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/025-2021

工业互联网
数控系统商用密码应用测评要求

Industrial internet—

Testing and evaluation requirement of commercial cryptographic application for CNC systems

工业互联网产业联盟

（2021 年 12 月 30 日发布）

工业互联网产业联盟

Alliance of Industrial Internet

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。

本文件在GB/T 39786-2021《信息系统密码应用基本要求》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、《数控系统商用密码应用技术要求》（制定中）、《信息系统密码应用测评要求》等技术类标准的基础上，根据现有技术的发展水平，提出和规定了针对于数控系统商用密码应用特点的数控系统商用密码应用测评要求。

本文件与《数控系统商用密码应用技术要求》（制定中）、《信息系统密码应用测评要求》共同构成了数控系统商用密码应用测评要求的相关标准。本文件是根据数控系统的特点，在《信息系统密码应用测评要求》基础上的进一步细化和扩展。

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这些专利的责任。

本文件由工业互联网产业联盟提出并归口。

标准牵头单位：工业和信息化部电子第五研究所、广州数控设备有限公司。

标准起草单位和主要起草人：

- 工业和信息化部电子第五研究所：吴波、韦永霜
- 广州数控设备有限公司：何英武、陈剑飞
- 北京交通大学：陶耀东、李浥东
- 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
- 中国信通院：徐秀，马聪
- 奇安信科技集团股份有限公司：纪胜龙、靳佑鼎
- 天润工业技术股份有限公司：宋协君、安传忠
- 郑州信大捷安信息技术股份有限公司：刘为华

引　言

在制造数字化与工业互联的趋势下，数控网络中敏感性的工艺信息、生产信息、运营信息成为制造企业关键数字资产，采集、传输、存储等环节的身份信息、权限信息、数字签名、控制指令等可能成为导致生产事故、环境灾害、人身财产安全等的重要安全要素。为了应对数控系统日益严峻的信息安全问题，开展数控系统商用密码应用测评规范研究，建立系统化、标准化的测评规范，是掌握数统系统信息安全风险、明确数控系统信息安全防护需求、验证和改进信息安全防护方案的重要支撑。

数控系统信息安全基础差、缺少以国产商用密码为核心的信息安全防护措施、缺少信息安全标准规范，使得研发基于密码技术的数控系统信息安全防护方案缺少参考依据，缺少方向指引，进而导致数控系统安全保障水平提升困难重重，进步缓慢。通过开展数控系统商用密码应用测评规范研究，可为数控系统信息安全防护方案研发提供参考依据，为数控系统信息安全防护方案改进升级提供方向，助力数控系统安全保障能力快速、有效提升。

本文件针对数控系统安全、数控系统数据安全、数控系统与数控网络和外部存储介质的通信安全、以及密码配置和密钥管理等内容，围绕密码在机密性、完整性、抗抵赖、身份鉴别、访问控制、安全审计等方面的应用，依据商用密码测评有关要求，从总体测评要求、基本测评要求两个方面研究建立数控系统商用密码应用安全性测评规范。

工业互联网 数控系统商用密码应用测评要求

1 范围

本文件规定数控系统不同安全等级商用密码应用的测评要求，从密码算法、密码技术、密码产品和密码服务、密码应用等方面，提出了商用密码应用总体测评要求；从数控系统的机密性、完整性、抗抵赖、身份鉴别、访问控制、审计记录和密码模块等技术层面提出商用密码应用基本测评要求，适用于指导不同安全保护等级的数控系统的商用密码应用安全性评估工作的开展。

本文件以数控系统采用的以商用密码技术为核心的信息安全防护技术、装置和产品为对象，适用于相关对象在设计、研发、测试、应用等环节的商用密码应用安全性评估工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 8129-2015 工业自动化系统 机床数值控制 词汇

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 39786-2021 信息系统密码应用基本要求

GB/T 37092-2018 信息安全技术 密码模块安全要求

GM/Z 4001-2013 密码术语

3 术语和定义

GB/T 39786-2021、GB/T 37092-2018、GM/Z 4001-2013中界定的相关术语和定义，以及下列术语和定义适用于本文件。

3.1 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]

3.2 密码应用安全性评估人员 commercial cryptography application security evaluation staff

是指密码应用安全性评估机构中从事密码应用安全性评估的人员，简称“密评人员”。

3.3 测试 test

密评人员采用预定的方法/工具使测评对象产生特定的运行结果，将运行结果与预期结果进行比对的过程。

3.4 访谈 interview

密评人员通过引导密码测评对象相关人员进行有目的的（有针对性的）交流以帮助密评人员理解、澄清或取得证据的过程。

3.5 核查 examine

密评人员对测评对象进行观察、查验和分析，以帮助密评人员理解、澄清或取得证据的过程，核查方式包括访谈、文档审查、实地查看、配置检查、测试等。

3.6 计算机数值控制 computerized numerical control

用计算机控制加工功能，实现数值控制。

3.7 数控系统 CNC system

计算机数值控制系统。

数控系统的基本组成包括数控装置和驱动装置两部分。其中驱动装置又包括完整驱动单元和电机二部分。

3.8 数控装置 NC device

数控装置为数控系统的控制部分，一般由微处理器、存储器、位置控制器、输入/输出、显示器、键盘、操作开关等硬件电路和包括相关的控制软件所组成。

3.9 驱动装置 driving device

数控系统的驱动装置是由完整的驱动单元加上相应的电机而组成。

3.10 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。

3.11 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。

3.12 数控系统敏感数据（CNC sensitive data）

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，账号口令密码，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。

4 符号和缩略语

4.1 缩略语

CNC: 计算机数值控制（Computerized Numerical Control）
HMI: 人机交互界面（Human Machine Interface）
IPSEC: IP 安全协议 （Internet Protocol Security）

MAC: 消息鉴别码(Message Authentication Code)
NC: 数值控制（Numerical Control）
PLC: 可编程逻辑控制器（Programmable logic controller）
SSL：安全套接层 （Secure Socket Layer）
TLS：传输层安全 （Transfer Layer Secure）
VPN：虚拟专用网络 （Virtual Private Network）

5 概述

本文件将数控系统商用密码应用测评要求分为总体测评要求和基本测评要求。其中评要求，适用于基础级和增强级的数控系统商用密码应用测评。基本测评要求，总体测评要求对“密码算法”“密码技术”“密码产品和密码服务”三个方面提出测，对数控系统的身份鉴别、访问控制、机密性、完整性、抗抵赖、安全审计分别提出了基础级和增强级二个级别密码应用技术的测评要求。

本文件第 6 章总体测评要求的内容不单独实施测评，也不单独体现在密码应用安全性评估报告的单元测评结果和整体测评结果中，仅供第 7 章基本测评要求的测评实施引用。资料性附录 A 给出了数控系统商用密码应用检测评估技术要点，供密评人员在对数控系统中具体使用的密码产品或应用的密码功能进行测评实施时参考。

本文件中的测评单元是对应一组相对独立和完整的测评内容，由测评指标、测评对象、测评实施和结果判定组成。

a) 测评指标：来源于 GB/T 39786-2021、GB/T 37092-2018、《数控系统商用密码应用技术要求》、《信息系统密码应用测评要求》等标准规范中各级的要求项。

b) 测评对象：数控系统商用密码应用测评过程中不同测评方法作用的对象，包括数控系统、数控系统数据、数控系统通信接口，以及相关配套密码产品、通用设备、人员、制度文档等。

c) 测评实施：针对某个测评指标，规定了数控系统商用密码应用的测评要点。

d) 结果判定：根据测评实施取得的证据，判定数控系统的密码应用是否满足某个测评指标要求的方法和原则。

密评人员在开展实际测评时，对于 GB/T 39786-2021、GB/T 37092-2018、《数控系统商用密码应用技术要求》、《信息系统密码应用测评要求》中的不同安全保护等级的“可”“宜”“应”的条款，按照如下方法确定是否将其纳入测评范围。

- 对于“可”的条款，由数控系统责任方自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第 7 章相应的指标要求进行测评和结果判定；否则，该测评指标为“不适用”。
- 对于“宜”的条款，密评人员根据数控系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照第 7 章相应的指标要求进行测评和结果判定。否则，密评人员应根据数控系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的数控系统中是否被满足，且数控系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照第 7 章相应的指标要求进行测评和结果判定。
- 对于“应”的条款，密评人员应按照第 7 章相应的指标要求进行测评和结果判定；若根据数控系统的密码应用方案和方案评审意见，判定数控系统确无与某项或某些

项指标相关的密码应用需求，则相应测评指标为“不适用”。

对于特殊指标，根据数控系统的密码应用方案和方案评审意见，若方案所选取的指标要求与数控系统相对应的密码应用基本要求等级的指标要求不一致（例如，根据密码应用需求，对基础级的数控系统，选取了增强级数控系统的相关指标要求），则密评人员应按照密码应用方案中的指标要求所在等级的相关测评实施要求进行测评；若所选取的测评指标超出GB/T 39786-2021、GB/T 37092-2018、《数控系统商用密码应用技术要求》、《信息系统密码应用测评要求》的范畴，如指标来自于数控系统所在行业的其他标准规范，则按照相关标准中的要求完成测评。对特殊指标实施情况的测评结论应体现在密码应用安全性评估报告中。

数控系统的密码应用测评的最终输出是密码应用安全性评估报告，在报告中应给出各个测评单元（见第 7 章）的测评结果、整体测评结果（见第 8 章），以及在进行风险分析和评价（见第 9 章）后给出的测评结论（见第 10 章）。其中，整体测评结果是以测评单元的判定结果为基础，经单元间测评相互弥补后得出的纠正结果；风险分析和评价是对整体测评结果中的不符合项和部分符合项，判断所产生的安全问题被威胁利用后对数控系统业务安全造成影响的程度；测评结论是由综合得分以及风险分析和评价共同决定，表示数控系统达到相应密码等级保护要求的程度。

6 总体测评要求

6.1 密码算法

具体测评单元如下：

a) 测评指标

数控系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。（基础级和增强级）

b) 测评对象

数控系统中的密码产品、密码服务以及密码算法实现。

c) 测评实施

了解系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意其使用的证明文件。

d) 结果判定

本单元测评指标不单独判定符合性。

6.2 密码技术

具体测评单元如下：

a) 测评指标

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。（基础级和增强级）

b) 测评对象

数控系统中的密码产品、密码服务以及密码技术实现。

c) 测评实施

核查系统所使用的密码技术是否以国家标准或行业标准形式发布。

d) 结果判定

本单元测评指标不单独判定符合性。

6.3 密码产品和密码服务

具体测评单元如下：

a) 测评指标

数控系统中使用的密码产品、密码服务应符合法律法规的相关要求。（基础级和增强级）

b) 测评对象

数控系统中的密码产品、密码服务以及密码算法实现和密码技术实现。

c) 测评实施

1) 核查系统所采用的密码产品是否获得密码认证机构颁发的密码产品认证证书以符合法律法规的相关要求；

2) 核查系统所使用的密码服务是否获得密码认证机构颁发的密码服务认证证书以符合法律法规的相关要求。

d) 结果判定

本单元测评指标不单独判定符合性。

7 基本测评要求

7.1 机密性

7.1.1 敏感数据传输机密性

具体测评单元如下：

a) 测评指标

采用密码技术保证数控系统的敏感数据在传输过程中的机密性。（基础级和增强级）

b) 测评对象

数控系统，以及提供机密性保护功能的密码产品。

c) 测评实施

1) 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2) 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；

3) 核查数控系统是否采用密码技术的加解密功能对敏感数据、或通信过程中的通信报文在传输过程中进行机密性保护，并验证传输数据机密性保护机制是否正确和有效。

d) 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.1.2 敏感数据存储机密性

具体测评单元如下：

a) 测评指标

采用密码技术保证数控系统的敏感数据在存储过程中的机密性。（基础级和增强级）

b) 测评对象

数控系统，以及提供机密性保护功能的密码产品。

c) 测评实施

1) 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2) 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；

3） 核查数控系统是否采用密码技术的加解密功能对敏感数据在存储过程中进行机密性保护，并验证存储数据机密性保护机制是否正确和有效。

d） 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.2 完整性

7.2.1 敏感数据传输完整性

具体测评单元如下：

a） 测评指标

采用密码技术保证数控系统的敏感数据在传输过程中的完整性。（基础级和增强级）

采用密码技术保证数控系统在数控与应用信息系统通讯、数控移动端远程监测应用场景中的敏感数据在传输过程中的完整性。（增强级）

b） 测评对象

数控系统，以及提供机密性保护功能的密码产品，数控系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。

c） 测评实施

1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；

3） 核查数控系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对敏感数据、或通信过程中的通信报文在传输过程中进行完整性保护，并验证传输数据完整性保护机制是否正确和有效。

d） 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.2.2 敏感数据存储完整性

具体测评单元如下：

a） 测评指标

采用密码技术保证数控系统的敏感数据在存储过程中的完整性。（基础级和增强级）

采用密码技术保证数控敏感信息存储、数控与应用信息系统通讯、数控移动端远程监测应用场景中的敏感数据在存储过程中的完整性。（增强级）

b） 测评对象

数控系统，以及提供完整性保护功能的密码产品。

c） 测评实施

1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；

3） 核查数控系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对敏感数据在存储过程中进行完整性保护，并验证存储数据完整性保护机制是否正确和有效。

d） 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.3 抗抵赖性

7.3.1 重要可执行程序、数控指令完整性和来源真实性

具体测评单元如下：

a） 测评指标

采用密码技术对数控系统在线升级的重要可执行程序、数控指令等进行完整性保护，并对其来源进行真实性验证。（基础级）

采用密码技术对重要可执行程序、数控指令等进行完整性保护，并对其来源进行真实性验证。（增强级）

b） 测评对象

数控系统、重要可执行程序、数控指令、以及提供不可否认性功能的密码产品。

c） 测评实施

1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；

3） 核查是否采用密码技术对重要可执行程序、数控指令等进行完整性保护并实现其来源的真实性保护，并验证重要可执行程序、数控指令等完整性保护机制和其来源真实性实现机制是否正确和有效。

c） 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.3.2 行为的不可否认性

具体测评单元如下：

a） 测评指标

采用密码技术针对数控系统在线升级应用场景下，数控系统用户关键操作的数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。（基础级）

采用密码技术提供数控系统用户关键操作的数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。（增强级）

b） 测评对象

数控系统、数控系统用户关键操作，以及提供不可否认性功能的密码产品。

c） 测评实施

1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；

2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；；

3） 核查数控系统是否采用基于公钥密码算法的数字签名机制等密码技术对数控系统用户关键操作的数据原发行为和接收行为实现不可否认性，并验证不可否认性实现机制是否正确和有效。

d） 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.4 身份鉴别

7.4.1 账号和口令鉴别

具体测评单元如下：

a) 测评指标

采用账号和口令的方式对登录数控系统的用户，以及登录数控装置的用户进行身份鉴别，且用户口令信息采用密码技术进行保护，保证登录数控系统的用户身份的真实性。（基础级）

b) 测评对象

数控装置、数控系统。

c) 测评实施

1) 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2) 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3) 核查是否采用对称加密、密码杂凑算法、公钥加密等密码技术保证用户口令的安全性，并验证用户口令的保护机制是否正确和有效。

d) 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.4.2 唯一标识符鉴别

具体测评单元如下：

a) 测评指标

采用数控系统唯一标识符结合消息鉴别码的方式对使用的数控装置或数控系统进行身份鉴别，保证接入的数控装置或数控系统身份的真实性。（基础级）

b) 测评对象

数控装置。

c) 测评实施

1) 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2) 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制进行保护，且以数控系统唯一标识符作为必要输入，并验证身份真实性实现机制是否正确和有效。

d) 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.4.3 单双向身份鉴别

具体测评单元如下：

a) 测评指标

采用挑战响应鉴别方式对数控系统与其他系统之间身份的真实性进行鉴别，保证通信的其他系统身份的真实性。（基础级）

采用挑战响应鉴别方式对数控系统与其他系统之间身份的真实性进行双向鉴别，保证通信的其他系统身份的真实性。（增强级）

b) 测评对象

数控系统。

c) 测评实施

1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3） 核查是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对接入的其他系统进行身份鉴别（基础级）/双向身份鉴别（增强级），并验证接入的其他系统的身份真实性实现机制是否正确和有效。

d） 结果判定
如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.5 访问控制

7.5.1 数控装置资源访问控制信息完整性

具体测评单元如下：

a） 测评指标
采用密码技术来保证数控装置资源访问控制信息的完整性。（基础级和增强级）

b） 测评对象
数控装置(及其操作系统、数据库管理系统)、密码设备、各类虚拟设备，以及提供身份鉴别功能的密码产品等。

c） 测评实施
1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3） 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对数控装置资源访问控制信息进行完整性保护，并验证系统资源访问控制信息完整性保护机制是否正确和有效。

d） 结果判定
如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.5.2 数控系统访问控制信息完整性

具体测评单元如下：

a） 测评指标
采用密码技术来保证数控系统访问控制信息的完整性。（基础级和增强级）

b） 测评对象
数控系统，以及提供完整性保护功能的密码产品。

c） 测评实施
1） 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2） 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3） 核查数控系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对应用的访问控制信息进行完整性保护，并验证应用的访问控制信息完整性保护机制是否正确和有效。

d） 结果判定
如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.6 安全审计

7.6.1 审计记录完整性

具体测评单元如下：

a) 测评指标

采用密码技术来保证数控用户人员操作、数控移动端远程控制、数控系统之间文件加密拷贝应用场景的审计记录的完整性。（基础级）

采用密码技术来保证审计记录的完整性。（增强级）

b) 测评对象

数控装置、数控系统，以及提供审计功能的密码产品。

c) 测评实施

1) 核查是否符合第 6 章总体测评要求中“密码算法”和“密码技术”的测评要求；
2) 核查是否符合第 6 章总体测评要求中“密码产品和密码服务”的测评要求；
3) 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对审计记录进行完整性保护，并验证审计记录完整性保护机制是否正确和有效。

d) 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 3）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

7.7 密码模块

具体测评单元如下：

a) 测评指标

采用符合 GB/T 37092 对应安全级别要求的密码产品或模块实现数控系统相关的密码运算和密钥管理。（基础级和增强级）

- 采用的密码产品，达到 GB/T 37092 一级及以上安全要求。（基础级）
- 采用的密码产品，达到 GB/T 37092 二级及以上安全要求。（增强级）

b) 测评对象

提供密码功能的密码产品或模块。

c) 测评实施

1) 核查信息系统中用于密码运算或密钥管理的密码产品或模块是否符合法律法规的相关要求，需要依法接受检测认证的，检查是否经密码认证机构认证合格；
2) 了解密码产品或模块的型号和版本等配置信息，检查密码产品是否符合 GB/T 37092 相应安全等级及以上安全要求，并检查密码产品或模块的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件。

e) 结果判定

如果以上测评实施内容均为是，则符合本单元测评指标要求；如果测评实施 2）为否，则不符合本单元测评指标要求；否则，部分符合本单元测评指标要求。

8 整体测评要求

8.1 概述

整体测评应从单元、单元间等方面进行测评和综合安全分析。

单元间测评是指对两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对数控系统整体安全保护能力的影响。

8.2 单元间测评

在单元测评完成后，如果数控系统的某个测评单元的结果判定存在不符合或部分符合，应进行单元间测评，重点分析数控系统中是否存在单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的数控系统商用密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成数控系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

9 风险分析和评价

密码应用安全性评估报告中应对整体测评之后单元测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法，针对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，以及受到威胁利用的资产自身价值，综合评价这些不符合项或部分符合项对数控系统造成的安全风险。

10 测评结论

密码应用安全性评估报告应给出密码应用保护对象的测评结论，确认密码应用保护对象达到相应等级保护要求的程度。

应结合各类的测评结论和对单元测评结果的风险分析给出测评结论。

a)符合：数控系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为0。

b)基本符合：数控系统中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致数控系统面临高等级安全风险。

c)不符合：数控系统中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题会导致数控系统面临高等级安全风险。

附 录 A
（资料性附录）
数控系统商用密码应用测评要点

结合总体测评要求、基本测评要求等方面的检测评估能力需求，从总体要求检测评估、数控装置检测评估、数控系统通信检测评估、数控系统应用和数据检测评估四方面建立相应的数控系统商用密码应用检测评估要点。

数控系统商用密码应用测评要点如表A.1所示。

表 A.1 数控系统商用密码应用测评要点

层面	测评单元	测评内容	检测评估技术
总体要求检测评估	密码核心算法	检测信息系统中使用的密码核心算法是否符合法律、法规的规定和密码核心算法相关国家标准、行业标准的有关要求。	随机性检测技术、密码核心算法合规性检测技术
	密码技术	检测信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。	随机性检测技术、密码合规性检测技术、密码协议检测技术
	密码产品和密码服务	检测信息系统中采用符合GB/T 37092的相应等级的密码模块、使用的密码产品是否通过国家密码管理部门核准；使用的密码服务是否通过国家密码管理部门许可。	随机性检测技术、密码合规性检测技术、数字证书合规性检测技术
数控装置检测评估	身份鉴别	对登录用户进行身份标识和鉴别测评，验证身份标识的唯一性、身份鉴别信息复杂度及是否定期更换。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、数字证书合规性检测技术
	访问控制信息完整性	对系统资源访问控制信息的完整性进行测评。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术、
	重要可执行程序完整性、重要可执行程序来源真实性	验证是否采用可信计算技术建立从系统到应用的信任链，对系统运行过程中重要可执行文件完整性、重要可执行程序来源真实性进行测评。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术、数字证

层面	测评单元	测评内容	检测评估技术
			书合规性检测技术
数控系统通信检测评估	身份鉴别	在通信前基于密码技术对通信双方进行验证或认证，使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、数字证书合规性检测技术
		采用密码技术对连接到内部网络的设备进行身份认证，确保接入网络的设备真实可信。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、数字证书合规性检测技术
	访问控制信息完整性	使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性。	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术
	通信数据完整性	采用密码技术保证通信过程中数据的完整性	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术
	通信数据机密性	采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性	渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、机密性检测技术、IPSec VPN检测技术、SSL VPN检测技术
数控系统应用和数据检测评	身份鉴别	对登录用户进行身份标识和鉴别测评，验证应用系统用户身份的真实性实现情况。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、数字证书合规性检测技术

层面	测评单元	测评内容	检测评估技术
估	访问控制信息完整性	对业务应用系统访问控制策略、数据库表访问控制信息的完整性进行测评。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术
	数据传输机密性	对包括但不限于鉴别数据、重要业务数据和重要用户信息等的敏感数据在传输过程中的机密性进行测评。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、机密性检测技术、IPSec VPN检测技术、SSLVPN检测技术
	数据存储机密性	对包括但不限于鉴别数据、重要业务数据和重要用户信息、重要可执行程序等的敏感数据在存储过程中的机密性进行测评。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、机密性检测技术
	数据传输完整性	对包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等的敏感数据在传输过程中的完整性进行测评。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术
	数据存储完整性	对包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等的敏感数据在存储过程中的完整性进行测评。	端口扫描技术、渗透测试技术、漏洞扫技术描、安全配置核查技术、随机性检测技术、密码合规性检测技术、完整性保护检测技术
	抗抵赖性	对数据原发证据和数据接收行为的不可否认性进行测评。	随机性检测技术、密码合规性检测技术、流程不可抵赖检测技术

参考文献

[1]GB/T 22239-2019　信息安全技术 网络安全等级保护基本要求
[2]GB/T 39786-2021　信息系统密码应用基本要求
[3]GB/T 37092-2018　信息安全技术 密码模块安全要求
[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 38540-2020《信息安全技术 安全电子签章密码技术规范》
[6]GM/T 0037-2014《证书认证系统检测规范》
[7]GM/T 0038-2014《证书认证密钥管理系统检测规范》
[8]GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式规范》
[9]YD/T 3804-2020　工业互联网安全防护总体要求