ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1350—2017

信息安全技术　工业控制系统安全管理平台安全技术要求

Information security technology—Security technical requirements for security management platform of industrial control system

2017-11-20 发布　　2017-11-20 实施

中华人民共和国公安部　　发布

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、北京匡恩网络科技有限责任公司。

本标准主要起草人：张笑笑、沈清泓、邹春明、邱梓华、吴其聪、沈亮、李强强。

信息安全技术　工业控制系统安全管理平台安全技术要求

1　范围

本标准规定了工业控制系统安全管理平台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安全管理平台产品的设计、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

3　术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 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

对工业生产过程安全、信息安全和可靠运行产生作用和影响的人员、硬件和软件的集合。

4　缩略语

下列缩略语适用于本文件。

OLE：对象连接与嵌入(Object Linking and Embedding)

CPU：中央处理器 (Central Processing Unit)

OPC：用于过程控制的 OLE(OLE for Process Control)

5　工业控制系统安全管理平台产品描述

工业控制系统安全管理平台产品是适用于工业控制系统的安全管理平台，支持对工业控制系统安全产品(如工业控制入侵检测系统、工业控制防火墙、工业控制网络隔离产品、工业控制安全审计产品等)的安全策略和安全配置进行设置和检查，能获取安全审计日志信息，按照安全事件特征进行分析，发现并确认安全事件，并能进行报警响应处理。工业控制系统安全管理平台内置安全事件库，能够按照安全事件特征对收集的各类安全审计日志进行分析，发现安全事件并作出响应(如报警)。

6 总体说明

6.1 安全技术要求分类

本标准将工业控制系统安全管理平台产品的安全技术要求分为安全功能要求和安全保障要求两类。其中，安全功能要求是对工业控制系统安全管理平台产品应具备的安全功能提出具体要求，包括安全管理、统计分析、响应措施、标识与鉴别、管理安全和安全审计；安全保障要求针对工业控制系统安全管理平台产品的开发和使用文档的内容提出具体的要求，例如开发、指导性文档、生命周期支持、测试和脆弱性评定等。

6.2 安全等级划分

本标准按照工业控制系统安全管理平台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，安全功能强弱和安全保障要求高低是等级划分的具体依据。

7 安全功能要求

7.1 安全管理

7.1.1 设备管理

产品应能对运行于工业控制系统中的安全产品进行统一管理，并建立设备清单。设备清单应至少包括设备名称、设备类型、重要程度、所处位置和安全责任人等内容。

7.1.2 状态监测

产品应能够对工业控制系统安全产品的运行状态进行监测，并满足以下要求：

a) 监测频率支持自定义；

b) 监测的运行状态，包括在线状态、系统资源(CPU、内存和硬盘)使用情况等、网络流量等；

c) 支持工业控制系统安全产品网络拓扑图的绘制。

7.1.3 信息收集

产品应能对工业控制系统安全产品的信息进行收集，具体包括：

a) 硬件型号；

b) 软件版本；

c) 审计日志；

d) 安全策略，如工业控制系统入侵检测系统报警策略、工业控制系统防火墙的数据包过滤规则、工业控制系统网络隔离产品访问控制策略、工业控制系统安全审计产品的审计策略等；

e) 安全配置；

f) 硬件序列号。

7.1.4 基线检查

产品应提供基线检查功能，具体包括：

a) 建立和更新工业控制系统安全产品的安全基线；
b) 通过基线检查，比对工业控制系统安全产品当前安全配置、安全策略与基线的一致性，并给出比对结果；
c) 提供基线定时检查功能，当发现工业控制系统安全产品当前配置与基线不一致时，应进行报警。

7.1.5 策略配置

产品应能够对工业控制系统安全产品的安全策略进行设置，比如工业控制入侵检测系统报警策略，工业控制防火墙的数据包过滤规则、工业控制网络隔离产品访问控制策略、工业控制安全审计产品的审计策略等，并支持以下功能：

a) 对安全策略进行添加、删除、修改和分发；
b) 对安全策略进行导入和导出。

7.1.6 身份鉴别

产品应保证要通过鉴别才能够对工业控制系统安全产品进行管理，并且应保证存储在产品中的鉴别数据不被未授权查阅或修改。

7.2 统计分析

7.2.1 安全事件库维护

产品应建立安全事件库，并提供安全事件库的维护功能，具体包括：

a) 安全事件库内容应包括：事件名称、事件类型、事件级别、事件描述和事件特征；
b) 安全事件库支持工业控制协议(MODBUS、OPC 等)和工业控制系统的安全事件；
c) 提供开放接口，允许用户自定义安全事件；
d) 应提供安全事件库升级功能。

7.2.2 安全事件分析

产品应能对收集的审计日志进行分析，从中提取安全事件。

7.2.3 统计分析报表

产品应能够对安全事件进行统计，并生成汇总报表，并满足：

a) 报表应能够以通用格式(例如 html、pdf 或 doc)导出；
b) 报表应包含文字、图、表等表现形式。

7.2.4 潜在危害分析

产品应能设定单类事件累计发生次数或发生频率的阈值，当统计分析表明此类事件超出阈值时则表明工业控制系统出现了潜在的危害。

7.2.5 异常行为分析

产品应能对工业控制系统中的异常行为进行分析。

7.2.6 关联事件分析

产品应能制定关联分析规则，并基于不同的规则对不同设备上报的审计日志进行关联分析。

7.3 响应措施

7.3.1 告警

当发生以下情况时，产品应对以下事件进行告警：

a) 设备状态达到告警阈值；

b) 发现指定的安全事件。

7.3.2 推荐策略

产品应能根据统计分析的结果，自动生成推荐性安全策略。

7.4 标识与鉴别

7.4.1 唯一性标识

产品应为用户提供唯一标识，并能将标识与其所有可审计事件相关联。

7.4.2 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别用户的身份。

7.4.3 多重鉴别

产品应为用户提供两种或两种以上的鉴别机制。若产品支持口令方式进行鉴别，应能设置口令策略，对口令的长度和复杂性进行检查，并提供口令定期更新功能。

7.4.4 超时机制

产品应提供超时重新鉴别机制，如果产品用户停止操作的时间超过一定时限，应对用户身份重新进行鉴别。时限由产品的授权管理员进行设置。

7.4.5 鉴别数据保护

产品应保证鉴别数据不被未授权查阅和修改。

7.4.6 鉴别失败处理

当对用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

7.5 管理安全

7.5.1 安全角色管理

产品应能通过对授权管理员给以不同的管理角色，赋予授权管理员不同的管理权限。

7.5.2 管理方式

产品应支持本地管理。若提供远程管理方式，产品应能满足以下要求：

a) 对可远程管理主机的 IP 地址进行限制；

b) 对可远程管理主机的 MAC 地址进行限制；

c) 远程管理接口可由管理员关闭。

7.5.3 数据保护

7.5.3.1 数据存储保护

产品应能对存储的重要数据进行保护，以免被非授权访问。这些重要数据至少包括：

a） 用户及工业控制系统安全产品的鉴别信息；

b） 工业控制系统安全产品的审计日志、安全配置和安全策略等。

7.5.3.2 数据传输保护

产品应采取安全措施保护重要数据在传输过程中不被泄露和窃取。这些重要数据至少包括：

a） 用户及工业控制系统安全产品的鉴别信息；

b） 工业控制系统安全产品的安全配置和安全策略等。

7.5.3.3 数据备份和恢复

产品应提供重要数据的备份和恢复功能，这些重要数据包括：工业控制系统安全产品的安全配置、安全策略和审计日志等。

7.5.4 端口分离

产品应配备不同的端口分别用于产品管理和信息收集。

7.6 安全审计

7.6.1 系统日志生成

产品应对与自身安全相关的下列事件生成审计日志：

a） 用户登录成功和失败；

b） 对安全策略进行更改；

c） 对用户进行增加、删除和属性修改；

d） 因鉴别失败的次数超出了设定值，导致的会话连接终止；

e） 对事件记录、审计日志的操作。

7.6.2 系统日志内容

产品的系统日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

7.6.3 审计日志查阅

产品应提供多条件查阅工具，对系统日志和收集的审计日志进行查询。

7.6.4 审计日志存储

产品的审计日志应存储于掉电非易失性存储介质中，并满足以下要求：

a） 当审计日志存储空间超过阈值时，应能通知用户；

b） 当审计日志存储空间将要耗尽时，应采取相应的防止审计数据丢失的技术措施。

8 安全保障要求

8.1 开发

8.1.1 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。

8.1.2 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。

8.1.3 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。

8.1.4 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。

8.2 指导性文档

8.2.1 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。

8.2.2 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。

8.3 生命周期支持

8.3.1 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。

8.3.2 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。

8.3.3 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。

8.3.4 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。

8.3.5 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。

8.3.6 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。

8.4 测试

8.4.1 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。

8.4.2 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。

8.4.3 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，证实实际测试结果和预期的测试结果相一致。

8.4.4 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。

8.5 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。

9 等级划分要求

9.1 概述

工业控制系统安全管理平台产品的安全功能要求和安全保障要求划分为基本级和增强级。

9.2 安全功能要求等级划分

工业控制系统安全管理平台产品的安全功能要求等级划分如表1所示。

表 1　工业控制系统安全管理平台产品安全功能要求等级划分表

安全功能要求			基本级	增强级
安全管理	设备管理		7.1.1	7.1.1
	状态监测		7.1.2 a)、b)	7.1.2
	信息收集		7.1.3 a)～d)	7.1.3
	基线检查		—	7.1.4
	策略配置		7.1.5 a)	7.1.5
	身份鉴别		7.1.6	7.1.6
统计分析	安全事件库维护		7.2.1 a)、b)	7.2.1
	安全事件分析		7.2.2	7.2.2
	统计分析报表		7.2.3 a)	7.2.3
	潜在危害分析		7.2.4	7.2.4
	异常行为分析		7.2.5	7.2.5
	关联事件分析		—	7.2.6
响应措施	告警		7.3.1	7.3.1
	推荐策略		—	7.3.2
标识与鉴别	唯一性标识		7.4.1	7.4.1
	基本鉴别		7.4.2	7.4.2
	多重鉴别		—	7.4.3
	超时机制		7.4.4	7.4.4
	鉴别数据保护		7.4.5	7.4.5
	鉴别失败处理		—	7.4.6
管理安全	安全角色管理		—	7.5.1
	管理方式		—	7.5.2
	数据保护	数据存储保护	7.5.3.1 a)	7.5.3.1
		数据传输保护	7.5.3.2 a)	7.5.3.2
		数据备份和恢复	—	7.5.3.3
	端口分离		—	7.5.4
安全审计	系统日志生成		7.6.1 a)、b)	7.6.1
	系统日志内容		7.6.2	7.6.2
	审计日志查阅		7.6.3	7.6.3
	审计日志存储		—	7.6.4

9.3　安全保障要求等级划分

工业控制系统安全管理平台产品的安全保障要求等级划分如表 2 所示。

表 2　工业控制系统安全管理平台产品安全保障要求等级划分表

安全保障要求		基本级	增强级
开发	安全架构	8.1.1	8.1.1
	功能规范	8.1.2 a)～f)	8.1.2
	实现表示	—	8.1.3
	产品设计	8.1.4 a)～d)	8.1.4
指导性文档	操作用户指南	8.2.1	8.2.1
	准备程序	8.2.2	8.2.2
生命周期支持	配置管理能力	8.3.1 a)～c)	8.3.1
	配置管理范围	8.3.2 a)	8.3.2
	交付程序	8.3.3	8.3.3
	开发安全	—	8.3.4
	生命周期定义	—	8.3.5
	工具和技术	—	8.3.6
测试	覆盖	8.4.1 a)	8.4.1
	深度	—	8.4.2
	功能测试	8.4.3	8.4.3
	独立测试	8.4.4	8.4.4
脆弱性评定		8.5 a)	8.5

中华人民共和国公共安全
行　业　标　准

信息安全技术　工业控制系统安全管理平台安全技术要求

GA/T 1350—2017

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址:www.spc.org.cn
服务热线:400-168-0010
2018年3月第一版

*

书号:155066·2-32737

GA/T 1350-2017