WWW.HUACON.COM.CN

HUACON

力控华康

HC-ISD工控安全审计

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

从“震网”病毒到“HAVEX”，从“BlackEnergy”到“勒索”病毒，针对工业控制网络，特别是对关键基础设施的直接攻击、信息窃取和勒索事件等工控网络安全事件层出不穷。随着“两化融合”和“中国制造2025”战略的不断推进，工业控制系统的信息化程度会迅速逐步提高，针对工业控制网络的攻击将成为一种常态，工业控制系统的信息安全将会得到前所未有的高度关注。

工控网络首先要保证可用性，无法接受“漏报”和“误报”；传统安全产品无法识别工控协议，特别是众多的私有协议；工控网络内的所有产品为了保障数据的完整性，尽可能的避免升级，而传统安全产品需要频繁升级。

传统的入侵检测和审计产品也无法满足工控网络安全的需要，但是，入侵检测和安全审计是非常必要的安全技术手段，《中华人民共和国网络安全法》中明确要求 “采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。

HC-ISD工控安全审计系统正是专门为工业控制网络量身打造的工控网络安全产品。实时监测工控网络的状态，检测工控网络中入侵行为，根据用户定义的审计策略，追踪工控网络安全事件，并对工控网络的数据进行留存。

2. 产品特点

◆ **实时工控网络监测**

默认通过旁路的方式（也可以串接）对工控网络进行实时监测，对协议、流量等元素进行统计分析，实时显示网络的状态。
具备独有的异常流量检测方法。

◆ **实时入侵检测**

实时检测工控网络中的攻击行为，利用内置的工控威胁库，根据已知的威胁特征建立检测规则，实时对网络中的入侵进行告警。

◆ **工控行为和协议规则自学习**

通过深度解析工控协议、分析工控过程行为，自动学习基于工控协议的操作行为和规则，建立安全检测模型。

◆ **不合规行为监测**

通过自定义规则或白名单规则，检测业务流量中不合规的工控网络行为，对不合规行为进行实时的告警和响应，留存网络数据。

◆ **工控协议深度检测**

支持OPC协议的深度包检测、OPC动态端口开放；报文格式和完整性检查。
支持Ethernet/IP、Modbus/TCP、IEC104、DNP3、Profinet、MMS、S7、GOOSE、SV等工控协议的深度检测，例如报文格式检查、功能码控制、寄存器控制，连接状态控制等的检测。
支持自定义格式的工控协议检测。

◆ **工控网络数据留存**

根据用户自定义设置，留存所有网络的原始数据，可配置为留存六个月及以上时间。

◆ **系统自身安全性**

基于SSL的远程管理，通过网络可以直接对工控安全审计系统进行管理和配置。通讯采用了SSL加密技术，所有配置管理信息在网络上全部以密文传输，可以防止恶意攻击者使用网络监听工具窃取信息。

系统具备网络层恶意攻击检测及过滤控制能力（如抗SYN Flood、UDP Flood、ICMP Flood，抗Ping of Death、Smurf、Land attack攻击等）。

基于角色的分权分级管理，有利于减少对系统的滥用。

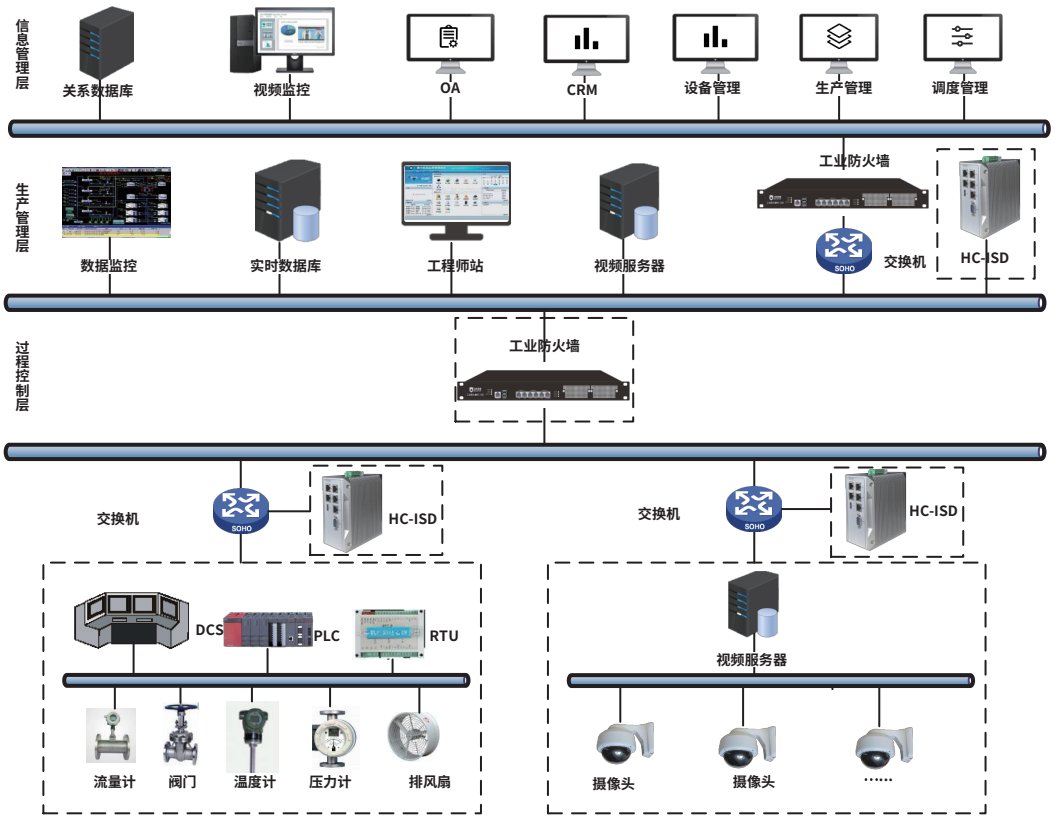
◆ **安全审计及响应**

对安全事件进行审计，及时追溯安全事件的轨迹。

对用户的操作行为进行细粒度审计，方便还原操作的真相。

独立的告警响应机制，可定义对不同安全级别的安全事件的响应方式。

3. 典型部署



广泛用于油气、石化、市政、环保、交通、烟草、智能制造、能源（电力）、冶金等各行业客户。为行业客户的工业控制系统提供适当的安全监测与审计，提升其工控网络的安全防范能力。

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