力控科技 FORCECON | HUACON 力控华康

工业防火墙
HC-ISG

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

在工业网络中，运行着SCADA、DCS、PLC等各种过程控制系统，它们往往是生产系统的核心，负责完成生产控制和监控。随着工业4.0时代的到来，两化的不断融合，工控系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，已经开始大量采用通用软件、通用硬件及通用协议，这使得传统封闭的工控系统逐步暴露出来，直接面对来自外界网络的种种威胁，增加了工控系统的安全隐患。工控系统通常是从简单独立的系统发展成为复杂的网络系统，各个子系统之间在设计上缺乏保护措施，从而导致一个区域出现问题，很快就会感染整个工控系统网络。这些过程控制系统一旦遭受干扰或破坏，就会对工业生产造成不同程度的影响，可能使企业蒙受重大的经济损失，危及人员的生命安全甚至造成重大社会危害。近年来发生的工业网络入侵事件给我们敲响了警钟，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针对工业网络进行安全防护的专业防火墙产品。

工业控制系统网络环境特点

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：

◉采用专用通信协议或规约（OPC、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。

◉具有应用场景特定、任务单一性强以及对系统稳定性要求高等特点，为保障生产的连续性，减少可能的风险，系统或设备很少升级，甚至不升级。

工业控制系统网络现状

◉ 防护意识不足

工业控制系统网络长期以来从管理者到一线员工对工控网络防护的认识普遍不足，认识程度不一，实际工作中普遍存在诸如不安全连接、不规范操作、随意远程、胡乱U盘接入等现象，给工控网络信息系统带来客观隐患，而人为主观带来的威胁则更具有不确定性、隐蔽性。

◉ 未知隐患的防护挑战

随着物联网的推广应用，信息基础设备设施的互联互通性迅速加强，给工控网络带来更多未知不可控的防护隐患。现有防护措施普遍是针对已知的攻击行为而制定的，而如何应对新型未知的工控网络攻击方式和手段，才是相关企业更应该关注也必须解决的问题。

传统防火墙在工业控制系统网络中的不足

传统防火墙是目前网络边界上最常用的一种防护设备，诞生于传统信息网络环境下，虽然经过了多年的发展和完善，但其应用环境还是局限于企业信息网络，它对于工业网络环境还有诸多的不适应，主要体现在以下几方面：

◉ 传统防火墙主要是针对通用网络协议进行审核和防护，不能对工业网络协议和应用数据的内容进行解析和检查。

◉传统防火墙基于黑名单机制，为及时应对新发现的系统和软件漏洞，以及面临不断更新的网络攻击手段和威胁需要不断升级，不符合工业现场特点。

力控华康工业防火墙

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，通过自主创新开发出HC-ISG系列工业防火墙为国内工业网络安全保驾护航。

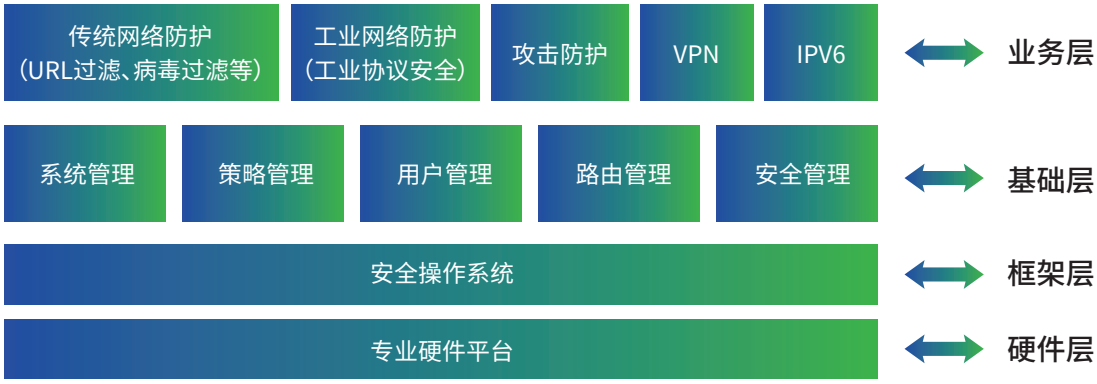
力控华康工业防火墙HC-ISG是专用于工业控制安全领域的增强级边界安全防护产品，能够有效对SCADA、DCS、PCS、PLC、RTU等工业控制系统进行网络安全防护。HC-ISG主要用于实现工业基础设施在网络环境中的边界防护，从而阻断攻击者的非法访问、病毒传播和恶意攻击等，同时也能有效避免工作人员因误操作导致的威胁扩散等安全问题。HC-ISG广泛应用于各种工业现场，包括核设施、钢铁、有色、石油天然气、化工、电力、城市燃气、机械、环保监测、城市供水、供热、水利枢纽、隧道、港口、铁路、城市轨道交通、民航以及其他与国家基础设施和国计民生紧密相关的工业控制系统和网络。

全新一代增强级工业防火墙HC-ISG，全面提升和扩展了入侵防御、URL过滤、病毒过滤、网络扫描防护、IP/MAC绑定等功能，可识别和预防网络中病毒传播、恶意攻击等行为，避免其影响控制网络和破坏生产流程；新增加并提供流量带 宽管理、NAT及IPv6隧道等功能，可满足更多维度的网络环境需求，更加适应当前工业网络环境与信息化网络环境相融合的发展趋势；工业协议方面，提供针对工业协议的指令级深度检测，实现对Modbus、OPC等主流工业协议和规约的细粒度检查和过滤，并支持智能协议识别和辅助规则生成；同时HC-ISG具备高可用性及全透明无间断部署功能，有效保证业务连续性。

产品架构

HC-ISG系列工业防火墙是HC-ISG的升级版，是力控华康不断探索、不断进步、自我完善的全新成果。产品在架构设计上充分地考虑了工业网络设备种类多、协议复杂、行业差别大的特点，将产品进行了深度的模块化封装，引入了功能插件的概念，使整个防火墙系统更加部件化。通过这种架构的实现一方面可以更好的适应现有工业网络安全防护的需要，另一方面为未来产品功能的扩展和用户定制开发打下良好的基础。

HC-ISG系列工业防火墙由业务层、基础层、框架层、硬件层四个部分组成。



◉ 业务层是HC-ISG系列工业防火墙的核心业务处理单元，主要用于完成对于工业网络协议的识别、解析、深度过滤和攻击防护。

◉ 基础层是由力控华康根据工业网络通信特点和安全防护要求定制开发的底层运行平台，为防火墙上层业务模块提供必要的运行环境和安全保障。

◉ 框架层是HC-ISG系列工业防火墙的核心软件平台

◉ 硬件层采用专业的硬件平台，保障系统运行的稳定性。

HC-ISG系列工业防火墙以专业的硬件平台为基础，高度融合安全操作系统平台和驱动配置模块形成稳定的框架层，然后在框架基础上进行系统管理、策略管理、用户管理、路由管理、安全管理等基础模块的开发。通过基础层和框架层的有效结合最终保障业务层的传统网络防护及工业网络防护功能的稳定运行。

产品特点

安全性

1.工业网络通信协议的深度包检测

传统防火墙主要是针对通用网络协议进行访问控制和安全过滤，完全不支持工业通讯协议。HC-ISG系列工业防火墙与传统防火墙最大的区别是提供了针对工业通讯协议进行深度包检测的功能。之所以称之为深度过滤，是因为HC-ISG系列工业防火墙不但可以针对工业网络协议进行基本的访问控制，而且可以针对工业网络协议（Modbus TCP、OPC、IEC104、S7、profinet、dnp3等约40种）的内容和数据进行细致的合规性检查。例如：HC-ISG系列工业防火墙的Modbus协议规则可以针对Modbus协议的设备地址、寄存器类型、寄存器范围和读写属性等进行检查，能有效地防范各种非法操作和非安全数据的产生，最大限度地保护控制系统的安全。

工业现场设备繁多，规格不一，通信协议和规约各异。这就要求安全设备可以支持多种工业网络通信协议，适用于各种网络环境，可与各种现场设备进行交互对接。针对这种现状HC-ISG系列工业防火墙将每一种工业协议作为一个独立的深度过滤单元，根据不同协议进行设置，并且可以根据用户现场的需要进行工业网络协议深度过滤的快速定制开发和响应，最大限度的满足工业现场的各种安全防护要求。力控华康公司具备专业的开发团队，可根据客户需求针对非主流或私有工业网络协议进行定制开发。

2.通用网络协议的防护

HC-ISG系列工业防火墙可对通用网络协议进行访问控制和安全过滤，具有4-7层包过滤，支持以五元组形式对通用协议数据包进行访问控制和安全过滤。

HC-ISG系列工业防火墙支持的通用网络协议（如TCP、UDP、HTTP、HTTPS、ICMP、FTP、TELNET、视频协议、数据库等）广泛，并能对HTTP、FTP、TELNET等协议提供深度及细粒度的过滤功能，支持网站安全浏览、邮件访问控制、FTP访问控制、数据库访问控制、文件同步等安全规则。支持即时聊天类应用、P2P流媒体类应用、网络流媒体类应用、网络游戏、股票软件、逃逸或隧道加密特点的应用，如HTTPS访问、翻墙软件、VPN访问等。同时也支持基于IP/MAC绑定的安全策略设置，使伪造IP的数据包无法通过防火墙。

3.安全攻击防护

HC-ISG系列工业防火墙具有以下攻击防护功能：

◉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）。

4.ALG应用层防护

支持ALG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，实现对多连接协议的父连接和子连接的控制。支持：FTP、SQLNET、H323、OPC协议。如：OPC运行正常，OPC数据连接所使用的动态端口被开放/放行。

5.入侵防御

HC-ISG系列工业防火墙具有入侵防御功能，内置IPS特征库（4万+）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）。能够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：

◉检测并抵御工业协议（例如OPC、Modbus、IEC）及设备（例如施耐德、西门子、欧姆龙）相关的攻击。

◉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。

◉检测并抵御文件类漏洞攻击。

◉检测并抵御ActiveX控件漏洞攻击。

◉检测并抵御常见web攻击，如SQL注入、XSS脚本和目录遍历等。

6.病毒过滤

HC-ISG系列工业防火墙具有文件病毒过滤功能，内置病毒特征库（600万+）可持续升级，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。

7.URL过滤

HC-ISG系列工业防火墙支持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。

8.地址绑定

HC-ISG系列工业防火墙的地址绑定功能通过检测非安全端的IP与MAC地址是否相同，防止遭受ARP攻击和IP冲突等安全问题。

9.用户认证

用户认证可采用本地认证、Radius认证和Ldap认证3种方式。

10.管理员鉴别

管理员可进行鉴别配置，并能绑定启用UKEY，实现双因子认证。

11.VPN功能

为设备间数据通信提供安全保障，通信过程采用加密传输，认证成功后可实现远程访问。

可用性

1.全透明无间断部署

考虑到工业网络对于可用性、持续性的要求，HC-ISG系列工业防火墙采用全透明接入的方式，提供学习、测试、管控三种工作模式，产品在部署、配置和使用过程中可以根据需要实时切换到适当的工作模式下，保证在整个部署过程中都不会阻断正常的业务数据传输，无需中断生产系统的运行，同时在启动深度过滤时可选择仅警告，等确认后再进行处理，保障生产系统不间断运行。

◉学习模式：默认开启学习模式，HC-ISG系列工业防火墙可允许所有数据包全部放行，用于学习策略，且不产生日志。

◉测试模式：开启测试模式，HC-ISG系列工业防火墙可允许黑名单外的数据包全部放行，未匹配策略将产生日志。

◉管控模式：开启管控模式，HC-ISG系列工业防火墙会按照所设定的策略进行运行，不符合规则的将被禁止通过，符合规则的则通过，并生成日志。

2.传输模式可配置

HC-ISG系列工业防火墙的每个网口均支持独立设置为透明（网桥）模式或路由模式。当网口处于透明模式时，可以根据二层信息在其他透明模式网口间进行数据包转发。当网口处于路由模式时，可以根据静态路由或策略路由信息，在其他路由模式网口间进行数据包转发。

3.工业网络OPC通讯协议动态端口开放

HC-ISG系列工业防火墙可提供对工业网络OPC通讯协议的动态开放端口功能，支持OPC通讯协议在通讯中的数据链接需要使用动态端口的开放，保证OPC协议正常运行。而传统防火墙一般不支持动态端口的开放。

4.智能协议识别和辅助规则生成

工业网络中设备众多、网络通信复杂，用户很难全面的掌握网络中所必须的通信业务需求，这会给防火墙的规则配置带来很大的困难。为了方便用户进行防火墙规则的配置，提高规则配置的准确性，减少规则配置的工作量，HC-ISG系列工业防火墙具备智能协议识别和辅助规则生成功能。

智能协议识别功能采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，帮助用户以最快捷的方式了解和掌握网络中的业务通信。

用户可以在测试模式下使用策略管理的辅助配置功能生成辅助规则，将网络交互信息与实际业务进行比对，给每一个网络交互过程配置适当的防火墙规则，从而准确、快捷的完成防火墙规则的配置。

5.安全审计

HC-ISG系列工业防火墙安全审计功能具有以下几个特点：

◉能够记录被防火墙允许、禁止的访问请求。

◉能够记录试图穿越或到达防火墙的违反安全策略的访问请求，检测出攻击行为。

◉能够记录试图登录防火墙管理端口和管理身份鉴别请求。

◉能够产生不同级别、类型的日志，并对日志进行管理。

◉支持多个Syslog日志服务器。

6.流量监控及会话管理

◉流量监控

HC-ISG系列工业防火墙能够通过IP地址、网络服务、时间和协议类型等参数对流量进行监控统计。并且可以根据策略和网络流量动态调整客户端占用的带宽。

◉会话管理

HC-ISG系列工业防火墙可以设置单IP的最大并发会话数，并且在会话处于非活跃状态的一定时间内或会话结束后主动释放其占用的状态表资源。

7.NAT网络地址转换

HC-ISG系列工业防火墙支持双向NAT：SNAT和DNAT。鉴于目前IPv4地址匮乏，SANT和DNAT可以有效的解决该问题。同时能够有效地避免来自网络外部的攻击，隐藏并保护设备IP，保障设备安全。该功能也可实现当大量客户端访问服务器时，通过负载均衡有效减轻服务器压力。

8.IPv6过渡网络环境

HC-ISG系列工业防火墙支持IPv4和IPv6两种协议同时存在的网络环境，支持IPV4和IPv6两种协议的相互转换。防火墙利用隧道技术，实现了IPv4和IPv6的网络互通，作为IPv4网络到IPv6网络的过渡。主要提供6over4隧道、6to4隧道以及isatap隧道功能。

9.简便的配置方法

HC-ISG系列工业防火墙采用B/S架构，通过浏览器直接对防火墙进行配置，无需安装应用软件，配置过程简单，容易上手。HC-ISG系列工业防火墙配置具有以下几个特点：

◉“白名单”配置方式

HC-ISG系列工业防火墙默认拒绝所有连接，用户只需根据工业现场实际的通信业务需要配置相关规则即可，无需关心其它网络通信协议。

◉内置各种常用协议

HC-ISG系列工业防火墙内置了常用工业网络协议、通用网络协议，在进行防火墙配置时直接引用即可。

可靠性

1.硬件可靠性

为了适应工业网络环境对于产品可靠性的要求，HC-ISG系列工业防火墙采用工业级产品硬件设计，在环境适应性、散热、故障处理等方面进行了全面的优化。

◉硬件平台专门面向工业应用场合设计，对PCB、电源、机箱结构、散热进行全面优化，采用低功耗、宽温、宽压电子元器件，多种模式的导散热方式，充分的减少产品的发热量，提高产品的稳定性和环境适应性，保证设备在各种恶劣环境下可以持续、稳定的运行。

◉网口支持Bypass功能，根据系统运行状态开启，即当系统断电、关机及启动过程中自动开启。

◉具备双机热备功能，当主防火墙出现故障情况时，备用防火墙会及时发现并接管主防火墙进行工作。

2.软件可靠性

为了符合工业现场生产的连续性及稳定性，HC-ISG系列工业防火墙在软件上实现了全面优化设计。

◉具有全透明无间断部署功能，保证系统运行稳定性和不间断性。

◉具有智能协议识别和辅助规则生成功能，方便用户进行协议规则配置。

◉具有负载均衡功能，可以根据安全策略将网络流量均衡到多台服务器上。

◉具有流量监控、动态调整带宽、并发会话限制、日志审计、策略路由、NAT等功能。

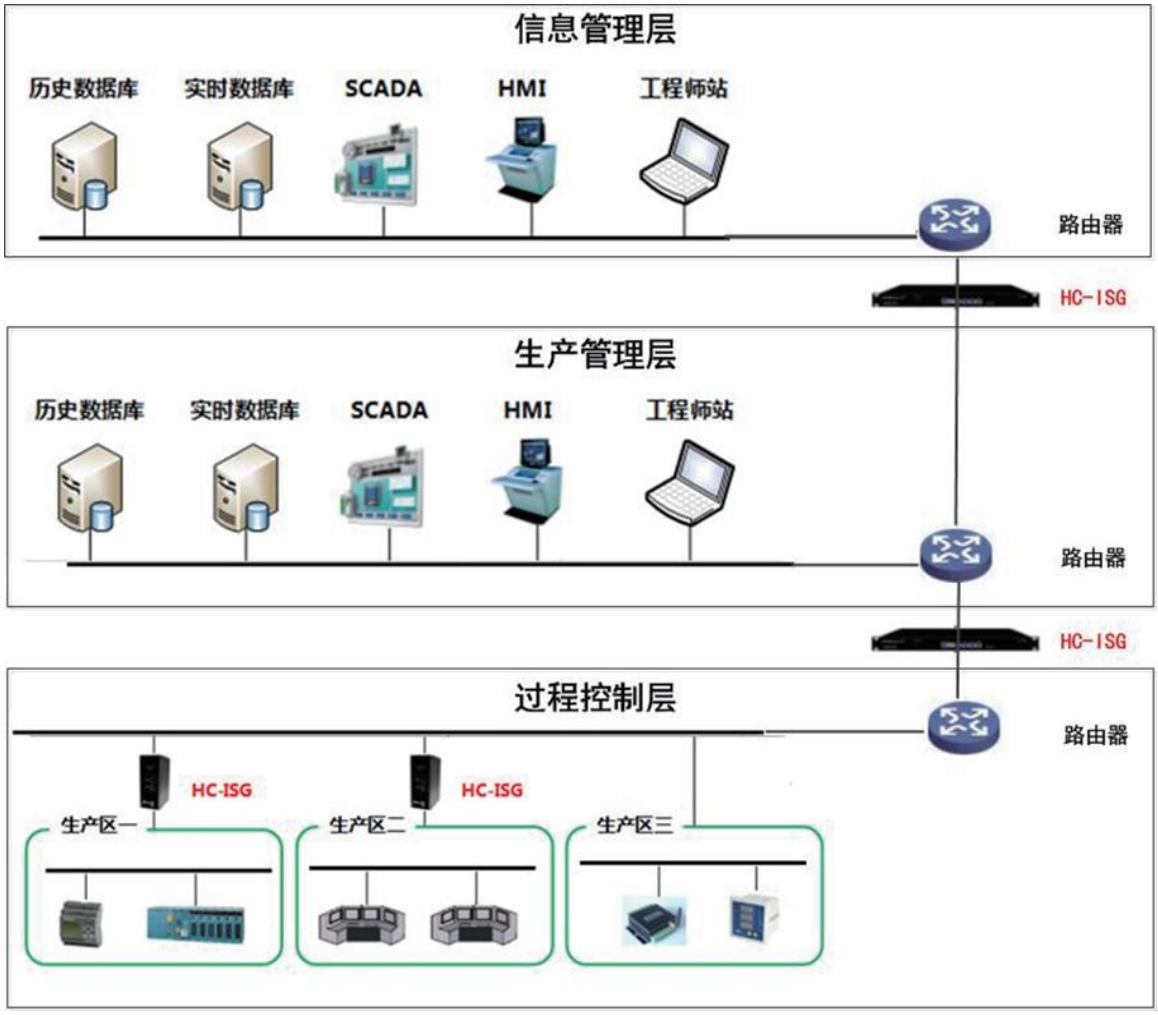
典型应用

安全区域之间的访问控制和安全防护

随着“两化融合”的全面推广，广大工业用户的网络结构发生了巨大变化，现场过程控制网络、生产管理网络、企业信息网络被打通，网络纵向分层、横向分区的模式正在形成。由于各个层次、各个区域网络的业务不同、作用不同，对于安全防护的要求也就不同，所以需要在不同安全区域之间进行必要的防护和控制。HC-ISG系列工业防火墙可以帮助用户很好的实现这一目标。

首先通过在纵向不同层次网络之间部署HC-ISG系列工业防火墙，并配置合理的访问规则，可以控制不必要的跨层访问，防止攻击者通过上层网络向下层网络的渗透和攻击，减少由于网络互联互通所带来的安全风险。同时可以对不同层次之间的工业协议数据交换进行深度过滤，屏蔽非法操作，保障生产安全。

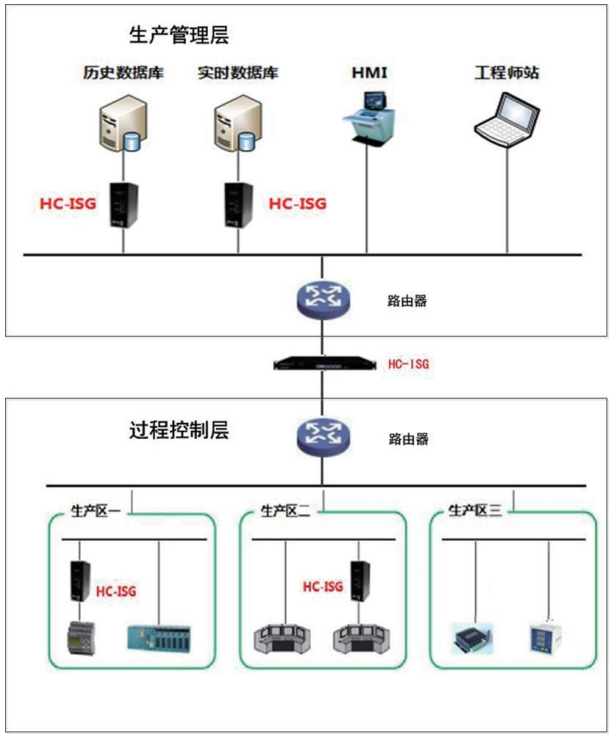
其次还可以在同一网络层次中平行的厂区、工艺流程和业务子系统之间部署HC-ISG系列工业防火墙，将它们划分成不同的安全区域，配置不同的访问规则，屏蔽不同安全区域之间不必要的访问，对不同安全区域之间的工业协议数据交换进行深度过滤，减少安全区域之间安全问题的扩散和影响。



重点设备的安全防护

在工业网络中存在很多核心的控制器、重要的数据存储和交换服务器，它们是整个工艺流程和生产过程的中枢，关系到生产能否正常、安全地进行，直接或间接影响到产品的质量。这些重点设备本身是用来完成特定生产任务的应用系统，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地访问。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。

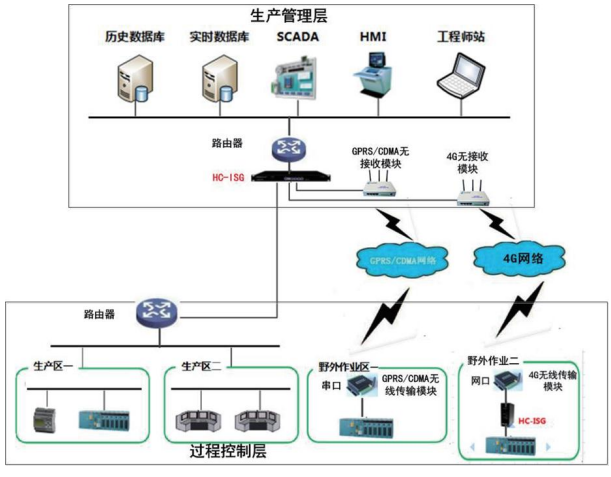
针对这些重点设备的特点，可以在其前端部署HC-ISG系列工业防火墙，限制可以访问它的IP地址、屏蔽非业务端口访问、过滤非法的操作指令、记录所有的访问和操作，对其进行全面的访问控制和安全防护。通过部署防火墙可以很好的实现对重点设备的事前安全防护、事中过滤检查和事后安全审计。



分散工业网络的安全互联

工业网络的设备可能分布于厂区各处，甚至野外、山区。由于网络基础设施的限制，经常需要通过租用公共的无线网络、卫星、GPRS/CDMA、4G等公用网络传输线路实现与调度中心的连接和数据交换。公用网络没有足够的安全保护和加密措施，很容易出现网络窃听、数据劫持、第三人攻击等安全隐患，而且攻击者还可以利用公用网络作为攻击工业控制网络的入口，实现对整个工业控制网络的渗透和控制。为了解决公用网络带来的安全隐患，用户通常都会租用或架设专用的通信线路，这样不但建设和运营成本高、而且需要专业的技术人员进行线路的保障和维护。

在这种应用环境下，可以在分散的作业区与公用网络接口的位置部署HC-ISG系列工业防火墙。通过防火墙的部署可以对作业区内部的工业网络进行安全方面的保护，阻断来自公用网络的网络攻击，实现作业区网络的边界安全防护。



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