ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1485—2018

信息安全技术　工业控制系统入侵检测产品安全技术要求

Information security technology—Security technical requirements for industrial control system intrusion detection products

2018-05-07 发布　　2018-05-07 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部信息系统安全产品质量监督检验中心、公安部第三研究所、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司。

本标准主要起草人：沈清泓、邹春明、顾健、张笑笑、俞优、邱梓华、王晓鹏、景晓晖。

信息安全技术　工业控制系统入侵检测产品安全技术要求

1　范围

本标准规定了工业控制系统入侵检测产品的安全功能要求、安全保障要求和安全等级划分要求。

本标准适用于工业控制系统入侵检测产品的设计、开发及测试。

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 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

GB/T 30976.1—2014　工业控制系统信息安全　第1部分：评估规范

GB/T 30976.2—2014　工业控制系统信息安全　第2部分：验收规范

3　术语和定义

GB/T 18336.3—2015、GB/T 25069—2010、GB/T 30976.1—2014 和 GB/T 30976.2—2014 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统入侵检测产品　industrial control system intrusion detection product

面向工业控制系统，旁路部署在工业控制网络中，以工业控制网络上的数据包作为数据源，监听所保护工业控制网络内的所有数据包并进行分析，从而发现异常行为的入侵检测产品。

4　总体说明

4.1　安全技术要求分类

本标准将工业控制系统入侵检测产品安全技术要求分为安全功能要求和安全保障要求两大类。其中，安全功能要求对工业控制系统入侵检测产品应具备的安全功能提出具体要求，包括数据探测、入侵分析、入侵响应、管理控制、检测结果处理、标识与鉴别、管理安全、安全审计、产品自身安全等；安全保障要求针对工业控制系统入侵检测产品的生命周期过程提出具体要求，例如开发、指导性文档、生命周期支持和测试等。

4.2　安全等级划分

本标准按照工业控制系统入侵检测产品安全功能的强度划分安全功能要求的级别，参照 GB/T 18336.3—2015 划分安全保障要求的级别。安全等级突出安全特性，分为基本级和增强级，安全功能要求强弱和安全保障要求高低是等级划分的具体依据。