中数国科工业安全隔离装置

产品白皮书

（中数国科集团有限公司）

■ 版权声明

产品部

2024 年 1 月

变更记录

序号	版本	变更记录	修改人/日期	检查人/日期	审批人/日期
1					
2					

目录

一、前言

近年来，随着信息技术的不断发展，能源、冶金、化工、制造、轨道交通等国家关键基础设施除了大量的应用自动化技术之外，还在应用信息系统技术提升生产业务的管理效率，如 MES、ERP 等。国家关键基础设施关系到国计民生，其安全问题一直是国家有关部门关注的重点。

随着通信技术和网络技术的发展，一方面，Internet 技术和因特网得到广泛使用，E-mail、Web 和 PC 的应用日益普及，但同时病毒和黑客也日益猖獗。另一方面，目前工控生产网一端在规划、设计、建设控制系统和数据网络时，对网络安全问题重视不够，使得具有实时远程控制功能的系统，在没有进行有效安全隔离的情况下与管理网的 MES/ERP/MIS 等系统或其他数据网络互连，引发对生产网安全运行的严重隐患。

按照国家发改委的 14 号令规定与国家能源局第 36 号文相关指导性方案，以及工信部发布的《工业控制系统信息安全防护指南》等政策指导文件均对工控企业生产网络防护有很高的安全要求，并提出了相应的解决方案。

二、产品概述

中数国科工业安全隔离装置（以下简称“工业安全隔离装置”）由内、外网处理单元和安全数据交换单元组成。安全数据交换单元在内外网主机间按照指定的周期进行安全数据的摆渡。从而在保证内外网隔离的情况下，实现可靠、高效的安全数据交换，而所有这些复杂的操作均由隔离系统自动完成，用户只需依据自身业务特点定制合适的安全策略既可实现内外网络的安全数据通信，在保障用户信息系统安全的同时，最大限度保证客户应用的方便性。

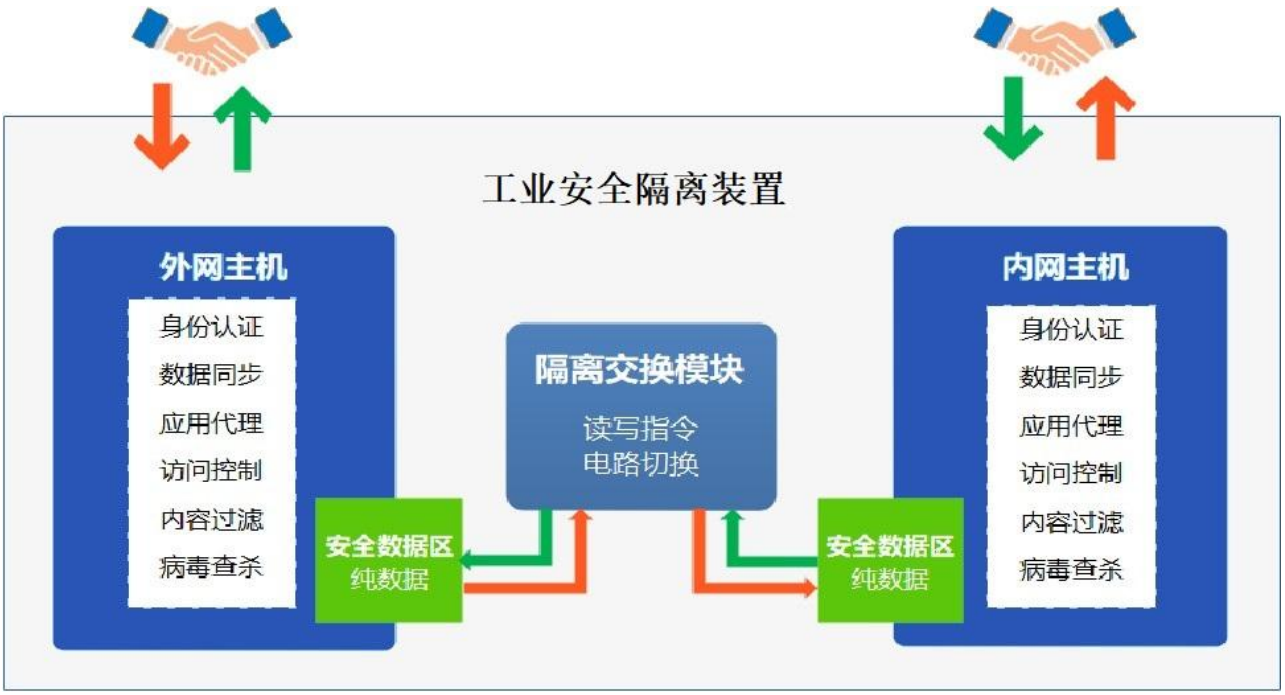
工业安全隔离装置采用专用的安全通道进行内外网信息交换，业务数据通过物理隔离、协议隔离、内容隔离等措施使外网网络数据及有害数据信息无法进入内网。工业安全隔离装置采用双重安全防护机制，白名单的防护机制保护客户业务系统免于遭受各种已知的安全风险和未知的安全隐患，内嵌的防病毒、入侵检测引擎为用户提供第二层保护，识别已发现的各种病毒和入侵时示警并记录日志。工业安全隔离装置采用具备丰富工业协议的采集与转发模块进行工业数据采集与转发，保障工业生产环境安全、高效的运行。

防止穿透性 TCP 连接：禁止两个应用网关之间直接建立 TCP 连接，将内外两个应用网关之间的 TCP 连接分解成内外两个应用网关分别到工控专用隔离工业安全隔离装置内外两个网卡的两个 TCP 连接。

三、关键技术

中数国科工业安全隔离装置对于接收到的任何外部会话连接，首先通过外网主机网络接口将会话终止，然后利用协议解析模块将 TCP/UDP 数据格式打破，并采用专有的封装协议将分解得到的数据打包后通过隔离开关传输到内网主机。在内网主机数据经过一系列安全检查之后，协议解析模块对数据重组，并在内网主机网络接口将重构的会话传送到内部服务器。

对于从内部到外部的 TCP 连接，中数国科工业安全隔离装置也具有对等的处理方式。事实上中数国科工业安全隔离装置已经将原来直接连通内外网络的 TCP 连接，从逻辑上分解为外网到工业安全隔离装置外网主机的 TCP 连接、外网主机到内网主机的专有封装协议连接、内网到内网主机的 TCP 连接的组合。因此，在添加中数国科工业安全隔离装置之后，可以阻断内外网络之间的 TCP 对话，其结构如图所示：

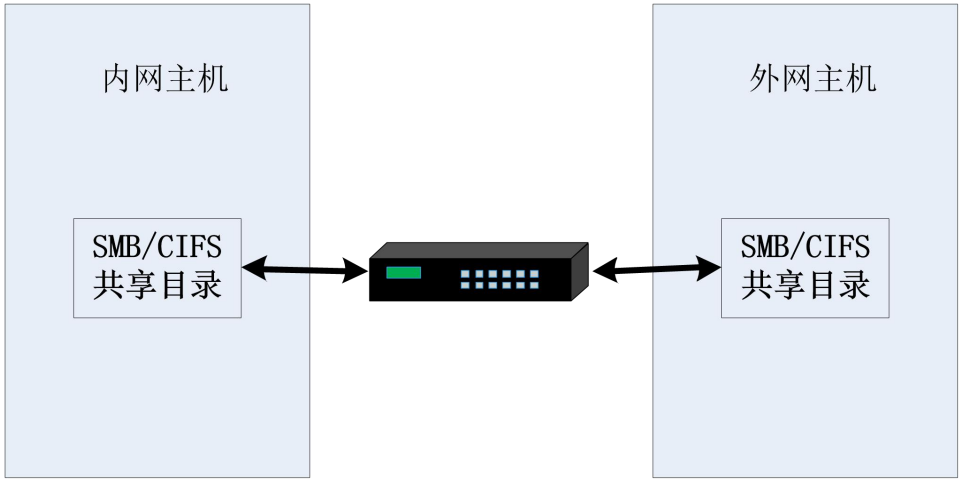


值得提出的是，中数国科工业安全隔离装置不但在逻辑上终止了 TCP 对话，还从物理上断开了内外网络之间的连接，使得内外网络之间在任何时候都不存在直接的物理层

和链路层连接通路。

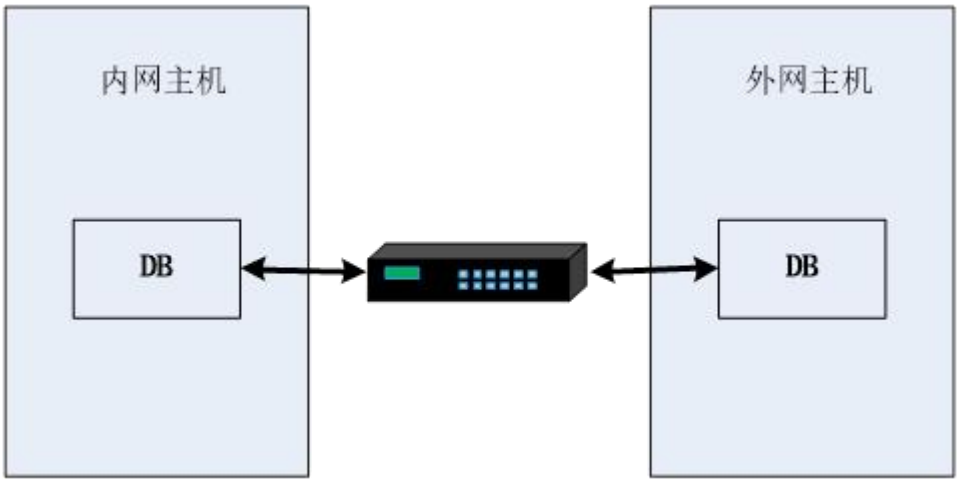
中数国科工业安全隔离装置技术的关键技术要点如下

文件交换



工业安全隔离装置主动抓取两侧共享目录中的文件，按设定的规则方向，做定时同步。支持单向（内到外或外到内）、双向、一对一、一对多、多对一的同步，支持文件后缀名过滤、防病毒功能，支持同步文件备份（即在同侧设定的备份目录下备份将要同步的文件）。

数据库同步



工业安全隔离装置主动抓取两侧数据库信息，按设定的规则方向，做定时同步。支持单向（内到外或外到内）、双向同步，支持同构、异构数据库同步，支持同步插入、同

步删除、同步更新。

四、产品功能

工业安全隔离装置作为生产非控制区与生产管理区必备的边界安全隔离设备，具有最高的安全防护能力，是生产防护的要点，主要功能有文件同步、数据库代理、数据库同步、音视频交换、组播代理等功能。

4.1. 隔离功能

实现两个安全区之间的非网络方式的安全的数据交换，并且保证内外两个处理系统不同时连通；

应用数据的单向传输，即从生产非控制区向生产管理区的生产数据单向上报；

实现两个安全区之间的非网络方式的安全的数据传递；

防止穿透性 TCP 连接：禁止两个应用网关之间直接建立 TCP 连接，将内外两个应用网关之间的 TCP 连接分解成内外两个应用网关分别到工控专用隔离工业安全隔离装置内外两个网卡的两个 TCP 连接。并具有可定制的应用层解析功能，支持应用层特殊标记识别。

4.2. 管理功能

4.2.1. 安全通信

工业安全隔离装置只允许从设备的管理控制端口进行管理，在通信端口不接受任何管理请求，避免了管理信息的旁入可能。管理者与工业安全隔离装置间采用加密的 HTTPS 协议进行交互，避免各类监听工具获取通信内容，保障管理信息的安全性。

4.2.2. 权限分配

工业安全隔离装置采取系统管理员、安全保密员、安全审计员三种角色分立的权限分配模式。各类用户只能维护本角色的功作，三员权限分立并相互制约。同时提供用户管理功能，

可分配相应的权限给特定用户，使用户管理更加方便且易于理解。

4.2.3. 策略配置

工业安全隔离装置采用图形化策略定制方式，即便是初次使用的用户也可依据界面向导，依次制定适应实际网络的交换策略。

4.2.4. 日志审计

工业安全隔离装置提供强大的日志和审计功能，日志默认存储在设备中，支持通过SYSLOG将日志发送到日志服务器，为日志审计提供了很好的数据支撑和便利性。日志内容完整记录并保存系统设定、通信控制、内容检查、连接限制、系统告警等各类信息。

审计模块可以多种方式进行查询、审计，并生成报表。系统具有日志告警信息的导入、导出、备份等功能，保证了日志告警信息的安全性与易用性。

4.3. 安全功能

产品支持OPC、Modbus TCP（ASCII/RTU）、IEC104、DNP3、SIEMENS S7、PROFIBUS/DP、PROFINET、PI、PHD等常见工业通信协议的深度检测、指令、功能码的控制。并且系统可通过导入协议分析模块来支持更多的工业通信协议的控制。系统也可对特定的功能码或通信内容做白、黑名单的内容过滤。

基于MAC、IP、传输协议、传输端口以及通信方向的工控协议报文过滤与访问控制，支持主流的OPC、Modbus、IEC-104、DNP3、MMS、IEC-61850等主流工控协议和电力单向1bit反馈传输协议；工业协议均支持信令控制与参数值域的控制，如只允许读，不允许设置等；支持常见工业电视等视频协议的传输。

动态适应OPC.DA：

OPC作为一种广泛应用于工业标准协议，为现场设备、自动控制提供了开放、统一的标准接口。但是由于OPC协议在建立之初，工业环境尚未联网等原因未考虑到网络安全问题。OPC.DA基于WINDOWS的DCOM组件进行分布式通信，WINDOWS系统的DCOM组件对环境依赖较

大，只支持在 WINDOWS 部署，并且采用 RPC 远程进程调用接口，业务通信端口随机，传统安全产品无法防范，存在很大的安全隐患。但是工业应用现场环境一旦建立不能轻易发生变更，因此这些隐患一直伴随着客户业务系统的存在而存在。

工业安全隔离装置作为一款工业专用的网络安全防护产品，其采用深度协议解析，并动态适应 OPC.DA 的随机业务端口，不会像传统防火墙类产品开启范围端口，从传输层杜绝了安全隐患。其次在 OPC 应用层安全上，依靠深度解析 OPC 协议，可识别信令、方法等参数，实现 OPC 只读控制等信令级的控制功能。

应用深度控制：

工业安全隔离装置采用高性能、可扩充的协议分析算法，深度识别、解析大量工业专用协议，并可依据不同的业务场景、不同的协议类型，进行相应的深度控制。如典型的 Modbus 协议，管理员可轻松在界面上定制相应的信令控制规则，控制内容包括功能码、地址范围、线圈值域等。

4.4. 高可用性功能

4.4.1 负载均衡

工业安全隔离装置支持两种方式的负载均衡功能：

- **基于带宽：**采用专有均衡算法，将大量的业务请求平均分配到各个安全区隔离，从而获得成倍的性能提升，适用于大流量、高负载的应用场合。
- **基于应用：**采用专用设备对各种网络请求进行预分流，将不同的网络应用交由不同的隔离设备处理，不仅实现性能的增长，同时也实现了应用分离与控制，加强安全性和可靠性。

4.4.2 双机设备

工业安全隔离装置提供双机热备功能，两台设备可组成热备组，组内设备有主设备与从设备之分，主、从设备之间使用心跳报文检测设备状态，并获取最新的访问策略，当主设备

发生故障，从设备会立即接替工作，从而避免影响用户业务系统正常使用，同时以声音与告警信息示警。如下图所示：

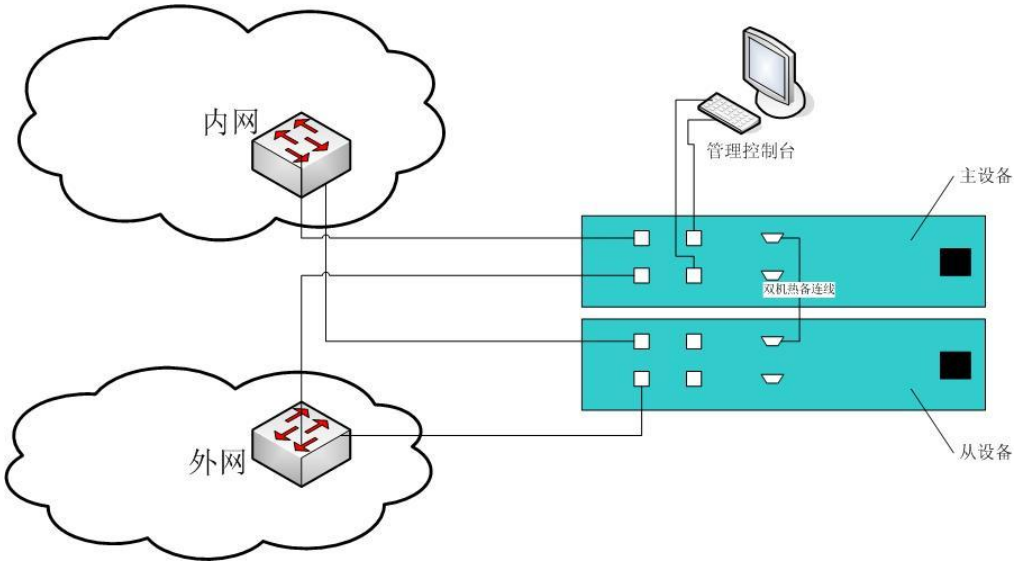


图 3.4 双机热备

4.5. 双协议栈支持

工业安全隔离装置支持纯 IPv4，纯 IPv6，IPv6 到 IPv4，IPv4 到 IPv6 等网络环境，支持 NAT6，NAT6to4 功能，可实现混合网络代理功能。

工业安全隔离装置内置的访问控制模块、文件交换模块、数据库同步模块、WEB 代理模块、组播模块全部支持 IPv4、IPv6 双协议。

4.6. 数据采集与转发

4.6.1. 主动采集工控协议采集

支持 OPC、 Modbus、 BACNET、 MQTT、全系列工业标准、全系列工业 PLC、全系列电力规约、全系列能耗规约的采集。

4.6.2. 协议转化及发布

通用标准、电力协议、OPC DA/UA(Linux)、BACNET 等十余种。大数据、工业云平台、行业定制。

4.6.3. 断点续传

支持工业云平台断点缓存，包括：住建部能耗规约(上、海)、建筑能耗/大型公建 xml（压缩加密）、MQTT 客户端、ICP_MQTT_LITAI 等。

4.6.4. 数据限制报警

中数国科工业数据采集模块支持对标签进行高限、低限、高高限、低低限等限制的报警值设置，可将超过设定值得报警限制通过报文的形式提供给上层平台。

4.6.5. 工程管理功能

工程管理、采集服务配置、数据服务配置、变量属性配置、简单 Java scrip 脚本操作、采集服务建立连接时可做主被动响应、备份工程、工程的上传下载、点位批量操作、点位系数计算、点位值报警值设置。完全适应工控人员操作惯性。

4.6.6. 部分协议列表

工业协议采集	通用标准	通用标准：BACNET IP、南瑞 DZ_NR_GAP_03、DZ_OPC_LINUX、CAN_TO_TCP、JT188_2004、modbustcp、opc da 客户端、OPC 客户端（异步通讯）、SNMP。 电力行业标准：376.1 主站、CDT91、DLT_645_07、DLT_645_97、IEC_101、IEC_103、IEC_104、IEC_104_EX、IIEC_61850、IEC_BALANCE_101。 PLC：AB_LOGIX_CIP、AB_LOGIX_5000TCP、德国倍福、GE_TCP、_MITSUBISHI_FX、MITSUBISHI_FX_TCP、MITSUBISHI_Q_TCP、MITSUBISHI_Q_TCPIP(3E)、NAIS_NEWTOCOL、OMRON_FINS_NET、OMRON_HOSTLINK、S7_1200_TCP、S7_1500_TCP、S7_200_SMART、S7_200_TCP、S7_300_TCP、S7_400_TCP。 大数据（包括但不限于）：断线缓存、mysql 客户端、redis 客户端 继电保护：南瑞网络 103、南自网络 103、磐能 103 智能楼宇：HPHW5 清华同方热泵热水集线器 CNC 机床：发那科机床、三菱机床、西门子机床、广数机床、新代机床、凯恩帝机床、兄弟机床
数据服务	通用标准	ALARM_SHORT_MES(短信报警)、376_1_SLAVER、ELE_CDT91、IEC_101、IEC_104、IEC_104_DZ(104 定制)、IEC_61850、IEC_61850_S、EMSERVICEPOST、HTTP_SERVER、101_NZ（101 南瑞）、IEC_60870_5_101_HN、BACNET、数据触发器、

		MODBUS_TCP、MODBUS_TCP 注册版、OPC_UA 服务器（linux）、SNMP_代理、OPC DA (Linux)。
	PLC	S7_1500_TCP、西门子 PLC 同步数据
	大数据	支持未正常传输的数据在网络恢复后，可断点续传
	工业云平台	百微蓝 HTTP、数据中心、中联环境、建筑能耗/大型公建 xml、住建部能耗规约(上、海)、建筑能耗/大型公建 xml（压缩加密）、演能科技、环保 212 协议、环保 212 协议（实时数据）、豫环明电、南乙环境、微软云、mqtt 客户端、ICP_MQTT_LITAI、断线缓存协议、腾讯微瓴、太阳能供水（定制）、数据报警/历史存储、中信
	行业定制	IEC-61850、亿百维设备管理平台、楼宇群控、http 数据推送、数据积分、莫迪康、NR_GAP_01（南瑞）、国网 I2、国网加密、
	定制开发	CACHE_CSV（莫迪康）
	定制 MQTT	mqtt 客户端（灵活数据类型版）、福州自来水
	MQTT	华为云、微软云、物联网（CACHE_V2）

五、产品亮点

5.1. 高安全性

工业安全隔离装置采用专有的安全操作系统，安全 OS 存贮于 DOM 中，无法被恶意修改，具有极高的安全性。系统内置高性能安全过滤引擎，可防止 Dos 和 DDos、缓冲区溢出、恶意编码、应用层洪水等攻击。

工业安全隔离装置采用专用的安全通道进行内外网信息交换，业务数据通过物理隔离、协议隔离、内容隔离等措施使外网网络数据及有害数据信息无法进入内网。工业安全隔离装置采用双重安全防护机制，白名单的防护机制保护客户业务系统免于遭受各种已知的安全风险和未知的安全威胁，内嵌的防病毒、入侵检测引擎为用户提供第二层保护，识别已发现的各种病毒和入侵时示警并记录日志。

5.2. 低延迟性

工业安全隔离装置的内、外网处理单元采用工控级低延迟处理机制，整机网络延迟小于 1ms，内部处理延迟小于 10ns，可满足工控环境对于实时性、低延迟的要求。

5.3. 高吞吐率

工业安全隔离装置的内、外网处理单元采用复杂对称多处理（RSMP）技术，在一台设备内集成多各处理模块，提升设备处理能力，使工业安全隔离装置具有很高的性能。

5.4. 高可靠性

工业安全隔离装置在硬件结构上采用专用工控安全主板设计，进一步提高了隔离系统的可靠性。工业安全隔离装置配置双电源供电，可在单电源掉电情况下自动告警，并稳定运行。双机热备的部署方式可使系统抵抗灾难性损坏时的可靠性成倍提高。

5.5. 高便利性

工业安全隔离装置为方便管理员使用，在出厂设置已提供了一套适合多数网络环境的常

用安全策略，管理员用户只需要将设备对应的 IP 地址修改为实际网络中的 IP 地址即可。日志用户与策略配置用户的权限分立以及层次化的权限划分允许用户可将各类管理工作交由不同的用户来完成，与管理需求相吻合。管理员用户及访问用户以及众多的日志审计记录均实现可导入导出操作，大大加强的工业安全隔离装置的便利性与可操作性。

六、应用场景

6.1 钢铁行业场景

6.1.1 安全需求

办公网与生产网边界对值守站隔离，杜绝外网非法威胁到生产网（炼钢厂等）的控制设备。

6.1.2 解决方案

工业安全隔离装置部署在办公网与生产网边界对值守站隔离，外网无法威胁到生产网（炼钢厂等）。

部署工业安全隔离装置，实现分层级的高安全隔离，抵御已知与未知威胁。工业安全隔离装置除了能主动采集 OPC Server 数据外，并能把采集后的数据进行单向上传至 MES 系统，并且通过配置做到数据零反馈，无任何数据返回工控网络中

6.1.3 方案价值

1.符合等保 2.0 三级要求:“工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。”

2.分级部署工业安全隔离装置进行防护，阶梯防护。

3.实现业务数据传输,做到业务数据零反馈，满足业务需求。

6.2 石化行业场景

6.2.1 安全需求

处于管理区的外网病毒经过与生产区的网络传输到内网侧,导致网络病毒在内网的泛滥,最终导致石化生产设备的故障。

6.2.2 解决方案

在 OPC 服务器与管理层之间部署中数国科工业安全隔离装置,实现分层级的安全防护,抵御已知威胁;在管理网/MES 和生产网之间部署中数国科工业安全隔离装置,避免管理网/MES 遭受攻击后威胁到生产网;

6.2.3 方案价值

1.符合等保 2.0 三级要求:“工业控制系统内部应根据业务特点划分为不同的安全域,安全域之间应采用技术隔离手段。”

2.工业安全隔离装置结合工业防火墙，提高对生产控制区的安全防护力度。

3.实现业务数据传输,满足业务需求。

6.3 油气运输场景

6.3.1 安全需求

处于办公楼与总调的外网病毒经过与生产区的网络传输到内网侧,导致网络病毒在内网的泛滥,最终导致运输设备的故障。

6.3.2 解决方案

在 DCS 生产控制网络的交换机与内部办公网络的交换机之间部署中数国科工业安全隔离装置,可以保障 DCS 生产控制网络在安全隔离的情况下,将生产数据安全的传输至处在内部办公网络的数据库服务器中,为决策提供数据支撑;

6.3.3 方案价值

1. 保障工控区生产持续进行。

2.能够采集生产区的油气流量、管道压力、生产数据、视频数据等信息，并将其数据传输给总调区进行查看。

3.符合等保 2.0 三级要求:“工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。”

6.4 在线监控场景

6.4.1 安全需求

外部入侵：监控中心实时查看工业数据，监控中心和工业网络互连有可能导致入侵者通过监控中心到工业控制网络，针对工业控制系统进行攻击。

病毒爆发：监控中心出现病毒，有可能会传播到工控系统中，导致病毒在工控系统网络中爆发。

6.4.2 解决方案

企业端：通过部署中数国科工业安全隔离装置实现企业生产网与专线网端的隔离。

企业安全参数采集：企业通过 ODBC、Modbus、OPC 等方式提供安全参数数据，传输到监控中心。(1:可燃、有毒气体浓度 OPC 服务。2. 罐内介质的液位、温度、压力通过 DCS 提供 OPC 服务)

企业视频图像采集：监控中心采集企业视频图像。（罐区、罐顶、高空瞭望、应急救援物资储备库视频和中控值班室音视频）

监控中心：市局通过监控中心监控企业实时数据和视频图像。

企业通过监控中心进行生产控制，通过安全管理中心进行安全控制

6.4.3 方案价值

1. 满足视频监控，业务数据采集与上传。

2.符合等保 2.0 三级要求:“工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。”