中数国科

工控主机接口管控系统

产品白皮书

（中数国科集团有限公司）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号 v21.1	■ 日　　期
■ 撰 写 人	■ 批 准 人

cdtc@cdtc.com.cn

■ **版权声明**

产品部

2025 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					
3					
4					

目录

1. 前言

经过多年的信息化与网络安全建设，大多数企业和组织已经从安全的局部建设进入到了整体优化阶段。当前的客户更加关注全网的整体安全，强调从业务信息系统安全风险的角度，而非从单一安全威胁和防御机制的角度，去更加主动地管理网络安全。而要做好整体的网络安全管理工作就需要一套相应的安全管理体系，在这个体系中除了组织保障和流程保障以外，很重要的一点就是技术保障。

同时，随着《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）标准的发布和实施，对于网络安全管理中心提出了明确的要求，二级及以上级别的等保系统都需要建设网络安全管理中心。

智能制造是制造强国建设的主攻方向，其发展程度直接关乎我国制造业质量水平。发展智能制造对于巩固实体经济根基、建成现代产业体系、实现新型工业化具有重要作用。世界处于百年未有之大变局，国际环境日趋复杂，全球科技和产业竞争更趋激烈，大国战略博弈进一步聚焦制造业，美国“先进制造业领导力战略”、德国“国家工业战略 2030”、日本“社会 5.0”等以重振制造业为核心的发展战略，均以智能制造为主要抓手，力图抢占全球制造业新一轮竞争制高点。

智能制造加工有高复杂、精密、高稳定性、特殊材料等特点，制造需求有高精度、多轴、高速等。但我国高档数控机床产品的使用寿命、性能、稳定性还远不如进口机床，市场长期被欧日美企业垄断，进口依赖度超过 90%。在高档数控系统领域，我国产品的使用寿命、性能、稳定性还远不如进口机床。重要制造领域使用的高端机床需要通过许多掩护才能成功进口我国，高端制造发展受制于人、被断供和卡脖子的形势依然非常严峻。进而，一些关键制造企业一般都是采用断网加工、断网保存的老办法，无法顺应“信息化和工业化”、“智能制造”、“工业互联网”等产业升级和发展趋势，严重制约智能制造高质量发展。

智能制造主要存在产品生产线设备安全接入、网络互联互通和智能化集成安全、生产线加工无差别精准执行、生产过程动态智能调度及状态数据安全审计等迫切需求。高端制造相

关单位的研发设计和经营管理类应用系统一般都部署在高密级网络环境，与部署在低密网络环境的 DNC 数据采集、MES、供应商协同、客户服务等应用系统物理隔离。在智能制造、工业联网、数据集成的背景下，智能制造企业需要构建全新的适应新时代要求的安全保密观，基于新的安全保密管理制度和技术手段，在满足国家安全保密要求的前期下，实现涉密与非密系统数据的集成应用。

2. 现状及问题

- 高端设备依赖国外，存在供应链后门

我国智能制造领域大量使用的高端数控机床、高端 PLC 以及操作系统、底层工具、协议大多依赖日本、德国、法国和美国供应。这些设备、工具等存在 GPS、远程控制、数据传输等后门的可能。后门程序可能包含有远程锁死产品使用权限、私自存储和上传数据等功能。因为有专门收发装置，有时即使断网也依旧能够偷偷连接网络发送信息，严重影响国家安全。

- “黑盒子”设备难于监管，安全管控复杂

国外厂商的设备只开放了其生产的必要接口和功能，我们对于其内部的运行原理和工作过程无从了解，且 NC 程序或者编程平台等上位机软件也来自国外，因此高端机床作为“黑盒子”设备难以进行安全审计、难以实施端口管控和防病毒等措施，进而导致设备面临恶意操作、感染及传播病毒、信息泄露等风险。

- 设备类型多样导致巨大管理难度

工业控制设备所使用的设备厂商、操作系统、传输协议、计算机语言多样，现有安全防护产品仅能实现对部分工控设备的局部防护，造成安全防护与监管难度大。

- 高隐蔽性业务操纵和供应链渗透攻击

大国战略博弈进一步聚焦制造业，针对工业网络的攻击行为日益呈现出专业性和严密的组织性，属于典型的 APT 攻击。业务操纵和供应链渗透是高隐蔽工控网络攻击的两类核心攻击手段。高隐蔽业务操纵可以篡改控制器运行逻辑或者虚构被控对象运行状态，可操纵工控设备在不触发故障报警的“安全临界状态”或“部件高损耗状态”下持续运行；高隐蔽供应

链渗透可利用供应链厂商自身的网络安全漏洞和管理漏洞入侵厂商内网，实现对产品的恶意代码预埋；攻击者还可针对特定产品的固件漏洞定制化开发新型恶意代码，实现针对特定产品的大规模恶意代码感染。而且目前部分制造企业的文件传输是采用 U 盘拷贝方式或无认证和加密的网络传输方式，大大增加了病毒感染、被网络攻击可能。震网病毒就是采用 U 盘传入伊朗铀浓缩工厂的离心机控制网络。

3. 产品概述

针对工控网络中数控系统与外界信息交互越来越紧密，网络威胁越多，另外一些关键文件（NC 文件）通过 USB 接口、串口传输到数控终端系统，存在安全隐患。我司自主研发了针对数控系统的安全设备“中数国科工控主机接口管控系统”，以下简称“机甲卫士”，该产品通过对网口、串口及 USB 口的多重安全防护，从而防止外部威胁对数控系统的侵害。与之搭配的“管理平台”可统一管理“机甲卫士”设备。

机甲卫士与数控终端一对一接入，对终端设备的所有通信端口进行全方位数据防护，及在线状态监测，识别非法接入数控终端的设备，并进行实时报警。

管理平台部署在工控网络机房中，通过独立的管理网络与设备通信，机甲卫士的策略配置、软件更新均可通过管理平台进行统一下发，同时机甲卫士系统的日志信息、数据传输信息、告警等信息也可通过管理平台实时查看。

4. 产品功能

机甲卫士产品实时监控外界与工控系统之间的信息交换，验证信息源可信性，检查各种协议的合规性和操作指令的合法性，核对和辨别信息载体的特征，以实现安全防护的目的，产品主要功能如下。

4.1. 集中管理

管理平台可集中管理网络内的机甲卫士设备，接收设备的告警信息，监测设备运行状态，并可统一管理设备的安全策略、固件升级、病毒库升级等。

4.2. 网络防护

网络数据防护功能支持基于白名单的网络访问控制功能，访问控制粒度可控制到 MAC、IP、端口及应用层协议，根据策略规则对数据包应用层内容判别，支持对 Modbus TCP、OPCDA、S7 等工控协议和通用协议 FTP、HTTP、STMP、POP3 等的深度过滤和控制。

4.3. 串口防护

串口数据防护功能可针对 RS232 串口进行防护，根据数据包地址信息、指令类型及数据内容进行筛查过滤，基于白名单的串口访问控制策略，保证在数据传输过程中的安全性，防止恶意指令下达至数控设备。

4.4. USB 防护

USB 设备防护功能可针对 USB 设备进行一些列的安全设置，包括设备注册、授权、注销、责任人设置，可通过管理界面查看 USB 端口状态、权限设置、文件管控、黑白名单策略、病毒查杀等功能。

端口状态主要显示 USB 外设连接至机甲卫士设备时的基本信息，包含设备名称、设备厂商、设备序列号、设备类型、设备大小、接入时间、身份授权、端口授权和状态等信息。

端口权限设置主要配置和展示每个端口的端口模式（禁用、过滤、直通）和端口授权（只读、读写），用于控制存储类 USB 外设读写权限，非存储类 USB 外设不作读写控制。

文件管控主要对已连接存储类 USB 外设上的文件进行杀毒、手动传输、规则匹配、关键字过滤等管控，可以按照目录层级查看文件，显示每个文件的详细信息及病毒扫描信息，便于追溯和管理，可以根据实际业务对威胁文件进行删除。

黑白名单策略主要用于配置对存储类 USB 外设文件读写权限控制，在端口模式是过滤情况下，策略才会生效；文件读写权限根据端口授权、USB 外设身份授权和策略来进行控制，

策略只针对从USB外设读取文件时进行控制；设备默认有黑名单和白名单两条策略，且默认黑名单启用、白名单禁用。

4.5. 安全审计

对审计日志进行管理。审计日志包括安全防护业务审计日志和设备系统审计日志两类，对两类日志提供日志查询、日志导出(备份)、日志统计操作。

5. 产品亮点

5.1. 端口全防护

对终端设备网口、串口、USB端口进行安全防护，端口支持禁用、透传及过滤三种模式，过滤模式下对所有经过端口数据按策略规则进行筛查防护。

5.2. 协议指令控制

机甲卫士搭载自主研发的数据包深度解析引擎，对工控协议（OPC DA/UA、Modbus、IEC 60870-5-104、IEC 61850 MMS、DNP3、S7等）进行深度解析，做到实时、精准的指令识别与控制。

5.3. 深度文件过滤

提供文件规则过滤功能，可对文件格式进行阻断和放行，以白名单方式限定传输的文件类型和 NC 代码格式，并通过检查文件的头部编码信息来识别文件实际结构，对文件类型的真实性进行审查，只允许符合白名单规则的传输数据内容进行透传；对文件内容的关键词审查，对黑名单内的关键词内容进行阻断，实现对受保护数控系统的数据传输内容过滤功能。

5.4. 多引擎病毒查杀

支持双引擎杀毒，对移动存储类设备进行手动、自动的病毒查杀，支持指定目录查杀和全盘查杀，检查移动存储设备文件是否安全，并提供查杀结果告警及处理方法。

6. 产品价值

整体方案落实了国家“十四五智能制造发展规划”等相关政策要求，基于工控安全、数据安全、5G 等安全体系架构设计；相关产品融合工控安全检测、商用密码、异常点分析等技术。面向企业智能制造生产应用场景，提供了融合网络安全、数据安全和功能安全的安全解决方案，提升了企业生产制造过程的整体安全水平，在保障企业的业务运营、生产安全甚至相关涉及的国家重要项目安全起到良好示范作用。随着智能制造、两化融合的深入发展，相关方案、案例也值得进一步扩大应用和推广，以增强我国智能制造的安全防御能力。

6.1. 以生产制造业务为中心

产品聚焦智能制造业务本身，而非单纯为了安全而做安全。各项安全能力的最终目标均是为智能制造生产精度、质量、效率、安全保密提供保障。

6.2. 降低进口设备风险

在制造业从传统方式向智能化发展的过程中，高端制造装备短期内无法实现完全自给自足。在此背景下，本系统能有效管控机床输入输出接口、传输的文件、融合机床运行和业务执行数据分析生产本质问题，全面降低进口生产装备联网生产安全风险。

6.3. 智能制造装备全生命周期管理

智能制造装备种类繁杂、时代跨度大、管理难度大、数据信息流转管控难度大等难题，产品面向生产制造过程中装备全生命周期管理，包括机床运行状态实时监控、产品进度监控、NC 文件管理，以及过程中网络和数据安全防护，全面覆盖智能制造装备使用全过程。

6.4. 系统能力和规模平滑扩展

系统基于工业互联网平台设计，可本地化部署，满足复杂业务和大数据应用场景，平台可依据项目规模平滑扩展；系统可面向企业扩展能耗管理、SM 移动应用管理端等能力提供功能扩展。