力控科技 FORCECON | HUACON 力控华康

工业网络安全隔离网关 pSafetyLink

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，对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：

◉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。

传统安全隔离设备在工业网络环境中的不足

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。

华康工业网络安全防护网关

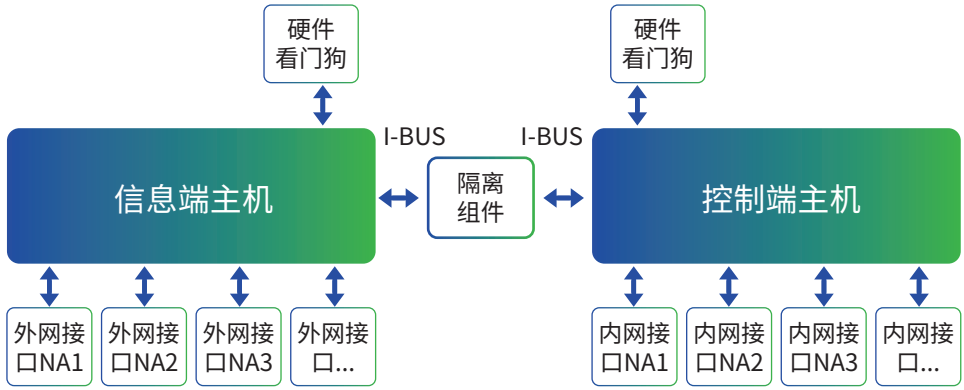
针对传统安全隔离设备在工控行业环境下应用的不足，作为国内工控行业的佼佼者，力控华康深知自己的社会责任所在。力控华康依托多年工控行业的技术积累，通过硬件和软件两方面的优化和创新，开发出了工业网络安全防护网关，不仅实现了对基于TCP/IP协议体系攻击的彻底阻断，也实现了对主流工业网络协议的广泛、深入支持和保证工业控制网络数据的安全传输，解决了传统安全隔离设备无法适用于工业控制网络的难题。

产品架构

硬件架构

工业网络安全防护网关采用“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，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。

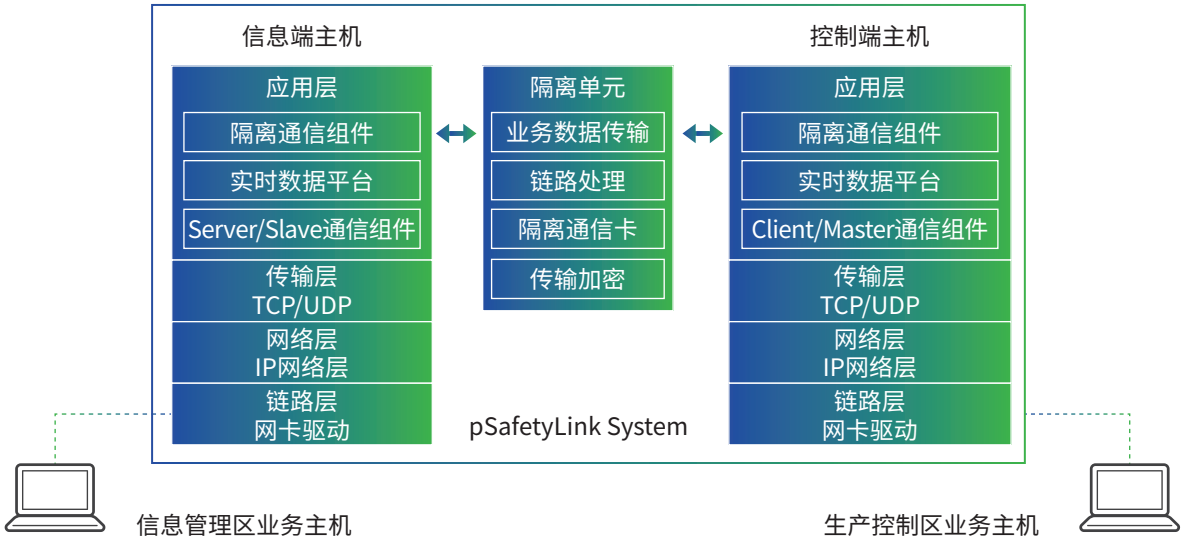
硬件看门狗实时监视系统状态，保证整套装置的稳定、持续运行。



软件架构

工业网络安全防护网关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。该系统支持各种主流工业网络协议，包括OPC DA、Modbus、BACNet、IEC 60870-5-104等，而且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信组件和中间的隔离单元三者构成了工业网络隔离系统的核心。隔离通信组件负责根据用户配置提取数据包中关键的应用层信息，并对数据进行必要的解析和安全检查；隔离单元负责使用加密的私有协议进行控制端和信息端之间的数据摆渡。



产品特点

安全性

1.自主开发工业网络隔离技术

工业网络安全防护网关的隔离技术是由硬件与软件相结合来完成的。物理层采用了两个独立高性能嵌入式主机，双主机之间采用基于总线通信的隔离装置来实现信息端与控制端之间的数据交换；数据链路层和应用层采用私有通信协议，数据流全部进行加密处理，在保证安全隔离的前提下，实现数据的高速交换。通过物理层和软件层的共同配合，彻底截断TCP连接，实现工业协议数据的定向采集和转发，达到数据完全自我定义、解析、审查，从根本上杜绝了非法数据的通过，确保控制网络不受攻击和入侵。

2.双模式数据摆渡

工业网络安全防护网关提供测点管控模式和隧道管控模式两种数据摆渡模式。测点管控模式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；隧道管控模式使用自主开发的安全数据传输方式支持数据库、SNMP管理等多样化的网络环境中的数据摆渡。

可用性

1.丰富的工业协议

工业控制网络中协议标准繁多，国际标准、国家标准、行业标准、企业标准并存，为满足工业控制网络协议多样化，工业网络安全防护网关提供了各种主流的工业网络协议接口，包括Modbus、OPC、DNP3、DLT 645、IEC 60870-5-104、西门子S7系列PLC、AB PLC、GE PLC等；当遇到不支持的私有协议时，力控华康具备专业的工控产品开发团队，可根据客户需求进行定制开发。

2.测点级访问控制

工业网络安全防护网关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 DA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。

可见范围控制可以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，可以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，从而实现了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。

3.分布部署和集中管理

工业网络安全防护网关提供了专用的配置管理工具，可以对网络中多台网关设备进行远程管理，方便用户进行集中化管控。而且配置管理工具可以自动查找网络中的工业网络安全防护网关设备，可以监控设备的网络状态、进行工程的配置和管理、查看测点数据、读取和分析设备日志。

4.数据断线缓存

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工业网络安全防护网关开发了断线缓存功能。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。

另外，工业网络安全防护网关还支持双机热备功能，在重要的网络通道上可以使用双机热备功能来保证数据链路的可靠性和持续性。

5.日志管理

工业网络安全防护网关 配有专门定制的日志管理工具，可以进行多网关日志数据同时监控、日志的清除和过滤、日志存储路径及最大存储设置（上限100万条或12月）、日志存满后自动清除或停止记录设置。

另外工业网络安全防护网关还支持多个Syslog日志服务器，可产生不同级别、类型的日志，并对日志进行管理配置。支持从信息侧或控制侧直接发送整机（两侧）的日志。

可靠性

1.硬件可靠性

◉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。

◉双侧主机均有独立硬件狗功能，时刻监视系统状态，保证设备的稳定运行。

2.软件可靠性

◉系统诊断子系统实时检测系统内各进程、线程的运行状态，当发现异常时自动产生报警信息，并在符合条件的情况下启动自动恢复逻辑。

◉I/O通信子系统具备完善的故障自动恢复功能。当发生网络通信中断的情况时，I/O通信子系统会立刻报告通信状态的变化，同时启动通信重连机制，当网络通信恢复后，能迅速重新建立网络连接，恢复数据通信。

◉具有工程备份、日志审计、双机冗余等功能。

主要功能

工业网络安全防护网关实现了控制网络与信息网络之间有效隔离，同时根据用户配置进行必要的数据摆渡。其主要功能包括：

◉支持各种主流的工业网络通信标准，包括Modbus、OPC、DLT 645、IEC 60870-5-104等，同时还提供自定义通信协议的扩展。

◉支持配置多个数据采集和转发通道，每个数据通道下配置多个设备；支持数据源和转发点之间一对一、一对多、多对一、多对多的转发。

◉支持测点的访问控制，从而提高数据采集和转发的安全性。

◉支持设备模板和点表导入功能，且提供了非常适用的模板功能，提高用户工程组态的效率，减少差错率。自动遍历OPC服务器所有测点并生成模板，也可以手动编辑模板然后导入到工程中。

◉专用的配置管理工具，具有设备自发现功能，可以帮助用户远程管理网络中多台设备，方便快捷。而且配置以工程化文件的方式存储，各设备的配置独立管理，独立分发应用。

◉具有远程监控运行状态、测点数据、通信报文、日志信息等的功能。

集成Log Server（系统日志），可以集中对日志进行存储、查询、导入和导出。

典型应用

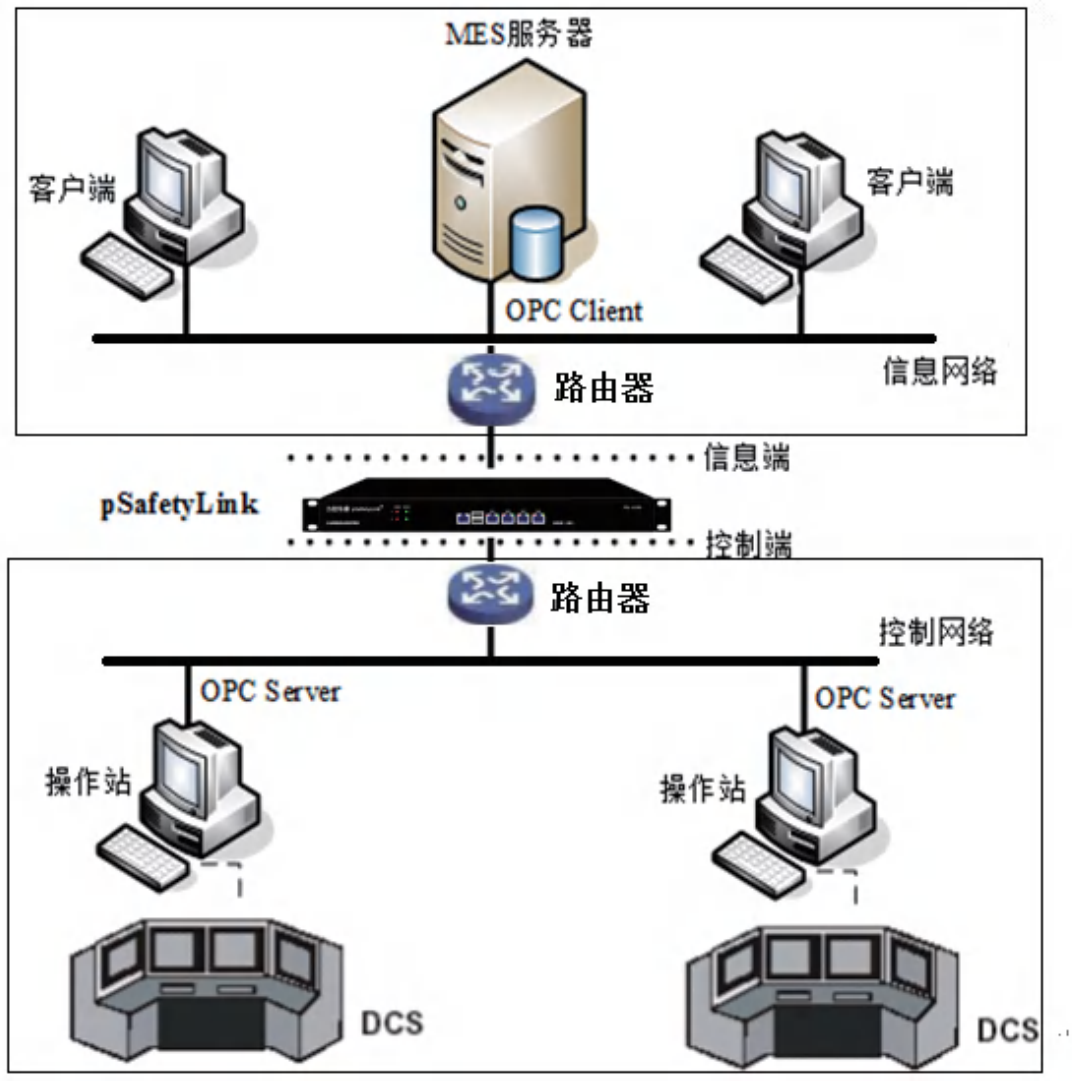
工业网络安全防护网关适用于各种控制网络的安全防护。典型应用领域包括DCS控制系统的网络安全防护、电力系统现场IED设备的网络安全防护、轨道交通ISCS的网络安全防护、煤矿、冶金行业现场控制系统的网络安全防护等。

下面分别介绍常见的典型应用场景。

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。

工业网络安全防护网关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。



基于Modbus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。

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。

工业网络安全防护网关内嵌力控华康自主定制的工业网络隔离系统，支持Modbus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