

中国计算机用户协会团体标准

《流程工业企业 工业互联网数据安全保障密码应用要求》

（征求意见稿）编制说明

一、标准编制的背景

流程工业企业工业互联网数据是国家基础性战略资源和数字经济的基石，其安全关乎国家安全和民生安全。2020年4月，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，正式明确数据是和土地、劳动力、资金等并列的生产要素。安全是发展的前提，《中华人民共和国网络安全法》、《促进大数据发展行动纲要》、《关于加强国家网络安全标准化工作的若干意见》、《关于深化“互联网+先进制造业”发展工业互联网的指导意见》、《加强工业互联网安全工作的指导意见》等一系列法规及政策文件，都明确提出了加强数据安全的相关要求。2020年，《数据安全法（征求意见稿）》也正式发布，将数据安全纳入国家安全观，更体现了数据安全日趋重要的发展趋势。数据是流程工业企业工业互联网的“血液”，加强流程工业企业工业互联网数据安全保障至关重要。

流程工业有别于离散工业，其主要数字化特点如下表所示：

离散工业	流程工业
1. 确定性系统（知识精确传承）	1. 非确定性系统（知识模糊性）
2. 部件的物理变化和顺序作业	2. 物料的物理和化学变化
3. 离散时间序列问题	3. 连续时间动态问题（因果不同同时性）
4. 模型和参数的复制性强（“乘法”方式推广）	4. 模型和参数的复制性弱（“加法”方式推广）
5. 无人化	5. 人工干预的不可缺少
6. 可精确测量和控制	6. 测量的不完备性，控制复杂
7. 和自然天气基本无关	7. 和自然天气关联紧密
8. 数字化效益：人力、时效、质量、市场	8. 数字化效益：安全、节能、质量、降耗
9. 容易和消费互联网连接和协同	9. 难以和消费互联网连接和协同

在流程工业企业中，生产控制大区与管理信息大区发生的数据交换、数据的共享和价值挖掘等过程面临更大安全风险，更需强调数据的完整性、实时性、可用性和可控性保护。密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。因此，研究制定流程工业

企业工业互联网数据安全保障密码应用规范，具有重要的现实意义。

二、任务来源

根据中国计算机用户协会下达的 2022 年第二批团体标准制修订计划，华能信息技术有限公司、郑州信大云谷科技有限公司作为主要牵头单位筹建了标准编写组，承担《新型电力系统数据安全保障商用密码应用规范》标准的研制任务。该标准的立项计划号为 T/CCUA LX013-2022，技术归口单位为中国计算机用户协会，本标准于 2023 年 5 月 15 日由中国计算机用户协会批复团标名称改为《流程工业企业 工业互联网数据安全保障密码应用要求》。

三、编制过程

在下达计划号前由华能信息技术有限公司、郑州信大云谷科技有限公司等单位相关人员组成的《新型电力系统数据安全保障商用密码应用规范》标准编写组，明确了各自的责任和任务，并开展工作。

2022 年 10 月至 12 月，项目组对流程工业企业进行了解学习，结合华能（浙江）能源开发有限公司玉环分公司科技计划项目交付工作，对火电流程工业企业进行了调研。

2023 年 1 月至 2 月，对《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》、工业和信息化部 2022 年 12 月 8 日发布的《工业和信息化领域数据安全管理办法（试行）》、《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》等标准以及相关法律法规进行了学习，结合流程工业企业工业互联网特点，对数据安全密码应用进行分析。

2023 年 4 月，标准编写组完成了标准草案的初稿，于 2023 年 4 月开始在编写组评审委员会内进行评审。共经历了 3 次组内评审，期间收到了 6 条意见。

2023 年 5 月，经专家讨论，将标准题目改为《流程工业企业 工业互联网数据安全保障密码应用要求》。

2023 年 10 月，编写组根据评审意见讨论修改后，形成征求意见稿。

四、编制原则

标准的用语、格式按照 GB/T 1.1-2020 给出的规则起草。

标准内容的编制坚持以下原则：

本标准规范的整个起草过程严格按照工作计划实施，并遵循“科学性、合理性、先进性、实用性、普遍性”原则。对标准从全面性、简便性、可操作性等方面进行了综合考虑，确保标准发布实施后能够得到有效应用。

五、标准主要内容

本标准规定了流程工业企业工业互联网特性及数据安全密码应用原则、总体框架、通用要求、技术要求和管管理要求，保障数据安全。

本标准适用于指导流程工业企业工业互联网数据安全保障密码应用的规划、建设、运行及测评，在本标准基础上，各领域与行业可结合本领域与行业的数据安全防护需求制定数据防护的密码保障方案。

六、有关技术的说明

有关本标准起草过程中的一些技术问题说明如下：

1、本标准将流程工业企业工业互联网系统内部基于计算机和网络技术的业务系统划分为生产控制大区和管理信息大区，根据“安全分区、网络专用、横向隔离、纵向认证”的基本防护策略，设计数据安全密码应用框架。

2、本标准针对流程工业数据的完整性、实时性、可用性和可控性保护要求，提出流程工业企业工业互联网数据生命周期的6个阶段相应密码应用规范；同时，增加策略管理相关密码应用规范。

本标准“数据安全密码应用技术要求”一节中根据数据生命周期展开的对于分级数据采取相应的密码保护机制要求如下表所示：

数据生命周期	密码保护机制	数据分级		
		一般数据	重要数据	核心数据
数据采集	实体身份认证	□	√	√
	完整性保证	√	√	√
	安全标识	□	▲	√
	不可否认	▲	√	√
	行为监管数据保护	√	√	√
数据传输	实体身份认证	√	√	√
	完整性保证	√	√	√
	机密性保证	□	√	√
	信道隔离	□	▲	√
	行为监管数据保护	√	√	√
数据存储	完整性保证	√	√	√
	机密性保证	□	√	√

	行为监管数据保护	√	√	√
数据处理	实体身份认证	√	√	√
	机密性保证		□	□
	访问控制	□	√	√
	行为监管数据保护	√	√	√
数据交换	实体身份认证	√	√	√
	完整性保证	√	√	√
	访问控制	□	√	√
	隐私保护	□	√	√
	行为监管数据保护	√	√	√
数据销毁	实体身份认证	√	√	√
	行为监管数据保护	√	√	√
策略管理	统一管理	▲	√	√
	实体身份认证	▲	√	√
	行为监管数据保护	▲	√	√

注：代表“可”，▲代表“宜”，√代表“应”。

3、参考的主要标准：

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 42021-2022 工业互联网 总体网络架构

GM/T 0115—2021 信息系统密码应用测评要求

GB/T 17901.1-2020 信息技术 安全技术 密钥管理 第1部分：框架

GM/Z 4001—2013 密码术语

七、关于标准的性质

鉴于本标准作为团体标准发布，属于推荐性标准。由本团体成员约定采用或者按照本团体的规定供社会自愿采用。

八、有关专利的说明

本标准不涉及专利问题。

标准编写组

2023年10月12日