基于工业母机防火墙的数控网络安全防护解决方案*

王晓鹏,张雄杰,陈毅真,周建伟,尹雅伟
(北京神州绿盟科技有限公司,北京 100089)

摘 要:随着针对数控机床的网络攻击日益严重,基于供给侧打造数控机床安全供给能力,成为制造强国之路的重要关切之一。立足于行业痛点,解决数控机床安全紧迫问题,实现需求侧安全保障。设计了一种同时将“NC 代码异常检测”“NC 代码病毒检测”“防碰撞检测”等安全机制结合起来的工业防火墙系统——工业母机防火墙,围绕安全通信网络、安全区域边界、安全计算环境、安全管理中心、专用防护设备等方面,给出了具体防护措施和建议。本文的研究设计及解决方案对于保障制造强国、建设数字中国等具有重要现实意义。

关键词:工业母机;数控机床;DNC 网络;网络安全
中图分类号:TP305 文献标识码:A DOI:10.19358/j.issn.2097-1788.2022.06.002
引用格式:王晓鹏,张雄杰,陈毅真,等. 基于工业母机防火墙的数控网络安全防护解决方案[J].网络安全与数据治理,2022,41(6):10-16,33.

CNC network security protection solution based on industrial master machine firewall

Wang Xiaopeng, Zhang Xiongjie, Chen Yizhen, Zhou Jianewei, Yin Yawei
(NSFOCUS Technology Co., Ltd., Beijing 100089, China)

Abstract: With the increasingly serious network attacks against CNC machine tools, the secure supply of CNC machine tools based on supply-side has become one of the important concerns of the road to manufacturing power. Based on the pain points of the industry, this paper solves the urgent security problems of CNC machine tools and realizes demand-side security. This paper designs an industrial firewall system which combines the security mechanisms such as “NC code anomaly detection”, “NC code virus detection” and “anti-collision detection” at the same time, and gives specific protective measures and suggestions around secure communication network, secure area boundary, secure computing environment, security management center, special protective equipment. Therefore, the research design and solutions in this paper closely serve the national strategic needs such as Manufacturing Power and Digital China.

Key words: industrial master machine; CNC machine; DNC network; cyber security

0 引言

数控机床作为当今智能制造领域的核心装备,是生产加工行业的关键设备。2021 年 8 月 19 日,国资委会议精神强调,加强针对工业母机、高端芯片、新材料、新能源汽车等关键核心领域的技术攻关。这次会议将工业母机(即机床)列于首位,足见其之于制造业的重要地位。

然而针对数控机床的网络攻击日益严重,多家国际知名制造业巨头屡遭攻击,如何保证数控机床网络与数据安全逐渐成为保障数控行业发展的关键问题之一。国内外现有的数控机床防护设备普遍存在专业性不足的问题,并不完全适用于数控网络。本文立足于行业痛点,解决数控机床安全紧迫问题,实现需求侧安全保障;同时,立足供给侧打造数控机床安全供给能力。安全问题是制造强国战略的核心关切之一,因此,本文的研究设计及解决方案紧密服务国家战略需求,对于保障制造强国、

*基金项目:工业互联网高质量发展工程联网数控数控机床安全项目(TC210H02L)

数字中国等战略具有重要现实意义。

1 我国数控机床的发展现状

机床作为“工业母机”，与国家制造业水平密切相关。经过多年发展，我国数控机床行业取得了长足进步，但“精度及稳定性差、故障多发”仍是国产数控机床亟需突破的技术难点，我国数控机床市场呈现出“国产中低端数控机床发展迅速，高端数控机床依靠进口，核心技术受制于人”的局面。

自 2006 年以来，国务院、发改委、工信部等部门陆续出台了针对高端数控机床的发展指引，在我国自主创新能力不断提升的背景下，广州数控、华中数控等厂商在国产高端数控系统市场逐步突破，未来有望打破国外垄断，实现进口替代。

2 我国数控机床网络安全典型问题分析

随着工业互联网的发展，数控机床行业逐渐向复合化、网络化、智能化发展，然而我国数控网络安全防护建设相对于数控行业的发展明显落后，安全防护的滞后成为其发展的制约因素，其中的典型问题如下：

(1)国产化不足：高端数控机床通常采用国外品牌，从而导致数控系统自身安全难以保证，可能存在系统设计漏洞和预留后门等安全隐患。

(2)网络边界无防护：数控网络边界无任何安全防护措施或安全措施失效，面临着被病毒感染、恶性攻击的风险。

(3)U 口无管控：很多数控车间直接使用 U 盘进行 NC 文件导入导出，并无管控措施，极有可能导致恶意代码的传播、核心生产工艺泄密。

(4)运维无管控：数控设备的维护往往依赖供应商，通过在服务器上安装向日葵、VNC 等互联网远程运维工具，进行无管控运维，导致设备的运维行为不可控，存在巨大的安全风险。

(5)主机防护不到位：操作系统老旧，很少更新补丁；主机普遍存在未关闭默认共享、开启高风险端口(80、135、443、445、3389)，不满足系统最小安装原则，未落实主机必要的安全配置。

(6)管理失位：工业企业针对数控系统安全防护意识淡薄险，缺乏相应的网络安全管理策略，如：未落实安全责任人、供应商管理不严等。

3 我国数控机床安全防护建设需求分析

3.1 我国数控机床网络组成

我国典型数控机床网络[1]如图 1 所示。图中虚线框内的部分为数控机床网络，由 NC 服务器、采集服务器、数控设备、网络通信设备等组成。

数控机床网络包括数控设备层和监督控制层。

(1)数控设备层：包含各类通过有线通信或无线通信方式联网的数控设备。通过数控网络可以实现 NC 代码的集中管理、数控设备的启停控制以及数

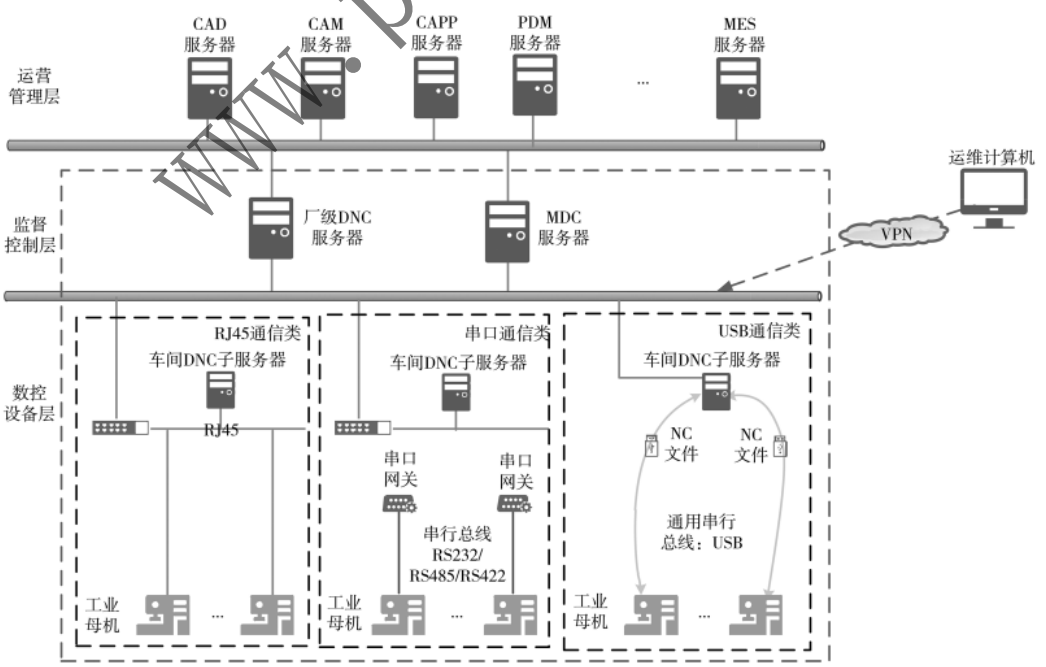

图 1 典型数控网络

控设备加工状态的自动采集。

(2)监督控制层:包含各类数据采集服务器和NC服务器。监督控制层的服务器与运营管理层的服务器进行信息交互。

3.2 数控机床网络安全风险分析

数控机床网络安全风险主要体现在如下五方面:

(1)网络安全风险:数控网络与管理网边界缺少必要的边界防护措施,导致管理网安全风险容易横向传播到数控网络;数控设备经常需要远程维护,却无专用的运维管理系统。

(2)设备安全风险:在数控网络中MDC服务器、DNC服务器、数控机床等设备普遍存在弱口令、漏洞未修复、USB无管控、无病毒防范措施等问题。

(3)应用安全风险:MDC、DNC等应用系统普遍存在弱口令、无身份鉴别措施、自身安全措施较少等问题,易受到病毒或黑客的攻击。

(4)数据安全风险:数控网络中的网络、设备和应用本身存在敏感数据泄露风险,数据的产生、使用、存储等方面缺乏防护,特别是NC代码,易造成数据的完整性和机密性受到破坏。

(5)安全管控风险:数控网络中部署的各类安全设备缺乏统一的安全管控,缺乏动态发现数控网络中的风险并预警能力。

3.3 现有数控机床安全防护技术分析

在数控机床安全防护技术领域,国内外厂商都在开展技术研究。日本大隈将OSP-VPS防病毒系统[2]内置在自家特定型号的数控机床中,侧重对NC文件传输过程中的病毒查杀;中国航天科工集团公司HT706-CISP边界安全网关[3],用于实现DNC网络与数控机床的逻辑隔离,侧重对数控机床接口(网口/串口/USB口)的综合管控。除了部署专用的防护设备外,目前,我国针对数控网络的主流防护方案是,使用工业防火墙[4]或工业网闸[5]进行安全域边界隔离,应对入侵活动和攻击性行为。

现有技术中,针对边界隔离、病毒查杀等方面都有探索及技术储备,而数控网络中最具防护价值的是加工文件"NC代码",因为NC代码以文件特征为核心,需要解析文本中的字符串,用于发现内容篡改等安全隐患;现有产品,如工业防火墙,以解析网络流量特征为核心,并不能解决"NC代码"防护需求。

纵观国内外现有的数控机床防护设备[6-9],都存在专业性不足的问题,并不完全适用于数控网络。所以,具备以解析"NC代码"为核心,同时拥有综合防护能力专用安全产品,成为我国数控机床安全防护的迫切需求。

4 工业母机防火墙研究及设计

4.1 工业母机防火墙功能设计

针对数控机床专用防护,应从防护效率、防护效力两个维度进行设计,为此,本文设计了一种以《GB/T 37933-2019 信息安全技术 工业控制系统专用防火墙技术要求》[4]为基础要求,同时将"NC代码异常检测""NC代码病毒检测""防碰撞检测"等安全机制结合起来的工业防火墙系统:工业母机防火墙。

工业母机防火墙由五部分组成:公共管理、安全引擎、高可用、数据通信引擎、国产化平台,如图2所示。其中安全引擎、高可用、数据通信引擎为设计核心。

(1)数据通信引擎:包含流转发、IP/MAC绑定、ACL、双向NAT、路由、VPN、串口透传、U口透传。

·访问控制模块:设置通信主客体的访问控制规则。

·VPN:包含IPSEC、SSLVPN。

·路由:包含静态、动态、策略路由。

·U口映射[10-11]:支持USB映射功能,用于U盘拷贝NC代码。

·串口透传[10-11]:串行接口方式串接在运维终端/采集终端与数控机床之间,实现远程运维及采集。

(2)安全引擎:包括病毒检测、NC代码合规性检测模块、NC代码异常检测模块、告警模块、知识库、文件代理模块、数控协议深度解析、工业协议识别等。

·NC代码合规检测模块:合规性检测组件用于对NC代码文件容量及扩展名格式检测;异常检测组件用于干涉检测及敏感信息监测。

·NC代码异常检测模块:包含词法/语法检测组件和防碰撞检测组件,词法/语法错误检测组件用于发现相应的词法/语法错误,防碰撞检测组件是对于非语法错误但可以降低碰撞事件的程序语句进行优化,进行注释行标记提醒。

·工业协议识别模块:基于工业协议特征值的识别。

·数控协议深度解析模块:基于数控协议

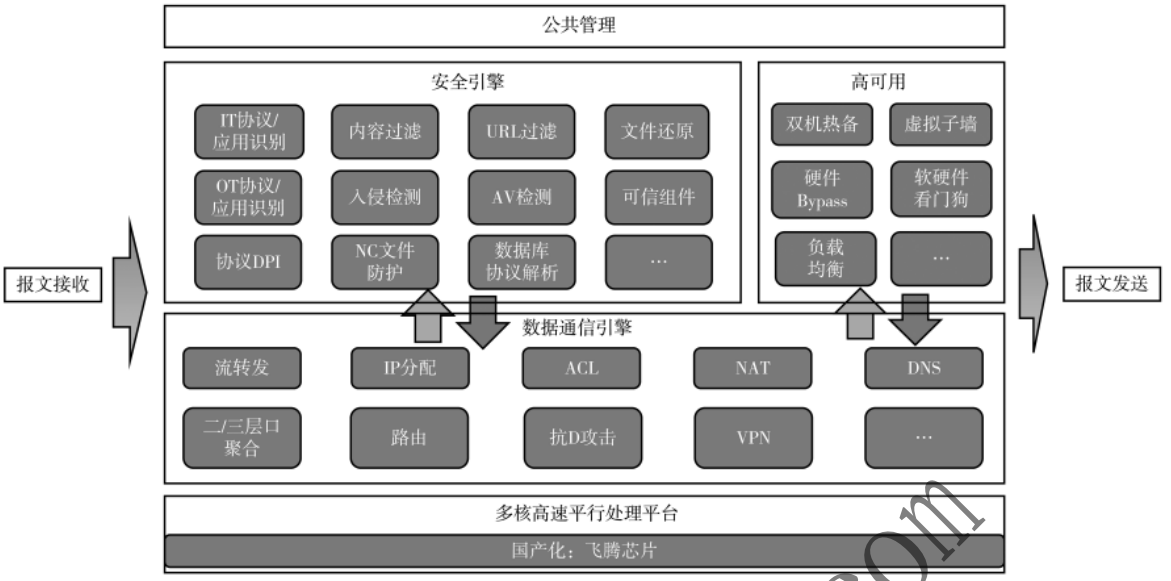

图 2 工业母机防火墙模块结构图

(MT－Connect、NC－LINK、OPC UA、FOCAS 等)及协议内容的解析及过滤。

·病毒检测模块：包含流式病毒检测组件和启发式病毒检测组件，流式病毒检测组件实现对通信流量的病毒查杀，启发式病毒检测组件实现对流量还原出的文件进行查杀。

·告警模块：针对检测过程中报警事件，进行告警。

·文件代理模块：实现 NC 代码文件的转发。

·知识库模块：包含工业母机防碰撞规则库和词法/语法库。

(3)高可用：包含双机热备、负载均衡、软硬件看门狗、硬件 Bypass 等功能。

4.2 工业母机防火墙业务流程设计

本文仅对 DNC 服务器与工业母机网络通信防护业务流程进行重点介绍，业务流程如图 3 所示。

(1)选择数控机床型号，关联相应 NC 代码词法/语法库、NC 代码防碰撞规则库。

(2)设置访问控制规则，确定通信主客体(DNC 服务器及工业母机)的 IP 五元组(源 IP、源端口、目的 IP、目的端口、传输层协议端口)信息，并完成通信主客体的 IP/MAC 绑定，进入步骤(3)。

(3)对通信主客体之间的流量完成 L1～L3 层报文解析，并进行 ACL 控制，如出现不符合 ACL 规则的流量，则进入步骤(9)，如符合则进入步骤(4)。

(4)通信流量进入病毒检测模块，病毒检测模块包含流式病毒检测组件和启发式病毒检测组件，两

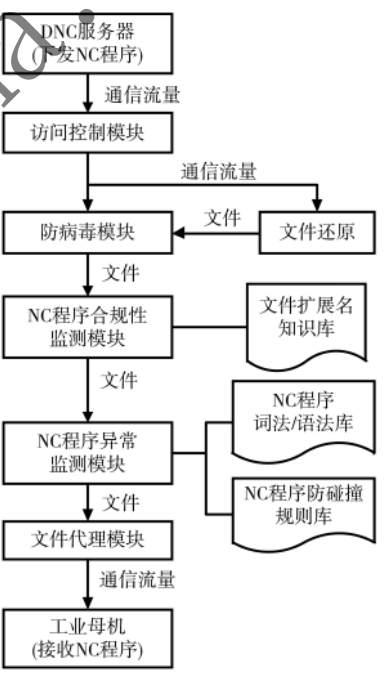

图 3 工业母机防火墙业务流程图

个组件同步检测，用于过滤阻断通信流量中存在的木马程序、蠕虫及勒索病毒、恶意邮件等威胁。流式病毒检测，对主客体通信流量的载荷，与流式病毒特征库进行比对，如命中病毒特征，将含病毒的流量留存为 Pcap 包，并进入步骤(8)。进行启发式病毒检测前，需要对流量中 NC 代码进行文件还原，生成 NC 代码文件，实现文件的病毒检测，如命中病毒特征，对 NC 代码文件进行留存，并进入步骤(8)。如同

时通过启发式和流式病毒检测,进入步骤(5)。

(5)NC 文件进入 NC 代码合规性检测模块,NC 代码合规性检测模块包括文件后缀名验证及文件容量验证。文件后缀名验证,检查文件是否符合 NC 文件的格式要求,只允许合规的文件(如 *.nc、*.mpf、*.h 等,如表 1 所示)进行传输;如不符合,对 NC 代码文件进行留存,进入步骤(8)。同时对 NC 文件容量进行检查,防止导入病毒文件或超大配置文件,避免系统中毒或崩溃,如超过 NC 代码规定的容量阈值,对 NC 代码文件进行留存,进入步骤(8)。如同时通过文件后缀名验证及文件容量验证,进入步骤(6)。

表 1 NC 代码常见扩展名

文件扩展名	备注说明
*.nc	发那科数控程序文件
*.mpf	西门子数控主程序文件
*.spf	西门子数控子程序文件
*.h	海德汉数控程序文件
.wpg	三菱数控 NC 代码文件
*.ct	广州数控刀具文件
*.wp	广州数控毛坯文件
*.wcd	三菱数控 NC 代码文件

(6)NC 文件进入 NC 代码异常检测模块,NC 代码异常检测模块包括内容过滤组件、词法/语法检测组件、防碰撞组件。

首先,由内容过滤组件,实现 NC 代码中涉密信息过滤,如删除代码注释行或删除注释行中关键字,防止敏感数据通过 NC 代码进行传递。

其次,同步进行词法/语法错误检测和防碰撞检测,此时需要对 NC 代码中的每个程序段进行逐行扫描,逐行检测。其中词法/语法检测组件,目的在于识别 NC 代码中的错误词法或语法;防碰撞组件,目的在于运行 NC 代码之前,自动检查刀具和工件、夹具、机床单元之间的干涉,进行程序优化,提出修订意见及标记注意事项,实现防碰撞。

词法/语法错误检测规则库[12-15]包括:出现小写字母,[]号不匹配;非法字地址;非法 G 代码;非法 M 代码;小数点错误;同组 G 代码缺少 G17/G18/G19;T 代码后无换刀 M06;某些系统程序开始需要有无条件倒带指令“%”,无此指令则出错;某数控系统要求 T 指令范围为 1~99,超出该范围,即出错。

防碰撞检测规则库包括:如坐标系原点未设定,程序段结束时模态指令未取消;公制单位与英制单位换算等。此规则库是实践经验集合,汇总了各类由编程间接引发的碰撞事故。

如命中词法/语法规则或防碰撞规则,则对该行程序注释行添加标记信息,如“非法 G 代码”“刀补值未设定,有撞刀风险”,被编辑后的 NC 代码进行本地留存并进入步骤(7)。如未命中词法/语法规则或防碰撞规则,则直接进入步骤(7)。

(7)通信代理模块将检查后的 NC 代码文件行通过文件共享协议(FTP、SMB 等)完成文件发送,通信结束。

(8)截断通信主客体之间的通信,错误警报模块完成告警日志生成,且可上传第三方应用及平台。

4.3 工业母机防火墙效果分析

工业母机防火墙通过访问控制模块进行通信认证,通过防病毒模块完成病毒查杀,通过 NC 代码合规性检测模块实现 NC 代码的后缀名及文件容量验证,通过 NC 代码异常检测模块实现 NC 代码的词法/语法错误检测及防碰撞检测,这些安全机制结合起来,不仅可解决 NC 代码被篡改、敏感信息泄露等技术问题,而且有效降低了数控机床干涉事故的发生,实现业务安全与网络安全的双防护。

2022 年 1 月份,工业母机防火墙正式部署在某大型汽车制造企业加工中心,自部署工业母机防火墙以来,已获取日志数量:6 037 949 条,触发检测规则:63 条(包含永恒之蓝漏洞利用(MS17-010)攻击;浏览器插件导致内存耗尽的攻击等),有效地防止了网络攻击事件的发生。此外,部署工业母机防火墙还取得了明显的经济效果,至今一年时间未发生一起因操作不当造成的碰撞事故。按此加工中心 2021 年有记录的碰撞事故计算,已避免损失近 50 万元。经过近一年的效果检测,完满地完成了产品既定设计目标。

目前,本文研究内容获得了“2021 年工业互联网高质量发展工程联网数控数控机床安全项目”(项目号:TC210H02L)支持,研究成果已完成产品化。

5 基于工业母机防火墙的数控网络安全防护方案

数控网络安全防护方案设计思路基于《网络安全法》和《关键信息基础设施安全保护条例》规定,按照《GB/T 37955-2019 信息安全技术 数控网络安全技术要求》《信息安全技术网络安全等级保护基本

要求》[16]中通用要求和工业控制系统的扩展要求，同时结合了 P2DR 安全模型和 IATF 信息保障技术框架理念，分别建设安全技术体系和安全管理体系。通过构建一个中心(安全管理中心)三重防护(安全通信网络、安全区域边界、安全计算环境)，打造数控网络安全纵深防护体系；再结合各种管理手段、安全策略，提供多维度、全方位的网络安全防护能力，从而形成有效防护、及时响应的安全防御体系。基于安全现状和安全设计思路，整体安全架构设计如图 4 所示。

5.1 安全通信网络建设

(1)安全域划分：根据数控网络的重要性、功能等因素划分不同安全域，包括数控设备层、监督控制层、运营管理层，其中数控设备层根据车间不同进行安全域区分。

(2)带宽管理：考虑到数控网络的健壮性，需要通过流量管理实现控制指令、NC 代码的有效传输，须部署工业母机防火墙，根据业务实际需求智能分配业务带宽，防止业务流量(NC 代码上传/下载、数控监控数据上传)抢占情况出现，保证了数控网络的高可靠性、高可用性。

(3)通信传输：考虑到数控网络数据机密性，需要通过加密数控网络流量来保护传输的关键信息不会被窃取和篡改，此时须部署工业母机防火墙。工业母机防火墙采用专用硬件进行加密，支持 SM2、SM3、SM4 国密算法，具有更高的安全强度和网络性能。

5.2 安全区域边界建设

(1)边界防护：根据安全域划分，监督控制层与运营监控层间、数控机床前端，分别部署工业母机防火墙进行逻辑隔离，实现身份认证和授权、非法内外联检查等能力。

(2)访问控制：在各个安全区域边界部署工业母机防火墙，依据最小化原则配置访问控制策略，实现基于五元组的访问控制、白名单匹配、工业协议深度包检测及过滤、NC 代码检测及过滤等能力。访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。

(3)入侵防范/恶意代码防范/安全审计：工业母机防火墙作为数控网络专用设备，实现了入侵防范、恶意代码查杀、安全审计功能的集成，该产品符合《GB/T 37933-2019 信息安全技术 工业控制系统专用防火墙技术要求》[16]《GA/T 1177-2014 信息安全技术 第二代防火墙安全技术要求》[17]的双标准测试认证要求，可以精简安全设备的部署。

通过在各个安全区域边界/数控机床前端部署

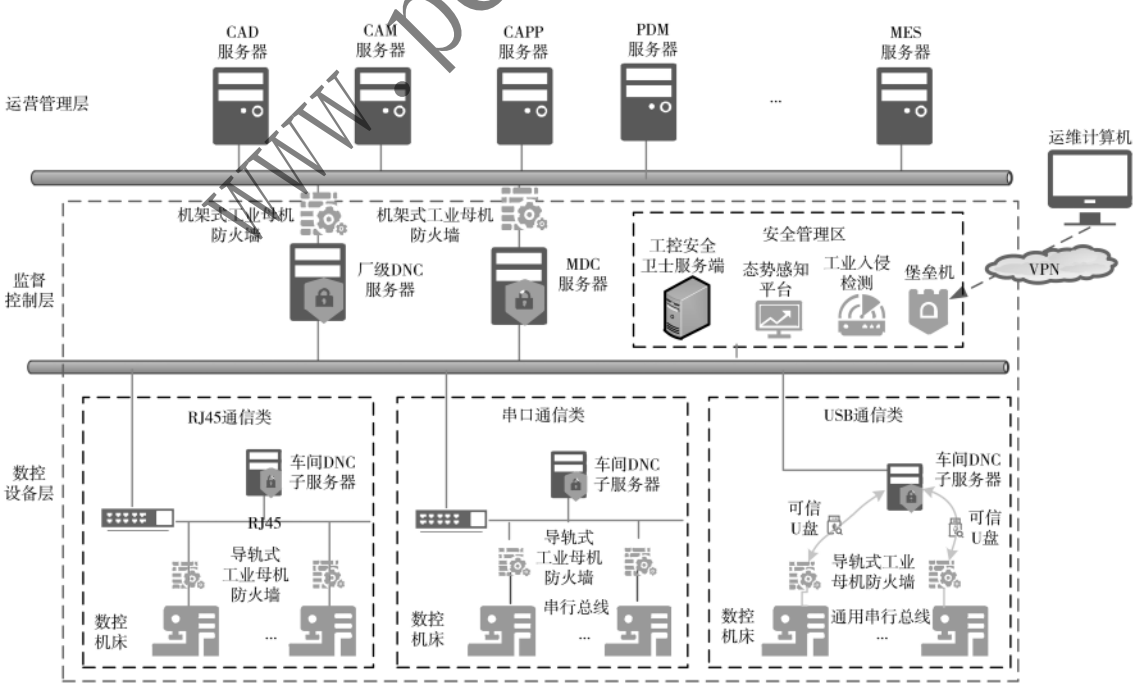

图 4 数控机床网络安全防护拓扑图

工业母机防火墙,实现基于攻击特征的网络攻击检测,提供数控通信协议审计、程序异常行为检测等事件的实时审计能力,实现基于通信流量的启发式和流式恶意代码查杀,阻止病毒传播和恶意软件入侵事件。

5.3 安全计算环境建设

(1)服务器计算环境安全

数控机床计算机一般采用专用系统或精简的Windows系统,且无法为系统及时的更新补丁,所以更适合用主机白名单软件做病毒防护和恶意软件防护。通过部署主机白名单软件,实现身份鉴别、访问控制、恶意代码防范等功能。

(2)数控机床计算环境安全

“应使用专用的设备及软件对控制设备进行更新”作为等级保护制度对工控设备运维的最新要求,市场却无专用的工控设备运维工具,堡垒机并不适用于工控设备运维,通过使用具备U口/串口/网口运维能力工业母机防火墙就显得尤为重要。通过在数控机床前端部署工业母机防火墙,作为数控机床运维专用设备,实现控制设备固件更新及运维。

5.4 安全管理中心建设

为实现安全设备的统一管理、策略下发、日志收集,须部署安全管理平台/厂级态势感知系统,实现对数控网络中的安全产品及安全事件进行统一管理。

为实现对运维操作行为的管控和审计,须部署安全运维管理系统(堡垒机),用于用户管理、授权管理、认证管理和综合审计,实现安全设备的运维管理。

5.5 安全管理要求建设

应从组织机构、管理制度、人员管理、系统建设、运维管理多个维度落实安全管理要求。首先,明确网络安全负责人和管理组织,企业主要负责人是网络安全第一责任人,明确关键岗位和职责等。其次,进行管理制度建设,涵盖一级文件(网络安全方针、战略),二级文件(管理规定、办法),三级文件(操作流程、作业指导书、模板等),四级文件(各类表单、报告等)。最后,对制度文件进行发布、执行等管理。

6 结论

随着先进制造技术、人工智能技术的发展,数控机床的技术创新及产品换代也将加速,数控机床呈现出“高速化、高精度化、复合化、智能化、开放化、网络化、绿色化”的技术趋势,也要求网络安全防护能力能同步适应行业技术发展。

本文通过对数控机床网络安全现状、数控机床发展趋势、数控机床防护技术的分析,提出了一种基于工业母机防火墙的数控机床网络安全防护体系建设思路,该安全防护体系主要从安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理要求、专用防护设备等方面给出了数控机床网络安全的具体防护措施和建议,以期推进打造数控机床安全供给能力,护航制造强国、数字中国等战略目标。

参考文献

[1] 国家标准化管理委员会.GB/T 37955-2019 信息安全技术 数控网络安全技术要求[S].2019-08-30.

[2] Okuma.OSP 用病毒防御系统 OSP-VPS[EB/OL].[2022-xx-xx].https://www.okuma.co.jp/chinese/smart-factory/osp-suite/osp-vps.html.

[3] 国家国防科技工业局.航天科工研制出国内首款数控加工信息安防产品[EB/OL].(2014-09-09).http://www.sastind.gov.cn/n137/n13098/c406631/content.html.

[4] 国家标准化管理委员会.GB/T 37933-2019.信息安全技术 工业控制系统专用防火墙技术要求[S].2019-08-30.

[5] 国家标准化管理委员会.GB/T 37934-2019.信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求[S].2019-08-30.

[6] 周晓枫,王子伟,张天赋,等.数控技术的国内外分析与发展趋势的展望[J].中国设备工程,2018(16):195-196.

[7] 蔡锐龙,李晓栋,钱思思.国内外数控系统技术研究现状与发展趋势[J].机械科学与技术,2016,35(4):493-500.

[8] 邹大均,黄沾.基于国产密码算法的数控系统安全解决方案[J].通信技术,2018(2):463-470.

[9] 赵甫,王琦魁,宋永立.一种针对数控系统的通信防护设备:中国,105978871[P].2016-05-09.

[10] 吴飞,霍松林.基于串口通信的DNC技术研究[J].武汉理工大学学报(信息与管理工程版),2009(6):41-43.

[11] 李存志,邢建国.NC代码检错与仿真系统的开发

(下转第33页)

(2016 年 4 月 19 日)[EB/OL].[2022-09-09].http://www.gov.cn/xinwen/2016-04/25/content_5067705.htm.
[7] 梁晴.绿盟科技战略解决方案系列介绍——金融行业供应链安全解决方案[Z/OL].[2022-09-09].https://mp.weixin.qq.com/s/Ms-3kxqQqEnFST6slGdlZA.
[8] 郭启全.认真落实网络安全等级保护制度,构建新时代国家网络安全综合防控体系[Z/OL].[2022-09-09].https://mp.weixin.qq.com/s?__biz=MzU1O-DM1Njc1Ng.
[9] 盘善海,裴华.高安全等级网络安全防护体系研究与设计[J].通信技术,2021,54(7):1715-1720.
[10] 魏昊.强化供应链安全保障工作,保护关键信息基础设施安全[EB/OL].[2022-09-09].http://www.cac.gov.cn/2021-08/31/c_1632032388356198.htm.

(收稿日期:2022-09-09)

作者简介:

庞彬彬(1985-),男,本科,高级安全顾问,主要研究方向:关键信息基础设施安全、云安全、数据安全。

(上接第 16 页)

研究[J].青岛大学学报(自然科学版),2015,28(4):72-76.
[12] 胡腾,郭曦鹏.机床空间误差完备建模方法与 NC 代码优化补偿技术[J].工程科学与技术,2019,51(6):190-199.
[13] 潘鋆,韩京辰,于丹,等.基于形式化模型的 NC 代码异常检测[J].微电子学与计算机,2021,38(11):81-87.
[14] 潘忠英.朴素贝叶斯中文文本分类器的设计与实现[J].电脑编程技巧与维护,2021(2):37-39.
[15] 国家标准化管理委员会.GB/T 25070-2019.信息安全技术 网络安全等级保护安全设计技术要求[S].2019-05-10.
[16] 国家标准化管理委员会.GA/T 1177-2014.信息安全技术 第二代防火墙安全技术要求[S].2014-07-24.

(收稿日期:2022-10-08)

作者简介:

王晓鹏(1979-),男,硕士研究生,高级工程师,主要研究方向:工业互联网安全、物联网安全、边缘计算安全、工业数据安全、智能制造安全。

张雄杰(1987-),男,本科,高级工程师,主要研究方向:工业互联网安全、物联网安全。

陈毅真(1982-),男,本科,高级工程师,主要研究方向:工业互联网安全、物联网安全。

(上接第 24 页)

参考文献

[1] 发改能源[2020]283 号文:《关于加快煤矿智能化发展的指导意见》[Z].2020.
[2] 王丹识,韩鹏军,王荣博,等.我国煤炭企业网络安全现状、问题分析研究与建议[J].中国煤炭,2022,48(7):34-40.
[3] ABDO H,KAOUK M,FLAUS J M,et al.A safety/security risk analysis approach of industrial control systems:a cyber bowtie-combining new version of attack tree with Bowtie analysis[J].Computers & Security,2018,72:175-195.
[4] SARKAR P,CHAKRABARTID,JORDAN M.Nonpara-metric link prediction in large scale dynamic networks[J].Electronic Journal of Statistics,2014,8(2):2022-2065.
[5] 张敏,魏伟,谭天怡,等.数据分类分级及其发展路径研究[J].网络安全与数据治理,2022,41(1):18-22,29.

(收稿日期:2022-10-25)

作者简介:

王许培(1989-),男,本科,助理工程师,主要研究方向:能源工业互联网安全、数据安全、物联网安全等。

王伟刚(1990-),男,本科,助理工程师,主要研究方向:能源工业互联网安全、移动互联网安全等。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部