ICS 35.240
A.90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

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

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 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、操作员站等工业控制系统主机的各类外设接口，如：VGA 接口、USB 接口、PS/2 接口等，实现对工业控制系统主机外设接口的接入控制；安全防护平台通过网络方式连接安全防护装置，主要用于接收安全防护装置上传的审计与监控数据，并支持下发安全策略，实现数据摆渡、数据分析等功能。此外，该产品提供恶意代码防御服务器，提供对摆渡数据的恶意代码查杀和数据封装等功能。

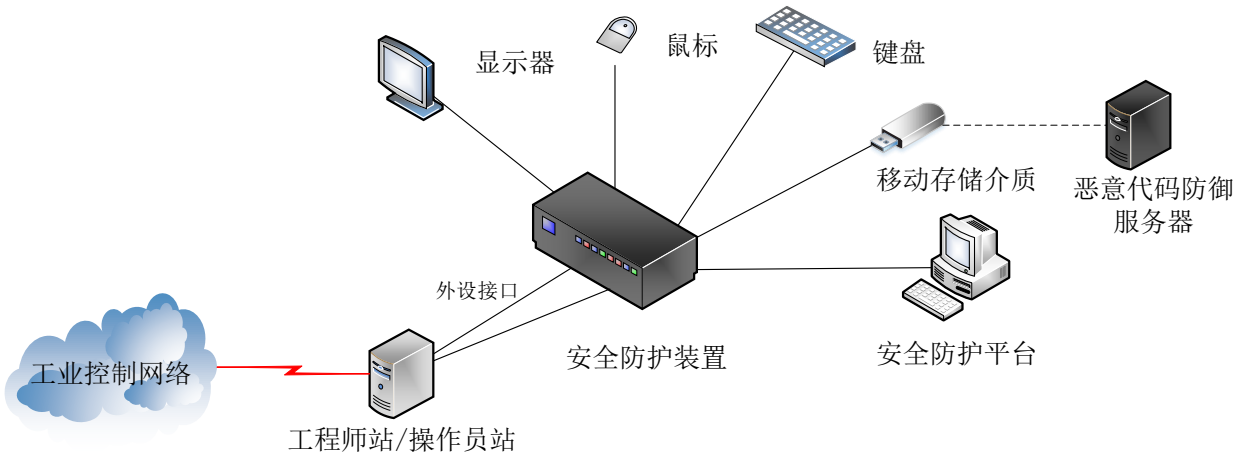

图 1 工业控制系统主机安全防护与审计监控产品典型部署环境

5 安全功能要求

5.1 访问控制

针对主体、客体以及主客体之间的所有操作，产品应能够执行以下访问控制策略：

a) 支持根据主体（如：访问用户等）、客体（如：被防护主机等）、访问权限设置访问控制策略；
b) 主客体之间发送和接收的信息流均经过安全策略允许后传输；
c) 主体访问权限至少包括：被防护主机管理权限、审计数据查询、访问控制策略等。

5.2 操作行为审计与监控

5.2.1 操作行为审计

产品应记录操作行为，包括但不限于：

a) 提供工业控制系统主机图形化实时监视功能；
b) 记录工业控制系统主机通过键盘、鼠标进行输入的操作行为；
c) 记录工业控制系统主体通过移动存储交换介质进行数据交换的操作行为；
d) 记录工业控制系统主机通过网络进行运维管理的操作行为。

5.2.2 操作行为响应

产品应对违反访问控制策略的操作行为进行响应，如日志审计、对话框报警等响应策略。

5.2.3 操作事件回溯

产品应支持操作事件回溯，包括：

a) 支持回溯用户通过移动存储交换介质进行数据交换的过程；
b) 支持选择指定节点进行回溯操作，并可按事件发生时间、审计事件类别、主体、客体等进行查询。

5.2.4 实时监控

产品应支持实时监控功能，包括：

a) 对被防护主机当前登录状态进行实时监控，当有访问人员登录时，能及时发现；
b) 对安全防护装置进行实时监控，当出现故障时断开时，能及时发现。

5.3 数据安全交换

5.3.1 摆渡式数据安全交换

产品应支持摆渡式数据安全交换，在主体执行数据拷贝操作时，应通过身份鉴别，利用移动存储介质和安全防护装置进行数据摆渡操作。

5.3.2 数据封装

产品应支持对拷入移动存储介质中的数据进行数据封装操作。

5.3.3 恶意代码防御

产品应支持恶意代码防御功能，对外部拷入的数据进行恶意代码查杀，支持恶意代码库的手动升级。

5.4 信息显示与数据分析

5.4.1 前端信息显示

产品应支持实时显示当前访问人员的登录信息，包括登录时间、登录用户、操作行为等。

5.4.2 数据分析与评价

产品应对上传至安全防护平台的各类数据分类统计，形成分析报告。

5.5 时间同步

产品应支持各个组件之间的时间同步，包括手动同步和自动同步。

5.6 用户标识

5.6.1 属性定义

产品应为每个管理员规定与之相关的安全属性，包括：管理角色标识、鉴别信息、隶属组、权限等。

5.6.2 属性初始化

产品应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

5.6.3 唯一性标识

产品应保证任何用户都具备唯一的标识，用户标识与产品自身审计相关联，并在产品的生命周期内唯一。

5.7 身份鉴别

5.7.1 基本鉴别

产品应在执行任何与管理员相关功能之前鉴别用户的身份。

5.7.2 多鉴别

产品应支持采用两种或两种以上的用户身份组合鉴别方式。

5.7.3 鉴别数据初始化

产品应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.7.4 鉴别失败处理

当管理员鉴别尝试失败连续达到指定次数后，产品应阻止管理员进一步的鉴别请求，并将有关信息生成审计事件。最多失败次数仅由授权管理员设定。

5.7.5 鉴别数据保护

应保护鉴别数据在传输和存储过程中不被未授权查阅和修改。

5.8 安全审计

5.8.1 自身审计数据生成

产品应对下列可审计事件生成一个审计记录：

a) 管理员的登录和退出；
b) 对安全策略进行更改的操作；
c) 对管理员进行增加、删除和属性修改的操作；
d) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；
e) 安全防护装置与安全防护平台状态日志；
f) 对其他安全功能配置参数的修改（设置和更新），无论成功与否。

对于每一个审计记录，产品应至少记录以下信息：事件发生的日期和时间、事件类型、主体身份和事件结果（成功或失败）等。

5.8.2 审计记录管理

产品应允许授权管理员创建、存档、删除和清空审计记录。

5.8.3 可理解格式

产品应使存储于永久性审计记录中的所有审计数据可为人所理解。

5.8.4 限制审计记录访问

除了具有明确的访问权限的授权管理员之外，产品应禁止所有其他用户对审计日志的访问。

5.9 安全管理功能

如果产品支持远程管理，应能通过加密的方式来保护远程管理会话内容不被非授权获取。

5.10 硬件失效处理

安全防护装置应提供硬件失效处理机制，如在断电或防护装置系统资源不足的情况提供硬件Bypass功能。

5.11 网络性能要求

产品接入工业控制系统网络后，不能影响工业控制系统原有网络设备和主机的功能，并且不能对原网络系统产生明显的影响。

6 安全保障要求

6.1 开发

6.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

6.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 完全描述产品的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯；
g) 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

6.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a) 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b) 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c) 以开发人员使用的形式提供。

6.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 根据子系统描述产品结构；
b) 标识和描述产品安全功能的所有子系统；
c) 描述安全功能所有子系统间的相互作用；
d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e) 根据模块描述安全功能；
f) 提供安全功能子系统到模块间的映射关系；
g) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

6.2 指导性文档

6.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的可用接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f) 充分实现安全目的所必须执行的安全策略。

6.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

6.3 生命周期支持

6.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

6.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；

b) 实现表示、安全缺陷报告及其解决状态。

6.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

6.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

6.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

6.4 测试

6.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；

b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

6.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；

b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

6.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果，表明测试成功后的预期输出；

c) 实际测试结果和预期的一致性。

6.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；

b) 具有增强型基本攻击潜力的攻击者的攻击。

7 安全等级划分及要求

7.1 等级划分

工业控制系统主机安全防护与审计监控产品的安全等级按照其安全功能要求和安全保障要求的强度划分为基本级和增强级，其中安全保障要求参考了 GB/T 18336.3—2015。

7.2 安全功能要求

不同安全等级的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如表 1 所示。

表 1 不同安全等级的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

安全功能要求		基本级	增强级
访问控制		5.1	5.1
操作行为审计与监控	操作行为记录	5.2.1 a) ～c)	5.2.1
	操作行为响应	——	5.2.2
	操作事件回溯	5.2.3	5.2.3
	实时监控	5.2.4	5.2.4
数据安全交换	摆渡式数据安全交换	5.3.1	5.3.1
	数据封装	5.3.2	5.3.2
	恶意代码防御	5.3.3	5.3.3
信息显示与数据分析	前端信息展示	5.4.1	5.4.1
	数据分析与评价	——	5.4.2
时间同步		5.5	5.5
用户标识	属性定义	5.6.1	5.6.1
	属性初始化	5.6.2	5.6.2
	唯一性标识	5.6.3	5.6.3
身份鉴别	基本鉴别	5.7.1	5.7.1
	用户多鉴别	——	5.7.2
	鉴别数据初始化	5.7.3	5.7.3
	鉴别失败处理	——	5.7.4
	鉴别数据保护	5.7.5	5.7.5
安全审计	审计数据生成	5.8.1 a) ～c)	5.8.1
	审计记录管理	5.8.2	5.8.2
	可理解格式	5.8.3	5.8.3

表1（续）

安全功能要求		基本级	增强级
安全审计	限制审计记录访问	5.8.4	5.8.4
安全管理功能		——	5.9
硬件失效处理		——	5.10
网络性能要求		5.11	5.11

7.3 安全保障要求

不同安全等级的的安全保障要求如表 2 所示。

表 2 不同安全等级的工业控制系统主机安全防护与审计监控产品的安全保障要求

安全保障要求		基本级	增强级
开发	安全架构	6.1.1	6.1.1
	功能规范	6.1.2 a) ～f)	6.1.2
	实现表示	——	6.1.3
	产品设计	6.1.4 a) ～d)	6.1.4
指导性文档	操作用户指南	6.2.1	6.2.1
	准备程序	6.2.2	6.2.2
生命周期支持	配置管理能力	6.3.1 a) ～c)	6.3.1
	配置管理范围	6.3.2 a)	6.3.2
	交付程序	6.3.3	6.3.3
	开发安全	——	6.3.4
	生命周期定义	——	6.3.5
	工具和技术	——	6.3.6
测试	覆盖	6.4.1a)	6.4.1
	深度	——	6.4.2
	功能测试	6.4.3	6.4.3
	独立测试	6.4.4	6.4.4
脆弱性评定		6.5 a)	6.5 b)