ICS 35.040
L 80

测绘仪有效用户全功能要求

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　安全[illegible]功能要求描述结构 ……

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。

引　言

现场测控设备是工业控制系统的基本功能执行设备，[illegible]对生产过程进行监视与控制。对于生产过程中的应用，现场设备的智能化程度逐渐增加，网络化和处理能力的增加使得这些设备所面临的信息安全风险较传统现场设备面临的风险种类更多，范围更大，层次

信息安全技术 工业控制系统现场

注：下列设备为典型的工业控制系统现场测控设备：

——远程终端单元(RTU,Remote Terminal Unit)；

——智能电子设备(IED,Intelligent Electric Device)；

——分散处理单元(DPU,Distributed Processing Unit)。

3.2

类别 category

息。每个要求类都有一个唯一的名称，类的分类信息

说明见附录 B。类名的简写也用于该类中族的族名规

主要作用。类

类名提供

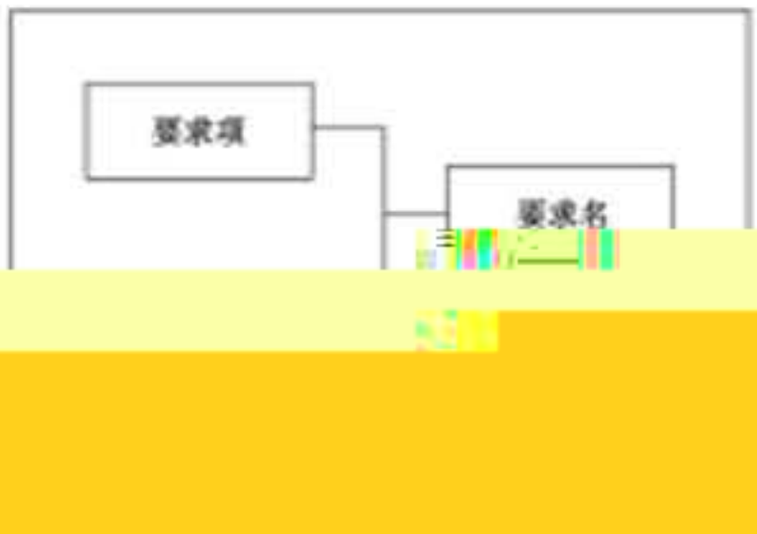
由三个字符的简写组成。要求类分类信息简写

范中。

类描述总体描述类中包含的族和该类要求

组件的层次结构。





签人员；

——设备

置软件；

——系统

6.2.2.2.2 要求说明

应对[illegible]录的用户完使身份标识、如配合管理用户、主控机控制台监等一类型的用户身份标识等

[illegible]

[illegible]

[illegible]

[illegible]功能的用户[illegible]

[illegible]

6.2.2.3.4 依[illegible]要求

FIA_IAM.2 将[illegible]及方式的依赖要求[illegible]

[illegible]

其中人员用户标识符管理的功能相当于普通 IT 应用系统的用户管理，针对直接使用控制面板对设备进行本[illegible]理的操[illegible]

6.2 FIA_IDM.1 操控人[illegible]标识符管理

6.2.3.2.1 要求

工控系统现场[illegible]控设备应具备向操控人员分配标识符的能力。

6.2.3.2.2 要求说明

设备应具备向具有运行参数或[illegible]

6.2.3.2.3 要求加强

FIA_IDM.1 操控人员标识符管理的要求加强包括：

a)设备支持对操控人员标识符进行添加、删除等管理；

b)设备支持对安全策略规定一段时间不使用的操控人员标识符进行锁定。

6.2.4.4 FIA_ACM.3 口令强度控制

6.2.4.4.1 要求

工控系统现场测控设备应提供支持安全管理员对口令强度要求的能力。

6.2.4.4.2 要求说明

在实现上，当用户设定口令强度不足时，工控系统现场测控设备应自动提醒用户口令强度应满足怎样的安全策略。

6.2.4.4.3 要求加强

FIA_ACM.3 口令强度控制的要求加强为设备应支[illegible]

FIA_ACM.3 口令强度控制的依赖关系是 FIA_IAM.2。

6.2.4.5 FIA_ACM.4 口令失效

6.2.4.5.1 要求

[illegible]

[illegible]能绕过用户创建的用户名/口令复杂的机制。如果设备没有这样的机制，应予以声明。

6.2.4.5.3 要求加强

无。

6.2.4.5.4 依赖要求

FIA_ACM.4 口令失效的依赖要求是 FIA_IAM.2。

6.2.4.6 FIA_ACM.5 证书及公私钥管理

6.2.4.6.1 要求

如果使用了公私钥或证[illegible]

应能够对配置用户的公钥进行管理，并对证书进行识别。

b) 现场测控设备应支持工控系统层面上的密钥管理体系，支持对密钥的分发、更新和撤销的

6.2.4.8.4 依赖要求

FIA_ACM.7 密码服务失效的依赖要求是 FIA_IAM.2 [illegible] M.5 和 FIA_ACM [illegible]

6.2.5 FIA_LGM 族：登录管理

[illegible]

操作配置软件登录、网络登录方式。

6.2.5.3.3 要求加强

无。

6.2.5.3.4 依赖要求

FIA_LGM.2 登录[illegible]规定 FIA_IAM.2。

6.2.5.4 FIA_LGM.3 登录历史

6.2.5.4.1 要求

用户验证成功后，工控系统现场测控设备[illegible]

6.2.5.4.2 要求说明

主要对管理员等实现鉴别了的重要用户的登录进行管理。登录方式涵盖本地面板登录、通过私有配置软件登录、网络登录等。

6.2.5.4.3 要求加强

无。

6.2.5.4.4 依赖要求

FIA_LGM.3 登录历史的依赖要求是 FIA_IAM.2 和 FIA_LGM.1。

6.2.5.5 FIA_LGM.4 多次登录失败

6.2.5.5.1 要求

当操控人员在一段时间内失败的登录尝试次数超过安全策略中的规定值，现场测控设备应执行限制机制。

6.2.5.5.2 要求说明

限制机制包括对操控人员进行锁定、发出警报等。

6.2.5.5.3 [illegible]

6.2.5.5.4 依赖要求

FIA_LGM.4 多次登录失败的依赖关系是 FIA_IAM.2 和 FIA_LGM.1。

6.2.5.6 FIA_LGM.5 鉴别反馈

6.2.5.6.1 要求

[illegible]

6.2.5.6.2 要求说明

反馈信息中不应包含非授权人员可以利用的能够绕过鉴别机制的信息。

6.2.5.6.3 要求加强

无。

6.2.5.6.4 [illegible]

6.3 FDC 类：使用控制

6.3.1 类描述

使用控制的目的是为了保护设备，在用户发起登录界面、到完成产品求告中使[illegible]

限,根据权限执行所请求的操作,并进行控制和审

6.3.2 FUC_ACA 族:访问控制授权

6.3.2.1 族描述

工控系统现场控制设备为不同访问用户
配权限,只允许通过
所分配角色
户设置可固定,如只有一个查看用户、一个配置用户、一个审计用户。

6.3.2.3.3 要求加强

无。

6.3.2.3.4 依赖要求

FUC_ACA.2 基于角色的访问控制的依赖要求是 FIA_IAM.1。

6.3.2.4 FUC_ACA.3 管理员用户

6.3.2.4.1 要求

现场测控设备访问控制功能应支持管理员用户角色（管理员

场设备）对设备的访问也应基于最 权限，如只能访问某一网

6.3.2.6.2 要求说明

分权管理的典型过程是操作用户和审核用户合作获得访问设备[illegible]或执行控制操作的权限。主要是针对重要操作流程就位的安全机制,实现审核与[illegible]前操作的执行和确认。

6.3.2.6.[illegible]

[illegible]活动时间进行配置。

6.3.2.9 依赖要求

无。

6.3.3.3 FUC_SEC.2 网络会话超时

6.3.3.3.1 要求

工控系统现场测控设备应在设备配置界[illegible]或配置软件与设备的会话[illegible]功能,[illegible]会话中无活[illegible]

6.3.3.3.2 要求说明

网络会话超时实现主要为了设备能自动[illegible]制。如果会话建立途经网[illegible]有完备物理访问控制机制的可信[illegible]

[illegible]控制。

6.3.3.3.3 要求加强

[illegible]

6.3.3.3.4 依赖要求

无。

6.3.4 FUC_ATC 族：审计踪迹产生

6.3.4.1 族描述

工控系统现场测控设备对安全相关的重要生产活动进行审计，对于修正错误、开放恢复、事件调查等相关工作。

6.3.4.2 FUC_ATC.1 审计事件

6.3.4.2.1 要求

工控系统现场测控设备应具备审计功能，对重要的安全性事件和重要生产活动进行审计。

[illegible]

[illegible]

[illegible]

6.3.4.3 FUC_ATG.2 审计踪迹的内容

6.3.4.3.1 要求

工控系统现场测控设备或承担审计功能的组件，其审计踪迹中应包含足够的可用于追踪与分析安全事件的内容。

6.3.4.3.2 要求说明

根据审计踪迹

踪迹内容包括：

——事件的日期和时间；

——事件的来源(例如，用[illegible])；

——事件的操作；

[illegible]。

6.3.4.3.3 要求加强

FUC_ATG.2 审计踪迹

的内容的要求加强[illegible]

[illegible]

计踪迹的内

[illegible]

[illegible]

[illegible]

6.3.4.5.3 要求加强

无。

6.3.4.5.4 依赖要求

FUC_ATC.4 用户关联的依赖要求是 FIA_IAM.1。

6.3.5 FUC_ATS 族:审计跟踪存储

6.3.5.1 族描述

工控系统现场测控设备存储并保护安全性事件和重要生产活动的审计跟踪,分析时获得足够的、正确的信息。

6.3.5.2 FUC_ATS.1 审计存储容量

6.3.5.2.1 要求

工控系统现场测控设备应具备一定的审计跟踪存储容量。

6.3.5.2.2 要求说明

如果由工控系统现场测控设备自身完成审计功能,那么设备能维护一个大小合理的存储空间,在满足审计功能的同时,保证不影响设备的可用性。

6.3.5.2.3 要求加强

无。

6.3.5.2.4 依赖要求

无。

6.3.5.3 FUC_ATS.2 审计功能异常

6.3.5.3.1 要求

工控系统现场测控设备或从事审计功能的组件应在审计失败时发出适当的告警。

6.3.5.3.2 要求说明

告警的方式如警示灯、响铃等

主机的审计踪迹进行过滤和分析，设备的审计踪迹格式应是统一的。

6.3.6.3.3 要求加强

无。

6.3.6.3.4 依赖要求

无。

6.3.6.4 FUC_ATR.3 审计报告

6.3.6.4.1 要求

工控系统现场测

的响应，审计报告生成支持在审核发现审计踪迹的情况下作安全事件的审后调查

验证与报警。

6.4.2.2.4 依赖要求

FDI_DSI.1 安全功能检测的依赖要求是 FUC_ATC.1。

6.4.2.3 FDI_DSI.2 异常处理

6.4.2.3.1 要求

工控系统现场测控设备应识别和处理异常情况并迅速产生安全相关错误消息。

6.4.2.3.2 要求说明

错误消息中应仅包含用于定位处理故

验码。

6.4.3.6.3 要求加强

FDT_DTI.3 数据包防篡改的要求加强为设备应具备基于密码的通信信息防篡改机制。典型机制

[illegible]

[illegible]

[illegible]方止中间人通过对协议观察分析从而加入或窃取通信会[illegible]。

[illegible]求说明

主要针对协议交互过程进行安全设计，

6.4.3.7.3 要求加强

无。

6.4.3.7.4 依赖要求

无。

6.5 FDC 类:数据保密性

6.5.1 类描述

[illegible]数据的保密性进行保护的目的是[illegible]

[illegible]数据被窃听，主要防护对象是信息[illegible]

6.5.2.2.3 要求加强

无。

6.5.2.2.4 依赖要求

无。

6.5.3 FDC_DSC 族:存储数据保密性

6.5.3.1 族行为

存储数据保密性的要求[illegible]

的存储数据保密性保护机制,如加

密等。

6.5.3.2.4 依赖要求

可以在应用

6.5.4.2.2 要求说明

传输的口令、密钥和用户隐私等敏感数据应以非明文方式传输。数据保密性保护机制可以在应用层实现,也可以当数据在非安全域内传输时,在网络层上实现。

6.5.4.2.3 要求加强

FDC_DTC.1 传输数据保密性的要求加强[illegible]

6.5.4.2.4 依赖要求

FDC_CRM.1 的依赖要求是 FDC_CRM.1。

6.6 FRF 类：数据流限制

6.6.1 类描述

数据流限制的目的是在网络与本地通过访问控制和分区限制不必要的数据流。

6.6.2 FRF_NAC 族：网络与端口访问控制

6.6.2.1 族描述

工控系统现场测控设备对网络[illegible]实施访问控制，主要基于[illegible]访问控制，配置[illegible]，其他现场设备或在[illegible]访问。

6.6.2.2 FRF_NAC.1 端口启用

6.6.2.2.1 要求

[illegible]

6.6.2.2.2 要求说明

[illegible]服务端口，同时也应关闭[illegible]本地配置的固件升级物理网络端口或中[illegible]开启的端口或服务均应具备用户鉴别机制。

6.6.2.2.3 要求加强

无。

6.6.2.2.4 依赖要求

无。

6.6.2.3 FRF_NAC.2 数据流控制

6.6.2.3.1 要求

[illegible]数据流的源宿访问控制信息[illegible]

6.6.2.3.2 要求说明

6.6.2.4 FRF_NAC.3 无线访问

6.6.2.4.1 要求

使用无线访问的工控系统现场测控设备，应能支持在物理上关闭无线功能（如硬压板），其具备的无线协议应具备安全机制。

6.6.2.4.2 要

6.6.3.1 概述

工控系统现场测控设备不同功能的分离通过分区与隔离机制实现。

6.6.3.2 FRF_FUP.1 应用分区

6.6.3.2.1 要求

工控系统现场测控设备应将数据获取服务与管理功能分区。

6.6.3.2.2 要

6.6.3.2.3 要求加强

无。

6.6.3.2.4 依赖要求

无。

6.6.3.3 FRF_FUP.2 安全功能隔离

6.6.3.3.1 要求

工控系统现场测控设备应将数据和可执行代码分别存储在不同的内存空间，并能够阻止数据内存空间内的代码执行。

6.6.3.4.2 要求说明

可静态分配内存[illegible]支持硬件 MMU 的 OS、或者支持分离内[illegible]计的 CPU。

6.6.3.4.3 要求加强

无。

6.6.3.4.4 依赖要求

无。

6.7 FRA 类：资源可用性

6.7.1 类描述

[illegible]保持业务连续性。

6.7.2 FRA_DSP 族：拒绝服务保护

6.7.2.1 族描述

工控系统现场测控设备抵[illegible]DoS 攻击或降低攻击的影响，保障[illegible]

6.7.3.1 族描述

6.7.3.3.2 要求说明

协议模糊攻击的[illegible]为保证系统设备所开启服务在开发实现过程中的安全要求。

6.7.3.3.3 要求加强

无。

6.7.3.3.4 依赖要求

无。

6.7.3.4 FRA_BUC.3 [illegible]

[illegible]

[illegible]

[

6.7.3.6 FRA_BUC.5 备用电源

6.7.3.6.1 要求

[illegible]

附 录 A
（资料性附录）
典型工业控制系统现场测控设备功能与构成

A.1 工业控制系统现场测控设备典型功能

工业控制系统现场测控设备位于工业控制系统的最底层，直接与生产过程设备连接，实现对现场



开启、诊断、掉电数据保持等。

不是所有现场设备都具备

提供所有的模块，

置运行设备内部逻辑控制与自定义功能，具体功能包括采集输入接口的所有数据

输出控制指令到输出接口并发送或接收通信数据至通信接口。作为系统核心的

处理器包括 MCU

和 MPU。

存储器包括有系统程序存储器、用户程序存储器和数据存储器。其

模块更代原有的输入和输出模块。

为模拟输入模块和数字输入模块。

输入模块接收电压、电流、温度、压力等现场测量量，可分

输出模块输入对

示与人机接口面板、调试软件、监控后台、工程

网口、电缆接口、RS232 串口、RS485 串口、

管理模块实现装置的管理和通信。具体功能包括实

师站、远动和打印机间的通信。

设备的对外物理接口形式包括有 IEEE 802.3 以

ISO 11898 '

附　录　B
（规范性附录）
要求类与要求族的分类信息简写说明

要求类的[illegible]写说明见表 B.1。

表 B.1　要求类的分类信息简写说明

要求[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
FDI类	Function-Data Inte[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

表 B.2（续）

要求族简写	要求族名称	简写对应的英文族名
FRE_FUP 族	功能分区	Funciton-Re[illegible]
FRA_DSP 族	拒绝服务保护	Funciton-Resource Avai[illegible]_Deny of Sevices Protection
FRA_BUC 族	业务连续性	Funciton-Resource Availability_Business Continuity

附 录 C
（规范性附录）
安全功能要求依赖关系表

表 C.1 列出了安全功能要求之间的依赖关系。每个依赖其他安全功能要求的要求项在表中占据一行。

表 C.1（续）

要求	FIA_IAM, 1 标识方式	FIA_IAM, 2 鉴别方式	FIA_IAM, 5 证书私钥管理	FIA_MOL, 6 对失败鉴别尝试管理	FIA_LGM, 1 登录记录	FIA_LGM, 2 登录失败	FIA_LGM, 4 多次登录	FPC_MCA, 1 权限访问控制	FPC_MCA, 2 基于角色的访问控制	FPC_ATC, 1 审计记录	FPC_ATS, 1 审计存储	FPC_ATS, 3 审计存储方式	FPC_ATR, 2 审计记录	FPC_CRM, 1 加密机制	FPF_NAC, 2 数据完整性	FPA_BUC, 1 关键性
FIC_ATC:[illegible]																

附 录 D
（规范性附录）

表 D.1（续）

要求类(6)	要求族(18)	要求项(58)
FUC 类：使用控制	FUC_ATR 族：审计踪迹访问	FUC_ATR.1 审计踪迹读取
		FUC_ATR.2 审计踪迹报送
		FUC_ATR.3 审计报告
	FDI_DSI 族：数据存储[illegible]性	FDI_DSI.1 安全功能检测
		FDI_DSI.2 异常处理
		FDI_DSI.3 输入验证
		FDI_DSI.4 静态数据
FRF 类：受限的信息流	FRF_NAC 族：网络与端口访问控制	FRF_NAC.1 端口禁用
		FRF_NAC.2 数据流控制
		FRF_NAC.3 无线访问
		FRF_NAC.4 可移动存储介质
	FRF_FUP 族：功能分区	FRF_FUP.1 应用分区
		FRF_FUP.2 安全功能隔离
		FRF_FUP.3 数据的非可执行性
	FRA_DSP 族：拒绝服务保护	FRA_DSP.1 数据洪泛保护
		FRA_DSP.2 关键[illegible]

参 考 文 献

[17] GB/T 19004.9—2015 [illegible]