ICS 35.040
L 80

中华人民共和国国家标准

GB/T 3[illegible]/

[illegible]

for data acquisition a[illegible]

2[illegible]8-06-[illegible]布　　2019-01-01实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

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

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

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别、[illegible]

[illegible]

本标准不涵盖与设备自身信息安全功能实现无关的[illegible]织管理和人员管理等。对于影响技术实施的[illegible]的描述中，不作关于管理和运行内容的强调；

——本标准不涵盖与设备自身信息安全功能无关的[illegible]容，对于影响信息安全技术防护效果的物理[illegible]作关于物理安全内容的强调；

——本标准不对[illegible]工业控制系统中机电式[illegible]的信息安全功能进行要求；

——本标准不覆盖传感器、变送器、阀门等生产过程设[illegible]开关/断路器[illegible]节点。

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[illegible]适用于本文件。

[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(R[illegible]U,Remote Terminal Unit)；

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

——分散处理单元(D[illegible]U,Distributed Processing Unit)。

3.2

鉴别 authentication

信息系统中，在用户、进程或设备接入[illegible]源之前，对其身份进行验证。

[NIST SP 800-53 R3]

3.3

泛洪 flooding

通过向计算系统或其他数据处理实体提供大于其处理能力的输入，企图引起其在信息安全方面的故障的攻击。

[RFC 2828]

4 缩略语

下列缩略语适用于本文件。

API:应用程序编程接口(Application Programming Interface)

CA:认证中心(Certificat[illegible]Authority)

CRC:循环冗余校验(Cy[illegible]ic Redu[illegible]

[illegible]

[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[illegible]以框图形式[illegible]

组件的层次结构。

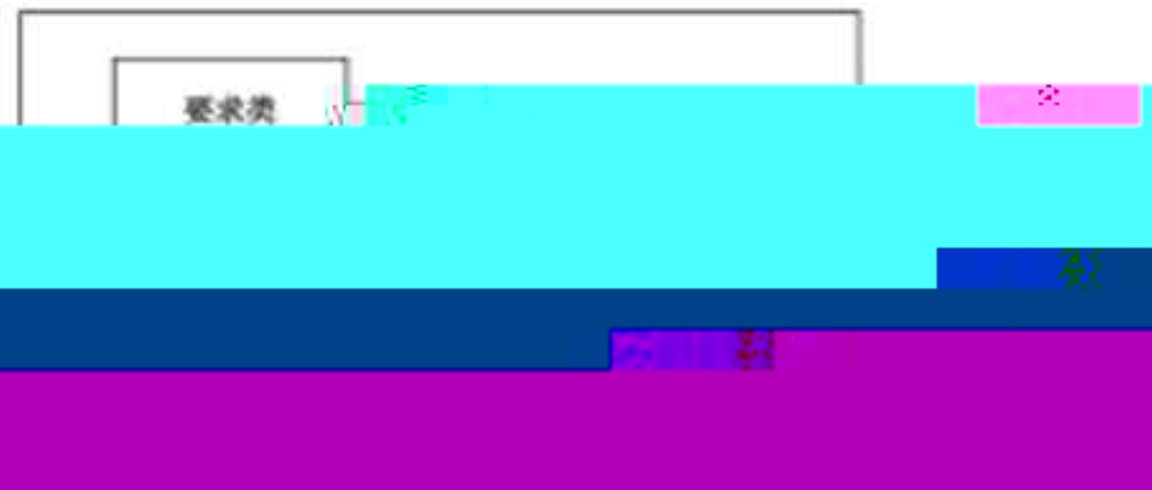
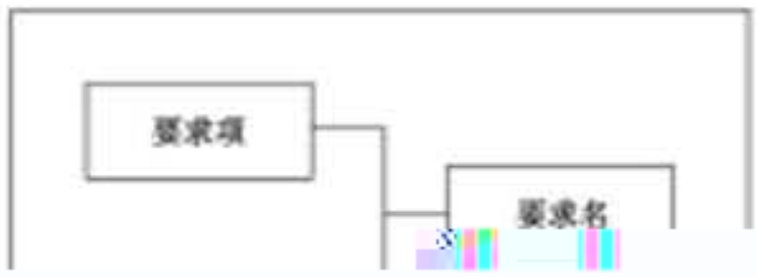


图 2　要求族结构

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、分簇不同的要求。


要求项
要求名

6.2.2.2.2 要求说明

[illegible]

[illegible]

[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

6.2.4.4 FIA_ACM.3 口令强度控制

6.2.4.4.1 要求

[illegible]

业系统主与用户设定口令强度是否满足要求，在系统或物联网设备应具备功能使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]口令的最小长度、使用周期和字母或特[illegible]

应能够对配置用户的公钥进行管理，并对证书进行识别

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

密钥的安全，同时满

实现。

6.2.4.7.4 依赖要求

部验证服务。对于远程访问关键功能的情况，可酌情考虑使用。

6.2.4.8.3 要求加强

无。

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_AC[illegible]M.6[illegible]

6.2.5 FIA_LGM 族：登录管理

[illegible]主要对管理员等实现鉴别了的重要用户的[illegible]录失败行为进行管[illegible]

[illegible]别了的重要用户的登录成功进行管理。登录方式包括本地面板登录、通过

FIA_LGM.2 登[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。

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了限制机制。

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]

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]

[redacted]对权限的管理。

6.3.2.2.2 要求说明

需要授权的典型功能包括：

[redacted]

[redacted]技和[redacted]的[redacted]文[redacted]更现有配置（如修改输入值、设定值、工艺参数值等）；

——固件变更：对不需要变更其硬件的设备进行新固件加载；

[redacted]

[redacted]

[redacted]

6.3.2.3.3 要求加强

无。

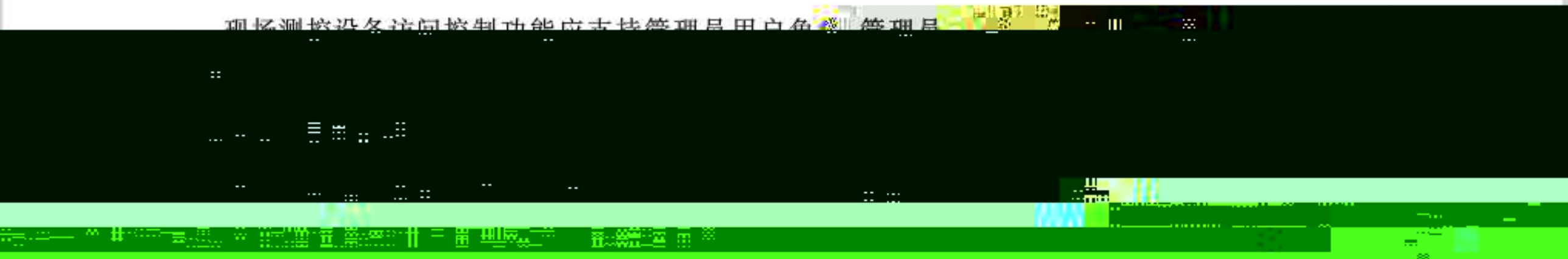
6.3.2.3.4 依赖要求

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）对设备的访问也应基于最[illegible]权限，如只能访问某一网[illegible]端口、只能进行某一类操作。

6.3.2.5.3 要求加强

无。

6.3.2.5.4 依赖要求

FUC_ACA.4 最小权限原则的[illegible]

6.3.2.6 [illegible]权分离

6.3.2.6.1 要求

6.3.2.6.2 要求说明

分权管理的典型过程是操作用户[redacted]

6.3.3.3.2 要求说明

网络会话超时终止主要用于设备配置用户的网络访问，特别是远程访问，不对上位机进程进[redacted]超时进行[redacted]控制。

6.3.3.

3 要求加强

[redacted]

UC_SEC.2 网络会话超时的要求加强[redacted]设备应支持管理员对会话终止前的不活动时间进行配置。

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

工控系统中现场控制设备对安全相关事件和重要生产活动均应进行审计，对于修正错误、事故恢复、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

工控系统中现场控制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非行审计。

非法连接尝试：不符合访问控制策略的连接尝试，如连接非法的 IP、MAC 或不允许访问的端口。

审计事件要与具备并开启的安全功能相对应，如不具备访问控制功能的设备不需要记录“非法连接尝试”事件。

6.3.4.2.3 要求加强

FUC_ATC.1 审计事件的要求加强为设备应支持管理员对需要审计的事件清单进行配置。

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。

的审计。

6.3.2 要求说明

由于嵌入式设备的物理空间限制存储容量是有限的，宜从多

用户为外部 IT 实体时，信息应以电子方式无歧义的表示。

6.3.6.2.3 要求加强

6.3.6.3.1 要求

主机的审计踪迹进行过滤和分析，设备的审计踪迹格式实现是统一的。

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

要求加强为

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某

6.4.3.3 要求说明

可以通过全系统应用层面上收发[illegible]包机制获得信息，使用时间或设定阈时容忍时间来处理对应延迟的数据包。

6.4.3.4.3 要求加强

无。

6.4.3.4.4 依赖要求

无。

6.4.3.5 FDI DT1.4[illegible]数据包重放

验码。

6.4.3.6.3 要求加强

FBE_BT1.3 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

对数据的保密性进行保护的目的是防止数据被窃听，主要防护手段是[illegible]并被获取后在传输或存储的状态

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[illegible]

[illegible]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[illegible]

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]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。

6.6.2.2 FRF_NAC.1 端口禁用

6.6.2.2.1 要求

[illegible]

6.6.2.2.2 要求说明

设备上线后通常不需要使用[illegible]配置应用,应关闭对应的[illegible]服务端口,同时也应关闭用于本地配置的固件升级物理网络端口或串口。开启的端口和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

工控系统现场测控设备应具备对流入设备数据流的源端访问控制信息进行维护的机制。

6.6.2.3.2 要求说明

设备网络层面的访问控制信息包括源 IP 地址、物理地址、可访问服务及服务中的内容有效性和合理性,应通过这些内容实现对源端身[illegible]的识别。

6.6.2.3.3 要求加强

FRF_NAC.2 数据流控制的要求加强为设备应维护公钥、对称密钥等基于密码的设备身份鉴别机制,以证实通信对端的身份。

6.6.2.3.4 依赖要求

FRF_NAC.2 数据流控制的依赖要求是 FIA_IAM.1。

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

[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[redacted]

[redacted]应在安全计划书[redacted]求该情况开制定风险缓解方法。

6.6.3.3.3 要求加强

无。

6.6.3.3.4 依赖要求

[redacted]执行性

6.6.3.4.1 [redacted]

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应具备业务连续性保[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[...]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]

[illegible]

[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，实现对现场数据的

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。

备通

常由微处理器、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。其中

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

示与的调整值和能量的总和。

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	要求类简写	简写字母的含义
[illegible]	[illegible]	[illegible]
FDC 类	Function-Data Confidentiality	数据保密性
FRF 类	Function Restrict Data Flow	受限的信息[illegible]
FRA 类	Function Resource Availability	资源可用性

[illegible]fidentiality_Confidentiality

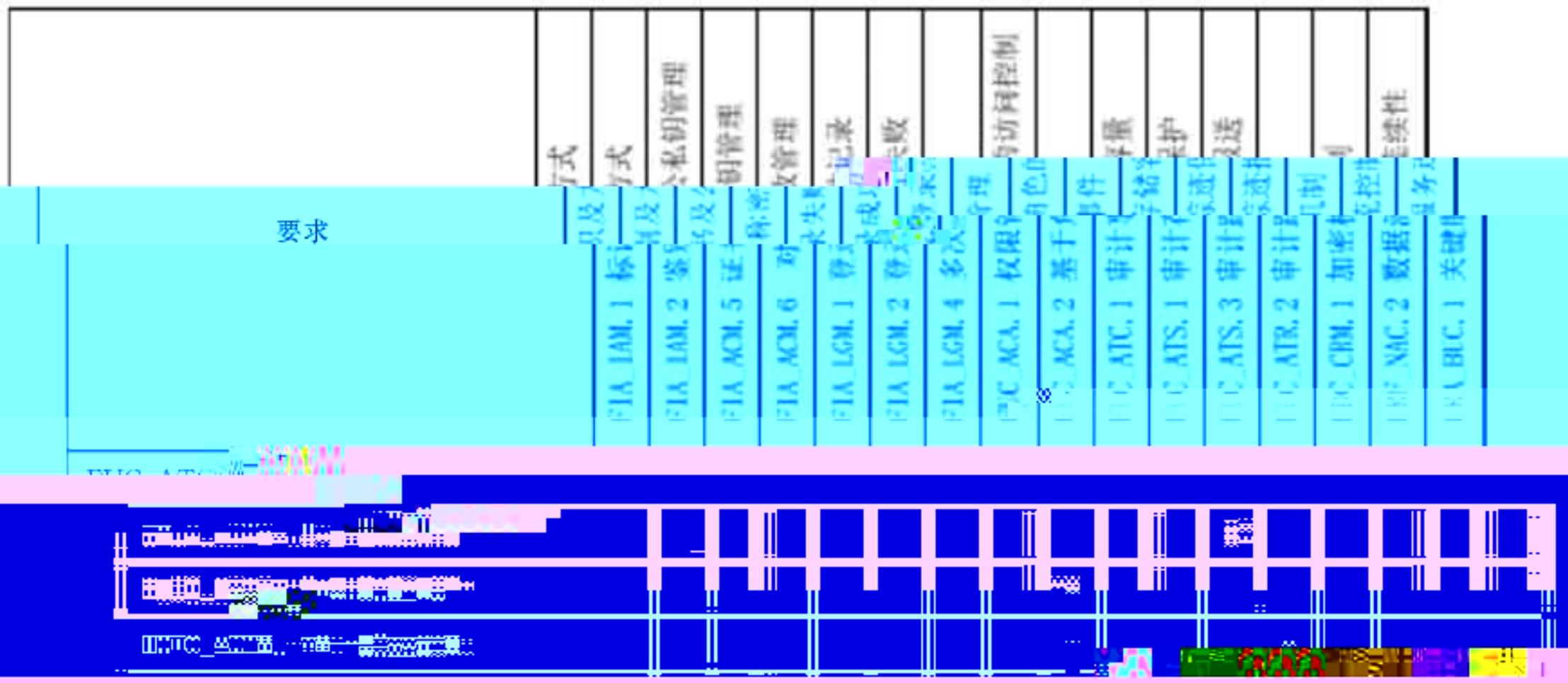
表 B.2（续）

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[illegible]
FRA_DSP 族	拒绝服务保护	Funciton-Resource Avira[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，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）



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：数据存储完整性	FDI_DSI.1 安全功能检测
		FDI_DSI.2 异常处理
	FDI_DTI 族：数据传输完整性	FDI_DTI.3 数据包延迟
		FDI_DTI.4 数据包重放
		FDI_DTI.5 数据包防篡改
		FDI_DTI.6 会话保护
FDC_CRM 族：加密机制	FDC_CRM.1 加密机制	
FDC 类：[illegible]		
	FRA_BUC.1 关键服务连续性	
	FRA_BUC.2 参数模型故障报警	
FRA_BUC 族：业务连续性	FRA_BUC.3 数据备份	
	FRA_BUC.4 设备恢复	
	FRA_BUC.5 备用电源	
FRA 类：资源可[illegible]性		

参 考 文 献

[17] ISA-62443-4-2(99.04.02)Security for industrial automation and co

ntrol [illegible] Technical secu-