ICS 35.040
L 80

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 …

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，[illegible]对[illegible]工业生产过程进行监视与控制。对于生产[illegible]

随着信息通信技术在工业控制系统中的应用，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测设备面临的风险种类更多，范围更大，层次[illegible]

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)；

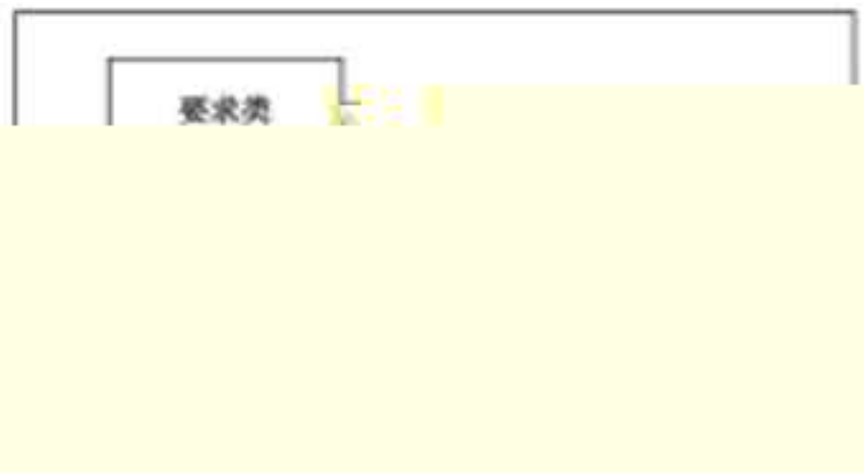
——分散处理单元(DPU,Distributed Processing Unit)。

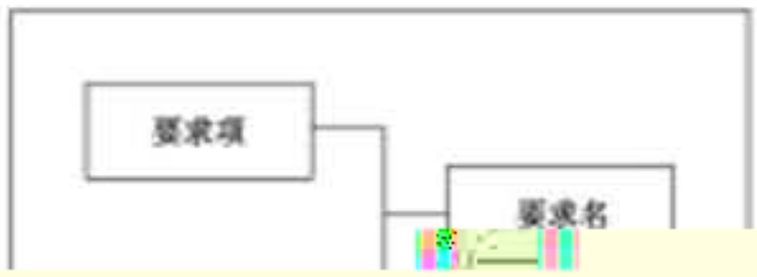
3.2

鉴别 identification

信息系统中，在用户、进程或设备接入

组件的层次结构。




要求项
要求名

6.2.2.2.2 要求说明

应对[illegible]读写工控设备身份标识、知识管理中、工控性能测量[illegible]实现的用户身份标识等[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；

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 FIA_ACM 族：鉴别凭证管理

6.2.4.1 族描述

[illegible]

6.2.4.3 [illegible]

[illegible]

6.2.4.3.4 依赖要求

[illegible]

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配置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持[redacted]口令的最小长度、使用场景和字母或特殊[redacted]

应能够对配置用户的公钥进行管理，并对证书进行识别。

6.2.4.7 EK_ACM6消息鉴别信息

6.2.4.7.1 要求

如果使用了对称密钥作为密码机制实现密钥数据加解密系统现场调控设备应提供对对称密钥进行管理的能力。

6.2.4.7.2 要求说明

对称密钥可用于现场测控设备和其他设备与监控后台或上位机的通信身份鉴别。设备应能保证本地存

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

6.2.5.4.2 要求说明

_LGM.1。

全策略中的规定值，现场测控设备应执行

2 和 FIA_LGM.1。

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 FI

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安
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 要求加强

进行配置。

6.2.5.5.4 依赖要求

FIA_LGM.4 多次登录失败的依赖要求是 FIA_IAM

6.2.5.6 FIA_LGM.5 鉴别反馈

6.2.5.6.1 要求

现场测控设备应在鉴别过程中对鉴别的返回信息模

6.2.5.6.2 要求说明

6.2.5.6.3 要求加强

无。

6.2.5.6.4 依赖要求

FIA_LGM.5 鉴别反馈的依赖要求是 FIA_IAM.2。

6.3 FUC 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，在用户发起请求之前，确定每个请求访问设备的用户标识

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

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]的对端设[redacted]上位机或其他现

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[illegible]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]

[illegible]规定的一段时间内不活动时，动时间

[illegible]会话进行终止。

6.3.3.2 要求说明

[illegible]终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[illegible]

[illegible]设备物理访问控制机制的可信网络，也可依照本地会话超时进行[illegible]控制。

6.3.3.3.3 要求加强

FUC_SEC.2 网络会话[illegible]超时的要求加强，[illegible]设备应支持管理员为会话终止前的不活动时间部[illegible]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

工控系统现场测控设备对安全事件和重要生产活动的进行审计，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

工控系统现场测控设备应具备审计功能，对重要的安全事件和重要生产活动进行审计

——登录成功：操控人
——非法登录尝试：
——正常退出：操控
——超时退出：在预
——访问配置：将配
——配置更改：在设
——固件更换：在内
——创建用户名/口
——删除用户名/口令
——访问审计踪迹：操
盘）；
——修改时间/日期
典型的重要生产活动
——参数修改：上位
——设备重启：由于

员成功[illegible]地/远程登录设备；
操控人员连续多次输入口令错误；
人员发起的退出；
无定义好的一段时间内不活动，系统注销操控人员此次登陆；
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）；
备中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；
存中增加新的设备运行固件；
令或更改：创建新的操控人员用户名/口令或者修改权限；
户名/删除操控人员用户名/口令；
控人员查看日志或将日志保存在外部设备或存储空间（计算机、内存条、光

用户修改时间和日期。
包括：
机或其他设备修改设备的开关量、档位等参数；
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；

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[redacted] ID、应用地址、设备 IP 等）；

——事件的操作；

[redacted]

——事件的结果（成功或失

以）。

6.3.4.3.3 要求加强

FUC_ATG.[redacted]

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

工控系统现场测控设备应支持或采用审计功能对自己或其备审计记录的报告功能，以实现对审计踪迹的自动的审查。报告里要支持在不改变原始审计踪迹的情况下作安全事件的事后调查。

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[illegible]并在检测到产生安全相关错误信息。

6.4.2.3.2 要求说明

错误消息中应仅包含用于定位处理及

[illegible]

6.4.2.4.1 要求

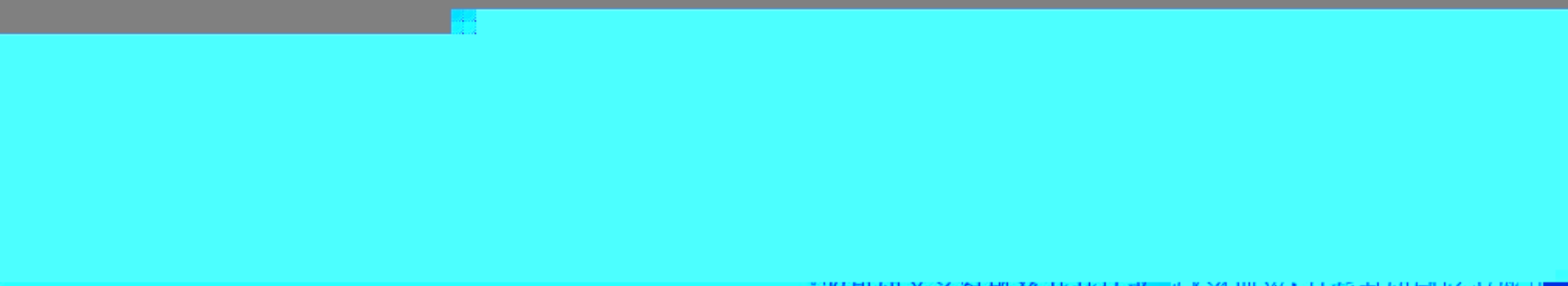
工控系统现场测控设备应检查输入信息的一致性、完整性、有[illegible]性和真实性。

6.4.2.4.2 要求说明

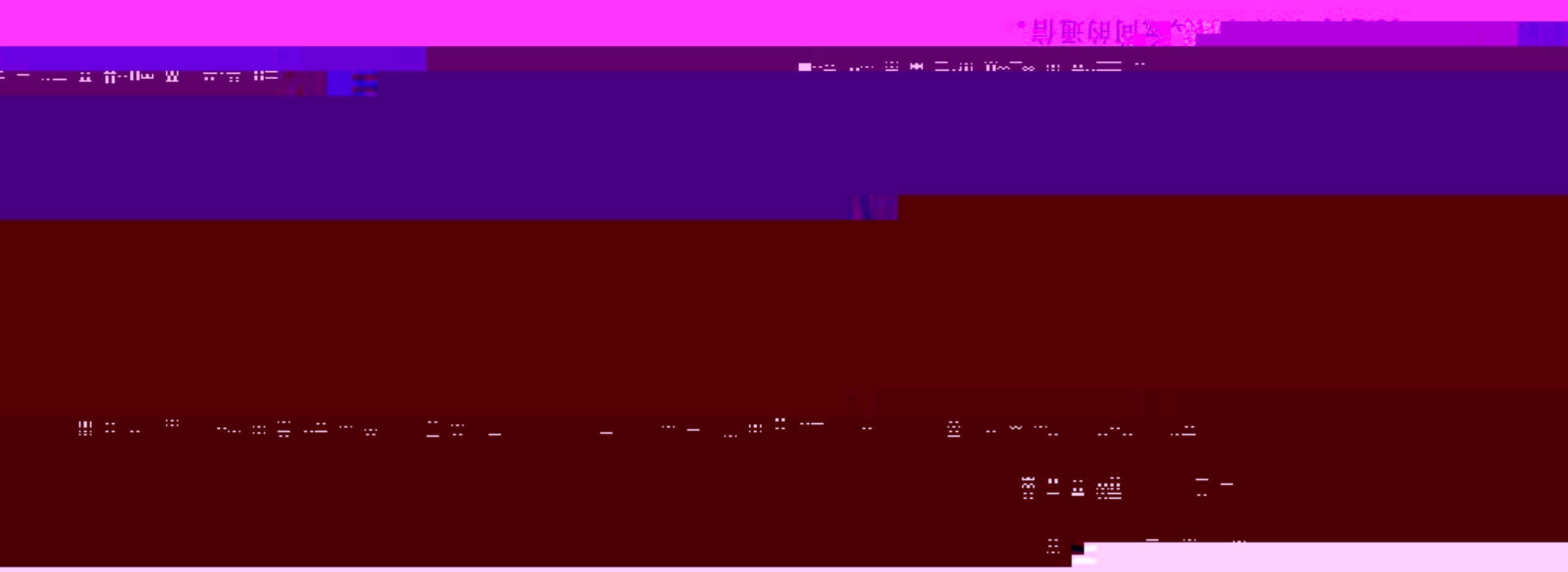
外[illegible]

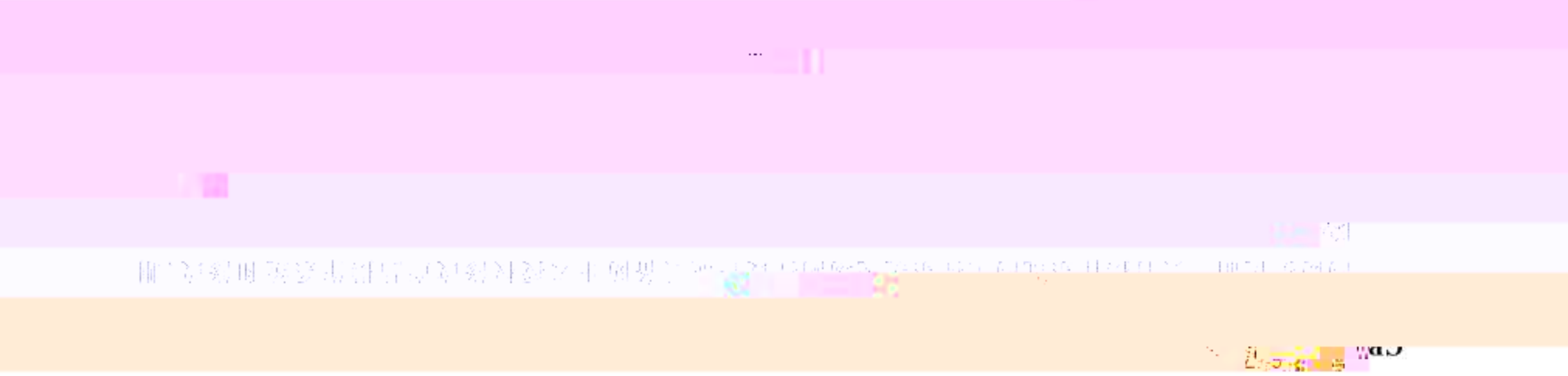
—应用输入：用于作为过程控制的输入（如：操作员的输入、I/O 输入和其他现场设备传输的数[illegible]据）；

—程序配置：用于对设备进行[illegible]









6.4.3.3.3 要求

验码。

6.4.3.6.3 要求加强

FDP_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

[redacted]

[redacted]

[redacted]

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

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，主要用于单向安全隔离认证、配置工作站、其他现场设备或有管个项目设备对专访问

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**

[redacted]

[redacted]

[redacted]

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

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]S攻击或降低攻击的影响，保障[illegible]

6.7.3 FRA_DSP 族：拒绝服务保护

6.7.3.1 族描述

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]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，进行应用层和系统级信息（包括系统

6.7.3.5.3 要求加强

无。

6.7.3.5.4 依赖要求

无。

6.7.3.6 FRA_BUC.5 备用电源

6.7.3.6.1 要求

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[illegible]

[illegible]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[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
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。

表 C.1（续）

| 要求 | | |

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_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_RUS 族：关键	

参 考 文 献

[1] GB/T 18884.9—2015 信息技术 数字化仪器仪表通信协议 第9部分：电能量测量仪器（设备）的应用层协议

[2] IEC 62056-6-2:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 6-2: COSEM interface classes

[3] IEC 62056-7-5:2016 Electricity metering data exchange—The DLMS/COSEM suite—Part 7-5: Local data exchange using wired M-Bus

[4] IEC 62056-8-3:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 8-3: Communication profile for PLC S-FSK neighbourhood networks

[5] IEC 62056-8-5:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 8-5: Communication profile for PLC OFDM neighbourhood networks

[6] IEC 62056-8-6:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 8-6: Communication profile for PLC G3 neighbourhood networks

[7] IEC 62056-9-7:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-7: Communication profile for TCP-UDP/IP networks

[8] IEC 62056-9-8:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-8: Communication profile for PLC FSK networks

[9] IEC 62056-9-9:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-9: Communication profile for PLC CENELEC B networks

[10] IEC 62056-9-10:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-10: Communication profile for PLC FSK B networks

[11] IEC 62056-9-11:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-11: Communication profile for PLC CENELEC A networks

[12] IEC 62056-9-12:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-12: Communication profile for PLC FSK A networks

[13] IEC 62056-9-13:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-13: Communication profile for PLC CENELEC C networks

[14] IEC 62056-9-14:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-14: Communication profile for PLC FSK C networks

[15] IEC 62056-9-15:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-15: Communication profile for PLC OFDM A networks

[16] IEC 62056-9-16:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-16: Communication profile for PLC OFDM B networks

[17] IEC 62056-9-17:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-17: Communication profile for PLC OFDM C networks

[18] IEC 62056-9-18:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-18: Communication profile for PLC OFDM D networks

[19] IEC 62056-9-19:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-19: Communication profile for PLC OFDM E networks

[20] IEC 62056-9-20:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-20: Communication profile for PLC OFDM F networks

[21] IEC 62056-9-21:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-21: Communication profile for PLC OFDM G networks

[22] IEC 62056-9-22:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-22: Communication profile for PLC OFDM H networks

[23] IEC 62056-9-23:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-23: Communication profile for PLC OFDM I networks

[24] IEC 62056-9-24:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-24: Communication profile for PLC OFDM J networks

[25] IEC 62056-9-25:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-25: Communication profile for PLC OFDM K networks

[26] IEC 62056-9-26:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-26: Communication profile for PLC OFDM L networks

[27] IEC 62056-9-27:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-27: Communication profile for PLC OFDM M networks

[28] IEC 62056-9-28:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-28: Communication profile for PLC OFDM N networks

[29] IEC 62056-9-29:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-29: Communication profile for PLC OFDM O networks

[30] IEC 62056-9-30:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-30: Communication profile for PLC OFDM P networks

[31] IEC 62056-9-31:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-31: Communication profile for PLC OFDM Q networks

[32] IEC 62056-9-32:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-32: Communication profile for PLC OFDM R networks

[33] IEC 62056-9-33:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-33: Communication profile for PLC OFDM S networks

[34] IEC 62056-9-34:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-34: Communication profile for PLC OFDM T networks

[35] IEC 62056-9-35:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-35: Communication profile for PLC OFDM U networks

[36] IEC 62056-9-36:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-36: Communication profile for PLC OFDM V networks

[37] IEC 62056-9-37:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-37: Communication profile for PLC OFDM W networks

[38] IEC 62056-9-38:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-38: Communication profile for PLC OFDM X networks

[39] IEC 62056-9-39:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-39: Communication profile for PLC OFDM Y networks

[40] IEC 62056-9-40:2013 Electricity metering data exchange—The DLMS/COSEM suite—Part 9-40: Communication profile for PLC OFDM Z networks

[41] IACS UR E22 Requirements for IACS components Draft 1, Edit 1