CAICT 中国信通院　NSFOCUS

集智 蓝皮报告

数控机床网络安全研究报告

(2023 年)

中国信息通信研究院安全研究所

工业互联网安全技术试验与测评工业和信息化部重点实验室

北京神州绿盟科技有限公司

2023年4月

版权声明

前　言

数控机床作为制造业的“工作母机”，是工业领域生产加工的关键设备，数控机床本身的安全性以及在应用过程中的网络安全防护能力直接影响工业生产和业务，其存在的漏洞及后门程序将对整个工业领域形成巨大的威胁，这些威胁既包含其自身被入侵的威胁，也包含对网络和云平台的威胁。同时，随着工业互联网的快速发展，数控机床打破原有的封闭性，实现互联互通已成为企业发展的必然要求，数控机床联网运行已成为趋势，管理机、服务器盗用权限登录等都会带来安全隐患，如何保证数控机床联网运行的网络与数据安全逐渐成为制约工业互联网发展的关键问题之一。

对于海量、多种类的数控机床，传统单一的安全防护技术手段无法解决数控机床网络安全问题，需要从安全基线、主机安全、网络边界等各个层次提升数控机床的安全防护能力。本报告以工业互联网背景下数控机床的发展为基础，从数控机床国内外政策、安全技术研究、技术标准规范等方面分析了数控机床的网络安全现状。同时，详细分析了数控机床存在的漏洞隐患、入侵攻击等网络安全风险及深层次原因，并给出安全防护实施方案建议。最后，从标准、技术研究、评估评测等方面提出数控机床网络安全未来的工作方向。

目 录

图 目 录

表 目 录

一、工业互联网背景下数控机床的发展

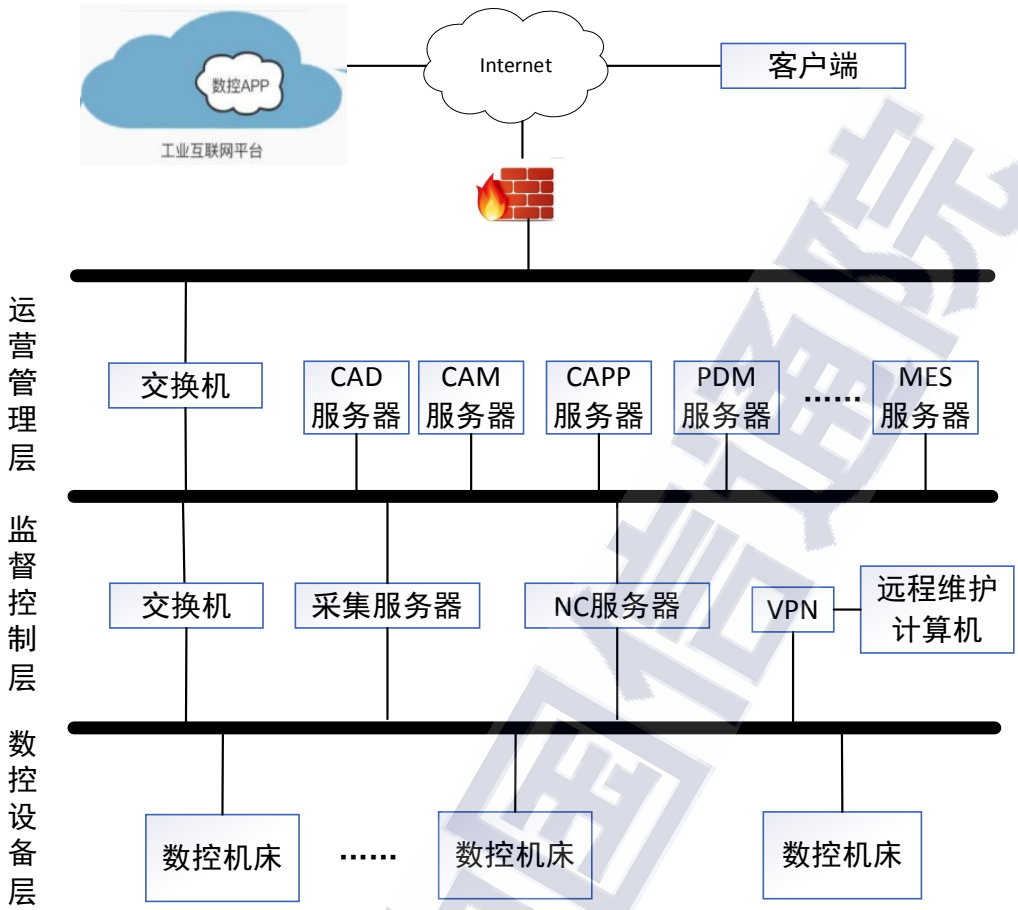
数控机床是工业领域生产加工的关键设备，广泛应用于航空航天、车辆制造、船舶制造等关系国防安全、经济安全和社会安全的关键行业。随着智能制造的深度推进和工业互联网的发展，工控系统逐步从单机走向互联、从封闭走向开放，我国数控加工行业也开始大力推进数控机床的网络化，单点通信数控机床控制方式逐渐被淘汰，如今数控机床多数采用的分布式数控系统，可以使用一台计算机对多台数控机床实现数字控制，并且能够执行计划调度、程序分配、远程监控和控制管理等功能。数控机床等设备联网程度及应用范围不断扩大，并且不断发展以适应生产加工的需要。

（一）数控机床典型网络架构

工业互联网背景下数控机床典型网络架构如图 1 所示，包括数控设备层、监督控制层和运营管理层。数控设备层中是通过有线通信或无线通信方式联网的数控机床等设备。监督控制层中是各类数据采集服务器及 NC(Numerical Control, 数字控制) 服务器。运营管理层包括 CAD（Computer Aided Drafting，计算机辅助设计）、CAM (Computer Aided Manufacturing，计算机辅助制造）、CAPP(Computer Aided Process Planning，计算机辅助工艺过程设计）、PDM (Product Data Management，产品数据管理）、MES(Manufacturing Execution Systems，制造执行系统)等各类服务器。监督控制层中是各类数据采集服务器和 NC 服务器。根据生产规模的不同，NC 服务器、采集服务器可能会分级部署，如（厂级）NC 代码服务器、（车间级）NC 代码子服务

器，（厂级）采集服务器、（车间级）采集子服务器。监督控制层的服务器和运营管理层的服务器进行信息交互。PDM 实现设计图纸、工艺文件、加工程序的集中管理。企业的设计图纸、工艺文件、加工程序可以分散在 CAD、CAM、CAPP 等不同的系统中进行管理。NC 服务器从运营管理层系统获取设计图纸、工艺文件以及定型的 NC 代码并进行存储，根据 MES 下达的生产任务向设备下发加工程序。采集服务器接收设备采集的加工状态信息并将设备加工状态信息反馈给 MES 系统。设备根据预先编制的程序指令，控制生产过程的运行，采集设备运行状态信息传送给采集服务器。

数控网络通过交换机等设备与互联网连接，在运行过程中，不断地引入数值数据，从而实现设备工作过程的自动化控制。数控网络同时连接工业互联网平台及数控 APP（Application，应用软件），查看业务流程数据、设备状态信息、模型信息等。通过网络可以实现 NC 代码的集中管理、设备的启停控制以及设备加工状态的自动采集。



来源：中国信息通信研究院

图 1 数控机床典型网络架构

（二）数控机床逐步从单点封闭走向开放互联

数控机床是一种高精度、高效率的自动化机床，配备多工位刀塔或动力刀塔，具有广泛的加工工艺性能，在复杂零件的批量生产中发挥了良好的经济效果。传统数控机床多数采用工程师手动编辑控制程序的方式工作，此类传统控制方式机械而繁琐，消耗人工成本同时又不利于生产效率的扩张。虽然有些数控机床采用了计算机与数控机床进行单点通信，但所用的通信程序是基于 Windows 操作系统的单机通信程序，必须在机床端和计算机端交替操作才能完成通信，且通信距离十分有限，给操作带来许多不便。随着智能制造的深度推进和工

业互联网的发展，手动编程和单点通信数控机床控制方式逐渐被淘汰，如今数控机床多数采用的分布式数控（Distributed Numerical Control, DNC）系统，可以使用一台计算机对多台数控机床实现数字控制，并且能够执行计划调度、程序分配、远程监控和控制管理等功能。DNC 系统的出现使数控机床摆脱了单点站控方式并实现了基本的互联。

DNC 大致经历了四个发展阶段。第一阶段使用串口通讯（多为 RS232 和 RS485）进行分布式控制组网，可以进行控制程序的在线下装和参数读取以及指令控制，这也是 DNC 系统的雏形，但是串口通讯方式开放性比较差，通讯带宽小。第二阶段是采用以太网通讯方式，此类方式由于具备高带宽，相较于串口组网场景能够适应更多的 DNC 系统功能，不过通讯协议多为厂商私有协议，如 FANUC 的 FOCAS、三菱的 EZSocket。第三阶段仍是以太网通讯方式，为改变厂家私有协议的闭塞性，提高 DNC 系统应用的开放性，出现了 OPC UA 和 MTConnect 以及 NC-Link（国内制定）等面向互联网应用的通讯标准，极大地提高了数控系统的开放性。

（三）数控机床智能化技术的发展逐渐成熟

近年来，智能化数控机床在工业中的应用广泛，为我国工业发展带来了巨大的经济效益。数控机床智能化在工业发展中的主要应用应该归功于其全自动化的运行模式，自动化数控机床在每个工作环节中都采用自动工作的方式，减轻了工作人员的负担，并且降低了企业发展的成本。

在数控系统智能加工方面，数控化系统的加工技术能够提高机床

工业部件的加工水平，提高工业生产效率。运用优化“预判”功能的精细曲面控制技术可以利用前进后退的工作路径，实现优化压缩机的合理运用，确保其工作过程中的精准程度以及加工工作。在数控机床远程控制方面，专业人员利用软硬件实现对数控机床高级别的控制，包括设备的启动、停止，设备状态的查看、设备维护等，无须工作人员值守，通过对数控机床运行参数的收集和分析，可以及早地发现存在的隐性故障，降低机床的故障率。

通过对网络技术的应用，不断优化数控机床生产加工流程，提升生产和工作效率。数控机床在此背景之下也不断地优化升级，开放网络端口或远程控制端口借助互联网实现进程控制数控机床生产和操作，智能化水平越来越高。

二、数控机床网络安全防护现状

随着制造行业分布式数控系统逐步从封闭走向开放，数控机床联网运行已成为趋势，数控机床本身存在不可控的漏洞、后门等安全隐患。同时，互联网安全威胁向工厂内逐渐渗透扩散，针对数控机床等设备的勒索病毒持续发酵，将会导致数控机床乃至整个生产线停机，造成企业重大损失。亟需开展数控机床安全防护技术研究，建立数控设备网络信息安全防护体系，提升我国数控机床网络安全防护供给侧能力，为保障国家网络安全、护航新基建夯实产业基础。

（一）国内外相关政策法规对数控机床网络安全提出要求

近年来，美国、欧盟等国家强化政策法规引导，将数控机床等工业设备网络安全作为重要部署方向。美国在 2018 年《美国先进制造业领导力战略》报告中将制造业的网络安全作为发展的重点方向，提出实施制造系统中网络安全的新兴技术。2017 年，欧盟网络空间安全局发布《欧盟关键信息基础设施环境中的物联网安全基线指南》，将设备安全作为物联网系统安全的重要内容。我国工业和信息化部联合国家能源局等十个部门出台了《加强工业互联网安全工作的指导意见》，要求“加强工业生产、主机、智能终端等设备安全接入和防护，强化控制网络协议、装置装备、工业软件等安全保障，推动设备制造商、自动化集成商与安全企业加强合作，提升设备和控制系统的本质安全”。

（二）国内外针对数控机床等智能制造系统安全防护技术开展积极研究

在技术研究方面，美国国土安全部制定了专门的工业控制系统安全计划，形成了由国家职能部门协调管理、国家级专业队伍、实验室和科研机构提供技术支撑、用户及厂商共同参与的技术研究体系，并制定了国家 SCADA 测试床计划，针对数控机床等开展网络信息安全测评。日本大隈（Okuma）的 OSP 病毒防护系统在 Okuma OSP-P 控制系统中内置了病毒扫描应用接口来防止感染从网络或 USB 设备传播的病毒，在数控机床网络安全防护中得到广泛应用。国内高校提出

一种数控加工网络信息安全防护方案，部署数控加工网络边界隔离设备和数控系统终端防护设备，保障数控网络安全[1]。

（三）数控机床的网络信息安全防护体系日渐完备

国内相关科研机构提出了 DNC 数控网络系统安全防护架构，部署防火墙在办公局域网和 DNC 数控网之间过滤数据，然而该方案对于内部信息泄露缺乏有效的防护[2]。刘杰等人提出一种数控网络信息安全综合防护方案，采用可信安全防护技术，融合基础数据和系统安全防护技术，形成数控机床自动化网络安全综合防护功能[3]。国内学者对数控机床控制系统的信息安全防护技术体系与评估机制开展了深入的研究，研发“数控系统终端信息安全防护设备”、“单向数据安全交换设备”及“边界安全专用网关”等产品，该系列产品被广泛应用于工控网络、数控加工网络、重点作业站点的数据安全防护。此外，国内已经拥有涵盖西门子、发那科、海德汉以及国内一线数控品牌在内的综合试验环境，拥有针对智能制造基础设施、网络安全、功能安全等的攻防验证平台。

（四）数控机床相关安全标准和技术规范仍需完善

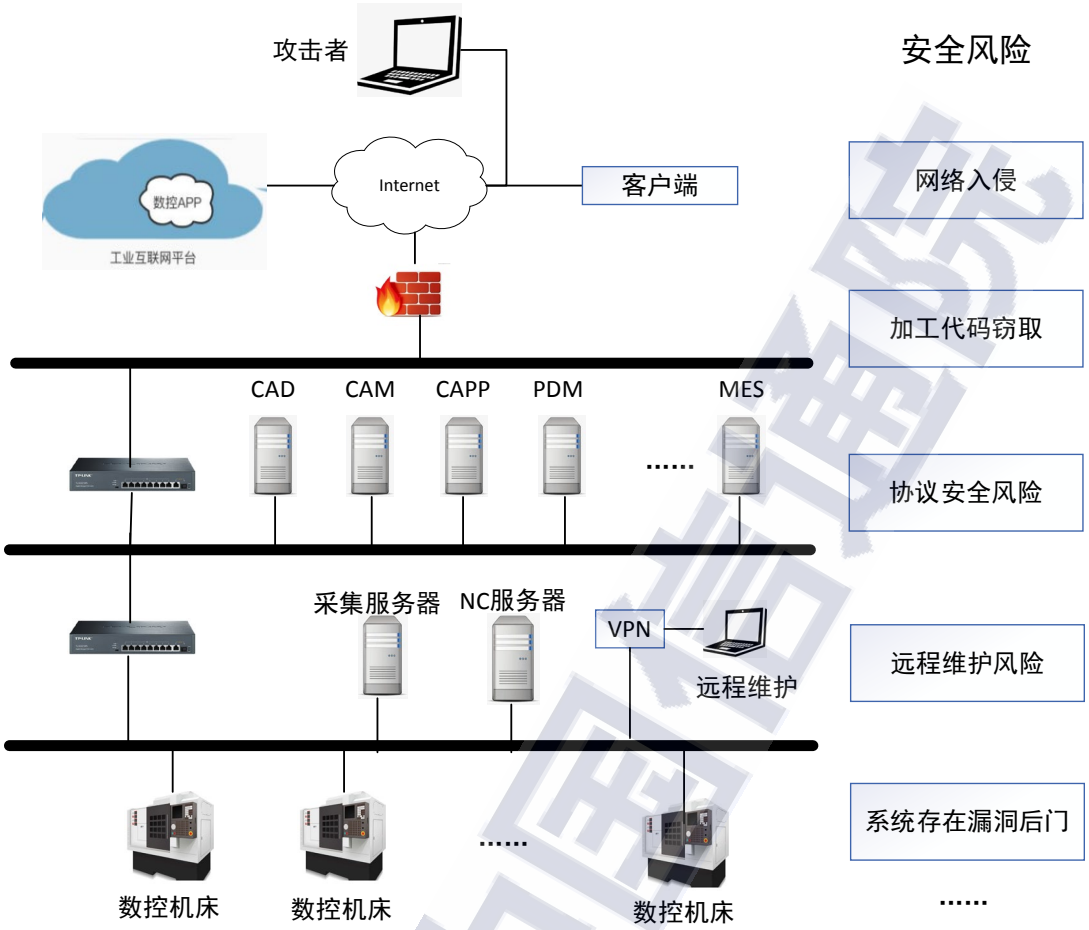
美国能源部国家 SCADA 测试床计划(NSTB)发布了防护控制系统路线图。欧洲网络与信息安全局（ENISA)制定的防护控制系统的指导文件也于 2011 年发布。目前，我国相关标准技术委员会及联盟组织推动数控机床安全相关标准制定发布，信息安全标准化委员会（TC260）在 2019 年发布的 GB/T 37955-2019《信息安全技术 数控网络安全技术要求》标准针对数控网络的设备安全、网络安全、应用

安全、数据安全等方面提出明确的技术要求。中国通信标准化协会（CCSA）正在报批阶段的行业标准《工业互联网 数控加工制造系统信息安全风险评估指南》中规定了数控加工制造系统的信息安全风险评估的对象、内容及实施过程以及安全措施有效性测试流程。工业互联网产业联盟（AII）已发布 2 项关于数控系统密码应用技术及测评要求。

三、数控机床网络安全风险分析

随着工业互联网的发展，数控机床网络安全防护成为数控领域网络化、智能化发展的关键问题。数控加工设备联网进程的加快导致了传统信息网络的各种黑客攻击和恶意代码等安全威胁快速进入数控网络，一旦被不法分子利用，后果极为严重。然而我国数控网络安全防护体系建设相对于数控网络的快速发展存在明显滞后，工业企业没有充分考虑数控网络与其它网络互联互通带来的网络安全风险，相关标准体系建设也几乎为空白，缺乏必要的安全防护措施。

典型数控机床网络安全风险如图 2 所示，原本封闭可信的数控机床生产网络接入企业管理网和互联网后网络安全风险增加，机床设备本身可能存在系统设计漏洞和后门，数控协议及网络传输安全风险导致加工代码被非法获取，存在机床远程运维不可控等安全威胁。



来源：中国信息通信研究院

图 2 典型数控机床网络安全风险

（一）数控机床系统设计漏洞和预留后门存在安全隐患

由于运行在数控机床计算机中的工控软件与其操作系统存在兼容性问题，数控机床计算机一般采用专用系统或经精简的 Windows 系统[4]。**一方面**，复杂的数控机床中所包含的软件代码量级巨大，其中可能存在系统设计漏洞和预留后门等安全隐患[5]，一些数控机床还开放了 SSH、HTTP、时钟同步等服务，可能成为攻击者的攻击目标。**另一方面**，部分数控机床所采用的系统版本较为老旧，计算机操作系统平台缺少补丁，导致系统发现漏洞后难以进行修复，极有可能存在

远程代码执行漏洞或拒绝服务漏洞，从而使攻击者完全控制数控终端或使其宕机，在这种情况下，轻则严重影响工厂生产，重则对终端造成不可恢复的破坏。

（二）数控协议及传输链路存在安全风险，导致数据泄露

数控 DNC 网络采用 TCP/IP 协议将原独立运行的数控机床组成数控机床网络，数控机床通常采用工业 WiFi 等无线通信方式。**一方面**，无线接入方式避免了有线接入物理环境限制和铺设线路的成本，但在网络安全层面上相较于有线网络更具风险性，无线 WiFi 易发生会话劫持数据泄露的风险，利用对无线信号的监听窃取传输数据，通过伪造指令或者数据拦截进行恶意攻击。**另一方面**，多数数控机床控制系统使用明文方式传输和管理加工代码，这样容易导致未加密的加工代码被非法获取，并通过专用软件对加工物品进行还原，导致制造数据泄密。2018 年，克莱斯勒、福特、特斯拉等全球 100 家车企的 47000 多个机密文件遭外泄，泄露的数据包括产品设计原理图、装配线原理图等敏感信息。

（三）对移动存储介质及数控机床串口缺乏技术管控，存在网络入侵安全风险

一般数控设备中的控制系统计算机，无法安装使用终端行为控制软件，对外来的移动存储介质及数据传输介质的使用进行监控。**一方面**，在数控机床网络中随意接入 U 盘、移动硬盘、光盘等移动存储介质，对网络中的关键生产数据任意访问和操作，导致机密生产数据的

泄露。Honeywell 报告显示，2020 年，其 USB 安全产品在客户扫描的驱动器上发现的恶意软件中有 79%能够中断 OT (Operational Technology，运营技术）系统，相比 2019 年的 59%上升了近乎一半。**另一方面**，对于车间里没有安全防范机制的终端，可以通过网口、串口及 USB 口等传输 NC 程序及其他数据到数控机床内，同时终端也会通过网络接口上传一些数据到 DNC 服务器，无技术监管手段，管理难度大，如果在终端上传不安全的数据到 DNC 服务器也会危及其他设备安全。

（四）用户身份认证能力不足，数控机床远程监测和维护存在风险

对于数控系统的远程监测和安全运维，运维人员通过采集数控系统中的温度、振动、转速等数据，对数控机床的运动轴、刀具等进行故障预测性分析，对可能发生的故障提出预警信号，在此过程中存在维护人员身份仿冒以及系统账号滥用风险。**一方面**，机床设备进行基础数据采集及上报时，如果通信双方没有进行身份认证，可能会因为身份假冒出现数据泄露等安全问题。**另一方面**，数控设备的升级维护严重依赖生产和供应厂商，很多设备允许通过网络远程控制，系统缺少用户身份认证和访问控制等安全机制，设备的升级维护过程行为不可控，存在巨大的安全风险。

（五）网络边界扩大导致网络入侵安全风险

随着工业互联网的不断发展，原本独立封闭的数控生产网络接入企业管理网和互联网，网络安全风险向数控网络渗透。**一方面**，数控

网络中的主机易成为网络入侵的主要攻击点，传统信息通信行业的杀毒软件并不适用数控网络主机的安全防护，或者会严重影响企业的生产效率，数控系统通常不安装杀毒软件，为病毒蔓延提供了入口。**另一方面**，对数控机床进行远程监控的工程师站和远程的 PLC 站之间是通过互联网进行连接的，攻击者可利用边缘终端设备漏洞作为跳板对数控系统实施入侵或发起大规模网络攻击。

（六）数控机床缺乏内部安全防护机制

近年来，数控机床国产化市场规模逐年变大，根据工控网数据，2016 年，数控机床专项支持研发的高档数控系统已累计销售 1000 余套，国内市场占有率较专项启动前也有所提高，但目前国内使用的高端主流数控设备大部分仍是国外厂家产品。**一方面，**进口设备通常使用黑盒设计，内部结构不可知，硬件架构不明晰，数据通信行为不可控，存在设备内嵌后门的安全风险，容易遭受核心生产数据窃取和控制系统破坏攻击。**另一方面，**不同数控机床厂商设计支持不同的控制协议，如表 1 所示，包括 OPC UA、MTConnect、umati、NC-Link 等协议，协议种类繁多且兼容性差，难以进行统一管控。

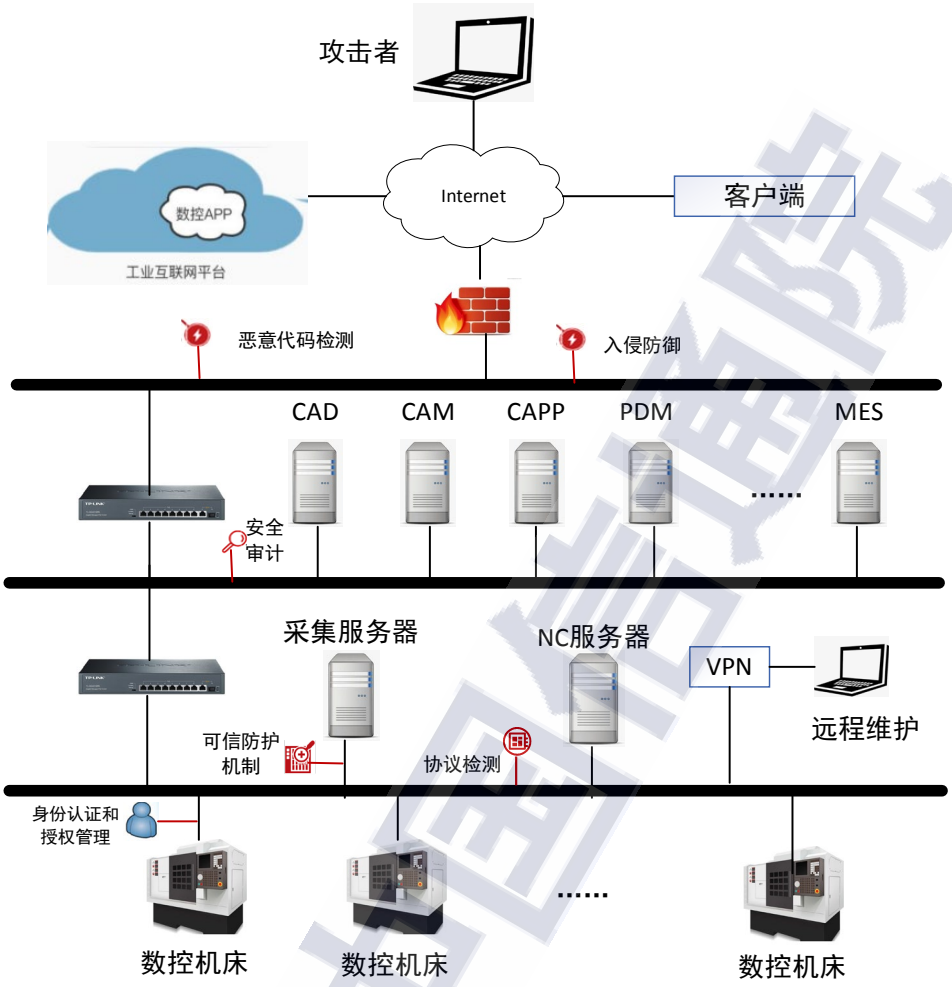
表 1：数控机床协议分布

OPC UA 协议
● **西门子**、发那科、**德国倍福**、ABB、罗克韦尔**等。**
MTConnect 协议
● 西门子、发那科、山崎马扎克、海德汉**等。**
umati 协议
● **西门子**、**德国**倍福**等。**
NC-Link 协议
● 华中数控、广州数控**等。**
FOCAS 协议
● **发那科**

来源：《新一代智能化数控系统》

四、数控机床网络安全防护实施

数控系统作为数控设备的“大脑”成为工业控制系统的重要组成部分，正面临工业病毒和网络攻击，网络与信息安全问题日益凸显。为帮助企业加强数控机床安全防护上的短板，本章针对以上数控机床安全风险提出安全防护实施思路，如图 4 所示，数控机床网络安全体系的构建需从安全基线管理、网络边界防护措施部署和数控机床内生安全等方面进行考虑，来保证数控机床及网络的保密性、可用性和完整性。



来源：中国信息通信研究院

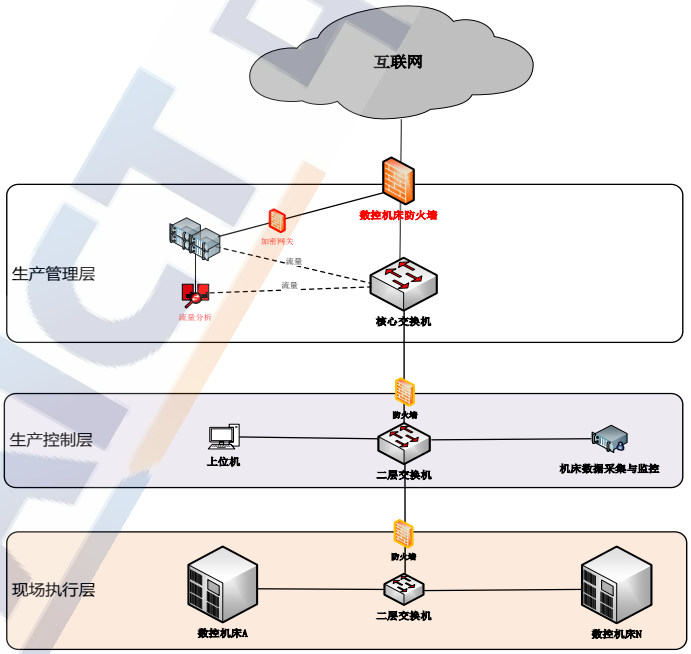
图 3 数控机床网络安全防护示意图

（一）开展数控机床网络安全基线管理

根据生产环境场景建立数控机床网络安全基线。**一方面**，明确数控机床网络安全基线具体内容，建立安全基线更新机制。企业梳理自身数控机床应用场景及技术特点，根据安全基线实施安全防护，包括消除弱密码、安全配置加固、去除不必要的介质接口等。**另一方面**，开展数控机床网络安全风险评估和漏洞管理。定期对数控机床网络架构、管理主机、控制协议等开展全方位安全评估，发现安全风险隐患，一旦发现安全漏洞，及时选择安全补丁或升级组件。

（二）加强数控网络边界防护

分析数控网络的组网特点，根据 IEC62443-3-3 等标准中的网络区域划分原则，将数控网络划分为合理安全区域，采用分层分域，纵深防御的策略进行网络安全防护，如图 5 所示。**一方面**，对企业信息系统与 DNC 系统进行分层、分域，建立安全缓冲区，生产网络与管理网络、研发网络连接采用网闸、光闸进行强隔离；生产网络进行内部的分区分域，区域间应采用工业防火墙实现逻辑隔离，并建立白名单，实现基于白名单的访问控制。**另一方面**，采用数据防泄漏、深度协议数据包解析等边界安全防护技术针对数据采集和交换过程中的数据泄露、病毒入侵以及异常行为进行告警，并对各类安全威胁进行监控，从而为数控网络提供全方位的监测、过滤、报警和阻断能力。

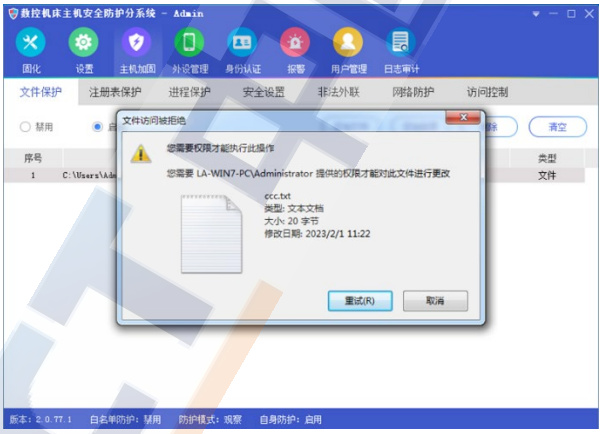


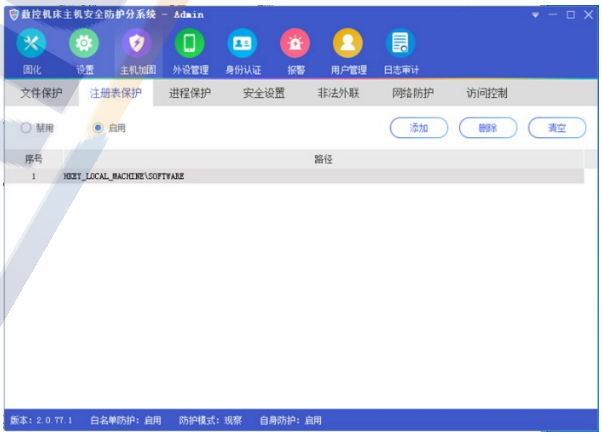
来源：北京神州绿盟科技有限公司

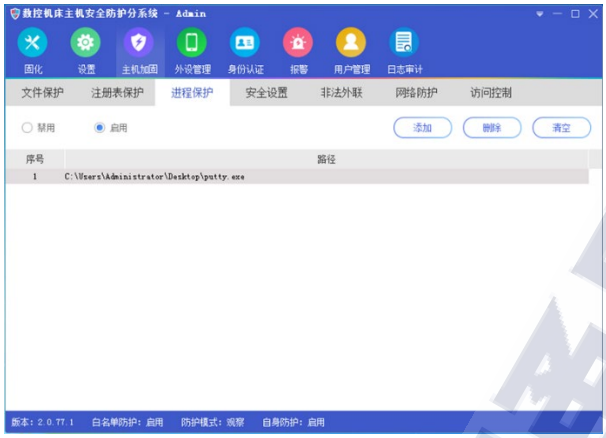
图 4 数控机床网络边界安全防护示例

（三）加强数控主机安全防护

通过安装工业主机端点侧安全监测、防护软件，对数控主机进行有效防护，包括操作系统加固、病毒防护、恶意行为监测等。**一方面**，针对数控网络中 DNC、MES、PDM、CAM、CAPP 等服务器及终端主机部署安全防护软件，从端点侧加强针对勒索病毒等安全防护，防止病毒传播、对恶意代码进行有效地消除。**另一方面**，通过对数控主机文件、目录、进程、注册表和服务的强制访问控制，如图 6 所示。采用“三权分立”的管理机制，有效制约和分散原有系统管理员的权限，并结合文件和服务的完整性检测、防缓冲区溢出等功能，将普通操作系统透明提升为安全操作系统，增强数控主机的安全性。







来源：北京神州绿盟科技有限公司

图 5 数控机床主机安全防护实施示例

（四）完善数控机床网络资产管理和安全监测审计

建设数控机床网络资产管理机制，开展安全监测和审计，及时发现异常资产及网络安全威胁。**一是**梳理数控机床生产环境的网络资产，建立资产台账，定期探测梳理资产现状及数据流转和处理节点，识别和发现异常资产，对未知设备接入等异常行为及时发现并处置。**二是**采用入侵检测、全流量检测、安全审计等方式监测数控机床生产环境，发现恶意行为和恶意代码，对数控机床生产环境行为进行审计，协助事后分析取证溯源。**三是**通过态势感知等技术手段，汇集流量侧、端点侧、日志侧等数据，进行关联分析和深度安全监测、研判和应急响应，并实现数控机床网络安全集中管理。

（五）可信计算技术提高数控机床内生安全

面对数控机床联网开放、互通互联可能带来的安全威胁，可以通过可信计算技术实现数控机床的内生安全[3]。**一方面**，数控机床在主机层面支持“硬件级部件（安全芯片或安全固件）”作为系统信任根，

建立从系统到应用的信任链，实现从设备加电到应用加载过程的安全启动和运行，从根本上解决工业互联网可信、可控、可靠等方面的问题。**另一方面**，在系统运行过程中，实时监视数控系统内关键进程、模块、可执行代码、关键数据结构等，对进程的资源访问行为进行实时度量和控制，依据动态的可信性对发生变化的度量对象依据策略采取报警、终止运行、更新度量预期值等措施，从而确保数控系统运行状态的可信。

（六）打造数控机床安全综合防护体系

针对数控机床所面临未知网络威胁的持续性、组合性、跨域性和定向性等特点，逐一应对解决传统被动防护难以应对利用逻辑缺陷的攻击等问题。**一方面，**对数控机床安全关键技术的联合攻关和创新，打造集事前预警、事中感知防御、事后审查等功能于一体的“数控机床安全增强防护设备”体系。实现防护思路由被动“封堵查杀”到主动免疫防御的转变，建立了云、边、端的内生安全防护架构，确保设备、系统、网络的可靠性、稳定性，有效提升制造企业生产网络的整体安全性。**另一方面，**建设覆盖设备、主机、网络、数据的数控机床综合防护体系，建立事前身份认证、加密，事中感知、防御，事后审计、追溯等多路径闭环的安全防护体系，提升数控机床领域的整体安全能力。

五、数控机床网络安全发展建议

近年来，数控机床联网运行已成为趋势，同时也暴露出很多安全

问题。基于所梳理的数控机床安全现状与安全风险，我们对数控机床网络安全提出如下建议:

（一）推进数控机床相关安全标准规范制定

目前针对数控机床网络安全标准和技术规范储备不足，需推动出台数控机床相关网络安全防护要求、安全评估评测规范、密码应用等相关安全标准规范。**一方面**，面向数控机床边界防护、入侵防范、安全审计等安全需求，制定亟需数控机床内生安全及评估测试等行业标准和企业标准，强化数控机床在设计、开发、实施、运行维护等全生命周期过程的网络安全规范要求，为企业产品安全开发、第三方机构测试认证、设备部署运行提供可参考的依据。**另一方面**，研制数控系统密码应用技术要求及测评要求等标准，规范和评估数控系统密码应用的设计、实现和使用；鼓励安全设备制造商积极参与标准研制与贯标试点工作，以标准规范指导数控机床网络安全防护部署。

（二）提升数控机床网络安全综合技术防护能力

数控机床作为工业控制系统的重要组成部分，网络安全防护依然依赖传统“外挂式”安全措施，需产业各方加强数控机床安全技术研究，提升网络安全综合防护能力。**一方面**，建立数控机床多重安全防护的纵深防御体系框架，采取事前身份认证、加密、预警、漏扫、评估机制，事中防御攻击机制，事后审计、追溯等，以提升数控网络的整体安全。**另一方面**，加强数控机床内生安全能力建设，通过自主可控加可信计算的总体思路，用主动免疫的思想对网络空间尤其是数控

机床等设施领域的安全防护思路进行研究和探索，基于国产密码算法构建内生安全能力。

（三）开展数控机床网络安全评估评测

目前，数控设备的远程维护需要通过互联网进行，存在的漏洞容易被攻击者利用进行恶意攻击，导致数控设备直接面临互联网中的安全风险。应建立数控机床网络安全评估评测体系，开展数控机床网络安全评估评测。**一方面**，围绕数控机床系统固件安全、网络安全、应用安全、数据安全、接入安全等要求，建立数控机床网络安全测试评估体系，建立安全能力评估模型。**另一方面**，针对数控机床抗渗透能力、恶意代码防范、抗 DDoS 能力、漏洞隐患情况等漏洞隐患防护能力等进行安全能力分析研究和攻击防护测试，推动数控机床安全检测认证和设备能力提升。

（四）推动数控机床相关安全产品应用及市场发展

目前国内使用的主流数控设备，其核心系统大部分是国外厂家产品，特别是高端数控机床控制系统和数控机床整体联网解决方案。因此，应加快对数控机床核心关键技术攻关，推动相关安全产品和服务的开发应用。**一方面**，鼓励国内重点企业、科研机构、高校等加强合作，推动研制具备访问控制、数据安全防护、病毒防护与分析、NC 文件语义分析与审计、链路加密、智能预警等能力的数控机床安全增强防护设备。**另一方面**，围绕数控机床安全产品的功能、性能及安全性等设计安全认证级别，开展数控机床相关安全产品及服务分类分级管

理，为不同部门、行业企业提供安全级别选择，遴选达标安全产品目录清单，推动数控机床安全产品市场发展。

参考文献

[1]王琦魁，李昕，赵甫．工控系统信息安全与加工网络防护方案研究[J]. 信息网络安全，2022(9)

[2]王剑，郭照敏，王国营．DNC 数控网络系统的安全防护[J]. 保密科学技术，2012(8):4.

[3]刘杰, 汪京培, 李丹, 等． 数控机床自动化网络信息安全综合防护方案[J]. 组合机床与自动化加工技术, 2016(3):82-85,89.

[4]钟诚, 李凯斌, 孟曦. 智能制造联网数控加工系统的网络安全威胁与防护[J]. 自动化博览, 2018,35(S2):44-49

[5]尚文利, 佟国毓, 尹隆, 陈春雨. 数控系统信息安全现状与技术发展趋势[J].自动化博览, 2019(06):50-53.

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-88192304

传真：010-62300264

网址：www.caict.ac.cn