ICS 35.040
L 80

[redacted]

中国国家标准化管理委员会　发布

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。

本标准起草单位：全球能源互联网研究院有限公司、中国电力科学研究院有限公司、北京和利时系统工程有限公司、[illegible]四方继保自动化股份有限公司、华北电力大学、国电南瑞科技股份有限公司、沈阳工业电气安装有限公司、中国信息安全测评中心、[illegible]国家电网有限公司信息通信分公司、国网电力科学研究院有限公司、国家信息技术安全研究中心。

本标准主要起草人：[illegible]

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，对于生产的安全稳定运行至关重要。

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、使用控制、数据完整性、数据保密性、数据流限制、资源可用性6类通用的安全功能要求。

本标准适用于指导设备的安全设计、开发、测试

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 authentication

信息系统中，在用户、进程或设备接入资源之前，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(Certificate Authority)

CRC：循环冗余校验(Cyclic Redundancy Check)

DoS：拒绝服务攻击(Deny of Service)

DPU：分散处理单元(Distributed Processing Unit)

IED：智能电子设备(Intelligent Electric Device)

I/O：输入/输出(Input/Output)

MAC：消息鉴别码(Message Authentication Code)

MCU：微控制单元(Microcontroller Unit)

MMI：人机接口(Man Machine Interface)

MMU：内存管理单元(Memory Management Unit)

MPU：微处理器单元(Microprocessor Unit)

RAM：随机存取存储器(Random Access Memory)

RTOS：实时多任务操作系统(Real-time Operating System)

RTU：远程终端单元(Remote Terminal Unit)

TCP：传输控制协议(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

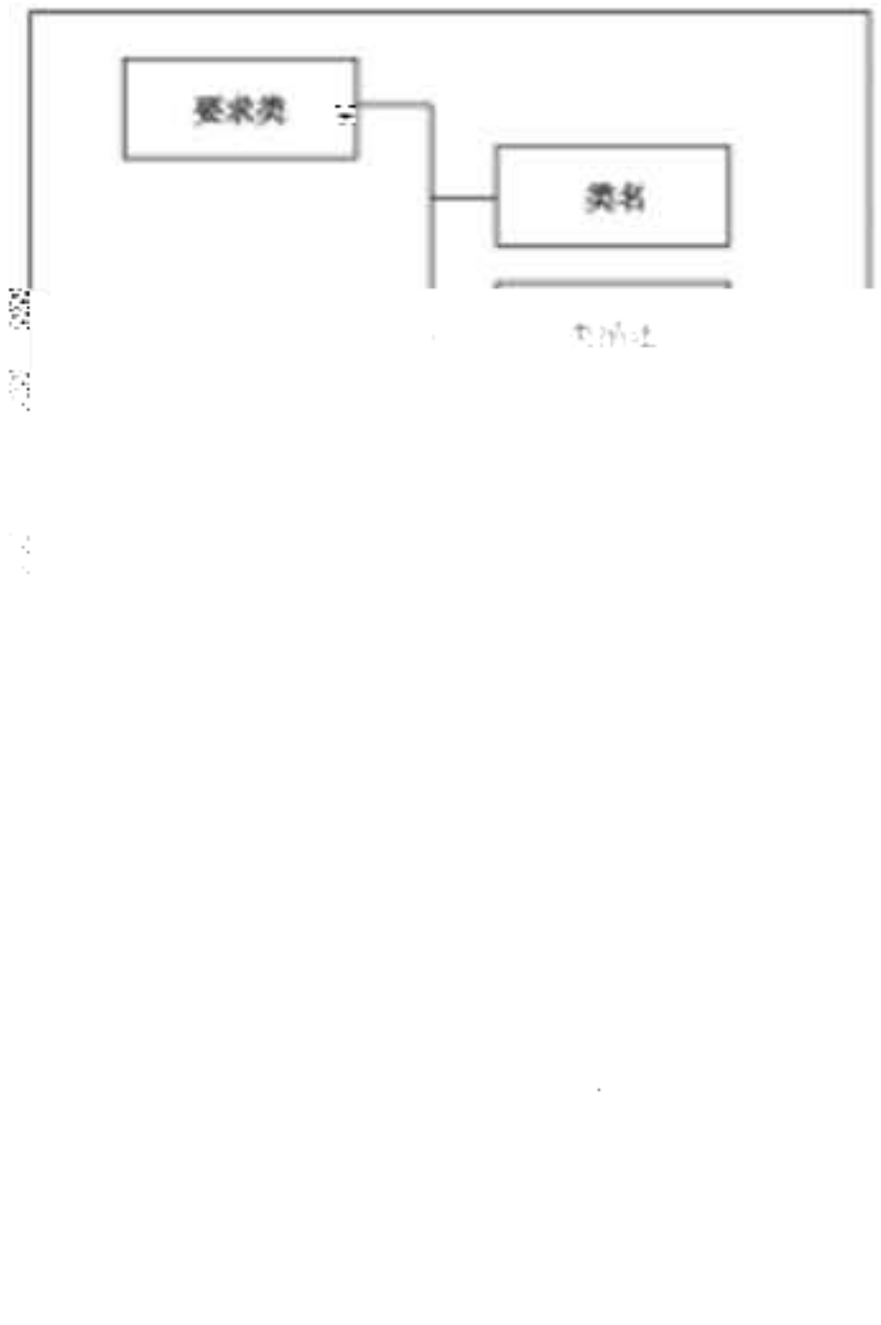
5.1 要求类结构

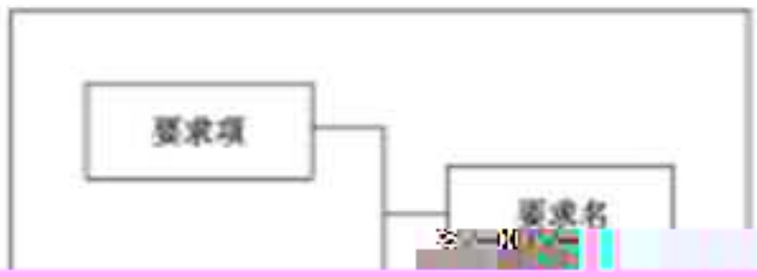
图 1 以框图形式示意了要求类的结构。每个要求类包括一个类名、类描述和一个或多个要求族。

类名提供标识和划分不同要求类所必需的信息。每个要求类都有一[illegible]的名称，类的分类信息由三个字符的简写组成。要求类分类信息简写说明见附录 B。类名的简写也用于该类中族的族名规范中。

类描述总体描述类中包含的族和该类要求的主要作用。[illegible]还用图来描述类中的族以及每个族中

组件的层次结构。




要求项
要求名

6.2.2.2.2 要求说明

应对重要的用户提供身份标识，如配
管理用户、上位机控制实体等。典型的用户身份标识符包括
网络地址（如物理地址、IP 地址）、操作人员

6.2.2.2.3 要求加强

FIA_IAM.1 标识及方式的要求加强
a) 设备在所有对外接口上具有标
b) 设备在所有对外接口上都具备

6.2.2.2.4 依赖要求

无。

6.2.2.3 FIA_IAM.2 鉴别及方式

6.2.2.3.1 要求

工控系统现场测控设备应具备在对

6.2.2 [illegible] 要求说明

设备应对开启的网络服务接口和
等。典型的身份鉴别方式包括：口令、

6.2.2.3.3 要求加强

FIA_IAM.2 鉴别及方式的要求加
a) 设备在远程网络访问接口上
b) 设备对所有远程网络访问接

6.2.2.3.4 依赖要求

FIA_IAM.2 鉴别及方式的依

6.2.3 FIA_IDM 族：标识符管理

6.2.3.1 族描述

工控系统现场测控设备能用
地址、TCP/UDP 端口、应用地址
其中人员用户标识符管理
设备进行查看或配置的操控人

6.2.3.2 FIA_IDM.1 操控人

6.2.3.2.1 要求

工控系统现场测控设备

6.2.3.2.2 要求说明

设备应具备向具有运行

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。

6.2.3.2.4 依赖要求

FIA_IDM.1 操控人员标识符管理的依赖要求是 FIA_IAM.1。

6.2.4 FIA_ACM 族：鉴别凭证管理

6.2.4.1 族描述

工控系统现场测控设备管理用户身份鉴别凭证的能力主要包括对鉴别凭证的强度和使用的管理。由于对设备的访问方式可能包括本地面板访问、串口访问、网络访问、上位机应用访问，因此鉴别凭证的使用和管理涵盖设备层和网络层的鉴别。

6.2.4.2 FIA_ACM.1 口令修改

6.2.4.2.1 要求

工控系统现场测控设备应支持管理员等操控人员在不影响正常操作的情况下修改他们管理范围内口令。设备应支持并提示对出厂默认口令的修改。

6.2.4.2.2 要求说明

主要针对管理员、配置查看用户、配置修改用户等设备操控人员口令进行管理。

6.2.4.2.3 要求加强

无。

6.2.4.2.4 依赖要求

FIA_ACM.1 口令修改的依赖要求是 FIA_IAM.2。

6.2.4.3 FIA_ACM.2 口令更换周期

6.2.4.3.1 要求

工控系统现场测控设备应支持安全策略中要求的口令使用周期。

6.2.4.3.2 要求说明

操控人员验证成功后，工控系统现场测控设备应提供必要的自动提醒能力，通知用户距离上次修改密码时间已经超过了安全策略要求的密码使用周期。

6.2.4.3.3 要求加强

FIA_ACM.2 口令更换周期的要求加强为设备应支持管理员对口令更换周期进行配置。

6.2.4.3.4 依赖要求

FIA_ACM.2 口令更换周期的依赖要求是 FIA_IAM.2。

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中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管[illegible]

应能够对配置用户的公钥进行管理，并对证书进行识别；

备和其他设备、远程配置系统、监控后台或上位机的通信

应能够对证书进行正确解析，对证书的真实性和有效性进

强包括：

照安全策略要求定期更新公私钥；

钥管理设施，如 CA。

要求是 FIA_IAM

通信身份鉴别。设备应能保证本

持对密钥的分发、更新和撤销的

户的现场访问不得依赖于外部密

信层面上，公私钥可用于现场测控设

身份鉴别。设备应保证本地存储私钥的安全，

行验证。

6.2.4.6.3 要求加强

FIA_ACM.5 证书及公私钥管理的要求加

a) 现场测控设备及其配置软件应支持

b) 在工控系统层面上建立有效的公

6.2.4.6.4 依赖要求

FIA_ACM.5 证书及公私钥管理的依赖

可用于现场测控设备和其他设备、监控后台或上位机的

地存储密钥的安全，同时满足密钥管理策略。

6.2.4.7.3 要求加强

FIA_ACM.6 对称密钥管理的要求加强包括：

a) 现场测控设备应支持按照安全策略要求定期更新对称密钥；

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

实现。

6.2.4.7.4 依赖要求

FIA_ACM.6 对称密钥管理的依赖要求是 FIA_IAM.2。

6.2.4.8 FIA_ACM.7 密码服务失效

6.2.4.8.1 要求

如果使用基于密码的鉴别机制，工控系统现场测控设备的重要用

的服务。

6.2.4.8.2 要求说明

如果外部密码（如加密、密钥临时）服务

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_ACM.6。

6.2.5 FIA_LGM 族:登录管理

6.2.5.1 族描述

工控系统现场测控设备登录管理主要包括对管理员、配置查看用户、配置修改用户等操控人员登录行为的成功、失败和登录历史等进行管理。

6.2.5.2 FIA_LGM.1 登录失败管理

6.2.5.2.1 要求

工控系统现场测控设备应管理和记录操控人员[illegible]从最近的成功登录后的登录失败的次数和时间。

6.2.5.2.2 要求说明

[illegible]

6.2.5.4.2 要求说明

限，根据权限执行所请求的操作，并进行控制和审计。

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分配权限，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、控制参数变更、系统应用层面的控制命令上传/下发、数据

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，管理员主要负责用户账户管理和安全功能管理。

6.3.2.4.2 要求说明

仅允许管理员角色权限建立和管理其他账号。对于功能简单的设备，管理员、配置用户和审计用户可由一个用户承担，不设置复杂的用户管理模式。系统运行中可采用"操作票"等管理手段实现用户和操作人员的对应关系。

6.3.2.4.3 要求加强

无。

6.3.2.4.4 依赖要求

FUC_ACA.3 管理员用户的依赖要求是 FIA_IAM.1、FUC_ACA.1 和 FUC_ACA.2。

6.3.2.5 FUC_ACA.4 最小权限原则

6.3.2.5.1 要求

用户仅具备完成任务所需的最小权限。

6.3.2.5.2 要求说明

新建普通操作人员用户应由管理员来根据[illegible]现场设备的对端设备(上位机或其他现场设备)对设备的访问也应基于最小权限，如只能访问某一服务端口、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 最小权限原则的依赖要求是 FIA_IAM.1 和 FUC_ACA.1。

6.3.2.6 FUC_ACA.5 权限分离

6.3.2.6.1 要求

现场测控设备应支持用户修改重要参数或进行重要控制操作的权限分离管理。

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数据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，实现重要控前操作的执行和确认。

6.3.2.6.3 要求加强

无。

6.3.2.6.4 依赖要求

FUC_ACA.5 权限分离的依赖要求是 FIA_IAM.1、FUC_ACA.1 和 FUC_ACA.2。

6.3.3 FUC_SEC 族：会话控制

6.3.3.1 族描述

工业系统现场同类设备或不同设备配置软件和操作人员门户会话进行控制，通过终止或锁定超时会话保证会话的安全性。

[illegible]

就定的一段时间内不活

动时对会话进行终止。

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

制。如果会话建立途经网络是具有完备

控制。

6.3.3.3.3 要求加强

FUC_SEC.2 网络会话超时的要求为

里户的网络访问，特别是远程访问，不对占位拟进程进行限

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

强为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

——登录成功：操控人员成功[illegible]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
——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
——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：删除操控人员用户名/口令；
——访问审计踪迹：操控人员查看日志或将日志保存在外部设备或存储空间
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
——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、
端口。
审计事件要与设备具备并开启的安全功能相对应，如不具备访问控制功能
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

6.3.4.2.4 依赖要求

FUC_ATC.1 审计事件的依赖要求是 FIA_UGM.2、FIA_UGM.4、FRF_NA

6.3.4.3 FUC_ATC.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。大多数审计踪迹内容包括：

——事件的日期和时间；

——事件的来源（例如，用户 ID、应用地址、设备，

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：审计踪迹存储

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踪迹，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踪迹存储容量。

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、鸣笛等。审计处理失败包括软件或硬件错误、生成审计踪迹过程中的错误、审计踪迹存储空间满载等。

6.3.5.3.3 要求加强

FUC_ATS.2 审计功能异常的要求加强为设备应支持管理员配置设备在审计踪迹存储空间满载时可自动执行的操作，如覆盖旧的审计踪迹或停止生成审计踪迹等。

6.3.5.3.4 依赖要求

FUC_ATS.2 审计功能异常的依赖要求是 FUC_ATS.1。

6.3.5.4 FUC_ATS.3 审计踪迹保护

6.3.5.4.1 要求

工控系统现场测控设备或从事审计功能的组件应保护审计踪迹和审计工具不被非授权访问、修改或删除。

6.3.5.4.2 要求说明

应保证只有授权用户可对审计踪迹进行操作。可通过增加校验码实现审计踪迹的防篡改。

6.3.5.4.3 要求加强

FUC_ATS.3 审计踪迹保护的要求加强为设备应为审计踪迹提供基于密码的保护功能。

6.3.5.4.4 依赖要求

FUC_ATS.3 审计踪迹保护的依赖要求是 FUC_ACA.1。

6.3.6 FUC_ATR 族:审计踪迹访问

6.3.6.1 族描述

工控系统现场测控设备支持用户对审计踪迹进行访问[便于查看、分析和集中处理]。

6.3.6.2 FUC_ATR.1 审计踪迹读取

6.3.6.2.1 要求

[工控系统现场测控设备或从事审计功能的组件应]保证以便于用户理解的方式提供审计踪迹,且仅[有授]权用户可读取审计踪迹。

6.3.6.2.2 要求说明

[只有授权用户具备获得和解释审计踪迹的能力。用户是操控人员时,信息应以可理解的方式表示;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

[无要求]

6.3.6.2.4 依赖要求

FUC_ATR.1 审计踪迹读取的依赖要求是 FUC_ACA.1 和 FUC_ATS.3。

6.3.6.3 FUC_ATR.2

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

工控系统现场测控设备或承担审计功能的组件应具备审计归纳和报告功能，以实现对审计踪迹的归纳与查看，报告可呈现存在不改变原始审计踪迹的情况下作安全事件的事后调查。

6.3.6.4.2 要求说明

一般情况下，审计踪迹的归纳和报告的生成会在一个独立的信息系统中执行，比如在系统范围审计工具中实现。

6.3.6.4.3 要求加强

无。

6.3.6.4.4 依赖要求

FUC_ATR.3 审计报告的依赖要求是 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

验证与报警。

6.4.2.2.4 依赖要求

的防护机制。具有操作系统的工控系统现场测控设备应具备防止未授权修改产品操作系统和修改、删除或插入运行数据的机制。

工控系统现场测控设备应能够自动检测对内存中的应用配置数据的修改，自动检测对内存中可执行代码的修改与插入，防止非授权的修改或插入。设备应针对当可执行代码的修改和加载不是厂商授权版本更新的情况进行防护。

工控系统现场测控设备应能够自动检测对内存中操作系统配置的修改。设备应针对当操作系统配置的修改不是厂商的授权版本更新的情况进行防护。典型操作包括非法修改处理系统异常的中断向量表和进程调度算法。

6.4.2.5.3 要求加强

FDI_DSI.4 静态数据防篡改的要求加强为设备应具备基于密码的静态数据未授权修改的防护机制。

6.4.2.5.4 依赖要求

无。

6.4.3 FDI_DTI 族：数据传输完整性

6.4.3.1 族描述

工控系统现场测控设备对传输数据的完整性，主要针对系统应用通信数据的安全，例如设备与上位机之

[illegible]

[illegible]新序列码的连续性，从而识别是否存在数据包丢失的情况。

6.4.3.3.3 要求加强

无。

6.4.3.3.4 依赖要求

无。

6.4.3.4 FDI_DTI.3 数据包延迟

6.4.3.4.1 要求

工控系统现场测控设备应能够处理过度延迟的数据包。

6.4.3.4.2 要求说明

可以通过在系统应用层面上收方发送收包确认信息、使用时间窗或设定超时容忍时间来处理过度延迟的数据包。

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_DTI.4 数据包重放

6.4.3.5.1 要求

工控系统现场测控设备应具备机制抵御数据包的重放。

6.4.3.5.2 要求说明

主要通过添加序列码或时间标签，设备判断序列码或时间标签是否新鲜，从而识别是否存在数据包的重放。

6.4.3.5.3 要求加强

无。

6.4.3.5.4 依赖要求

无。

6.4.3.6 FDI_DTI.5 数据包防篡改

6.4.3.6.1 要求

工控系统现场测控设备应具备识别篡改通信信息的机制。

6.4.3.6.2 要求说明

检测通信过程中出现的错误的典型机制为CRC

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

[redacted]要求

无。

6.4.3.7 FDI_DTI.6 会话[redacted]保护

6.4.3.7.1 要求

工控系统现场测控设备应具备保护会话完整的机制，以防止中间人攻击。

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。

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防止数据被窃听，主要防护对象是[redacted]储的敏感数据。

6.5.2 FDC_CRM 族：加密机制

6.5.2.1 族描述

加密算法的使用、加密设备的采购需符合国家和行业的相关规定。

6.5.2.2 FDC_CRM.1 加密机制

6.5.2.2.1 要求

工控系统现场测控设备采[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 族描述

密性进行保护，防止未授权的通信数据窃听，主要针对口
信数据。

传输数据的保密性

数据保密性保护机制可以在应用

的传输数据保密性保护机制，如

保密性

6.5.4.1 族描

工控系统现场测控设备对传输数据的
令、密钥等安全管理数据和重要的系统应用

6.5.4.2 FDC_DTC.1 传输数据保密性

6.5.4.2.1 要求

工控系统现场测控设备应具备机制保

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。
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为设备应具备基于密
加

6.5.4.2.4 依赖要求

EDC_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和本地端口实施访问控制，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

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)，且其采用的无线协议应具备安全机制。

6.6.2.4.2 要求说明

关闭设备上的无线访问物理开关后，将不能通过交换机或软件配置开启设备的无线功能。无线协议应具备鉴别、完整性保护和加密等安全机制。

6.6.2.4.3 要求加强

FRF_NAC.3 无线访问的要求加强为设备应禁用无线通信方式。

6.6.2.4.4 依赖要求

无。

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安全功能与非安全功能隔离,使用的

[redacted]

[redacted]设备,应在安全计划中记录该情况并制定风险缓解方法。

6.6.3.3.3 要求加强

无。

6.6.3.3.4 依赖要求

无。

6.6.3.4 FRF_FUP.3 数据的非可执行性

6.6.3.4.1 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[redacted]支持硬件 MMU 的 OS、或者支持分离内存硬件设计的 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

资源可用性的目的是确保设备可适应对不同类型的拒绝服务事件,并保持设备在降级情况[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抵御 DoS 攻击或降低攻击的影响，保障重要服务。在实际防护中还要综合考虑网络上的隔离手段，例如在网络边界设备上降低 DoS 攻击成功的可能性。

6.7.2.2 FRA_DSP.1 数据洪泛保护

6.7.2.2.1 要求

工控系统现场测控设备应能够抵御一定的数据洪泛攻击或降低攻击的影响，保证重要业务功能的通信。

6.7.2.2.2 要求说明

常用的抵御洪泛攻击或限制其影响的机制包括：现场设备在遭遇洪泛攻击时，以降级模式（限速）运行直至攻击结束；在网络边界上使用数据包过滤设备。

6.7.2.2.3 要求加强

无。

6.7.2.2.4 依赖要求

无。

6.7.3 FRA_BUC 族：业务连续性

6.7.3.1 族描述

工控系统现场测控设备应具备业务连续性保护机[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 数据备份

6.7.3.4.1 要求

工控系统现场测控设备应直接或依靠其他工具提供备份功能，进行应用级和系统级信息（包括系统安全状态信息）的备份。

6.7.3.4.2 要求说明

备份的功能和方法应在用户手册中说明。

6.7.3.4.3 要求加强

FRA_BUC.3 数据备份的要求加强为设备应能够验证备份机制的可靠性和备份信息的完整性。

6.7.3.4.4 依赖要求

无。

6.7.3.5 FRA_BUC.4 设备恢复

6.7.3.5.1 要求

工控系统现场测控设备应具备在中断或故障后，恢复和重构到已知安全状态的能力。

6.7.3.5.2 要求说明

工控系统现场测控设备应提供恢复功能，即能够恢复到预先定义的安全状态，或在中断或故障后由用户恢复并重组先前保存的备份。

预先定义的状态包括：

——未上电状态；

——可知的最后的好值；

——由资产属主或应用确定的固定值。

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

工控系统现场测控设备或附属组件应支持在不影响业务运行情况下的备用电源切换。

6.7.3.6.2 要求说明

无。

6.7.3.6.3 要求加强

无。

6.7.3.6.4 依赖要求

无。

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，实现对现场的测量与控制，如图 A.1 所示。现场设备具备的典型功能包括：通过现场总线与生产过程上的传感器、调节器、变送器、开关或 I/O 单元进行通信；进行控制逻辑运算；通过本地或远程以太网上传数据给实时数据库服务器及操作员站，接受本地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。

图 A.1 工业控制系统现场测控设备逻辑概念图

A.2 工业控制系统现场测控设备典型硬件结构

模块取代原有的输入和输出模块。

输入模块接收电压、电流、温度、压力等现场测量量，可分为模拟输入模块和数字输入模块。

输出模块输入对开关、调节器等设备的控制信号。

人机接口(MMI)一般固定在装置前面板上，有液晶显示屏、参数设置键和就地功能按钮。可以显示当前的测量值、配置信息等。

管理模块实现装置的管理和通信。具体功能包括实现与人机接口面板、调试软件、监控后台、工程师站、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 以太网口、电缆接口、RS232 串口、RS485 串口、ISO 11898 串口等。

A.3 工业控制系统现场测控设备典型软件结构

目前工业控制系统现场测控设备的软件架构都是基于嵌入式软件。

嵌入式系统的发展主要经历了三个阶段。无操作系统的嵌入式系统的出现最初是基于单片机，这类嵌入式系统具有与一些监测、伺服和指示设备相配合的功能。它无操作系统支持，而是通过汇编语言编程对系统进行直接控制，此外，它系统结构和功能相对单一，针对性强，几乎没有用户接口。简单监控式的实时操作系统主要以嵌入式处理器为基础，以简单监控式系统为核心。系统的优点是处理器种类繁多，开销小，效率高一般配备系统仿真器，具有一定的兼容性和扩展性。但是此时的系统通信性较差，用户界面不够友好，主要用来控制系统负载以及监控系统应用程序运行。随着对实时性要求的提高和软件规模不断扩大，实时多任务操作系统(RTOS)成为目前国际嵌入式系统的主流，包括 VxWorks、Windows CE、Linux 等，VxWorks 以其强实时性、高性能的内核和良好的开发界面成为了嵌入式实时操作

附 录 B
（规范性附录）
要求类与要求族的分类信息简写说明

要求类的分类信息简写说明见表 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	简写对应的英文类名
用户标识与鉴别	FIA 类	Function-Identification and Authentication
使用控制	FUC 类	Function-Use Control
数据完整性	FDI 类	Function-Data Integrity
数据保密性	FDC 类	Function-Data Confidentiality
受限的信息流	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

要求族简写	要求族名称	简写对应的英文族名
FIA_IAM 族	标识与鉴别方式	Funciton-Identification and Authentication _ Identification and Authentication Methods
FIA_IDM 族	标识符管理	Funciton-Identification and Authentication _ Identities Management
FIA_ACM 族	鉴别凭证管理	Funciton-Identification and Authentication_Authentication Credential Management
FIA_LGM 族	登录管理	Funciton-Identification and Authentication_Login Management
FUC_ACA 族	访问控制授权	Funciton-Use Control_Access Control Authorization
FUC_SEC 族	会话控制	Funciton-Use Control_Session Control
FUC_ATC 族	审计踪迹产生	Funciton-Use Control_Creation of Audit Trail
FUC_ATS 族	审计踪迹存储	Funciton-Use Control_Storage of Audit Trail
FUC_ATR 族	审计踪迹访问	Funciton-Use Control_Report of Audit Trail
FDI_DSI 族	数据存储完整性	Funciton-Data Integrity_Integrity of Stored Data
FDI_DTI 族	数据传输完整性	Funciton-Data Integrity_Integrity of Transmitted Data
FDC_CRM 族	加密机制	Funciton-Data Confidentiality_Cryptographic Mechanisms
FDC_DSC 族	存储数据保密性	Funciton-Data Confidentiality_Confidentiality of Stored Data
FDC_DTC 族	传输数据保密性	Funciton-Data Confidentiality_Confidentiality of Transmitted Data
FRF_NAC 族	网络入口的访问控制	Funciton-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-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，被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。如果表格单元为空，则该行要求不依赖于对应列中要求。

表 C.1 安全功能要求依赖关系表

要求	及方式	及方式	及公私钥管理	密钥管理	失败管理	成功记录	导失败	管理	角色的访问控制	事件	数据库	成保护	成报告	制	控制	务连续性
要求																

表 C.1（续）

要求	只及方式	用及方式	书及公私钥管理	称密钥管理	次失败管理	次成功记录	录失败	管理	角色的访问控制	事件	字储保护	完整报告	日制	包控制	务连续性
FUC_ATC.4 用户[illegible]															

附 录 D
（规范性附录）
通用安全功能要求汇总表

通用安全功能要求汇总表见表 D.1。

表 D.1 通用安全功能要求汇总表

要求类(6)	要求族(18)	要求项(58)
FIA 类:用户标识与鉴别	FIA_IAM 族:标识与鉴别方式	FIA_IAM.1 标识及方式
		FIA_IAM.2 鉴别及方式
	FIA_IDM 族:标识符管理	FIA_IDM.1 操控人员标识符管理
	FIA_ACM 族:鉴别凭证管理	FIA_ACM.1 口令修改
		FIA_ACM.2 口令更换周期
		FIA_ACM.3 口令强度控制
		FIA_ACM.4 口令失效
		FIA_ACM.5 证书及公私钥管理
		FIA_ACM.6 对称密钥管理
		FIA_ACM.7 密码服务失效
	FIA_LGM 族:登录管理	FIA_LGM.1 登录失败管理
		FIA_LGM.2 登录成功记录
		FIA_LGM.3 登录历史
		FIA_LGM.4 多次登录失败
		FIA_LGM.5 鉴别反馈
FUC 类:使用控制	FUC_ACA 族:访问控制授权	FUC_ACA.1 权限管理
		FUC_ACA.2 基于角色的访问控制
		FUC_ACA.3 管理员用户
		FUC_ACA.4 最小权限原则
		FUC_ACA.5 权限分离
	FUC_SEC 族:会话控制	FUC_SEC.1 本地会话超时
		FUC_SEC.2 网络会话超时
	FUC_ATC 族:审计踪迹产生	FUC_ATC.1 审计事件
		FUC_ATC.2 审计踪迹的内容
		FUC_ATC.3 审计的时间戳
		FUC_ATC.4 用户关联
	FUC_ATS 族:审计踪迹存储	FUC_ATS.1 审计存储容量
		FUC_ATS.2 审计功能异常
		FUC_ATS.3 审计踪迹保护

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	FDI_DSI.1 安全功能检测
		FDI_DSI.2 异常处理

参 考 文 献