



# 中华人民共和国国家标准

GB/T 37954—2019

---

## 信息安全技术 工业控制系统漏洞检测产品技术要求及 测试评价方法

Information security technology—  
Technique requirements and testing and evaluation approaches for industrial  
control system vulnerability detection products

2019-08-30 发布

2020-03-01 实施

---

国家市场监督管理总局  
中国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 .....	1
5 产品描述 .....	2
6 安全技术要求 .....	2
6.1 安全功能要求 .....	2
6.2 自身安全要求 .....	4
6.3 安全保障要求 .....	5
7 测评方法 .....	6
7.1 安全功能测试 .....	6
7.2 自身安全测试 .....	11
7.3 安全保障评估方法 .....	14
附录 A (规范性附录) 工业控制系统漏洞检测产品安全功能等级划分 .....	18
附录 B (规范性附录) 工业控制系统漏洞检测产品测评方法分级及其测评项 .....	19
参考文献 .....	20

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全测评中心、中国电子技术标准化研究院、北京工业大学、北京匡恩网络科技有限公司、中国科学院沈阳自动化研究所、北京和利时系统工程有限公司、公安部第三研究所(国家网络与信息系统安全产品质量监督检验中心)、北京交通大学、解放军战略支援部队信息工程大学、中车株洲电力机车有限公司。

本标准主要起草人:张大江、胡仁豪、范科峰、周睿康、赖英旭、谢丰、邸丽清、叶润国、尚文利、赵剑明、陆臻、邹春明、谢安明、郑伟、魏强、安高峰、王春霞、梁猛、汪义舟、王弢、张胜、刘勇。

# 信息安全技术

## 工业控制系统漏洞检测产品技术要求及 测试评价方法

### 1 范围

本标准规定了针对工业控制系统的漏洞检测产品的技术要求,包括安全功能要求、自身安全要求和安全保障要求,以及相应的测试评价方法。

本标准适用于工业控制系统漏洞检测产品的设计、开发和测评。

### 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 25069—2010 信息安全技术 术语

### 3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

#### 3.1

**漏洞 vulnerability**

资产中能被威胁所利用的弱点。

#### 3.2

**测试用例 test case**

为某个特定目标而编制的一组输入、执行条件以及预期结果,以核实是否满足某个特定需求。

#### 3.3

**测试集合 test set**

测试用例的组合。

#### 3.4

**工业控制组态软件 industrial control configuration software**

在控制系统监控层的软件平台和开发环境,使用灵活的方式为用户提供快速配置现场系统状态的软件工具。

### 4 缩略语

下列缩略语适用于本文件。

DNP:分布式网络协议(Distributed Network Protocol)

HTML:超文本标记语言(Hypertext Markup Language)

HTTP:超文本传输协议(HyperText Transfer Protocol)