力控科技 FORCECON | HUACON 力控华康

工业安全隔离与信息交换系统
IN-GAPS 2000

北京力控华康科技有限公司
www.sunwayland.com

目 录

产品概述

行业背景

在现代工业企业的信息系统中，由各种SCADA、DCS、PLC、测控设备构成的过程控制系统位于底层车间，负责完成基本的生产控制。随着企业信息化全面应用，越来越多的过程控制系统网络与上层管理信息网络之间进行互联互通，实现了经营管理层与车间执行层的双向信息交互。但在这种信息交互的过程中，如何保障过程控制系统的安全就变成了一个严峻的问题。特别是对于石油、石化、电力、钢铁、煤矿等生产行业以及连续生产的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，从而面临被攻击的可能。控制系统网络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甚至造成重大社会危害。

近年来发生在发电厂、污水处理厂、天然气管道以及其他大型设备的工业控制系统网络入侵事件已经给我们敲响警钟，如何保证过程控制系统的运行安全迫在眉睫，广大工业企业急需一款适用于工业控制系统网络的专业安全防护产品。

工业控制系统网络特点

工业控制系统网络是由工业自动化生产设备，如SCADA、DCS、PLC等各种过程控制系统组成的网络，不同于IT网络，工业控制系统网络具有以下特点：

◉专用通信协议或规约（OPC DA、Modbus、DNP3等）。

◉系统传输、处理信息的实时性要求高，尽量避免停机、重启等操作。

◉系统故障必须及时响应处理，不可预料的中断会造成经济损失或其他危害。

◉为满足特定应用场景、任务单一性以及系统稳定性；为保障生产的连续性，减少可能的风险，因此系统或设备很少升级，甚至不升级。

传统网络隔离产品的不足

传统安全隔离设备是信息安全领域一个热门的防护产品，它通常使用双主机或三主机的硬件结构，实现不同网络安全区域之间的隔离，在隔离的同时还可以实现不同安全区域之间适度的数据摆渡。

传统安全隔离设备虽然可以阻断不同网络安全区域之间的攻击，也可以用于控制网络与信息网络之间的隔离和数据摆渡，但是其不能很好的满足工业现场实际要求，因为它主要是针对通用网络协议进行处理，不支持工业网络协议，更不能对工业网络中大量的测点数据进行细粒度的管理。虽然很多传统隔离设备厂商给用户提供开发接口，去支持用户专有的协议，但是这对于用户的开发能力要求较高，实际当中的可操作性很差。

综上所述，传统安全隔离设备在工业网络中确实有其不足之处。在实际的工业网络环境中用户需要专门针对工业控制系统网络、支持广泛工业协议的安全隔离设备来实现控制网络与信息网络之间的有效隔离和数据的安全传输。

工业安全隔离与信息交换系统

针对传统安全隔离设备在工控行业环境下应用的不足，作为国内工控行业的佼佼者，力控华康深知自己的社会责任所在，依托多年工控行业的技术积累，通过硬件和软件两方面的优化和创新，开发出了IN-GAPS工业安全隔离与信息交换系统，不仅实现了对基于TCP/IP协议体系攻击的彻底阻断，也实现了对主流工业网络协议的广泛、深入支持和保证工业控制网络数据的安全传输，并解决了传统安全隔离设备无法适用于工业控制网络的难题。

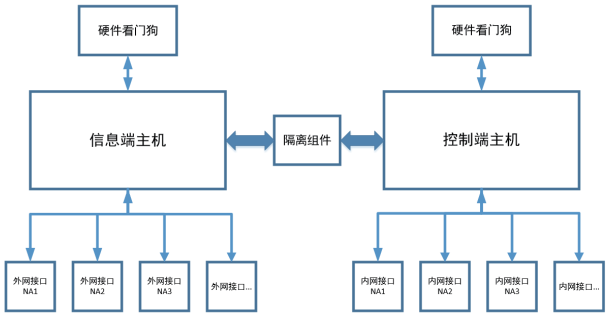
针对传统安全隔离设备在工控行业环境下应用的不足，IN-GAPS不仅实现了传统网闸用于控制网络与信息网络之间的隔离、数据摆渡和不同区域间的攻击防护，同时也实现了对工控协议内容如功能码、寄存器地址等进行精准识别和安全控制和工业网络中大量的测点数据进行细粒度的管理。

产品架构

硬件架构

采用“2+1”的物理结构，内部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，不同的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。

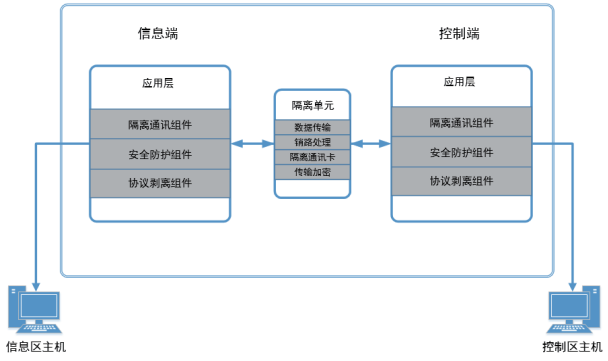
硬件看门狗实时监视系统状态，保证整套装置的稳定、持续运行。



软件架构

控制端与信息端主机分别运行力控华康自主定制的操作系统，主机之间的通讯使用私有协议，保证数据传输的安全。该系统支持通用网络协议访问控制及安全过滤，并且全面支持各种主流工业网络协议，包括OPC DA、Modbus、Siemens S7、DNP3、IEC 60870-5-104等，系统可以深度解析各种工业网络协议，对协议数据进行细粒度的处理。

控制端和信息端系统中的隔离通讯组件以及中间的隔离单元三者构成了工业控制网络隔离系统的核心。隔离通讯组件负责根据用户配置取出数据包中关键的应用层信息，并对数据包进行必要的解析和安全检查，隔离单元负责使用私有协议进行控制端和信息端之间的数据加密摆渡。



产品特点

安全隔离

◉ 单向隔离

IN-GAPS 2000实现了对TCP、UDP应用数据传输方向的控制。通过对TCP、UDP协议数据包的深度解析，做到对应用数据的访问控制，可实现应用数据的单向传输。在开启单向传输功能后，应用数据只允许单方向传输，反方向的传输将会被阻断，确保不会有任何敏感数据泄露到安全区域以外。在数据单向传输的同时，隔离单元会将数据包进行拆解，使基于TCP、IP等网络协议的攻击无法通过。

◉ 双向隔离

IN-GAPS 2000在硬件方面采用了两个独立高性能嵌入式主机，双主机之间通过隔离单元采用私有协议实现两个安全区之间的数据交换。在启用数据双向隔离功能后，IN-GAPS 2000对所有数据包进行拆解和还原，通过私有通信方式进行数据双向传输。

在数据双向传输的同时，IN-GAPS 2000的隔离单元会将数据包进行拆解并在另一侧进行重组，使基于TCP、IP等网络协议的攻击无法生效，且数据传输时采用私有通信方式，在保证安全隔离的前提下，实现数据的高速交换。

工业协议深度解析

IN-GAPS 2000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，为解决工控网络的安全问题提供了技术基础保障，其全面支持各大主流工业控制协议，并且能够对各类数据包进行快速有针对性的捕获与深度解析。对不同行业的工控系统，可以采取相应针对性的数据包探测机制和解析策略。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。解析引擎执行时能够满足工业控制系统在生产和制造过程中的通信效率的保障要求。

深度数据包解析引擎支持OPC DA 、Modbus、DNP3、IEC 60870-5-101、IEC 60870-5-104、西门子S7系列PLC、AB PLC、GE PLC等在内的各大主流工控网络协议，可以对工业协议进行解析，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。

业务可靠性

IN-GAPS 2000为了符合工业现场生产的连续性及稳定性在软件上进行全面优化设计

◉ 断线缓存

工业控制网络对于数据的连续性要求极高，针对工业控制网络中这种特有的要求IN-GAPS 2000支持断线缓存功能。

可以在信息端网络暂时性中断的情况下将控制端数据缓存在本地网关设备中，并不断检测信息端网络的连通性状态，当信息端网络连接恢复时将缓存的数据补报到监控系统中，保证数据的连续性。

◉ 其他功能

系统内嵌自诊断程序，实时监测系统的运行情况，支持系统故障自恢复功能。

具有软件狗、工程备份、流量限制、日志审计、双机热备等功能。

ALG应用层防护

IN-GAPS 2000支持FTP、SQLNET、H323、OPC协议的动态端口应用防护功能，通过对父连接的应用层信息进行解析，获取子连接信息，实现对多连接协议中父连接和子连接的控制。如：OPC运行正常，OPC数据连接所使用的动态端口开放或放行。

数据库同步

用户的实际应用系统中，往往具有不同的用户群及不同的网络应用。但应用之间共享应用数据却往往是必要的。因此，IN-GAPS 2000将数据库同步功能作为其数据交换的基本功能之一。

IN-GAPS 2000数据库访问模块通过数据库应用代理的方式将数据库服务映射到网闸的一端，应用程序可以直接访问映射的数据库服务，由网闸完成数据库的数据内容安全传输。数据库同步模块可以将一端网络中的数据库内容同步复制到网闸另一端网络的数据库中。

◉ 数据库单向同步及双向同步

◉ 数据库全表复制及增量复制

◉ 数据库同构及异构同步

同步任务配置，包括主键冲突处理、同步动作、启动模式、时间及间隔、表字段等属性的控制。

统一安全管理

工业互联网等技术快速发展的形势下，越来越多的工业控制网络和信息网络连接在一起。企业加大了对工控网络安全的投入，纷纷开始规划工控网络安全的建设，使得工控网络中多种技术类型的安全设备迅速增加。《等保2.0》里则提出了“集中管控”的要求，即对分布在网络中的安全设备或安全组件进行管控，对网络链路、安全设备、网络设备和服务器等的运行状态进行集中监测，以及对分散在各个设备上的审计数据进行收集汇总和集中分析等。

IN-GAPS 2000满足安全运维及等保政策需求，支持syslog日志外发、SNMP设备状态外发及安全策略统一配置下发API接口等功能。

双模式数据摆渡

IN-GAPS 2000支持工业测点数据同步和安全隧道数据流两种模式进行数据摆渡。

冶金系统、电力系统、煤炭、石油、石化、化工、环保等单位的生产内网需要将生产数据及时提交到办公网络的实时数据库中，保证生产内网的绝对安全。IN-GAPS 2000工业数据同步模块针对工业现场数据通信需要，提供测点数据的解析和安全保护。使用离线工具配置工程文件后上传到控制端，保证专用安全通道只传输工控生产数据信息，即可保证生产内网的绝对安全。

安全隧道数据摆渡模式是使用力控华康自主开发的安全数据传输方式建立安全通道，支持TCP、UDP、OPC、HTTP、RTSP、SIP、FTP、视频协议管理等多样化的网络环境中的数据摆渡。

安全防护

◉ 入侵防御

IN-GAPS 2000具有入侵防御功能，内置工业IPS库，可持续升级，通过流量检测和报文深层次分析，可全方位防御注入攻击、XSS攻击、目录遍历攻击、操作系统漏洞利用攻击等。通过可持续升级的入侵规则库对流量进行检查，判断为入侵行为后有两种处理方式：告警或拒绝（用户可自行配置）。这样则可对工业系统中无法升级更新的系统进行更好的安全保护。具体包括：

能够检测并抵御操作系统类、应用服务器类（例如web服务器、ftp服务器）的漏洞攻击。

能够检测并抵御文件类漏洞攻击。

能检测并抵御ActiveX控件漏洞攻击。

能检测并抵御常见web攻击，如SQL注入、XSS脚本和目录遍历等。

◉ 病毒过滤

IN-GAPS 2000具有文件病毒过滤功能，当通过HTTP、SMTP、POP3、FTP、IM（如QQ、微信）等进行文件传输时，防火墙能够对文件进行病毒检测，如果发现其中含有病毒则能够进行告警或阻断，避免恶意文件进入被保护的网络。

◉ 安全攻击防护

· 支持单包攻击的检测和防御：teardrop、Land、Ping of death。

· 支持flood攻击的检测和防御：ICMP flood、UDP flood、SYN flood。

· 支持检测、记录和抵御网络扫描行为（端口扫描、漏洞扫描）。

◉ URL过滤

IN-GAPS 2000具有URL过滤功能。用于对互联网上的网站进行分类，将所有Web流量与URL过滤数据库进行比较，并通过引用已经分类的中央数据库或根据分类中包含的信息来允许/阻止对组织的Web用户的访问。如：恶意类网站、成人类网站、赌博类网站以及其他非法类网站。

◉ 黑名单过滤

IN-GAPS 2000具有关键字及文件类型过滤功能。使用正则表达式方式配置关键字内容和策略条件协议类型、流量方向进行关联过滤。可通过文件传输协议深度识别病毒文件，可对多级压缩文件进行解压查杀。

◉ 自身防护

IN-GAPS 2000具有自身安全防护功能。支持网络扫描共计防护、管理口访问地址限制、WEB管理界面开关、SSH管理功能开关、禁止网络探测诊断PING等。

典型应用

IN-GAPS 2000适用于各种控制网络的安全防护。典型应用领域包括工业DCS控制系统的网络安全防护、电力系统现场IED设备的网络安全防护、轨道交通ISCS的网络安全防护、煤矿、冶金行业现场控制系统的网络安全防护等。

下面分别介绍三种常见的典型应用场景。

工控网络中控制网到信息网间的应用

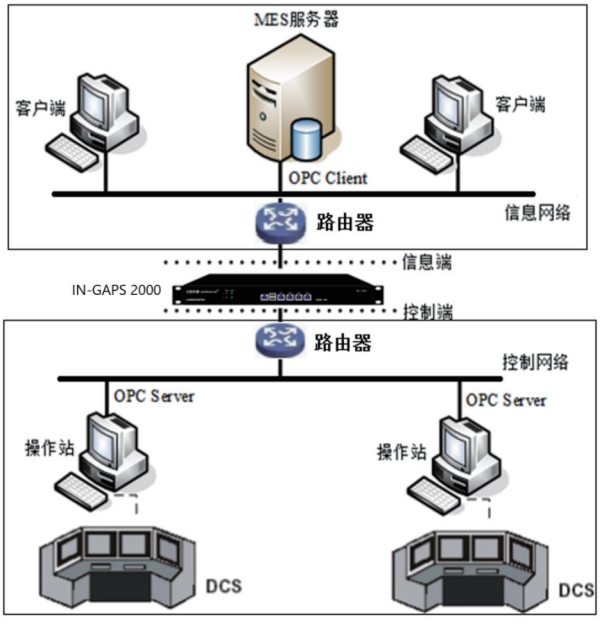
IN-GAPS 2000部署在信息网络与控制网络之间，能有效的对两网之间数据进行隔离，阻止来自信息网的DOS/DDOS攻击、恶意扫描、异常数据包等安全威胁。IN-GAPS 2000可对通用网络协议（如TCP、UDP、HTTP、HTTPS、ICMP、FTP、视频协议、数据库等）进行访问控制和安全过滤，也支持工控主流协议（Modbus、OPC、DNP3、IEC 60870-5-101、IEC 60870-5-104、西门子S7系列PLC、AB PLC、GE PLC3等）进行访问控制及深度解析，通过对工控网络数据深度解析及规则设置，可以保证只有可信任的数据能够在工控网络中传输，有效防护了工控网络的安全。

基于OPC数据、交互的应用

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信息管理中。目前大多数DCS系统、SCADA系统对外都提供OPC Server，以便为上层MES、生产调度等管理信息系统提供实时生产数据。同时几乎所有的MES系统、生产调度系统的数据采集接口也都提供了OPC Client以便能实现对OPC Server数据的采集。然而OPC Server与OPC Client之间的通信依赖控制网络与信息网络的直接连通。管理信息系统的网络出于业务需要一般会连接到互联网，这样会给控制网络的安全带来极大的隐患。

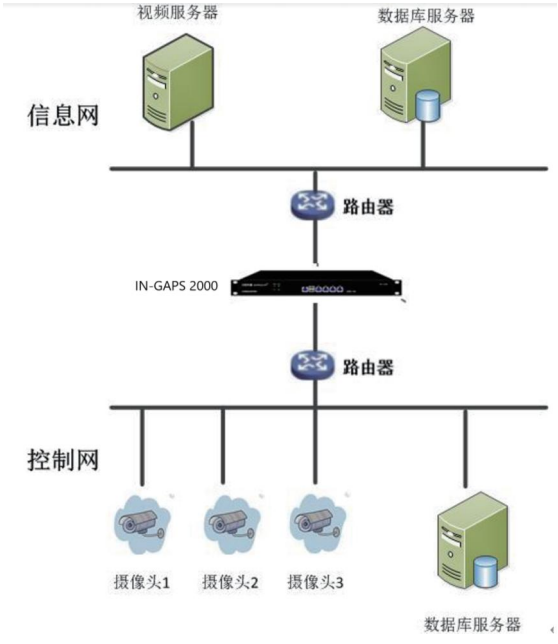
IN-GAPS 2000的双独立主机系统分为控制端和信息端，

分别接入控制网络和信息网络，完成与OPC Server和OPC Client的通信，同时两主机之间采用专用网络隔离技术，在保证OPC数据快速交互的同时彻底阻断其它网络连接，保证了控制网络的安全。



支持关系数据库、视频的应用

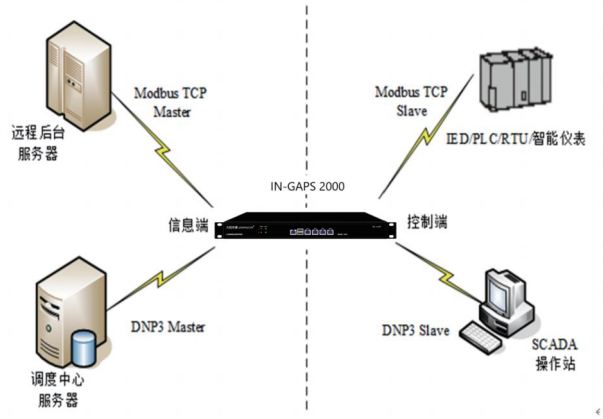
在工业网络中存在很多关系数据库、视频监控，这些重点设备本身是用来完成特定生产、监控任务的应用系统，其自身没有任何的安全防护措施，可以通过网络对其进行任意的访问。一旦这些重点设备受到恶意攻击或者有人为误操作的影响，将会直接危及整个生产过程，影响生产安全，甚至发生事故。



基于Modbus、DNP3的应用

Modbus是基于PLC的一组通信协议。它已经成为行业内设备互相通信的标准协议，也是目前最常用的工业系统设备之间的通信协议。

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，它主要用于电力、水力等公共事业领域。此外，它的发展使得不同形式的数据获取与控制设备之间的交流更为便利。



调度自动化系统的后台为了实时获取现场设备的数据，经常需要通过网络使用Modbus、DNP3等通信协议进行数据传输。然而调度数据网络与现场控制设备的直接连通就相当于将控制系统直接暴露给外网而面临被攻击的可能。

IN-GAPS 2000内嵌力控华康自主开发的工业网络隔离系统，支持Modbus、DNP3等标准通信协议，可以实现调度自动化后台系统与现场设备的实时通信，并根据需要可设置数据方向、访问权限等。当设置为单向方式，后台系统的所有数据回置操作将被屏蔽，以保证现场控制设备的安全。

力控科技 FORCECON

北京力控华康科技有限公司

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
总机：010-62839678
全国统一服务热线：400 650 1353
www.huacon.com.cn

关注公众号　关注小程序