ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41400—2022

信息安全技术　工业控制系统信息安全防护能力成熟度模型

Information security technology—Information security protection capability maturity model of industrial control systems

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、太极计算机股份有限公司、江苏赛西科技发展有限公司、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、广州赛宝认证中心服务有限公司、中国石油天然气股份有限公司西北销售分公司、中国石油天然气股份有限公司长庆石化分公司、宁波和利时信息安全研究院有限公司、国家工业信息安全发展研究中心、国家信息技术安全研究中心、中国信息安全测评中心、浙江省能源集团有限公司、浙江浙能乐清发电有限责任公司、上海三零卫士信息安全有限公司、陕西省网络与信息安全测评中心、西门子(中国)有限公司、上海工业控制安全创新科技有限公司、华东师范大学、杭州安恒信息技术股份有限公司、中国网络安全审查技术与认证中心、昆仑数智科技有限责任公司、西安电子科技大学、国网新疆电力有限公司电力科学研究院、中电长城网际系统应用有限公司、中国石油天然气股份有限公司新疆油田分公司数据公司、杭州立思辰安科科技有限公司、东莞市擎洲光电科技有限公司、柳州源创电喷技术有限公司、江苏省电子信息产品质量监督检验研究院(江苏省信息安全测评中心)、北京六方云信息技术有限公司、中国科学院软件研究所、烽台科技(北京)有限公司、上海化工宝数字科技有限公司、北京和仲宁信息技术有限公司、杭州木链物联网科技有限公司、陕西科技大学、中石油华东设计院有限公司、中国能源建设集团浙江省电力设计院有限公司、陕西延长石油富县发电有限公司、上海大学、海澜智云科技有限公司、成都航天通信设备有限责任公司。

本文件主要起草人：姚相振、李琳、甘俊杰、周睿康、龚洁中、周峰、李尧、刘贤刚、赵振学、赵金元、郝志强、赵梓桐、方进社、李俊、郭娴、夏冀、许玉娜、闵京华、邸丽清、孙彦、胡影、王惠莅、李弘彦、马强、程宇、陈柯宇、张宏伟、陈曦、牟文彪、张坚群、仵大奎、刘盈、杨帆、高瑞、闫涛、蒲戈光、刘虹、费敏锐、彭晨、杜大军、布宁、申永波、焦程鹏、刘鸿运、张芝军、王飞、索涛、戴赟、张建新、强剑、石永杰、于慧超、王小宏、赵朋、沈玉龙、李峰、王斌、周燕华、孙军、于盟、肖威、林昕、姜亚光、刘丕群、孙军军、刘志乐、吴兰、杨晨、龚亮华、段沛鑫、陈艳、刘克松、高智伟、张浏骅、刘冬、李敏、张晓菲、曹禹、郝鑫、马孝磊、杨立军、林洪俊、陈若春、纪璐、晏敏、方静、莫韬、何双羽、赵峰、张俊峰、刘志刚、赵学全、程薇宸、王一蔚、赵建宏。

信息安全技术　工业控制系统信息安全防护能力成熟度模型

1　范围

本文件给出了工业控制系统信息安全防护能力成熟度模型，规定了核心保护对象安全和通用安全的成熟度等级要求，提出了能力成熟度等级核验方法。

本文件适用于工业控制系统设计、建设、运维等相关方进行工业控制系统信息安全防护能力建设，以及对组织工业控制系统信息安全防护能力成熟度等级进行核验。

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 25069　信息安全技术　术语

GB/T 32919—2016　信息安全技术　工业控制系统安全控制应用指南

3　术语和定义

GB/T 25069、GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统　industrial control system

由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。

注：工业控制系统包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC）等。

[来源：GB/T 36323—2018，3.1，有修改]

3.2

工业控制系统信息安全防护能力　information security protection capability of industrial control system

组织为避免工业控制系统遭到非授权或意外的访问、篡改、破坏及损失，在机构建设、制度流程、技术工具和人员能力等方面对工业控制系统的安全保障。

3.3

能力成熟度　capability maturity

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

[来源：GB/T 37988—2019，3.6]

3.4

能力成熟度模型　capability maturity model

对一个组织的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或者