ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1560—2019

信息安全技术　工业控制系统主机安全防护与审计监控产品安全技术要求

Information security technology—Security technical requirements for security protecting and audit monitoring products for industrial control system host

2019-04-16 发布　　2019-04-16 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：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所。

本标准主要起草人：田晓鹏、沈清泓、邹春明、顾健、张艳、赵婷。

信息安全技术　工业控制系统主机安全防护与审计监控产品安全技术要求

1　范围

本标准规定了工业控制系统主机安全防护与审计监控产品的安全功能要求、安全保障要求及等级划分要求。

本标准适用于工业控制系统主机安全防护与审计监控产品的设计、开发与测试。

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 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 18336.3—2015、GB/T 25069—2010 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统主机　industrial control system host

应用于工业控制系统领域，主要用于监控管理的计算机，包括工业控制系统上位机等。

3.2

安全防护装置　security protecting device

监控被防护主机键盘输入、鼠标操作、移动存储介质拷贝和显示器画面的装置。

3.3

安全防护平台　security protecting platform

接收安全防护装置上传的审计与监控数据，并进行数据分析及安全策略配置的平台。

3.4

数据摆渡　data ferrying

利用安全防护装置，实现工业控制系统主机与移动存储介质之间进行数据交换的一种机制，内外接口在物理链路上不能同时与安全防护装置连通，利用摆渡方式完成信息传输。

4　工业控制系统主机安全防护与审计监控产品描述

工业控制系统主机安全防护与审计监控产品在结构上主要由安全防护装置、安全防护平台等组件构成，主要用于对工业控制系统主机进行安全防护与审计监控。

图1为该产品的典型部署环境，其中安全防护装置利用铠甲式方式部署，主要用于连接工程师站、