WWW.HUACON.COM.CN

HUACON

力控华康

IN-GAPS 2000 工业网络安全防护网关

工业网络安全守护者

Industrial Network Security Guardian

北京力控华康科技有限公司
Beijing ForceControl-Huacon Technology Co.,Ltd

1. 产品简介

随着工业4.0时代的到来，两化的不断融合，工控统管控一体化趋势逐渐加强，使得工控系统、信息管理系统与互联网相连通，同时工控系统日益复杂化，各种SCADA、DCS、PLC、测控设备组成的过程控制系统越来越多地涉及到通用网络协议（HTTPS、HTTP等）、通用软件以及大流量的数据（数据库、视频等），以各种方式与互联网等公共网络连接。特别是石油、石化、电力、钢铁、煤矿等生产行业，对生产的连续性、安全性和可靠性有着极高的要求，一旦实现了信息网络与控制系统网络之间的高度互联，就相当于将控制系统网络直接暴露给互联网，从而面临被攻击的风险，一旦受到恶意攻击或感染病毒，很可能导致系统中的主机崩溃、整个控制网络瘫痪，造成重大安全事故、危及人员的生命财产安全乃至造成重大社会危害。

为满足这种高度信息化的互联，保障工业网络系统安全稳定运行，力控华康基于多年工业控制领域经验，通过不断研发并结合工业现场环境，推出了IN-GAPS2000系列工业安全隔离与信息交换系统，既实现了工业控制系统与互联网等公共网络间的有效隔离，又解决了两者之间高度信息化互联问题，同时在此之上增加多种应用功能，满足各式各样的工业现场安全防护需求。

2. 产品特点

◆ “2+1”隔离技术架构

即内控制端主机系统、信息端主机系统加上隔离交换系统。由两个独立主机系统组成，每个主机系统分别具有独立的运算单元和存储单元，各自独立运行力控华康自主定制的操作系统。一端的主机系统为控制端，用于连接控制网络；另一端的主机系统为信息端，用于连接信息网络。两端主机均采用高性能嵌入式硬件，主板上各有多个以太网接口用来连接要隔离的两个网络，两端主机通过隔离装置进行连接，保证数据交互的安全性。

◆ 工业协议测点级访问控制

在对工业协议进行解析时，可以针对测点一级进行访问控制。例如：OPC标准可以控制到Item（项）、Modbus协议可以控制到寄存器地址,并且可以对测点进行可见范围和读写权限两方面的控制。

可见范围控制可指定控制端允许或不允许接入哪些测点，从而实对现场设备数据读取范围的控制；同时当信息端有多个监控系统时，可指定哪些测点允许暴露给哪个监控系统，哪些测点要进行屏蔽，从而实现现场设备数据的定向传输管理。

读写权限控制是在测点可见时对每个测点赋予“只读”或“读/写”两种不同的权限。当设为“只读”权限时，所有数据禁止被修改，从而实现单向数据传输，达到保护现场设备安全的目的。

◆ 多协议数据汇聚转换及分发

支持OPC、Modbus、IEC60870-5-101/102/103/104及各种PLC以太通讯等常用工业协议汇聚采集并转换成用户需要的工业协议，同时可以多路分发给不同上位系统。

◆ 白名单管理

通过提前计划好的协议规则来限制网络数据的交换，在控制网到信息网之间进行动态行为判断。
通过对约定协议的特征分析和端口限制的方法，从根源上节制未知恶意软件的运行和传播。

◆ 工业网络协议的深度解析

搭载了自研的深度数据包解析引擎，可对工控协议做到实时和精准的识别，在遵循工业控制系统可用性与完整性的基础上，能够检测出数据包的有效内容特征、负载和可用匹配信息，如恶意软件、具体数据和应用程序类型。
深度数据包解析引擎支持OPC、Modbus、DNP3、IEC 60870-5-101、IEC 60870-5-104、西门子S7系列PLC、AB PLC、GE PLC等提取其中的关键字段（如：控制指令、寄存器区域、寄存器地址、数据范围等）进行访问控制。

◆ 文件同步

具备跨系统平台文件的同步功能；支持单向和双向同步；支持多种文件格式，支持Windows平台和Linux平台；支持内容过滤和病毒检测；支持强制性的文件类型、文件内容（黑、白名单）等检查。

◆ FTP访问

支持FTP的安全访问，对用户、命令、文件类型等进行细粒度访问控制；支持主动模式和被动模式，支持动态建立数据通道，支持访问端口号自定义；支持中文文件名的过滤控制等多种功能。

◆ 邮件传输

支持基于SMTP协议的邮件发送和POP3协议的邮件接收；支持透明访问模式式和普通访问模式；
普通访问模式下，可对邮件服务器地址和端口控制等多种访问控制。

◆ 安全浏览

支持本地认证、Radius、LDAP认证，支持URL过滤、ActiveX、Cookie、JavaApplet等恶意代码过滤。实现控制网用户安全浏览信息网资源，有效保证控制网数据的安全。

◆ 安全通道

支持高速代理、路由和透明三种模式，可以对源地址和端口、目的地址和端口进行访问控制；支持多种应用服务类型，如H323、H323_GK、SNMP、DNS等协议。

◆ 应用协议

支持应用协议有HTTPS、HTTP、FTP、SMTP、POP3、TNS、DNS、Telnet、SAMBA、NFS、IMAP、定制TCP和UDP、SNMP、SSH、RTSP、MMS、H.323、LDAP协议、IRC等协议。

◆ 数据库访问/同步

支持MySql、Oracle、SQL Server等主流数据库间单向和双向同步；支持同构、异构同步；支持一对多，多对一同步；支持字段级的同步，具有条件同步等多种同步策略。

实现对多种主流数据库系统的安全访问；支持SQL Server和Oracle数据库SQL语句过滤功能；支持对源地址、目的地址的访问限制。

◆ 视频协议

支持视频协议传输包括：RTP实时传输协议，RTCP实时传输控制协议，RTSP实时流协议，SRTP实时传输协议RTP的伴生协议，SRTCP实时传输控制协议伴生协议，MMS实时流传输协议等。在绑定视频媒体协议后，确保通道中传输的数据必须符合以上的媒体格式，否则丢弃。

◆ 安全攻击防护

DDoS攻击防护：包括TCP Flood、UDP Flood、SYN Flood、ICMP Flood、IP Flood。

异常数据包攻击：包括Ping of death、IP碎片攻击、TCP碎片攻击。

病毒检测：包括HTTP、SMTP、POP3、FTP、IM即时通讯、S7_300等多种协议双向检测。

◆ IP/MAC绑定

通过对指定接口所连接的网络中主机的IP和MAC地址进行绑定，防止IP地址被非法盗用同时校验主机的合法性，并对非法IP地址的访问进行详细记录，以便管理员查看。

◆ 时间段模式

支持提供时间段模式设置，允许用户在设置的特定时间内通过工业网络安全防护网关访问应用系统。

◆ VLan功能

支持多VLan，并且对VLan数据进行安全检查。

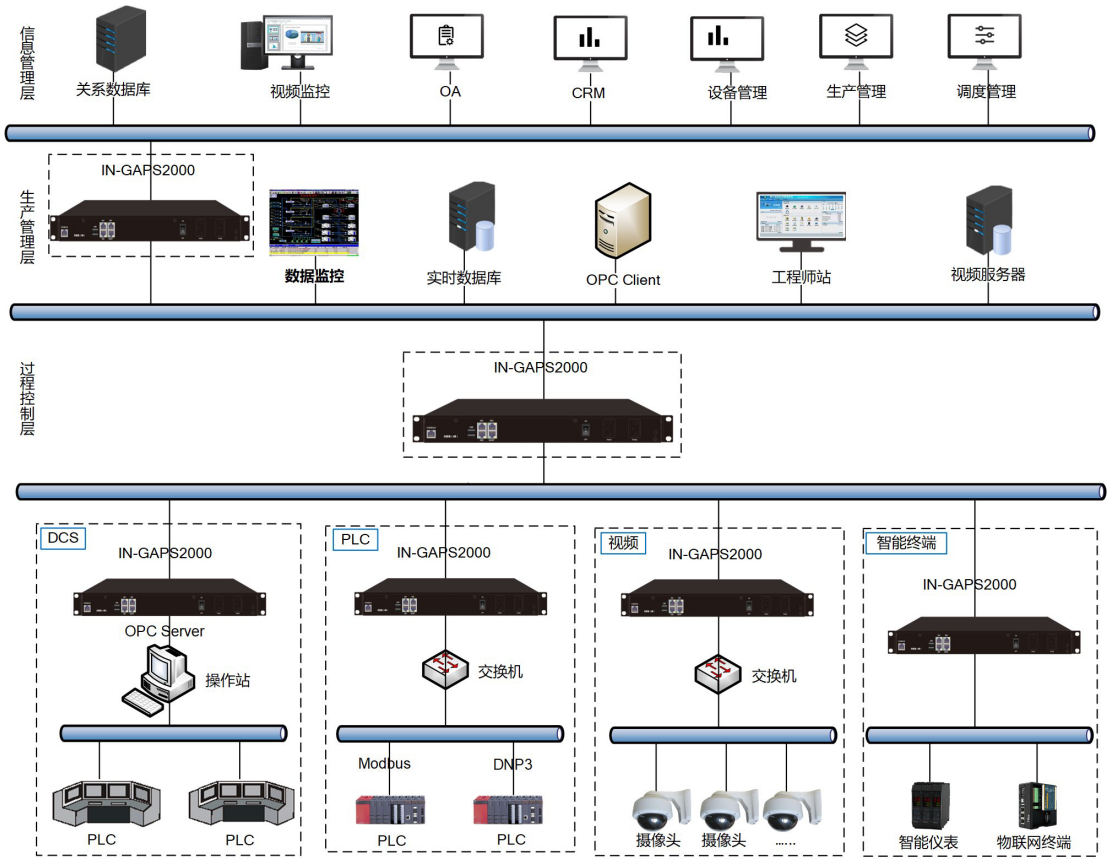
◆ 断线缓存

保证数据的完整性、连续性、可靠性，当信息测网络故障时数据缓存到本地，等待网络恢复后数据补报。

◆ 双机热备

双机热备模式下，两台工业网络安全防护网关通过心跳检测进行互相监控，如果其中的一台出现故障（宕机、网络故障），那么另一台就顶替出现故障的网关提供服务。保证了网络的高可用性和高安全性，提升了系统的可靠性。

3. 典型部署



IN-GAPS2000部署在信息管理层与生产管理层之间，用来阻止来自信息网的DOS/DDOS攻击、恶意扫描、异常数据包等安全威胁；可对通用网络协议进行访问控制和安全过滤，并且支持对工控主流协议进行访问控制及深度解析，可以限制只有可信任的数据能够在工控网络中传输，有效保护了工控网络的安全。

OPC标准由于其开放性和高效性，现在已被广泛应用于自动化控制领域及生产管理中。然而OPC Server与OPC Client之间的通信依赖控制网络与管理网络的直接连通，这样会给控制网络的安全带来极大的隐患。

Modbus是基于PLC的一组通信协议，已经成为行业内设备互相通信的标准协议。DNP3（分布式网络协议）是使用在工序自动化系统各部件之间的通信协议，主要用于电力、水力等公共事业领域。

在工业网络中存在很多关系数据库系统、视频监控系统，是用来完成特定生产、监控任务的应用系统，其自身没有任何的安全防护措施，一旦这些重点系统受到恶意攻击或者有人为误操作的影响，将会直接危及整个生产过程，影响生产安全，甚至发生事故。

IN-GAPS2000的双独立主机系统保持OPC Server、Modbus设备、DNP3设备、关系数据库、视频监控等和上层间的通信，同时两主机之间采用专用网络隔离技术，在保证数据快速交互的同时彻底阻断所有网络连接，保证了控制设备的安全。

Industrial Network Security Guardian

全国统一服务热线：**400-650-1353**

北京力控华康科技有限公司

Beijing ForceControl-Huacon Technology Co.,Ltd

地址：北京市海淀区天秀路10号中国农大国际创业园1号楼625室

邮编：100193

电话：010-62839678

010-62839687

网址：www.huacon.com.cn

全国服务热线：400-650-1353