中数国科工业数据采集与单向上传系统

产品白皮书

（中数国科集团有限公司）

■ **版权声明**

产品营销部

2022 年 4 月 20 日

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

目录

一、前言

在“两化融合(信息化和工业化)”的科学发展推动和激烈的市场竞争形势下，越来越多的工业控制网络和信息网络连接在一起。比如 MES 系统从生产网络采集数据，这种应用使得工控网络自身的安全漏洞突显出来，传统物理隔离的工控生产网络已经不能作为一个独立的信息孤岛存在。自身原本存在的安全隐患例如不能及时更新操作系统、没有杀毒软件、使用未验证的通信协议、使用默认的密码、工控厂商的远程维护等。

在一个充满病毒、黑客、罪犯和恐怖分子的世界里，工控网络这些脆弱的漏洞赤裸裸地暴露给潜在的攻击者。实践表明，来自工厂信息网络、移动存储介质、因特网以及其它因素导致的网络安全问题正逐渐在控制系统中扩散，直接影响了工业生产的稳定与安全。

Stuxnet 病毒与乌克兰国家电网受到黑客攻击而大面积断网作为标志性的事件，证明网络虚拟空间与现实空间的融合的越来越紧密，工业系统的网络安全成为国家安全的重要环节。工业网络安全已经成为与传统的战争威胁、恐怖主义威胁相当的问题。因此，未来的世界，工业企业的网络，尤其是关键基础设施的安全问题是一个关系到国家核心利益的问题，必须重点关注，并采取切实的行动。

目前市场上存在的安全产品均无法解决既保持原有工控生产网络隔离又同时可以实现生产数据的绝对单向上传。同时 GB-T 22239-2019 信息安全技术_网络安全等级保护基本要求-正式稿（20190517）(即：等级保护 2.0)中明确增加了工业控制系统与办公网数据交互时需要

单向的隔离技术，所以市场急需一种能够真正解决用户安全需求的产品出现。

二、产品概述

中数国科工业数据采集与单向上传系统（以下简称“数采光闸”）是中数国科集团有限公司独立自主研发，采用多核多线程并行安全操作系统，实现 Linux 系统下采集工业数据并单向导出数据的安全产品。具有主动采集生产数据、组态、以对外提供数据服务等功能，可主动采集工控网的实时生产数据，并将数据绝对物理单向地导出至管理网（或工业云平台）的对接平台。产品基于“2+1”的硬件架构，利用光信号的单向传输特点，将数据绝对单向地传输到管理网，从而屏蔽了安全威胁从管理网络向生产网络传输的风险。

产品同时支持断点续传功能，当网络产生故障时，数据可在设备中做缓存；当网络故障恢复时，可以将缓存数据提供给数据接收方。

三、产品功能

中数国科工业数据采集与单向上传系统的主要作用是实现工业实时数据采集后单向上传，主要体现在以下几个方面：

3.1 绝对物理单向安全隔离

采用双主机系统架构，内置自主知识产权的多核多线程并行安全操作系统，利用光器件的发光与收光模块的特性，实现数据的物理单向传输。

3.2 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。

3.3 工业协议转化、数据发布

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。

3.4 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。

3.5 无需 OPC 桥接程序

因工业现场系统比较敏感，客户通常不允许任何人操作、调整正在运行中的系统。中数国科数采单向光闸可以规避此类情况，无需触碰用户系统，只要网络可通，就可以实现数据采集。

3.6 实时数据限制报警功能

中数国科工业数据采集与单向上传系统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。

3.7 通讯类型管理

可选 TCP、UDP、虚拟端口可做主被动区分，可设置允许客户端进入列表。

3.8 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。

3.9 安全管理

操作系统自主可控，具有主机安全，可对访问主机的用户进行严格管理，并提供安全策略配置工具，防止自身被攻击破坏。

四、产品亮点

4.1 继承传统光闸所有功能

中数国科工业数据采集与单向上传系统由中数国科工业数据采集与单向上传系统演变而来，具有中数国科工业数据采集与单向上传系统的所有功能，文件交换、数据库同步、数据单向传输、邮件中继、组播代理、DTCP 功能、校验传输、访问控制、三权分立、安全管理、系统监测、SNMP、日志分类、日志导出、双机、多机热备支持、负载均衡。

物理单向：中数国科工业数据采集与单向上传系统由内网处理单元、外网处理单元和光单向传输单元三个物理部分组成。光单向传输单元采用发光器、单向光纤、接收器实现物理单向。

协议隔离：中数国科工业数据采集与单向上传系统的内网处理单元、外网处理单元均采用了我司具有自主知识产权的安全操作系统，各自独立完成网络协议的终止。使内外网业务系统无法直接建立通用协议会话，从而阻断以共有协议为载体的风险传递。

应用隔离：中数国科工业数据采集与单向上传系统采用应用解码技术，客户传输的应用数据经过模块编码验证，只有符合白名单编码规则的数据才可被传输至内网处理单元。

内容隔离：外网处理单元在将数据传输至内网处理单元之前，会将待传输的数据进行内容检查与病毒查杀，不符合安全规定的数据会被直接删除，只有合法的数据才被允许交换至内网处理单元，从而保证了数据内容的安全性。

风险隔离：中数国科工业数据采集与单向上传系统支持白名单机制+防病毒双重防护机制。白名单仅允许用户许可的应用数据通过，防范了未知的安全风险；系统集成的防病毒模块可扩展多种常规安全防护引擎。双重防护机制在最大程度上实现了风险隔离，保证了数据传输的安全性。

4.2 自研 Linux 系统可适用于 OPC DA/UA，更安全

内外预置 Liunx 操作系统，模拟 Windows DCOM 配置过程，不依赖 Windows 形成 OPC DA Server，自身安全性更高。

4.3 内网采集 OPC DA Server 无需 OPC bridge

LINUX 环境下集成了 OPC 桥接程序，客户数据源无需再安装桥接程序，只需保持网络连

通性即可与中数国科工业数据采集与单向上传系统内网通讯。

4.4 对接工业云平台支持断线续传功能

可选择是否开启断线续传功能，且可以选择存储路径、存储周期、是否加密等等功能。

4.6 专用硬件设计高可靠

中数国科工业数据采集与单向上传系统在硬件结构上采用专用安全主板设计，进一步提高了隔离系统的可靠性，使单向光闸设备可在超重负荷的环境下长期稳定运行。在实施中，配合双机热备的部署方式可使系统抵抗灾难性成倍提高。

五、应用场景

5.1 OPCDA 采集与发布

钢铁行业控制系统内存在 OPC Server 通讯。中数国科数采单向光闸在生产控制网与数采网之间，数采网中的 OPC Clinet 可用过数采单向光闸访问到生产控制区中的 OPC Server。内网主动抓取生产网内 OPC Server 数据，推送至外网，外网形成 OPC Server，等待客户访问。数据只能从生产控制区推送到数采网，数采网只能访问数采光闸的外网数据，无法下置任何数据到生产控制区。

5.2 与工业防火墙结合

工业现场存在不同控制区之间控制器 IP 冲突的现象，使用工业防火墙进行 NAT 转化后，破解 IP 冲突的问题。数采单向光闸内网采集 NAT 转换后的 PLC IP 地址，外网侧形成客户需要

的数据服务供客户采集。产品集合使用，既不用更改现场控制器 IP，又可做到区域的隔离。

5.3 对接工业云平台

中数国科工业数据采集与单向上传系统支持不同的云平台对接：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、中信云。

5.4 对接关系数据库

中数国科工业数据采集与单向上传系统部署在生产控制区和数采网之间，中数国科工业数据采集与单向上传系统内网采集生产控制区的数据，外网形成关系数据库例如 MySQL、非关系型数据库 REDIS 等。