面：

3.1 业务功能

3.1.1 工业协议深度识别

IAF 采用高性能的可扩充的协议分析算法，深度识别、解析大量工业专用协议，并可依据不同的业务场景、不同的协议类型，进行相应的深度控制参数。如典型的 Modbus 协议，管理员可轻松在界面上定制相应的信令控制规则，控制内容包括功能码、地址范围、线圈值域等。

3.1.2 业务保障

IAF 支持 BYPASS 模块，系统发生故障，IAF 会在 1 秒内启动 BYPASS 模式，保障业务运行的连续性。

3.1.3 Dos 攻击防护

IAF 具备 Dos 攻击防护功能，可以抵御多种 Dos 拒绝服务攻击，如 SYN Flood、TearDrop、Land 攻击、超大 ICMP 数据攻击、ICMP Flood 攻击、网络风暴限制等网络攻击，进而保障业务系统免受外部攻击。

3.1.4 状态监测

IAF 的监控中心实时显示当前设备状态以及通信状态。并根据网络情况智能分析当前应用通信的健康状态。如有异常，会及时产生报警。

3.1.5 日志审计

IAF 提供了丰富的日志类型和强大审计功能，如系统日志、管理日志、通信日志、

内容过滤日志、告警日志等。系统具备日志存储空间管理功能，当日志存储空间将满时，系统会产生告警。当日志存储空间已满时，系统会滚动删除最早的日志，以满足新产生日志的存储。

3.1.6 多工作模式

IAF 支持针对不同应用场景而采用不同的部署模式，有防护模式、告警模式和学习模式三种模式。

学习模式：针对工控现场环境开启学习模式后，IAF 会允许全部流量通过，IAF 会自动分析、智能学习其流量特征，并将特征提纯为安全策略，反应到策略库中。

防护模式：IAF 采用标准防护工作模式时严格按照安全策略进行安全防护，采用白名单工作模式，阻断异常指令、告警可疑操作、隔离威胁数据，保障工控系统可靠运行。

警告模式：开启告警模式后，IAF 会依据设定的安全策略对网络协议、数据进行安全检测，对异常流量、非法行为、恶意攻击等进行告警，但并不阻断。

3.1.7VPN 隧道

中数国科 IAF 工控防火墙具备 IPSEC VPN 功能，可提供虚拟专用网络，在打通内部控制网络的同时，对来往数据进行安全检测，保障网络安全。

同时，IAF 可以对工业协议做基于国密算法 SM2-SM4 的加密算法防护，具有稳定强、易用强、网络环境适应性强，性能高的特点，确保用户的生产、经营数据的机密、完整。

3.1.8 防护策略

中数国科 IAF 工控防火墙具备白名单防护策略、漏洞防护策略、ACL 防护策略、IP/MAC 防护策略、入侵防护策略。

3.2 管理功能

3.2.1 三权分立

系统管理功能按照最新的国家标准，系统具有相互独立、相互制约的系统管理员、安全保密管理员和安全审计员三个管理员角色。系统管理员主要负责生成用户身份标识符和系统运行维护；安全保密管理员主要负责用户权限设置、访问控制策略设置，以及系统运行日志、用户和安全审计员操作日志的审查分析；安全审计员主要负责系统管理员和安全保密管理员操作日志的审查分析。

3.2.2 带外管理

IAF 采用带外管理。保证管理通信与业务通信互不干扰。

3.2.3 策略管理

系统预置部分常用的策略模板，管理员只需要修改相应的 IP、MAC 等信息即可适应自身的网络安全需求。此外系统支持各个工控协议通信模块的深度定制功能，比如允许读取状态，不允许设置参数等功能。

3.2.4 备份恢复

系统支持策略的导出备份与导入恢复，支持策略自动备份到远端 FTP 服务器。

3.2.5 带内管理

系统业务口可作为管理口对 IAF 进行管理，针对现场网络设备较少，无法为管理口提供接口的情况。

四、 产品亮点

4.1 工业协议指令级控制

IAF 搭载自主研发的数据包深度解析引擎，对工控协议（OPC DA/UA、Modbus、IEC 60870-5-104、IEC 61850 MMS、DNP3、S7 等）进行深度解析，做到实时、精准的指令识别与控制。

4.2 高安全性的操作系统

系统基于中数国科自研的安全操作系统运行，所有的运行库以及组件全部定制化，去除了非本系统所需的多余功能。系统对通信内容进行完全控制，只允许策略里明确允许的协议行为，除此之外的行为一律丢弃，并通过控制中心给予提示或告警。

4.3 高便利性的产品应用

IAF 产品用全透明的即插即用模式接入，在系统接入后会自动到控制中心进行注册，并通过控制中心获得防护策略后执行防护工作。为管理员省去了大量的现场部署和配置时间。系统内置的典型策略防护模板也为管理员提供了更简便的防护策略定制功能，将专业的策略防护功能转变为简便的选择模式。

4.4 高可用性的产品设计

系统部分型号支持双联路（A/B 网）功能，当一组通信接口出现故障时，通信可通过另一组接口继续通信，满足电力等高安全等级网络的双冗余设计功能。

4.5 多种工作模式

IAF 支持针对不同应用场景而采用不同的部署模式，有防护模式、告警模式和学习模式三种模式。

4.6 支持国密算法 VPN

可以对工业协议做基于国密算法 SM2-SM4 的加密算法防护，具有稳定强、易用强、网络环境适应性强，性能高的特点，确保用户的生产、经营数据的机密、完整。

五、 应用场景

边界防护：工业防火墙部署于生产控制区、生产监控区、管理信息大区三区之间，实现纵向防护。

区域防护：工业防火墙部署于 OPC 服务器与 OPC 客户端之间，实现不同控制区域间横向隔离。

核心防护：工业防火墙部署于上位机和核心控制器之间，实现操作控制。