ICS 35.040
L 80

信息安全技术 工业控制系统现场设备数据采集和控制

Information security technology—Security requirements for data acquisition and control field devices of industrial control systems

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　安全相关功能要求描述结构 …… 2
5.1　要求类结构 …… 2
5.2　要求族结构 …… 3
5.3　要求项结构 …… 3
6　通用安全功能要求 …… 3
6.1　总述 …… 3
6.2　FIA 类：…… 3

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。

本标准起草单

引　言

现场测控设备是工业控制系统的基本功能执行设备，直接对工业生产过程进行监视与控制，对于生产……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 工业控制系统现场测控设备通用安全功能要求

1 范围

本标准规定了工业控制系统现场测控设备的用户标识与鉴[illegible]

[illegible]

[illegible]

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

组件的层次结构。

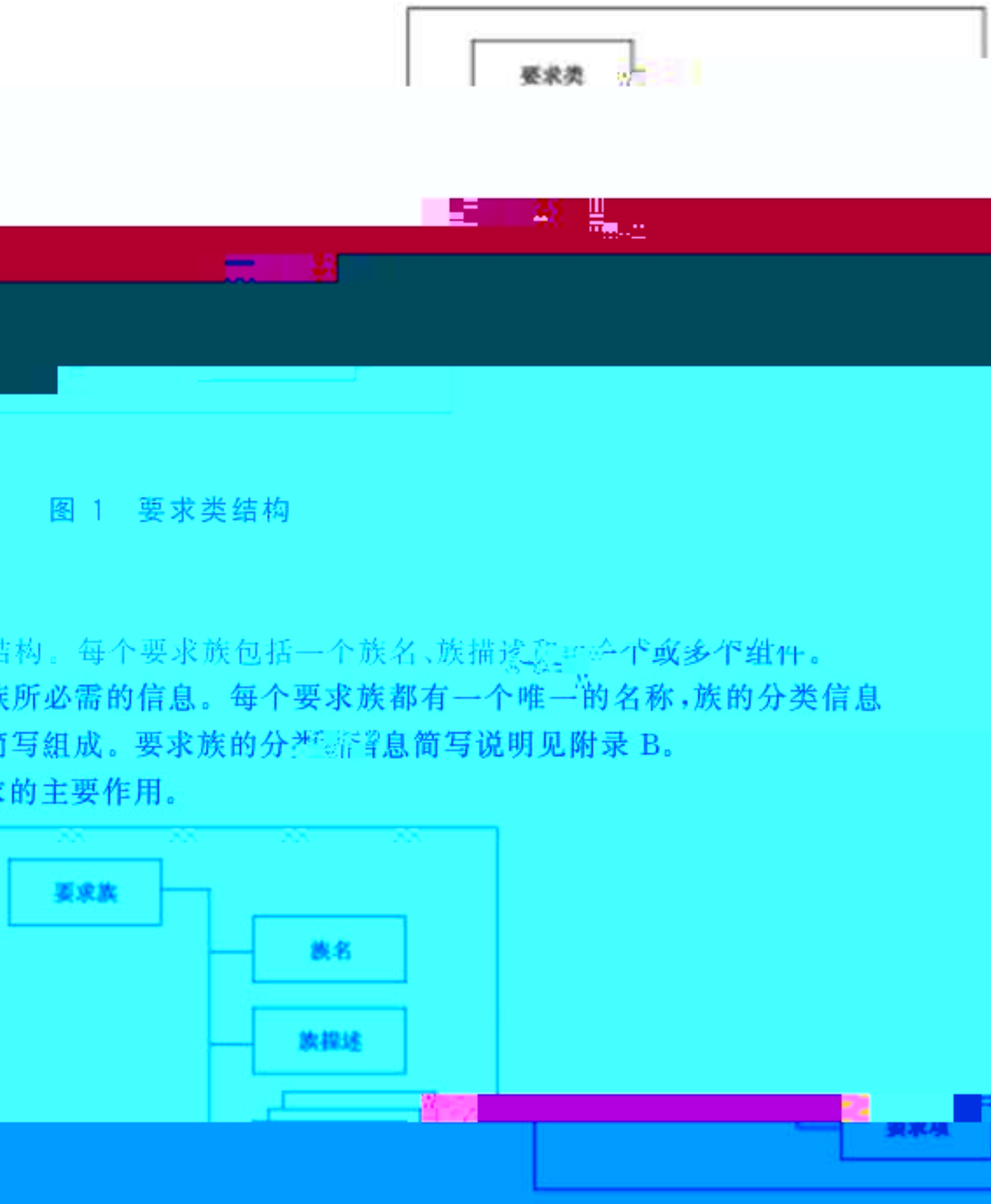


图 1　要求类结构

5.2　要求族结构

图 2 以框图形式示意了要求族的结构。每个要求族包括一个族名、族描述和一个或多个组件。

族名提供标识和划分不同要求族所必需的信息。每个要求族都有一个唯一的名称，族的分类信息由所属类的简写和族名三个字符的简写组成。要求族的分类标识信息简写说明见附录 B。

族描述总体描述族和该族要求的主要作用。

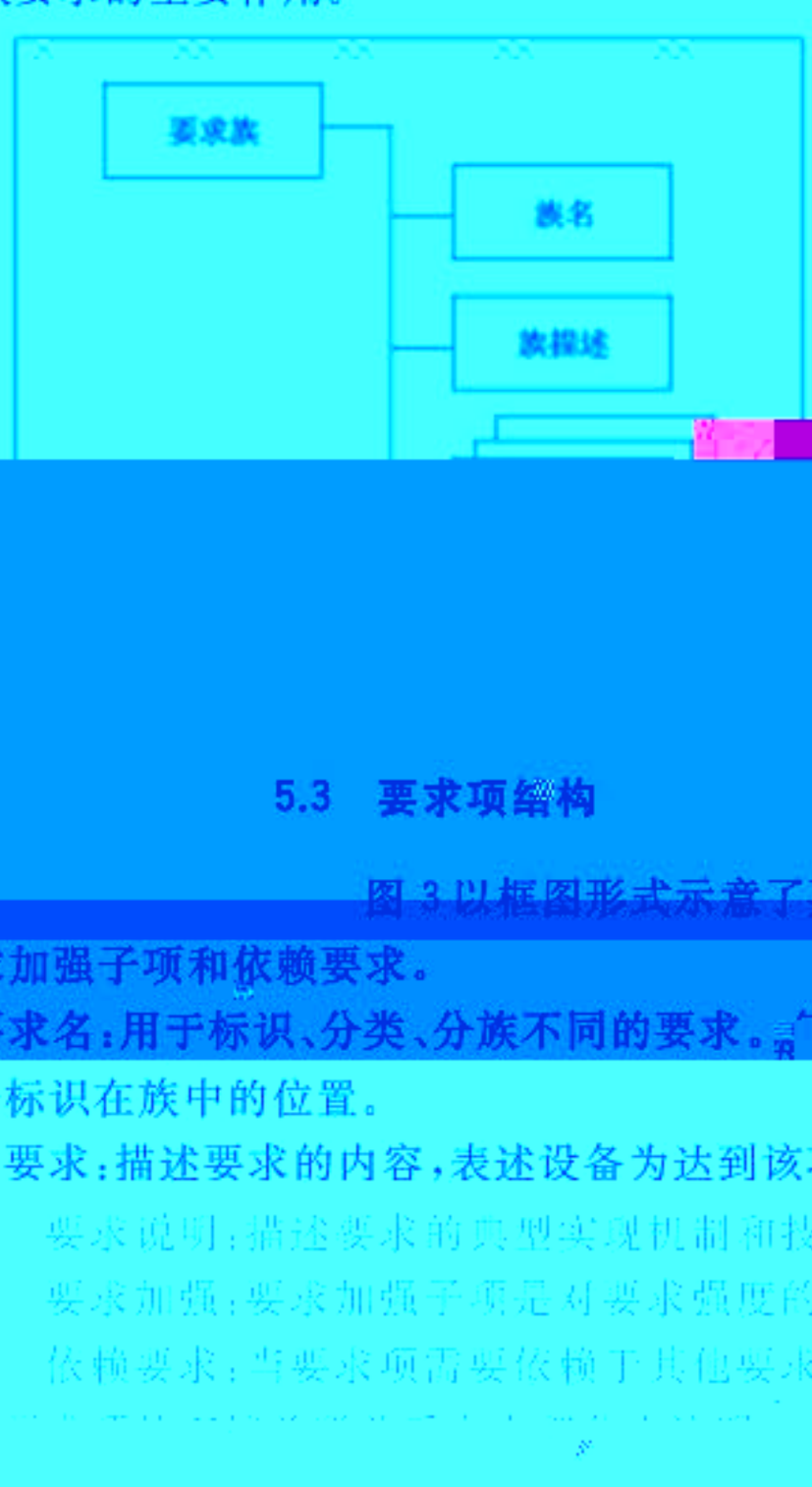


图 2　要求族结构

5.3　要求项结构

图 3 以框图形式示意了要求项的结构。每个要求项包括要求名、要求的内容、要求说明、零个或多个要求加强子项和依赖要求。

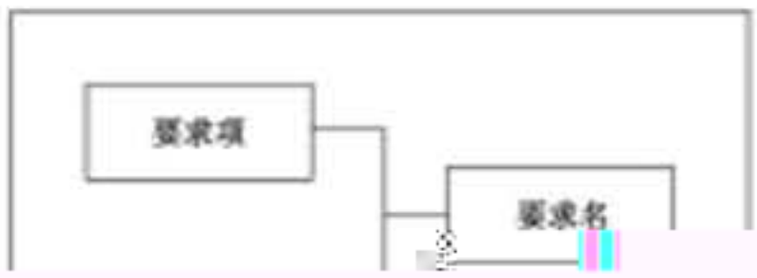
要求名：用于标识、分类、分族不同的要求。每个要求都有一个唯一的名称，表明该要求的目的。用序号标识在族中的位置。

要求：描述要求的内容，表述设备为达到该项要求应满足的条件。

要求说明：描述要求的典型实现机制和技术原理。

要求加强：要求加强子项是对要求强度的加强或内容的增加，用序号标识在要求内的位置。

依赖要求：当要求项需要依赖于其他要求项，或与其他要求项共同使用才能发挥作用时，这种对其


要求项
要求名

6.2.2.2.2 要求说明

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、删除策管理；

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

[redacted]

6.2.4.4.3 要求加强

FIA_ACM.3 [redacted] 口令的最小长度、使用周期和字母或特殊字符等[redacted]

应能够对配置用户的公钥进行管理，并对证书进行识别

[illegible] 信层面上，公私钥可用于现场测控设备和其他设备、远程配置系统、监控后台或上位机的通信

[illegible] 密钥的安全，同时满足

实现。

6.2.4.7.4 依赖要求

[illegible] 部软件服务，对于远程访问类型功能的实现，可参考使用

6.2.4.8.3 要求加强

[illegible]

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]

[illegible]

通过相关能直接登录、网络登录等方式。

6.2.5.2.3 要求加强

无。

6.2.5.2.4 依赖要求

FIA_LGM.1 登录失败管理的依赖要求是 FIA_IAM.2。

6.2.5.3 FIA_LGM.2 登录成功记录

6.2.5.3.1 要求

工控系统现场测控设备应管理和记录操控人员最后一次登录成功的日期[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[illegible]

IA_LGM.1。

了安全策略中的规定值，现场测控设备应执行

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 F

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
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]

AM.2 和 FIA_LGM.3

6.2.5.6 FIA_UGM.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[illegible]

宝鉴别机制，[illegible]

6.2.5.6.3 要求加强

无。

6.2.5.6.4 [illegible]

FIA_IAM.2

6.3 FDC 类：使用控制

6.3.1 类描述

[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

工控系统现场测控设备为不同访问用户

配权限，只允许通过身份鉴别的用户访问已授权的资源。

权限包括设备操控层面的运行数据查看、控

参数变更、系统应用层面的控制命令下发、安装下发、数据

户管理：创建、删除或修改账户内容；

计日志：查看或下载审计日志；

控制命令：上位机对设备下发控制命令、。

权项管理包括：对于设备便用、配置人员和配置软件，依据配置、查看、审计等角色分配权

解释，对于访问现场设备的

6.3.2.3.2 要求说明

基于角色的访问控制，根据具体的用户

所分配角色

功能相对简单的设备，现场测控设备的用户角色和权限可在出厂时完成

，如配置用户、查看用户、审计用户IP或用访问实时网口或FTP等角色访问、控制上位机和配置用

户，

用户设置可固定，如只有一个查看用户、一个配置用户、一个审计用户、一个管理员用户。

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[redacted]

[redacted]

[redacted]

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的安全机制，实现重要控制操作的执行和确认。

6.3.2.6.[illegible]

[illegible]控系统现场测控设备应在设备配置层[illegible]取配置软件与设备的会话在[illegible]

6.3.3.3.2 要求说明

[illegible]会话时应在应用于设备配置层[illegible]的网络访问特别是在[illegible]网络中对全面机密性进行限制。如果会话建立途经网[illegible]一[illegible]在完备物理方面控制机制的可[illegible]网络，也可依照个把会话密钥进行[illegible]等级

6.3.3.3.3 要求加强

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事件和重要生产活动的进行审计，对无线干扰、事故恢复、事件

典型的重要设备操作事件包括：

——登录成功：操控人员成功本地/远程登录设备；

——非法登录尝试：操控人员连续多次输入口令错误；

——正常退出：操控人员发起的退出；

——超时退出：在预先定义好的一段时间内不活动，系统注销操控人员此次登陆；

——访问配置：将配置文件从设备下载存储到外部设备中（例如，计算机，记忆棒，光盘）；

——配置更改：在设备由传入新配置或者通过面板输入新配置参数，使设备的配置发生改变；

——固件更换：在内存中增加新的设备运行固件；

——创建用户名/口令或更改：创建新的操控人员用户名/口令或者修改权限；

——删除用户名/口令：删除操控人员的用户名/口令；

——访问审计踪迹：操控人员查看日志或将日志备份至外部设备或存储空间（计算机、内存、光盘）；

——修改时间/日期：用户修改时间和日期。

典型的重要生产活动包括：

——参数修改：上位机或其他设备修改设备的开关量、档位等参数；

——设备重启：由于断电、按下重启按钮、修改上电顺序或配置修改导致的设备重启；

——非法连

6.3.4.2 依赖要求

.2、FIA_LGM.4、FRF_NAC.2 和 FRA_BUC.1。

FUC_ATC.1 审计事件的依赖要求是 FIA_LGM

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，用户能够确定有哪些事件发生，事件发生时间，事件来源和事件结果。大多数审计

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

中实现。

.4.3 要求加强

无。

6.4.4.4 依赖要求

FUC_ATR.3 审计报告的依赖要求为是FUC_ATR.2。

6.4 FDI 类:数据完整性

6.4.1 类描述

对数据的完整性进行

6.4.2 FDI_DSI.1 安全功能检测

6.4.2.1 执行下述如在系统范围中对

6.4.2.2 FU

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[illegible]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发

[illegible]软件输入的参数应可见。

6.4.2.3.3 要求加强

无。

6.4.2.4.4 依赖要求

无。

6.4.2.5 FDI_DSI.4 静态数据防篡改

6.4.2.5.1 要求

工控系统现场测控设备应具备防止对静态数据进行非授权写操作的保护机制(

[illegible]执行代码时未授权修改、删除或插入

6.4.3.3.3 要求

验码。

6.4.3.6.3 要求加强

FDI_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

,防止中间人通过对协议观察分析从而加入或窃取通信会话。

6.4.3.7.2 要求说明

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

对数据的保密性进行保护的目的是

信中数据被窃听。主要防护对象是信息

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 族描述

FDC_DSC 族:存储数据保密性的要求确保[illegible]备应具备基于密码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

FDC_DSC.1 存储数据保密性的依赖要求是 FDC_CRM.1。

6.5.4 FDC_DTC 族:传输数据保密性

6.5.4.1 族描述

[illegible]码的传输数据保密性保护机制,如加密等。

6.5.4.2.4 依赖要求

FDC_DTC.1 传输数据保密性的依赖要求是 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,主要用于保证仅限合法上位机、配置工作站、其他现场设备或存储介质对设备进行访问。

6.6.2[illegible]

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 要求说明

[illegible]

[illegible]

[illegible]

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

硬件 MMU 的 OS、或者支持分离内[illegible]计设计的 CPU。

6.6.3.4 FRF_FUP.3 [illegible]数据的[illegible]

[illegible]求

工控系统现场测控设备应将数据和空间内的代码执行。

6.6.3.4.2 要求说明

可静态分配内[illegible]支持

6.6.3.4.3 要求加强

无。

6.6.3.4.4 [illegible]要求

无。

6.7 FRA 类：资源可用性

6.7.1 类描述

[illegible]资源可用性的目的是确保设备实[illegible]也服务[illegible]并保持[illegible]正常[illegible]情况下能够保持业务连续性。

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]

6.7.3.2 FRA_BUC.1 关键服务连续性

6.7.3.2.1 要求

工控系统现场测控设备即使发生一般故障也能保证主要的业务功能。

6.7.3.2.2 要求说明

设备[illegible]在出现一般故障(软件错误、缓冲区溢出、数据泄露等)中断时提供自动保护功能，当[illegible]发生时自动保护重要状态信息和进程，保证设备能够进行恢复。典型的机制如看门狗进程。

6.7.3.2.3 要求加强

FRA_BUC.1 关键服务连续性的要求加强为设备应具备[illegible]

6.7.3.2.4 依赖要求

FRA_BUC.1 关键服务连续性的依赖要求是 FUS_ATC.1。

6.7.3.3 FRA_BUC.2 协议模糊攻击保护

6.7.3.3.1 要求

工控系统现场测控设备应能够容忍针对通信协议的模糊攻击。

6.7.3.3.2 要求说明

协议模糊攻击的首要保护主要依靠设备所升层服务在开发实现过程中的安全水平。

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

6.7.3.6 FRA_BUC.5 备用电源

6.7.3.6.1 要求

[illegible]

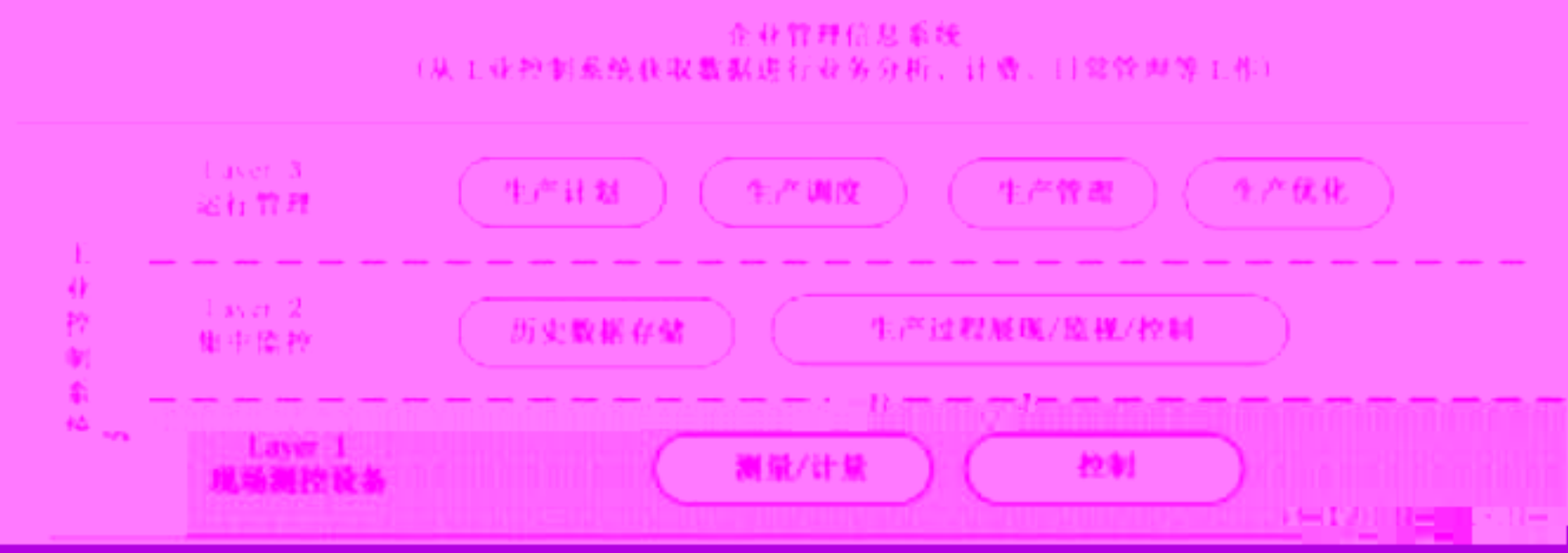
附 录 A
（资料性附录）
典型工业控制系统现场测控设备功能与构成

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

与中心操作员站的控制命令，完成控制参数调整与输出调整，接受

工程师站的控制方案更改、调试等操作；系统启动、诊断、掉电数据保持等。



模块取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

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

网口、电缆接口、RS232 串口、RS485 串口、

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

要求类名称	要求类简写	简写对应的英文类名
[illegible]	[illegible]	[illegible]
数据保密性	FDC 类	Function Data Confidentiality
受限的信息[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

要求族的分类信息简写说明见表 B.2。

表 B.2 要求族的分类信息简写说明

要求族名称	简写对应的英文族名
标识与鉴别方式	Funciton-Identification and Authentication _ Identification and Authentica[illegible]
标识符管理	Funciton-Identification and Authentication_ Identities Management
[illegible]	Funciton-Identification and Authentication_ Authentication Credentials Management
[illegible]	Funciton-Identification and Authentication_Login Management
[illegible]	Funciton-Use Control_Access Control [illegible]orization
[illegible]	Funciton-Use Control_Session Control
[illegible]	Funciton-Use Control_Creation of Audit Trail
[illegible]	Funciton-Use Control_Storage of Audit Trail
[illegible]	Funciton-Use Control_Report of Audit Trail
[illegible]性	Funciton-Data Integrity_Integrity of Stored Data
[illegible]性	Funciton Data Integrity_Integrity of Transmitted Data
[illegible]	Funciton-Data Confidentiality_Cryptographic Mechanisms
[illegible]	[illegible]

要求族简[illegible]	[illegible]
FIA_IAM 族	[illegible]
FIA_IDM	[illegible]
[illegible]	[illegible]
FIA_LGM 族	登录管理
FUC_ACA 族	访问控制授权
FUC_SEC 族	会话控制
FUC_ATC 族	审计踪迹产生
FUC_ATS 族	审计踪迹[illegible]
FUC_ATR 族	审计踪迹访[illegible]
FDI_DSI 族	数据存储完[illegible]
FDI_DTI 族	数据传输完[illegible]
FDC_CRM 族	加密机制
FDC_DSC 族	存储数据保[illegible]

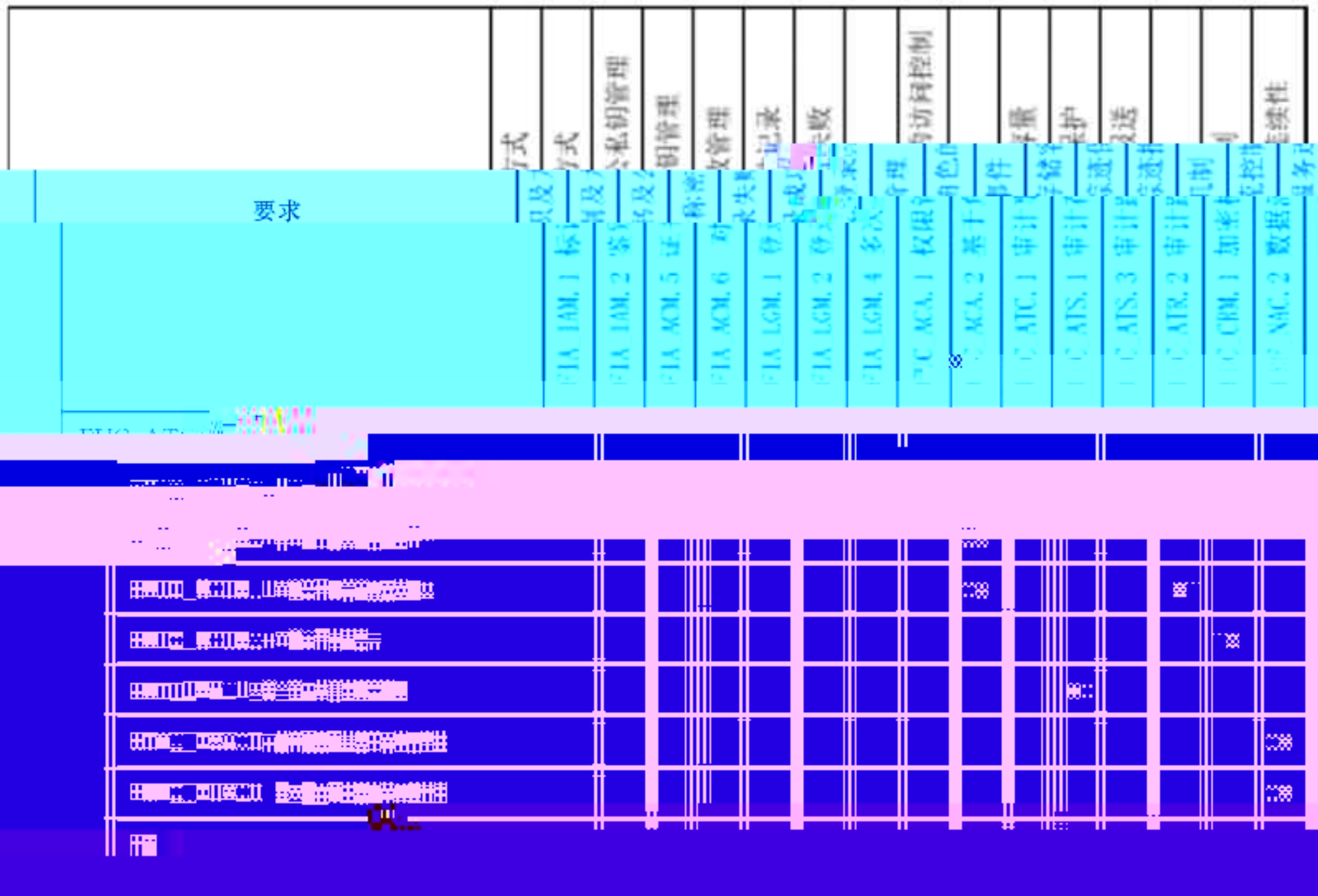
表 B.2（续）

要求族简写	要求族名称	简写对应的英文族名
FRF_FUP 族	功能分区	Funciton-R

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）



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[illegible]
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_RUL[illegible]	关键用[illegible]

参 考 文 献

[17] ISA-62443-3-2(99.04.92)Security for industrial automation and contro