ICS 35.040
L 80

测控设备通用安全功能要求

Information security technology—Common security functional requirements

目　　次

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]对工业生产过程进行监视与控制，对于生[illegible]

[illegible]安全攻击，将直接导致设备所辖区域内甚至连锁性的生产[illegible]，因此[illegible]信息安全不仅[illegible]

安全和经济安全密不可分，而且电力、[illegible]气、天然气等重要基础设施的现场安全水平直接关系到国计民生、社会稳定与公众利益。

为提高现场设备的信息安全能力，本标准提出针对现场测控设备的通用安全功能要求，[illegible]工设备的安全设计、开发、测试与评估。使用者应根据实际或计划使用环境的安全风险分析[illegible]果，选择设备应满足的安全功能要求。

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

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

[illegible]

DoS：拒绝服务攻击(Denial of Service)

[illegible]

协议(Transmission Control Protocol)

UDP：用户数据报协议(User Datagram Protocol)

5 安全功能要求描述结构

5.1 要求类结构

图1以框图形式示意了要求类的结构。每个要求类有且一个类名 [illegible]

组件的层次结构。

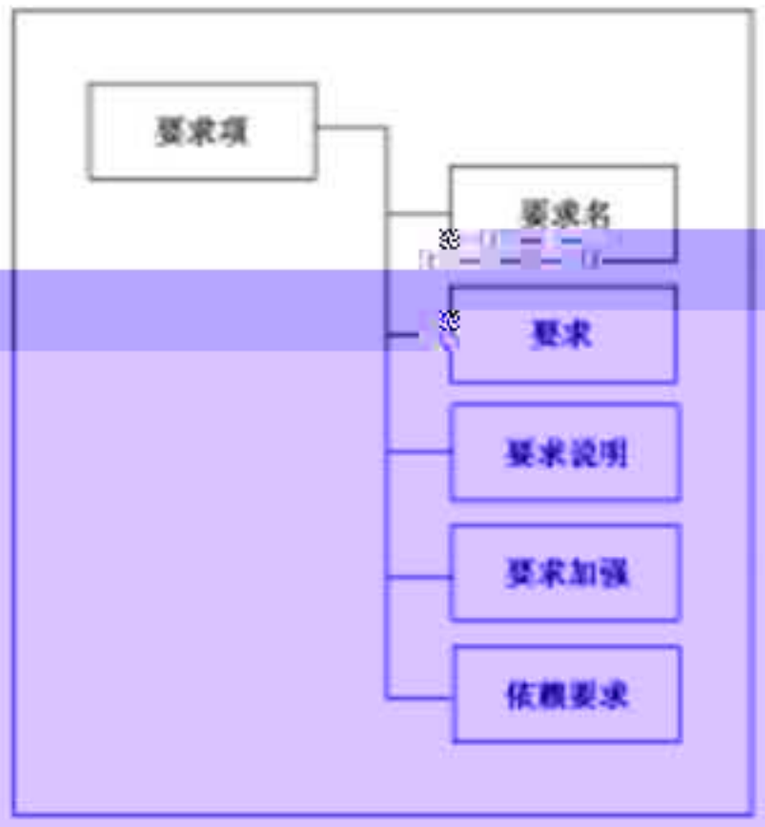


图 3　要求项结构

6　通用安全功能要求

6.1　概述

工业控制系统现场测控设备的通用安全功能要求归纳见附录 D。

6.2　FIA 类 用户标识与鉴

[illegible]设备的访问行为主体（人员、进程和设备），以及对访问行为进行

控制。

[illegible]禁非设

[illegible]数字与智能化型[illegible]

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、删除等管理

6.2.4.3.1 要求

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策略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告知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持[redacted]的最小长度、使用周期、字母或特[redacted]

FIA_ACM.3 口令强度控[redacted]

6.2.4.5.1 要求

[redacted]的用户[redacted]/口令鉴别控制不应被绕过。

6.2.4.5.2 要求说明

典型的绕过机制包括但不限于以下机制和技术：

——嵌入式主口令

——嵌入式芯片在硬件或软件故障时自动运行[redacted]

[redacted]公私钥

[redacted]作为鉴别机制，工控系统现场测控设备(及其配置软件)和证书进行管理的能力。

6.2.4.6.2 要求说明

用户使用配置软件对工业控制系统现场测控设备进行配置时，常使用证书进行身份鉴别，配置软件

应能够对配置用户的公钥进行管理，并对证书进行识别

面上建立有效的公私钥管理设施，如 CA。

及公私钥管理的依赖要求是 FIA_IAM

b) 在工控系统

6.2.4.6.4 依赖要求

FIA_ACM.5 证书

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，FIA_ACM.5 和 FIA_AC
M.4。

6.2.5 FIA_LGM 族：登录管理

9

6.2.5.4.2 要求说明

[redacted]

限制机制包括对禁控人员进行锁定、发出警报等。

6.2.5.5 [redacted]

6.2.5.6 [redacted]

6.2.5.6.3 要求加试

6.2.5.8 [redacted]

限，根据权限执行所请求的操作，并进行控制和审[redacted]

6.3.2 FUC_ACA 族：访问控制[redacted]

6.3.2.3.3 要求加强

无。

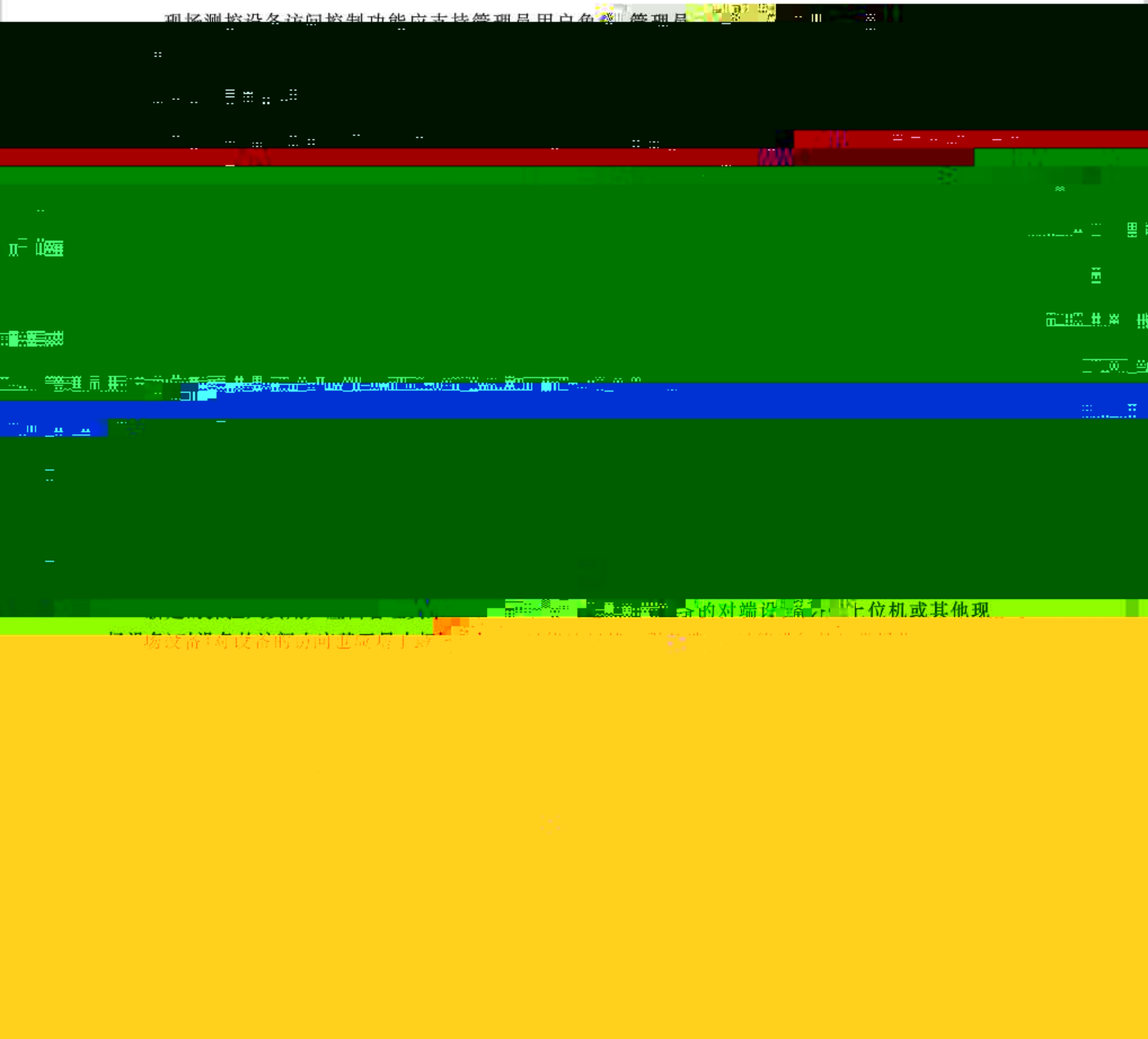
6.3.2.3.4 依赖要求

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



场设备与设备的访问进行最小权

6.3.2.6.2 要求说明

分权管理的典型过程是操作用户[redacted]

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关键功能和重要生产活动进行审计，对可能违规、事故恢复、事件

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，三元组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

6.3.5.3.2 要求说明

用户为外部 IT 实体向 .信息应以电子方式此处的表示。

用户为外部 IT 实体向 .信息应以电子方式此处的表示。

6.4.3.4.4 依赖要求

JE：

6.4.3.3 要求加强

具中突现。

6

6.4.3.4.2 EDL_DSL1 安全功能检测

6.4 EDL类：数据完整性

6.4.1 类描述

PUC_ATEC5 车由经台初次伸长实际 EDL类

验证与报警。

6.4.2.2.4 依赖要求

FDI_DSL.1 安全功能检测的依赖要求是 FUC_ATC.1。

6.4.2.3 FDI_DSL.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]

6.4.2.3.2 要求说明

错误消息中应仅包含用于定位处理[illegible]

6.4.3.3.3 要求

评出现的错误的典型机制为 CRC 校验用于对抗随机错误，比如 TCP 的循环校

验码。

6.4.3.6.3 要求加强

FDI_DTI.5 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。典型机制如 MAC、散列函数(HASH)等。

6.4.3.6.4 依赖要求

无。

6.4.3.7 FDI_DTI.6 会话保护

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,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信息。

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

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

加密等。

6.5.4.2.4 依赖要求

FDP_DSC_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的时在网络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]端口实施访问控制,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)，其采用的无线协议应具备安全机制。

6.6.2.4.2 要

……处理单元、不同的操作系统实例、不同的网络地址、不同的端口或其他方法。

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[redacted]址空间)。对于一些无法做到该点的老旧工

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]

6.7.3.3.2 要求说明

协议模糊攻击的防护主要依靠设备所开启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 [illegible]备份

6.7.3.4.1 要求

工控系统现场测控设备应直接或依[illegible]工具提供备份功能，进行应用级和系统级信息（包括系统

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；系统自动诊断、故中数据保持等

A.2　工业控制系统现场测控设备典型硬件结构

在硬件组成上，数字化的元其是使

理上一般并不是独立的硬件模块，而

术在工业控制系统中的标准化和应用，

场总线协议的处理和接口，但它，物

是和处理器在一个模块内。

通信模块实现设备的通信连接。随着总线技术以及网络

模块电位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

示与的调整值和能量的态。

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 '

现与人机接口面板、调试软件、监控后台、工程

网口、电缆接口、RS232 串口、RS485 串口、

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	简写对应的英文全名
[illegible]	[illegible]	[illegible]
数据保密性	FDC类	Function-Data Confidentiality
受限的信息[illegible]	FRF类	Function Restrict Data Flow
资源可用性	FRA类	Function Resource Availability

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	要求族简写	简写对应的英文全名
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
传输数据保密性	[illegible]	Funciton-Data Confidentiality_Confidentiality of Transmitted Data
[illegible]访问控制	FRF[illegible]	Function Restrict Data Flow_Network and Interface Access Control

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	Function-Re

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，其依赖的要求项在表中占据一列，表中行中标的要求项依赖列中标的要求项用“√”表示。如果表中单元为空，则该行要求不依赖于对应列中要求。

表 C.1（续）

要求	口令方式	口令及个人数字证书方式	个人私钥管理	用户口令管理	审计记录	审计记录产生	审计记录存储	自主访问控制	角色	单个用户多个角色	多个用户单个角色	基于角色的访问控制	数据完整性
FCC_ATR.3 审计报告												×	
FDI_DSL.1 安全功能检测										×			
FDC_DSC.1 存储数据保密性													×
FDC_DTC.1 传输数据保密性													×
FRA_FLC.1 流控制	×												
FRA_BUC.1 关键服务连续性												×	

附　录　D
（规范性附录）


SEC 族：会话控制
_SEC.2 网络会话超时
FUC 类：使用者控制
JC_ATC.1 审计事件
FUC_ATC.2 审计成迹的内容
FUC_ATC 族：审计成迹产生

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

参 考 文 献

[17] ISA-62443-4-2(99.04.02)Security for industrial automation and control system security requirements and security levels Draft 4,Edit 1

s— Technical secu-