



中华人民共和国国家标准

GB/T 41400—2026

代替 GB/T 41400—2022

网络安全技术 工业控制系统网络安全 防护能力成熟度模型

Cybersecurity technology—Cybersecurity protection capability maturity model of
industrial control systems

2026-07-02 发布

2027-02-01 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 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 工业控制系统网络安全防护能力成熟度模型 3

6 保护对象安全 7

7 通用安全..... 26

8 能力成熟度等级核验方法..... 43

附录 A（资料性） 能力成熟度等级描述与 GP 72

附录 B（资料性） 能力成熟度模型使用方法 75

附录 C（资料性） 能力成熟度等级核验流程 76

参考文献 79

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。

本文件代替 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》，与 GB/T 41400—2022 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 将全文“信息安全”相关表述更改为“网络安全”(见全文,2022 年版的全文)；
- b) 增加了分布式控制系统等术语和定义(见 3.2、3.3)；
- c) 更改了保护对象术语和定义(见 3.10,2022 年版的 3.10)；
- d) 更改了工业控制系统网络安全防护能力成熟度模型架构图及相关描述(见 5.1,2022 年版的 5.1)；
- e) 更改了能力成熟度等级中等级 2 的名称(见 5.3,2022 年版的 5.3)；
- f) 更改了能力建设过程的 PA 体系(见 5.4.1,2022 年版的 5.4.1)；
- g) 更改了数据完整性校验、设备资产生存周期管控和存储媒体销毁流程等要求(见 6.1,2022 年版的 6.1)；
- h) 更改了发现安全漏洞后的应对举措、系统启用前风险评估等要求(见 6.2,2022 年版的 6.2)；
- i) 更改了组网方式、远程维护等要求(见 6.3,2022 年版的 6.3)；
- j) 增加了工业平台安全要求(见 6.4)；
- k) 更改了配置变更、自主研发软件等要求(见 6.5,2022 年版的 6.4)；
- l) 更改了工业数据分类分级、数据出境等要求(见 6.6,2022 年版的 6.5)；
- m) 增加了工业企业工控安全主体责任、工控安全联合工作机制等要求(见 7.1.1、7.1.2)；
- n) 增加了密码算法应用等要求(见 7.3.1)；
- o) 增加了安全监测、安全运营平台等要求(见 7.4.2)；
- p) 增加了网络关键设备、供应商安全管理等要求(见 7.5)；
- q) 更改了保护对象安全、通用安全的能力成熟度等级核验方法(见第 8 章,2022 年版的第 8 章)。

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。

本文件由全国网络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、中国石油天然气股份有限公司长庆油田分公司、国家工业信息安全发展研究中心、国家计算机网络应急技术处理协调中心、公安部第三研究所、国家信息技术安全研究中心、宁波和利时信息安全研究院有限公司、中国电子技术标准化研究院华东分院、北京天融信网络安全技术有限公司、浙江中测数字信息技术有限公司、北京天地和兴科技股份有限公司、新华三技术有限公司、中控技术股份有限公司、杭州安恒信息技术股份有限公司、中国电子科技网络信息安全有限公司、启明星辰信息技术集团股份有限公司、北京江南天安科技有限公司、杭州迪普科技股份有限公司、中汽研华诚认证(天津)有限公司、中国石化集团共享服务有限公司、中国电力科学研究院有限公司、北京中关村实验室、中国科学院计算技术研究所、长扬科技(北京)股份有限公司、南京理工大学、罗克韦尔自动化(中国)有限公司、工业和信息化部电子第五研究所、广州赛宝认证中心服务有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、中国信息安全测评中心、昆仑数智科技有限责任公司、北京神州绿盟科技有限公司、上海交通大学、湖北省电子信息产品质量监督检验院、厦门赛西科技发展有限公司、福建省电力有限公司泉州电力技能研究院、国网北京市电力公司。

本文件主要起草人：李琳、蔡一鸣、夏冀、周睿康、郭娴、张晓明、邹春明、李世红、张芝军、楚兵、李伟晨、

赵梓桐、周燕华、寇增杰、郑元豪、朱伟光、万晓兰、余梦达、井柯、高津菁、杜俊卓、武卓、黄晶晶、石然、邹大均、胡月、陈冠直、宁力军、杜宏生、魏亮、肖红阳、刘敏、徐刚、赵华、于盟、高镜媚、刘烨、李尧、李婧、伊胜伟、罗革新、王晓鹏、李生红、徐煦、赵伟、宋一琦、周昊、李耕、刘瑞、刘鸿运、马少帅、郎俊奇、安高峰、王挺、翟胜军、刘啸、马洪涛、王小宏、于普漪、胡斌、邱旭东、徐海利、董佳涵、王大为。

本文件及其所代替文件的历次版本发布情况为：

——2022 年首次发布为 GB/T 41400—2022；

——本次为第一次修订。

网络安全技术 工业控制系统网络安全 防护能力成熟度模型

1 范围

本文件确立了工业控制系统网络安全防护能力成熟度模型,描述了保护对象安全和通用安全的成熟度等级,提出了能力成熟度等级核验方法。

本文件适用于使用、运营工业控制系统的相关方进行工业控制系统网络安全防护能力建设,以及对组织工业控制系统网络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

3 术语和定义

GB/T 25069 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 SCADA 系统、DCS、PLC 等。

[来源:GB/T 36323—2018,3.1,有修改]

3.2

分布式控制系统 distributed control system

以计算机为基础,在系统内部(单位内部)对生产过程进行分布控制、集中管理的系统。

注:DCS 系统一般包括现场控制级、控制管理级二个层次,现场控制级主要是对单个子过程进行控制,控制管理级主要是对多个分散的子过程进行数据采集、集中显示、统一调度和管理。

[来源:GB/T 36323—2018,3.2]

3.3

可编程逻辑控制器 programmable logic controller

采用可编程存储器,通过数字运算操作对工业生产装备进行控制的电子设备。

注:PLC 主要执行各类运算、顺序控制、定时等指令,用于控制工业生产装备的动作,是工业控制系统的基础单元。

[来源:GB/T 36323—2018,3.4]

3.4

工业控制系统网络安全防护能力 cybersecurity 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