工业互联网产业联盟
Alliance of Industrial Internet

工 业 互 联 网 产 业 联 盟 标 准

AII/026-2021

数控系统商用密码应用技术要求

Specifications of Commercial Cryptographic application for CNC systems

工业互联网产业联盟

（2021 年 12 月 30 日发布）

声 明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由工业互联网产业联盟提出并归口。

标准牵头：北京交通大学、广州数控设备有限公司。

标准起草单位和主要起草人：

- 北京交通大学：陶耀东、李浥东
- 广州数控设备有限公司：何英武、陈剑飞
- 工业和信息化部电子第五研究所：吴波、韦永霜
- 北京中宇万通科技股份有限公司：宁宇鹏 李季
- 江南信安(北京)科技有限公司：白锦龙，徐剑南
- 北京双湃智安科技有限公司：黄东华、徐书珩
- 北京信安世纪科技股份有限公司：汪宗斌，付军
- 奇安信科技集团股份有限公司：纪胜龙、靳佑鼎
- 中国信息通信研究院：徐秀，马聪
- 中国工业互联网研究院：于成丽 焦智灏
- 郑州信大捷安信息技术股份有限公司:刘为华
- 沈阳中科数控技术股份有限公司：胡毅、张丽鹏
- 北京凯恩帝数控技术有限责任公司：杨洪丽

引　言

随着新一代信息技术和制造业的深度融合，数控系统在制造业和国家产业布局中作用愈发重要，面对工业互联网的攻击手段对工控网络和工业生产带来的安全隐患，制造业的核心组件-数控系统的安全隐患也逐渐暴露出来，数控系统安全防护基础薄弱，缺乏基于密码学加密、数据存储、安全认证等信息安全防护措施。依据《密码法》、《数据安全法》、《网络安全法》等法律法规规定，结合数控系统网络化、智能化技术发展趋势，制定数控系统信息安全中的密码应用技术相关规范已势在必行。

本文件旨在指导智能制造及相关领域企业进行数控系统的设计开发、生产制造、应用场景等多个方面安全防护要求，保证数控系统稳定、高效、安全运行，推动密码技术在数控系统中标准化应用推广，提高数控系统的整体安全防护水平。

数控系统商用密码应用技术要求

1 范围

本文件规定了数控系统商用密码应用的技术要求，包括商用密码应用的总体要求、密码应用技术框架、对应不同安全级别的具体密码应用技术要求等。

本文件适用于指导、规范和评估数控系统中的商用密码应用的设计、实现和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 8129 工业自动化系统 机床数值控制 词汇

GB/T 25069-2010 信息安全技术 术语

GB/T 36968 信息安全技术 IPSec VPN技术规范

GB/T 37092-2018 信息安全技术 密码模块安全要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GM/T 0024 SSL VPN技术规范

GM/Z 4001 密码术语

3 术语和定义及缩略语

3.1 术语和定义

GB/T 8129、GB/T 25069、GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1.1

工业互联网 industrial internet

满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

[来源：YD/T 3804-2020，3.1.1]

3.1.2

数控系统 Computerized Numerical Control（CNC）

计算机数值控制系统。

3.1.3

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.1.4

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.1.5

公钥 public key

非对称密码算法中可以公开的密钥。

3.1.6

公钥证书 public key certificate

一种数字证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.1.7

会话密钥 session key

在一次会话中使用的数据加密密钥。

3.1.8

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.1.9

数据完整性 data integrity

数据没有遭受以非授权方式所做的篡改或破坏的性质。

3.1.10

真实性 authenticity

一个实体是其所声称实体的这种特性。真实性适用于用户、进程、系统和信息这类的实体。

3.1.11

抗抵赖 non-repudiation

也称不可否认，证明一个操作或事件已经发生且无法否认的机制。

3.1.12

鉴别 authentication

确认一个实体所声称的身份或信息的真实性。

3.1.13

密码模块 cryptographic module

实现密码运算功能的，相对独立的软件、硬件、固件及其组合。

3.1.14

密码算法 cryptographic algorithm

描述密码处理过程的运算规则

3.1.15

密码协议 cryptographic protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到特定目的而采取的一系列步骤。

3.1.16

密码杂凑函数 cryptographic hash function

又称密码散列函数或密码哈希函数，将一个任意长的比特串映射到一个固定长的比特串的函数，且满足下列特性：

为一个给定的输出找出一个能映射到该输出的一个输入是计算上困难的；

为一个给定的输入找出一个能映射到同一个输出的另一个输入是计算上困难的；

要发现不同的输入映射到同一个输出是计算上困难的。

3.1.17

密钥管理 key management

根据安全策略，对密钥进行的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.1.18

密钥协商 key agreement

两个或多个实体通过相互传送一些消息来共同建立一个共享的秘密密钥的协议，且各个实体无法预先确定这个秘密密钥的值。

3.1.19

审计 audit

对信息系统的记录和活动进行的独立观察和考核。

3.1.20

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗低赖性。

3.1.21

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.1.22

消息鉴别码 message authentication code

又称消息认证码，是消息鉴别算法的输出。

3.1.23

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

3.1.24

SM3 算法 SM3 algorithm

一种杂凑密码算法，其输出为256比特。

3.1.25

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

3.1.26

数控 APP（CNC APP）

依托于工业互联网平台、公有云或私有云，基于平台的技术引擎、资源、模型和业务组件，将数控领域工业机理、技术、知识、算法与最佳工程实践按照系统化组织、模型化表达、可视化交互、场景化应用、生态化演进原则而形成的**数控系统**应用程序。

3.1.27

数控应用信息系统（CNC Application information system）

指部署在工业互联网平台、公有云、私有云或企业内网服务器上，与数控系统进行直接或间接通讯，并完成某一类具体应用的各类应用信息系统的总称，包括：数控APP、CAD/CAM、CAPP、DNC/MDC等。

3.2 **缩略语**

下列缩略语适用于本文件。

CNC：数控系统（Computerized Numerical Control）

NC：数字控制（Numerical Control）

PLC：可编程逻辑控制器（Programmable Logic Controller）

SE：安全单元（Secure Element）

UID：用户身份证明(User Identification)

USB：通用串行总线（Universal Serial Bus）

4 总体要求

4.1 密码算法

数控系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，并使用保证安全强度的密码算法，不使用存在已知漏洞和缺陷的密码算法，如DES、SHA-1等。

4.2 密码技术

数控系统中使用的密码技术应遵循密码相关国家标准和行业标准。

4.3 密码产品

数控系统中使用的密码产品与密码模块应经商用密码认证机构认证合格。

4.4 密码服务

信息系统中使用的密码服务应符合法律法规的相关要求，需依法进行检测认证的，应经商用密码认证机构认证合格，并提供持续安全可靠的服务能力。

5 数控系统应用模型及密码应用技术框架

5.1 数控系统组成架构

数控系统一般由数控装置和驱动装置组成。数控装置主要由硬件、软件和数据组成，完成如编译、中断、诊断、管理、刀补、插补等各种控制任务，以及具备界面的显示、程序编程、手动操作和外部设备通讯等人机功能，是数控系统与外部交互的主要组件。硬件包括：处理器、运动控制器、存储器、内存、I/O 接口、USB 接口、现场总线接口、网络接口和符合要求的密码模块；软件包括：人机交互、解释器、运动控制器、I/O 控制器等；数据包括：NC 代码、PLC 程序、工艺参数、通信协议、日志、账户等。详细组成架构如图 1 所示。

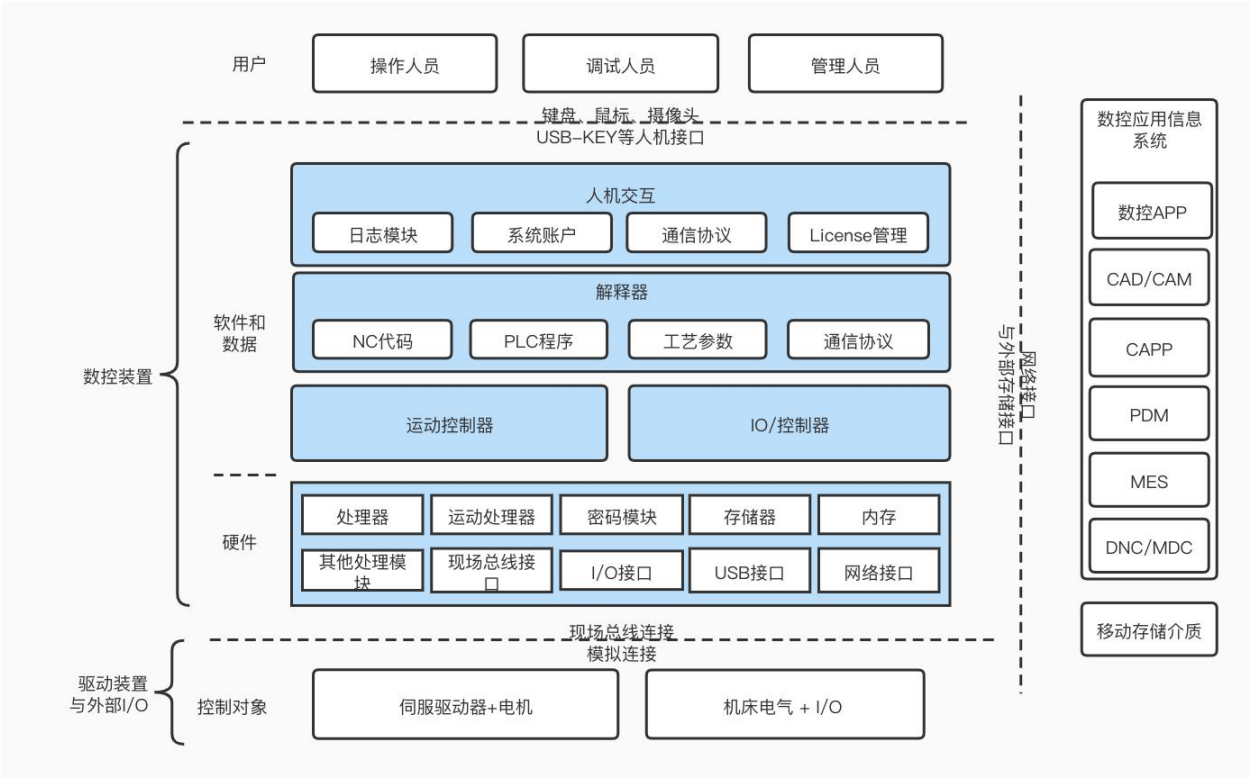

图 1 数控系统组成架构

5.2 数控系统安全需求

数控系统的关键操作被错误执行，关键指令被重放、篡改或未按照顺序执行，敏感数据泄露、丢失、被篡改时，将会影响数控系统功能正常运行。

a)关键操作包括：PLC 程序修改与拷贝、宏程序修改与拷贝、系统轴数修改、关键工艺包启用、License 更新、远程监视、远程控制等；

b）关键指令包括：数控系统启动或停止、PLC 启停、固件更新、密码功能开启或关闭等；

c）敏感数据包括：加工设备的 NC 代码、PLC 程序、工艺参数、运行数据、日志信息，身份信息，账号口令，位置信息等，数控云平台的云端多媒体信息，业务流程数据，设备状态信息等。

数控系统的安全需求主要包括：数控系统实体（数控设备、系统用户等）的身份鉴别和权限控制需求；数控系统固件、软件的完整性需求；NC 代码、PLC 程序、配置信息、工艺参数、状态信息、账号口令的机密性需求和完整性需求；系统配置、加工、系统维护中关键操作和关键指令的真实性和抗抵赖性需求；数据传输的机密性和完整性需求等。

5.3 数控系统应用模型

数控系统密码安全保护框架由数控系统本体安全（数控系统的固件、基础软件、配置信息、状态信息、身份信息、账号口令等的机密性、完整性）、数控系统数据安全（NC 代码、PLC 程序、工艺参数等的机密性、完整性）、数控系统与应用信息系统、移动存储介质、操作人员的通讯安全、密码配置和密钥管理，数控 APP 安全（数控 APP 中的多媒体信息、业务流程数据、设备状态信息、模型数据等的机密性、完整性）构成，其相互关系如图 2 所示。

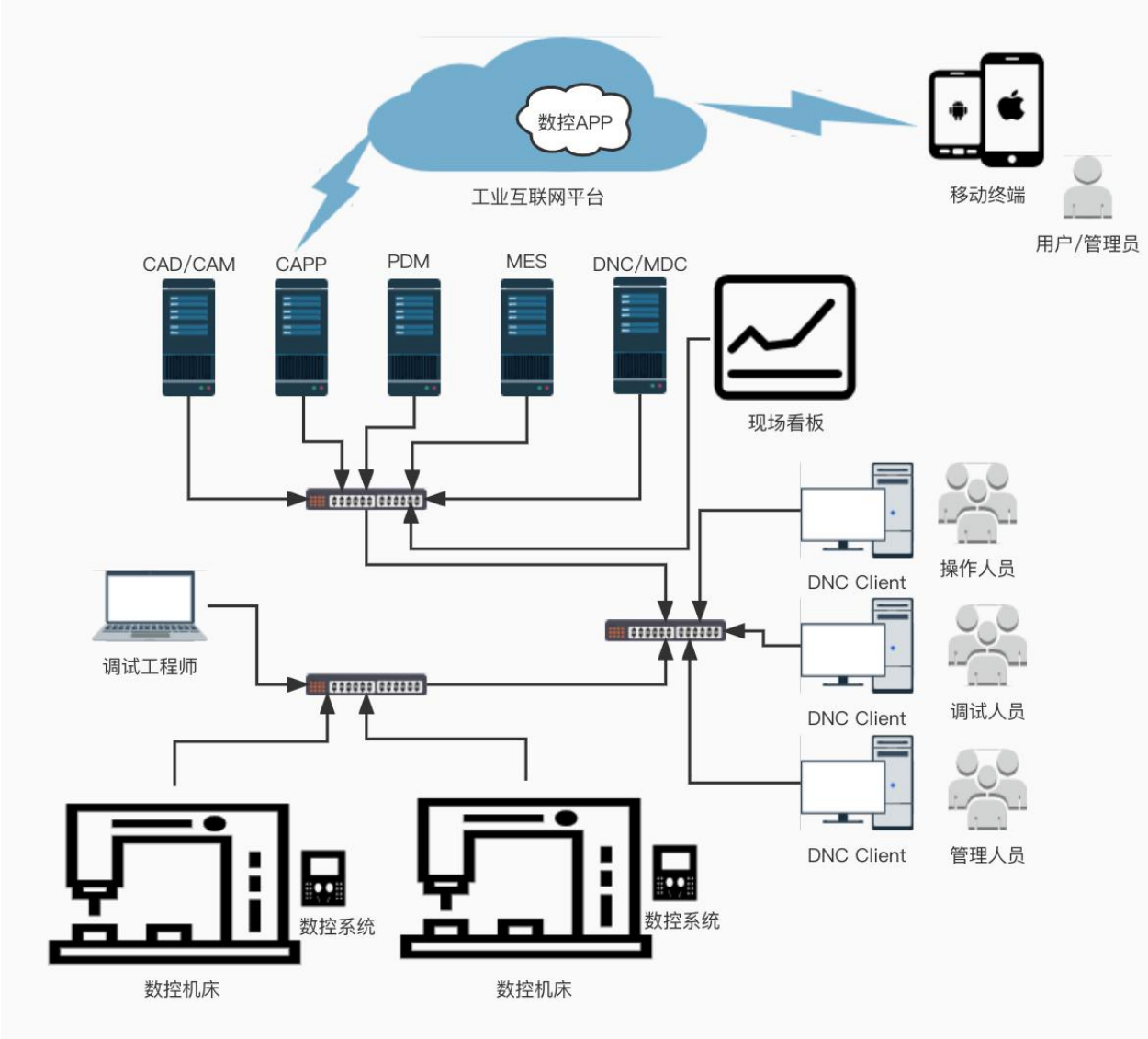

图 2 数控系统的安全应用环境

5.4 数控系统密码应用技术框架

数控系统密码应用技术框架如下图所示：

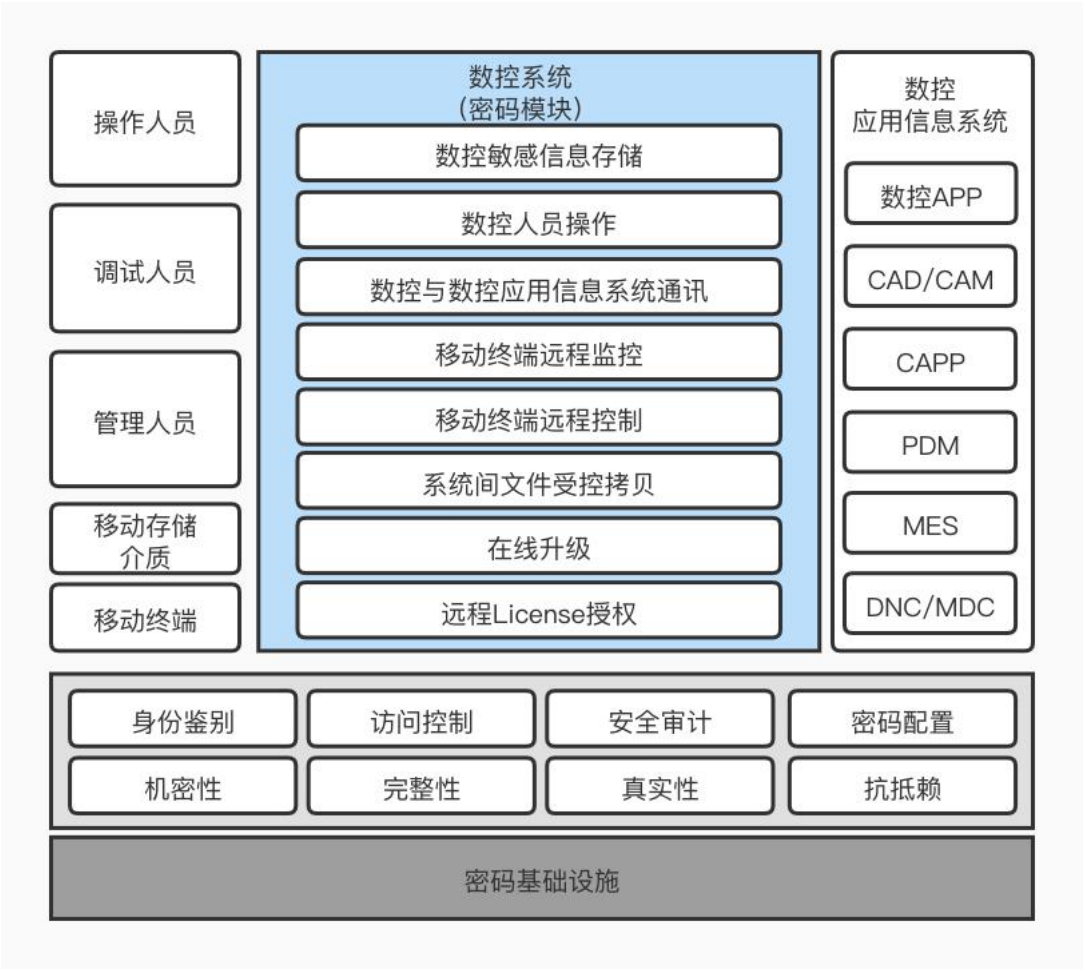

图 3 数控系统密码应用技术框架

数控系统密码应用与外部的交互对象主要包括：操作人员、数控应用信息系统和密码基础设施，依托密码基础设施，数控系统应用密码技术实现机密性、完整性、抗抵赖、真实性、身份鉴别、访问控制等功能。数控系统与数控 APP、CAD、CAM、CAPP、PDM、MES、DNC、MDC 等数控应用信息系统之间的通讯、文件传输等需要应用密码技术保护；操作人员对数控系统进行操作、系统间文件受控拷贝、移动终端远程监控、移动终端远程管理、远程 License 授权需要应用密码技术保护；数控系统进行远程 License 授权、在线升级等需应用密码技术保护。

5.5 机密性

5.5.1 存储信息的机密性

对存储在数控系统内的敏感信息数据、导入导出文件等采用密码算法进行加密保护。确保除合法主体外,其余任何主体不能获得该数据，即使数控系统的任何部分损坏或失效，以及非授权访问等都不会导致敏感信息的泄露,以保证数控系统数据存储的机密性。

存储信息的机密性保护应采用密码算法加密完成。

5.5.2 传输信息的机密性

数控系统与其他应用信息系统进行通信时，数控系统对传输的敏感数据或整个通信报文应采用密码算法进行加密保护，保证该传输数据在被截获后无法得到明文数据，达到数据传输的机密性要求。

数控系统与移动存储介质传输时，应传输经过密码算法进行加密保护后的文件，确保外部介质上的文件被非法窃取后，无法得到明文数据，达到数据离线传输的机密性要求。

数控系统与外部系统进行通信时，考虑到系统兼容性，数控系统应对传输的敏感信息数据或整个报文采用传输前加密、通过安全加密隧道传输等方式完成，保证该传输数据在被截获后无法得到明文数据，达到数据传输的机密性要求。建立安全加密隧道的具体规范可参考 GB/T 36968、GM/T 0024 等。

5.6 完整性

5.6.1 存储信息的完整性

数控系统采用密码技术对存储在数控系统内的敏感信息数据、导入导出文件等进行完整性保护，采用消息鉴别码数字签名的密码技术对数据进行校验计算，以发现数据被篡改、删除和插入等情况，确保存储数据的完整性。

5.6.2 传输信息的完整性

数控系统与其他系统进行通信时，数控系统对传输的敏感数据或整个报文应采用密码算法进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

数控系统与移动存储介质进行传输时，传输应采用密码算法进行加密保护后的文件的校验计算，以发现文件被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

5.7 抗抵赖

5.7.1 概述

使用数字签名等密码技术实现实体行为的不可否认性，针对在数控系统中所有需要无法否认的行为，包括 NC 代码导出导入和执行加工、PLC 程序导入导出、发送敏感数据等操作。

5.7.2 用户操作抗抵赖

用户进行关键操作（如 NC 代码导出、导入、执行加工等）时，需要使用用户证书对操作记录进行数字签名，用于关键事件回溯，达到用户操作抗抵赖要求。

关键操作包括：PLC 程序修改与拷贝、宏程序修改与拷贝、系统轴数修改、关键工艺包启用、License 更新、远程监视、远程控制等。

5.7.3 数控指令抗抵赖

具备数控关键指令抗抵赖功能的数控系统应用信息系统在发送关键指令（如数控系统启动或停止、PLC 启停、固件更新等）时，需要对发送数据进行数字签名。

具备指令验证功能的数控系统在接收到关键指令时，需要对接收指令进行数字验签，达到数控指令抗抵赖要求。

关键指令包括；数控系统启动或停止、PLC 启停、固件更新、密码功能开启或关闭等。

5.7.4 数控系统抗抵赖

数控系统抗抵赖是指数控系统采用密码算法对敏感数据进行数字签名操作，确保产生该数字签名的数控系统不能成功地否认曾经生成过该数据。接收数据的应用信息系统能获得证明数控系统生成数据的证据，而且该证据可由该主体或第三方验证。

数控系统应用信息系统或操作人员通过存储数控系统产生的数字签名来实现数控系统抗抵赖功能。

敏感数据包括：加工设备的 NC 代码、PLC 程序、工艺参数、运行数据、日志信息，身份信息，账号密码，位置信息等，数控云应用包含的多媒体信息，业务流程数据，设备状态信息等。

5.7.5 应用信息系统抗抵赖

支持应用信息系统抗抵赖时，应用信息系统应具有产生数字签名功能。

数控系统具有应用信息系统抗抵赖功能时，即数控系统作为签名信息的验证主体时，数控系统应能够对应用信息系统产生的数字签名进行存储和验证，达到应用信息系统抗抵赖的要求。

5.8 身份鉴别

5.8.1 账号与口令鉴别

数控系统应支持基于账号与口令方式的对用户身份真实性进行认证。

应对登录系统的账户进行验证，用户口令不能以明文方式存储，用户口令应使用 SM3 散列函数循环散列若干次，并保存最终的散列值。散列的次数宜不小于 500 次。

5.8.2 唯一标识符鉴别

采用与数控系统唯一标识符相关的验证码鉴别方式。

唯一标识符鉴别需要在数控系统中存储UID以及验证码(MAC)，该MAC是由UID与相关应用信息关联后采用密码算法计算产生并在数控系统写入。

5.8.3 身份鉴别

5.8.3.1 数控系统对应用信息系统的挑战响应鉴别

数控系统应采用基于数字证书的挑战响应鉴别方式对应用信息系统身份的真实性进行鉴别。

数控系统应设定不成功鉴别的尝试次数，当达到或超过规定的次数时，数控系统应停止再次尝试挑战响应鉴别操作。

5.8.3.2 应用信息系统对数控系统的挑战响应鉴别

应用信息系统应采用基于数字证书挑战响应鉴别方式对数控系统身份的真实性进行鉴别。

5.9 访问控制

数控系统数据访问控制采用密码算法对敏感数据读写、密钥存储、密钥更新等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制，阻止非授权访问。

对数控系统各个功能模块或组件的访问只能按照数控系统所设置的访问控制权限进行相关操作。对数控系统各个功能模块或组件进行访问的主体可能是操作员、应用信息系统等。

5.10 审计记录

数控系统应具备审计功能，对涉及数控系统安全的数据及相关操作（存在潜在的安全风险）进行记录并存储，内容至少包括操作主体、操作对象、操作时间、执行动作等，并采取有效措施保证记录信息的安全，用于数控系统对于异常事件的追溯并评估所记录数据和操作的安全性。

对于敏感数据的记录，需要使用信息校验码进行完整性保护后存储。

5.11 密码模块

5.11.1 基本要求

密码模块满足下列要求：

a） 应支持国产商用密码算法等标准算法；

b） 应符合国家密码管理政策法规和GB/T 37092的规范要求；

c） 关键密钥应采专用硬件密码模块进行保护，如SE、TEE等。

5.11.2 密码算法技术要求

密码算法满足下列要求：

a） 应支持对称密码算法 SM4，对数据信息的存取、传输进行机密性保护；

b） 应支持非对称密码算法 SM2，对数据信息进行签名和验签，达到对敏感信息和关键操作的抗抵赖保护；

c） 应采用密码散列算法 SM3，对数据信息的存取、传输进行完整性保护。

5.11.3 密码设备技术要求

密码设备满足下列要求：

a） 应具备密钥配置、密钥生成、密钥保存、密钥更新、密钥失效等密钥管理功能；

b） 应具备数字证书颁发、延期、更新及注销等数字证书管理功能；

c） 应通过商用密码检测机构的检测认证。

6 数控系统密码应用安全分级及技术要求

6.1 安全分级

根据不同场景的密码应用安全技术要求，参考 GB/T 39786，将数控系统划分为基础级和增强级二个级别，在各个级别规定了数控系统密码应用应支持的最低安全防范措施，用户可根据不同的安全需求进行级别选择。

a）基础级适用于一些对安全性具有一定要求的应用，应采用机密性、完整性、真实性、身份鉴别、访问控制、安全审计和密码配置功能；

b）增强级适用于一些对安全性具有较高要求的应用，应采用机密性、完整性、真实性、抗低赖性、身份鉴别、访问控制、安全审计和密码配置功能。

6.2 各级别密码应用安全技术要求

6.2.1 密码应用安全要素

6.2.1.1 机密性

数控系统应采用商用密码技术保证机密性，具体包括：

a) 采用密码技术保证存储信息数据在存储过程中的机密性，包括但不限于敏感信息数据、文件等；

b) 采用密码技术保证传输信息数据在传输过程中的机密性，包括但不限于敏感信息数据和文件的传输、关键操作指令的传输等。

6.2.1.2 完整性

数控系统应采用商用密码技术保证完整性，具体包括：

a) 采用密码技术保证存储信息数据在存储过程中的完整性，包括但不限于敏感信息数据、文件等；

b) 采用密码技术保证传输信息数据在传输过程中的完整性，包括但不限于敏感信息数据和文件的传输、关键操作指令的传输等。

6.2.1.3 真实性

数控系统应采用商用密码技术保证真实性，具体包括：

a) 采用密码技术对登录的用户进行身份鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，使用密码技术的真实性功能来实现鉴别信息的防假冒。

b) 采用密码技术在与数控应用信息系统通信前进行身份认证，实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和数控系统身份的真实性；

c) 采用密码技术对数控系统身份唯一标识符进行鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证数控系统用户身份的真实性；

6.2.1.4 抗抵赖

数控系统应采用商用密码技术保证操作和通讯的抗抵赖性，具体包括：

a) 采用密码技术实现数控指令的不可否认性，达到数控指令抗抵赖；

b) 采用密码技术实现用户操作的不可否认性，达到用户操作抗抵赖；

c) 采用密码技术实现数控系统的不可否认性，达到数控系统抗抵赖；

d) 采用密码技术实现其他系统的不可否认性，达到其他系统抗抵赖。

6.2.1.5 访问控制

数控系统应采用商用密码技术对各类操作进行访问控制，具体包括：

a) 采用密码技术对敏感数据读写、密钥存储、密钥更新等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制，阻止非授权访问；

b) 对数控系统各个功能模块或组件的访问按照数控系统所设置的访问控制权限进行相关操作。对数控系统各个功能模块或组件进行访问的主体可能是操作员、中间件、数控应用信息系统等。

6.2.1.6 安全审计

数控系统应采用商用密码技术对各类操作进行安全审计，具体包括：

a) 具备审计功能，对涉及数控系统安全的敏感数据数据和关键操作（存在潜在的安全侵害）进行记录并存储，内容至少包括操作主体、操作对象、操作时间、执行动作等，并采取有效措施保证记录信息的安全，用于数控系统对于异常事件的追溯并评估所记录数据和操作的安全性。

b) 对于敏感数据的审计记录，使用信息校验码进行完整性保护后存储。

6.2.1.7 密码配置

采用符合 GB/T 37092 的二级及以上密码模块或通过国家密码管理部门检测认证的硬件密码产品实现密码运算和密钥管理。

采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

6.2.2 数控系统密码应用安全分级要求

基于不同的应用场景，数控系统密码应用安全分级要求如下表所示：

表1 基于应用场景的数控系统密码应用安全分级

序号	应用场景	密码安全要素	基本级	增强级
1	数控敏感信息存储	机密性	6.2.1.1 a）	6.2.1.1 a）
		完整性	——	6.2.1.2 a）
		真实性	6.2.1.3 a）	6.2.1.3
		抗抵赖	——	6.2.1.4
		访问控制	6.2.1.5 a)	6.2.1.5
		安全审计		6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
2	数控人员操作	真实性	6.2.1.3 a）	6.2.1.3
		抗抵赖	——	6.2.1.4
		访问控制	6.2.1.5 a)	6.2.1.5
		安全审计	6.2.1.6 a)	6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
3	数控与数控应用信息系统通讯	机密性	6.2.1.1 b)	6.2.1.1 b)
		完整性	——	6.2.1.2 b)
		真实性	6.2.1.3 b）	6.2.1.3 b）c)
		抗抵赖	6.2.1.4 a)b)	6.2.1.4
		访问控制	6.2.1.5 a）	6.2.1.5
		安全审计	6.2.1.6 a）	6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
4	数控移动终端远程监测	机密性	6.2.1.1 b)	6.2.1.1
		完整性	——	6.2.1.2
		真实性	6.2.1.3 a) b)	6.2.1.3
		抗抵赖	——	6.2.1.4

		访问控制	6.2.1.15 a)	6.2.1.5
		安全审计	6.2.1.6 a）	6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
5	数控移动终端远程控制	机密性	6.2.1.1 b)	6.2.1.1
		完整性	6.2.1.2 b)	6.2.1.2
		真实性	6.2.1.5 a)b)	6.2.1.5
		抗抵赖	——	6.2.1.4
		访问控制	6.2.1.5 a)	6.2.1.5
		安全审计	6.2.1.6 a)	6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
6	数控系统之间文件受控拷贝	机密性	6.2.1.1	6.2.1.1
		完整性	6.2.1.2 a）	6.2.1.2
		真实性	6.2.1.3 a)	6.2.1.3
		抗抵赖	——	6.2.1.4 b)c) d)
		访问控制	6.2.1.5 a)	6.2.1.5
		安全审计	6.2.1.6 a)	6.2.1.6
		密码配置	6.2.1.7	6.2.1.7
7	数控系统在线升级	机密性	6.2.1.1 b）	6.2.1.1
		完整性	6.2.1.1 a)	6.2.1.1
		真实性	6.2.1.3 b)	6.2.1.3
		抗抵赖	6.2.1.4 b)	6.2.1.4 b)c)d)
		安全审计	6.2.1.6 a)	6.2.1.6
8	数控系统的License远程授权	机密性	6.2.1.1 b)	6.2.1.1
		完整性	6.2.1.2 a)	6.2.1.2
		真实性	6.2.1.3 b）	6.2.1.3 a） b）
		抗抵赖	——	6.2.1.4 b） d）
		安全审计	6.2.1.6 a）	6.2.1.6

参考文献

[1]GB/T 20518　信息安全技术 公钥基础设施 数字证书格式
[2]GB/T 22239-2019　信息安全技术 网络安全等级保护基本要求
[3]GB/T 25064　信息安全技术 公钥基础设施 电子签名格式规范
[4]GB/T 26220　工业自动化系统与集成 机床数值控制 数控系统通用技术条件
[5]GB/T 32905　信息安全技术 SM3密码杂凑算法
[6]GB/T 32907　信息安全技术 SM4分组密码算法
[7]GB/T 32918（所有部分）　信息安全技术 SM2椭圆曲线公钥密码算法
[8]GB/T 35275　信息安全技术 SM2密码算法加密签名消息语法规范
[9]YD/T 3804-2020　工业互联网安全防护总体要求