工业互联网密码支撑标准体系
建设指南

2022 年 11 月

目录

前言

工业互联网正在成为全球新一轮科技和产业革命的竞争高地。习近平总书记强调，要深入实施工业互联网创新发展战略。党中央、国务院作出加快工业互联网新型基础设施建设的决策部署。在政策与市场的双重驱动下，工业互联网产业发展步入快车道。

工业互联网离不开密码的核心保障和基础支撑。为促进工业互联网密码支撑体系的统一、科学、高效发展，推动商用密码在工业互联网领域的应用，保障工业互联网安全，工业和信息化部组织制定《工业互联网密码支撑标准体系建设指南》（以下简称《建设指南》），研究制定重点领域重点方向密码应用、检测相关标准规范。

目前，电力、装备制造、钢铁、石油化工、航空航天等多个行业应用密码技术对工业互联网进行安全保障的意识逐步增强，密码融合应用程度逐步向纵深推进。《建设指南》充分发挥标准在工业互联网产业密码支撑体系中的顶层设计和基础引领作用，提出了密码应用共性、设备密码应用、控制系统密码应用、网络密码应用、边缘计算密码应用、平台密码应用、数据密码应用、密码行业应用、密码应用管理与支撑等九个重点标准化领域及方向，强化工业互联网安全防护能力，为工业互联网产业高质量发展保驾护航。

一、建设思路及目标

（一）总体思路

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大、十九大和历次全会精神，贯彻党中央、国务院关于加快工业互联网新型基础设施建设的决策部署，落实《中华人民共和国网络安全法》和《中华人民共和国密码法》，深入发挥密码在工业互联网安全中的核心保障和基础支撑作用，建立适应我国技术和产业发展需要的国家工业互联网密码支撑标准体系。

（二）基本原则

统筹规划，全面布局。结合我国工业互联网产业和密码产业发展的现状及特点，发挥政府主管部门在顶层设计、组织协调和政策制定等方面的主导作用，制定政府引导和市场驱动相结合的标准体系建设方案，建立适合我国国情的工业互联网密码支撑标准体系。

基础先立，急用先行。优先研究制定基础共性相关标准，依据产业急需程度，科学确定工业互联网密码支撑标准体系建设的重点行业领域，优先制定适用行业特点的行业标准。实现标准与工业互联网产业、密码产业发展的结合，行业标准与国家标准的结合，国内标准与国际标准的结合。

多方参与，协同合作。充分发挥标准化组织、科研机构、工业企业、工业互联网企业、工业控制系统企业、密码企业

等各方主体的力量，充分利用现有基础和成果，整合工业互联网产业和密码产业现有资源，通力合作，共同构建工业互联网密码支撑标准体系。

（三）建设目标

到 2022 年，初步建立工业互联网密码标准体系，制修订相关标准 30 项，依据产业急需程度，研制重点行业的工业互联网密码支撑标准，为工业互联网落地推广提供安全保障。

到 2025 年，健全完善工业互联网密码标准体系，制修订相关标准 100 项，研制覆盖各垂直行业的工业互联网密码支撑标准，积极推动团体标准、行业标准向国家标准的转化，为工业互联网规模化应用提供支撑。

二、建设内容

（一）工业互联网密码支撑标准体系框架

工业互联网密码标准体系包括密码应用共性标准、设备密码应用、控制系统密码应用、网络密码应用、边缘计算密码应用、平台密码应用、数据密码应用、密码行业应用、密码应用管理与支撑等标准。工业互联网密码支撑标准体系如图 1 所示。

图 1 工业互联网密码支撑标准体系框架

（二）重点标准化领域及方向

1. 密码应用共性标准

密码应用共性标准是工业互联网密码基础性、通用性、指导性标准，包括术语定义、密码基础类标准、密码应用总体要求、密码应用测评总体要求等标准。如图 2 所示。

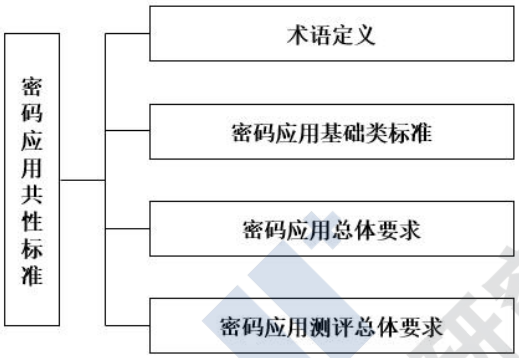

图 2 密码应用共性标准子体系

（1）术语定义标准

用于规范工业互联网密码相关概念，为其它各部分标准的制定提供支撑，包括工业互联网密码应用场景、技术、业务等主要概念定义、分类、相近概念之间关系等，避免不同行业间俗称不统一导致的理解歧义。

（2）密码应用基础类标准

用于规范工业互联网中应用的密码应用基础标准，包括密码算法、密码协议、密码基础设施等标准。

（3）密码应用总体要求标准

用于规范密码算法、密码技术、密码产品和密码服务使用的总体要求，以满足工业互联网平台、网络、边缘和终端

等方面的应用需求。

（4）密码应用测评总体要求标准

用于规范工业互联网平台、网络、边缘及终端所使用的密码算法、密码产品、密码技术及密码服务如何进行测评、测评的主要流程、评价指标等。

2.设备密码应用标准

用于规范工业互联网中各类终端设备在设计、研发、生产制造以及运行过程中的密码应用及其它技术要求，包括数据采集类设备密码应用、智能装备类设备密码应用、工业生产类设备密码应用、辅助生产类设备密码应用、远程控制类设备密码应用等标准。如图3所示。

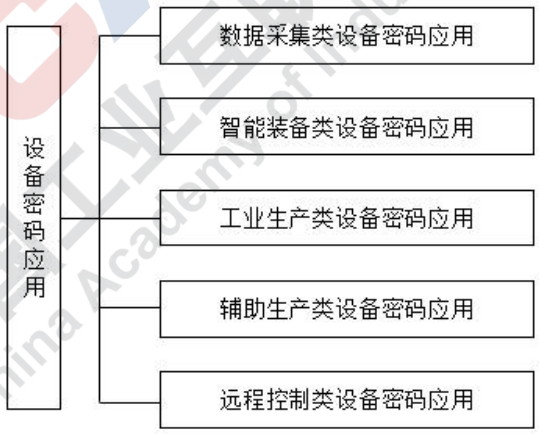

图 3 设备密码应用标准子体系

（1）数据采集类设备密码应用标准

用于规范工业互联网中数据采集类设备的密码应用及其它技术要求，包括工业数据采集类、控制数据采集类、设备数据采集类、系统数据采集类等设备密码应用标准。

（2）智能装备类设备密码应用标准

用于规范工业互联网中智能装备类设备的密码应用及其它技术要求，包括可编程逻辑控制器（PLC）、远程终端单元（RTU）、智能电子设备（IED）、数控机床等设备密码应用标准。

（3）工业生产类设备密码应用标准

用于规范工业互联网中工业生产类设备的密码应用及其它技术要求，包括各行各业生产类设备，如钢铁、石油、电力等行业。

（4）辅助生产类设备密码应用标准

用于规范工业互联网中辅助生产类设备的密码应用及其它技术要求，如工业机器人、巡视终端、视频监控等。

（5）远程控制类设备密码应用标准

用于规范工业互联网中远程控制类设备的密码应用及其它技术要求，如远程监控终端、远程诊断终端等。

3. 控制系统密码应用标准

用于规范工业互联网中各类控制系统中的控制软件与控制协议的密码应用及其它技术要求，包括数据采集与监视控制系统（SCADA）密码应用、集散控制系统（DCS）密码应用、现场总线控制系统（FCS）密码应用、人机接口（HMI）系统密码应用等标准。如图4所示。

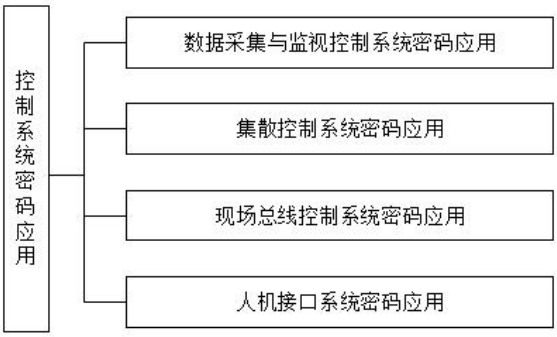

图 4 控制系统密码应用标准子体系

（1）数据采集与监视控制系统密码应用标准

主要结合数据采集与监视控制系统的特点，规范和细化数据采集与监视控制系统的密码应用技术要求。

（2）集散控制系统密码应用标准

主要结合集散控制系统的特点，规范和细化集散控制系统的密码应用技术要求。

（3）现场总线控制系统密码应用标准

主要结合现场总线控制系统的特点，规范和细化现场总线控制系统的密码应用技术要求。

（4）人机接口系统密码应用标准

主要结合人机接口系统的特点，规范和细化人机接口系统的密码应用技术要求。

4. 网络密码应用标准

用于规范承载工业智能生产和应用的通信网络密码技术和产品应用有关技术要求，包括生产控制网络密码应用、远程运维网络密码应用、办公内网密码应用、工业互联网企业外网密码应用、工厂内外网互联密码应用、工业互联网标

识解析密码应用等标准。如图5所示。

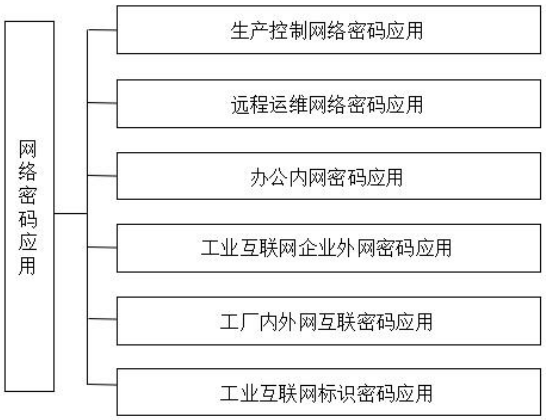

图 5 网络密码应用标准子体系

（1）生产控制网络密码应用标准

用于规范工厂内生产控制网络应用密码技术和产品有关要求，包括工业设备/产品、控制系统、信息系统之间网络互联通信时应用的密码技术和产品，实现对所传输生产控制数据的机密性和完整性保护。

（2）远程运维网络密码应用标准

用于规范工业互联网远程运维网络应用密码技术和产品有关要求，包括运维平台和售出智能产品之间网络互联应用密码技术和产品传输数据等。

（3）办公内网密码应用标准

用于规范工业互联网办公内网应用密码技术和产品有关要求。

（4）工业互联网企业外网密码应用标准

用于规范工业互联网企业外网应用密码技术和产品有关要求。

（5）工厂内外网密码应用标准

用于规范工厂内网与外网互联时应用密码技术和产品有关要求，包括工厂内网联接生产资源、商业资源以及用户、产品的公共网络（互联网、专网、VPN等）应用密码技术和产品等。

（6）工业互联网标识密码应用标准

用于规范工业互联网标识解析系统、网络和设备应用密码技术和产品有关要求，包括标识数据采集传输、标识解析通信协议、标识解析设备等应用密码技术和产品等。

5.边缘计算密码应用标准

用于规范边缘计算的密码应用及其相关技术要求，包括边缘数据采集与处理密码应用、边缘设备密码应用、边缘平台密码应用、边云协同密码应用等标准。如图6所示。

图 6 边缘计算密码应用标准子体系

（1）边缘数据采集与处理密码应用标准

用以规范边缘数据采集与处理密码应用及其相关技术要求，以保证数据的完整性与真实性。

（2）边缘设备密码应用标准

用以规范边缘设备密码应用及其相关技术要求，以确保海量边缘设备接入到边缘平台时身份进行快速有效认证、受限设备（性能受限、能量受限、存储受限等）的身份认证、安全存储等。

（3）边缘平台密码应用标准

用以规范边缘平台密码应用及其相关技术要求，以确保数据的安全存储、边缘设备接入认证等。

（4）边云协同密码应用标准

用以规范边云协同密码应用及其相关技术要求，以确保避免数据泄露、一致性被破坏等。

6.平台密码应用标准

用于规范工业互联网平台的密码应用及其它技术要求，包括云基础设施密码应用、工业云平台服务密码应用、工业应用密码应用等标准。如图7所示。

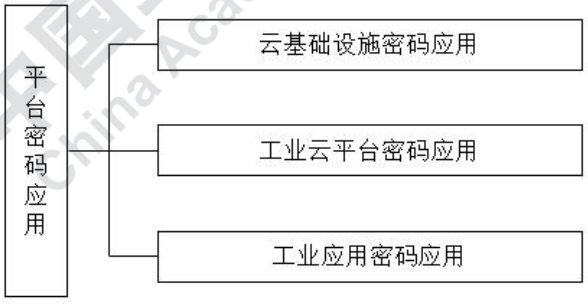

图 7 平台密码应用标准子体系

（1）云基础设施密码应用标准

用于规范云基础设施的密码应用及其它技术要求，主要包括计算、存储、网络和虚拟化技术等方面的密码应用，以

确保对各类重要数据进行机密性和完整性保护、对云密钥进行安全管理等。

（2）工业云平台密码应用标准

用于规范工业云平台的密码应用及其它技术要求，主要包括工具软件、开发工具、微服务组件和开发API（上行、下行）等方面的密码应用，以确保身份鉴别、权限控制等。

（3）工业应用密码应用标准

用于规范工业互联网平台应用软件和工业知识服务的密码应用及其它技术要求，主要包括工业应用接口、第三方依赖库、Web服务、开发API（上行、下行）等方面的密码应用，以确保身份鉴别、安全传输、安全存储等。

7. 数据密码应用标准

用于规范工业互联网数据相关的密码应用及其它技术要求，包括数据全生命周期密码应用、数据分类分级密码应用、工业大数据密码应用和用户个人隐私保护密码应用等。如图 8 所示。

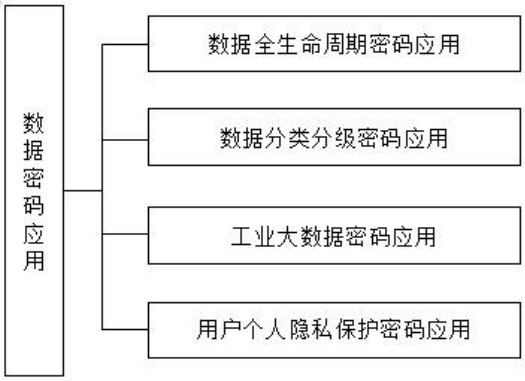

图 8 数据密码应用标准子体系

（1）数据全生命周期密码应用标准

用于规范利用密码技术、密码产品和密码服务如何确保各个阶段数据的完整性、真实性及机密性。

（2）数据分类分级密码应用标准

用于规范如何保证数据分类分级的结果和不同级别、类型数据的加密、脱敏、访问控制等密码安全防护措施。

（3）工业大数据密码应用标准

用于规范工业大数据如何实现安全的利用、协助，如多方安全计算、密文检索等。

（4）用户个人隐私保护密码应用标准

用于规范工业互联网中采集到的用户隐私数据如何利用密码技术、密码产品和密码服务进行保护，避免个人隐私泄露等。

8. 密码行业应用标准

密码行业应用标准依托密码基础共性、密码技术应用及密码检测评估等标准的指导，基于工业互联网行业特点及实际需求，制定电力、装备制造、钢铁、石油化工等行业的密码应用标准，推动各行业密码应用标准的落地。如图 9 所示。

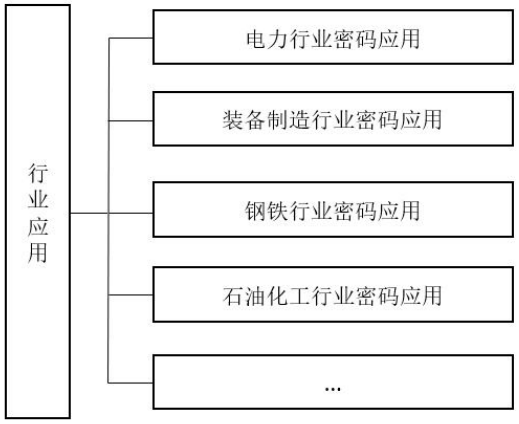

图 9 行业应用标准子体系

9. 密码应用管理与支撑标准

用于规范工业互联网密码应用管理与支撑要求，包括密码应用管理、密码应用支撑等标准。

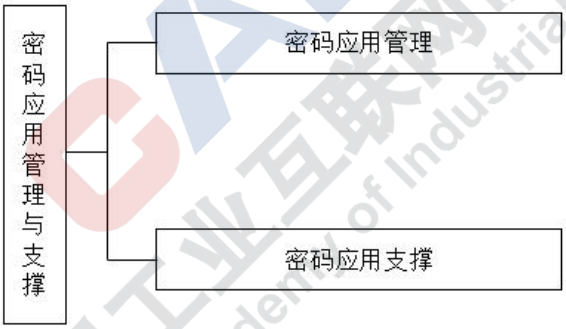

图 10 密码应用管理与支撑标准子体系

（1） 密码应用管理

用于规范工业互联网密码应用相关管理要求，包括密码人员管理、密钥管理、建设运行、应急处置、密码资产管理等标准。

（2） 密码应用支撑

用于工业互联网密码应用相关支撑要求，包括密码监测、密码态势感知、密码应用评估等标准。

三、组织实施

一是实施动态更新。实施动态更新完善机制，随着经济社会数字化转型持续推进、工业互联网密码应用认知与实践水平的提高，结合工业互联网密码应用相关法律法规的最新要求，适时滚动修订《建设指南》。

二是推进标准研制。组织行业协会及工业互联网企业、工控企业、工业企业、密码企业、科研院所、高校等单位，按照《建设指南》明确的标准研制路径，有序推进行业标准研制工作，注重工业互联网密码应用标准化工作与工业互联网密码应用最新研究成果、行业最佳实践的有机结合。

三是加强宣贯实施。充分发挥标准化组织、行业协会作用，组织相关专家开展标准研讨活动，通过培训、咨询、论坛等手段推进标准的宣贯。积极组织开展标准试点示范，形成最佳实践，促进标准在业界的应用推广。

四是加强国际交流合作。加强与国际标准化组织的交流与合作，积极参与国际标准化组织（ISO）、国际电信联盟（ITU）等国际标准化组织活动及国际标准研制。积极促进国内标准与国际接轨，推动国内先进标准向国际标准转化。

附件

工业互联网密码相关标准项目明细表

序号	标准编号	标准名称	标准化组织	进展	项目性质
100 密码应用共性标准					
101 术语定义					
1.	/	工业互联网密码术语	/	待制定	推荐
102 密码应用基础类标准					
2.	/	工业互联网轻量级对称密码算法	/	待制定	推荐
3.	/	工业互联网轻量级非对称密码算法	/	待制定	推荐
4.	/	工业互联网轻量级密码杂凑算法	/	待制定	推荐
103 密码应用总体要求					
5.	/	工业互联网密码应用基本要求	工业和信息化部商用密码应用推进标准工作组	制定中	推荐
104 密码应用测评总体要求					
6.	/	工业互联网密码应用测评要求	/	待制定	推荐
200 设备密码应用					
201 数据采集类设备密码应用					
7.	/	数据采集设备密码应用技术要求	/	待制定	推荐
202 智能装备类设备密码应用					
8.	/	智能装备设备密码应用技术要求	/	待制定	推荐
203 工业生产类设备密码应用					
9.	/	工业生产设备密码应用技术要求	/	待制定	推荐
204 辅助生产类设备密码应用					

10.	/	辅助生产设备密码应用技术要求	/	待制定	推荐
205 远程控制类设备密码应用					
11.	/	远程运维设备密码应用技术要求	/	待制定	推荐
300 控制系统密码应用					
301 数据采集与监视控制系统密码应用					
12.	/	数据采集与监视控制系统密码应用技术要求	/	待制定	推荐
302 集散控制系统密码应用					
13.	/	集散控制系统密码应用技术要求	/	待制定	推荐
303 现场总线控制系统密码应用					
14.	/	现场总线控制系统密码应用技术要求	/	待制定	推荐
304 人机接口系统密码应用					
15.	/	人机接口系统密码应用技术要求	/	待制定	推荐
400 网络密码应用					
401 生产控制网络密码应用					
16.	/	生产控制网络密码应用技术要求	/	待制定	推荐
402 远程运维网络密码应用					
17.	/	远程运维网络密码应用技术要求	/	待制定	推荐
403 办公内网密码应用					
18.	/	办公内网密码应用技术要求	/	待制定	推荐
404 工业互联网企业外网密码应用					
19.	/	工业互联网企业外网密码应用技术要求	/	待制定	推荐
405 工厂内外网互联密码应用					
20.	/	工厂内外网互联密码应用技术要求	/	待制定	推荐
406 工业互联网标识密码应用					
21.	/	工业互联网标识系统密码应用技术要求	/	待制定	推荐

500 边缘计算密码应用					
501 边缘数据采集与处理密码应用					
22.	/	边缘计算数据采集与处理密码应用技术要求	/	待制定	推荐
502 边缘设备密码应用					
23.	/	边缘设备密码应用技术要求	/	待制定	推荐
503 边缘平台密码应用					
24.	/	边缘平台密码应用技术要求	/	待制定	推荐
504 边云协同密码应用					
25.	/	边云协同密码应用技术要求	/	待制定	推荐
600 平台密码应用					
601 云基础设施密码应用					
26.	/	工业互联网云基础设施密码应用技术要求	/	待制定	推荐
27.	/	工业互联网密码计算资源池实施指南	/	待制定	推荐
602 工业云平台密码应用					
28.	GM/T 0088-2020	云服务器密码机管理接口规范	密码行业标准化组织	已发布	推荐
29.	GM/Y5002-2018	云计算身份鉴别服务密码标准体系	密码行业标准化组织	已发布	推荐
30.	/	工业互联网平台身份鉴别密码应用指南	工业和信息化部商用密码应用推进标准工作组	制定中	推荐
31.	/	工业互联网云平台密码技术应用指南	工业和信息化部商用密码应用推进标准工作组	制定中	推荐
603 工业应用密码应用					
32.	/	工业应用密码应用技术要求	/	待制定	推荐
700 数据密码应用					
701 数据全生命周期密码应用					
33.	/	工业数据生命周期管理密码应用指南	/	待制定	推荐

702 数据分类分级密码应用					
34.	/	工业互联网数据分类分级密码应用指南	/	待制定	推荐
703 工业大数据密码应用					
35.	/	工业大数据溯源密码应用技术规范	/	待制定	推荐
36.	/	工业大数据多方计算密码应用技术规范	/	待制定	推荐
704 用户个人隐私保护密码应用					
37.	/	个人数据隐私保护密码技术要求	/	待制定	推荐
800 行业密码应用					
801 电力行业密码应用					
38.	/	风力发电工控系统密码应用技术规范	工业和信息化部商用密码应用推进标准工作组	制定中	推荐
39.	/	电力行业信息系统密码应用技术要求	/	待制定	推荐
802 装备制造行业密码应用					
40.	/	装备制造行业信息系统密码应用技术要求	/	待制定	推荐
803 钢铁行业密码应用					
41.	/	钢铁行业信息系统密码应用技术要求	/	待制定	推荐
804 石油化工行业密码应用					
42.	/	石油化工行业信息系统密码应用技术要求	/	待制定	推荐
900 密码应用管理与支撑					
901 密码应用管理					
43.	/	工业互联网密码人员管理要求	/	待制定	推荐
44.	/	工业互联网密钥管理要求	/	待制定	推荐
45.	/	工业互联网密码应用运维管理要求	/	待制定	推荐
46.	/	工业互联网密码资产管理要求	/	待制定	推荐
47.	/	工业互联网密码应用应急处置要求	/	待制定	推荐

901 密码应用支撑					
48.	/	工业互联网密码应用态势感知技术要求	/	待制定	推荐
49.	/	工业互联网密码应用监测感知平台技术要求	/	待制定	推荐
50.	/	工业互联网密码应用评估规范	/	待制定	推荐