ICS 35.040
L80

中华人民共和国国家标准

GB/T 22239.4—XXXX

信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求

Information Security Technology- Baseline for Cybersecurity Classified Protection

Part 4: Special Security Requirements for Internet of Things

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

-XX-XX 发布 XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目　　次

前　言

本部分由全国信息安全标准化技术委员会提出。

本部分由全国信息安全标准化技术委员会归口。

本部分起草单位：公安部第一研究所、中国科学院信息工程研究所、公安部信息安全等级保护评估中心、山东微分电子科技有限公司、中国电子科技集团公司第十五研究所、工业和信息化部电信研究院、中国电子信息产业集团有限公司第六研究所、国家计算机病毒应急处理中心、华北电力大学、北京天融信科技股份有限公司、北京匡恩网络科技有限责任公司。

本部分主要起草人：蒋勇、李超、李秋香、吴薇、刘志宇、宫月、徐晓军、王昱镔、吕由、黄学臻、陈翠云、卢浩、张森、陶源、陈利民、霍珊珊、刘健、张益、刘美丽、师以贺、房华、唐良瑞、闫江毓、吴润泽、李冰、李建清、魏薇、封莎、李强、武传坤、朱建勇、杜旭阳、贡春燕、陈建民、杜振华。

引　言

国家标准 GB/T 22239-2008 信息安全技术 网络安全等级保护基本要求 在开展信息安全等级保护工作的过程中起到了非常重要的作用，被广泛应用于各个行业和领域开展信息安全等级保护的建设整改和等级测评等工作，但是随着信息技术的发展，GB/T 22239-2008 在时效性、易用性、可操作性上需要进一步提高。

为了适应无线移动接入、虚拟计算环境、云计算、大数据、物联网和工业控制系统等新技术、新应用情况下信息安全等级保护工作的开展，需对 GB/T 22239-2008 进行修订，修订的思路和方法是针对无线移动接入、虚拟计算环境、云计算、大数据、物联网和工业控制系统等新技术、新应用领域提出扩展的安全要求。

对 GB/T 22239-2008 的修订完成后，基本要求标准成为由多个部分组成的系列标准，目前主要有六个部分：

——GB/T 22239.1-XXXX　信息安全技术 网络安全等级保护基本要求
第 1 部分：安全通用要求；
——GB/T 22239.2-XXXX　信息安全技术 网络安全等级保护基本要求
第 2 部分：云计算安全扩展要求；
——GB/T 22239.3-XXXX　信息安全技术 网络安全等级保护基本要求
第 3 部分：移动互联安全扩展要求；
——GB/T 22239.4-XXXX　信息安全技术 网络安全等级保护基本要求
第 4 部分：物联网安全扩展要求；
——GB/T 22239.5-XXXX　信息安全技术 网络安全等级保护基本要求
第 5 部分：工业控制安全扩展要求；
——GB/T 22239.6-XXXX　信息安全技术 网络安全等级保护基本要求
第 6 部分：大数据安全扩展要求。

将来可能会随着技术的变化添加新的部分阐述特定领域的安全扩展要求。

在本部分文本中，黑体字表示较低等级中没有出现或增强的要求。

信息安全技术 网络安全等级保护基本要求
第 4 部分 物联网安全扩展要求

1 范围

本部分规定了不同安全保护等级物联网系统的安全扩展要求，适用于指导分等级的非涉密物联网系统的安全建设和监督管理。

本部分适用于基于传感器构成的物联网信息系统和基于RFID构成的物联网信息系统，扩展安全要求主要针对通用安全要求不能覆盖的感知节点设备（含RFID）和网关节点设备（含RFID读写器）。

2 规范性引用文件

下列文件中的条款通过在本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本部分。

GB/T 25069-2010 信息安全技术 术语

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239.1 信息安全技术 信息安全等级保护基本要求 第1部分：安全通用要求

GB/T 22239-2008 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2008 信息安全技术 网络安全等级保护定级指南

3 术语和定义

GB17859-1999和GB/T 22239.1确立的以及下列术语和定义适用于本部分

3.1 物联网 internet of things（IOT）

物联网是将感知节点设备（含RFID）通过互联网等网络连接起来构成的一个应用系统，它融合信息系统和物理世界实体，是虚拟世界与现实世界的结合。

3.2 网关节点设备 The sensor layer gateway

网关节点设备是一种以将感知节点设备所采集的数据传输到数据处理中心的关键出口，是连接传统信息网络（有线网、移动网等）和传感网的桥梁，其安全设置也区分对感知层的安全设置和对网络传输层的安全设置。简单的感知层网关只是对感知数据的转发（因电力充足），而智能的感知层网关可以包括对数据进行适当处理、数据融合等业务。

3.3 感知节点设备 sensor node

也叫感知终端设备（end sensor）、终端感知节点设备（end sensor node），是物联网系统的最终端设备或器件，能够通过有线、无线方式发起或终结通信，采集物理信息和/或接受控制的实体设备。

3.4 数据新鲜性 data freshness

数据新鲜性是防止已经成功接收的历史数据再次被接收处理（通过历史数据列表比对），或超出数据接收时间（时间戳过期）的数据被接收，或超出合法性范围（如计数器无效）的数据被接收。不满足新鲜性的数据一般不予处理，其目的是用于防止数据重放攻击。

4 物联网系统概述

4.1 物联网系统构成

物联网系统从架构上可分为三个逻辑层，即感知层、网络传输层、处理应用层。其中感知层包括传感器节点和传感网网关节点，或RFID标签和RFID读写器，也包括这些感知设备及传感网网关、RFID标签与阅读器之间的短距离通信（通常为无线）；网络传输层指将这些感知数据远距离传输到处理中心的网络，包括互联网、移动网，常包括几种不同网络的融合；处理应用层指对感知数据进行存储与智能处理的平台，并对行业应用终端提供服务。对大型物联网系统来说，处理应用层一般是云计算平台和行业应用终端设备。具体如下图1所示：

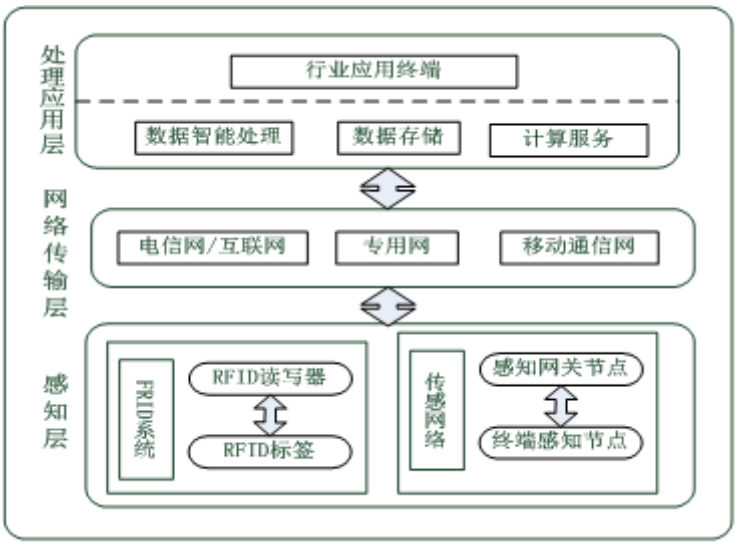

图1 物联网系统构成

4.2 物联网系统定级

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

5 第一级基本要求

5.1 技术要求

5.1.1 物理和环境安全

5.1.1.1 终端感知节点设备（包括 RFID 标签）的物理和环境安全

本项要求包括：

a) 感知节点设备所处的物理环境应该不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应该能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）。

5.1.2 网络和通信安全

5.1.2.1 数据源认证

应确保信息来源于正确的感知节点设备。

5.1.2.2 异构网安全接入

应建立异构网络的接入认证系统，实现安全的传输控制信息。

5.1.3 应用和数据安全

5.1.3.1 访问控制

对远程登陆的用户具有认证功能，确保只有合法用户才能登陆。

5.1.3.2 数据完整性

应能够检测到感知节点设备生存信息在传输过程中完整性受到破坏。

5.1.3.3 数据可用性

应保证感知网络实体间通信数据的新鲜性。

5.2 管理要求

5.2.1 安全建设管理

5.2.1.1 自行研发感知节点设备（包括 RFID）

本项要求包括：

a) 应确保终端感知节点设备、网关节点设备的主要部件（芯片、电池、天线等）参数满足系统功能需求；

b) 应确保研发环境与实际运行环境物理分开；

c) 应确保提供软、硬件设计的相关文档，并由专人负责保管。

5.2.1.2 外包研发感知节点设备（包括 RFID）

本项要求包括：

a) 应根据研发需求检测软、硬件质量；

b) 应在软件安装之前检测软件包中可能存在的恶意代码；

c) 应要求研发单位提供软、硬件设计的相关文档和使用指南；

d) 应根据研发单位提供的硬件设计图审查实物与设计是否一致。

5.2.2 安全运维管理

5.2.2.1 感知节点设备（包括 RFID）环境管理

本项要求包括：

a) 应指定人员定期巡视终端感知节点设备、网关节点设备的部署环境，对可能影响终端感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

b) 应记录终端感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关节点设备进行现场维护（除尘、充电、修理等）；

c) 应建立针对终端感知节点设备、网关节点设备部署环境的评估制度，编写可操作评估方法，并由专人完成评估；

d) 应制定终端感知节点设备、网关节点设备管理制度，对终端感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理。

5.2.2.2 感知节点设备（包括 RFID）备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定终端感知节点设备、网关节点设备备份信息的备份方式、备份频度、存储介质、保存期等。

6 第二级基本要求

6.1 技术要求

6.1.1 物理和环境安全

6.1.1.1 终端感知节点设备（包括 RFID 标签）的物理和环境安全

本项要求包括：

a) 感知节点设备所处的物理环境应该不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应该能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）。

6.1.1.2 感知网关节点设备（包括 RFID 读写器）的物理和环境安全

本项要求包括：

a) **网关节点设备所在物理环境应该具备防火、防静电的能力；**

b) **网关节点设备所在物理环境应该具备防潮、防水的能力；**

c) **网关节点设备的主要部件进行固定，并设置明显的不易除去的标记。**

6.1.2 网络和通信安全

6.1.2.1 数据源认证

应确保信息来源于正确的感知节点设备。

6.1.2.2 感知节点设备访问控制

本项要求包括：

a) **应设置传感网入网访问控制，对感知节点设备接入网络资源设置访问控制机制，防止感知网资源被非法访问和非法使用；**

b) **远程配置感知节点设备上软件应用时应当提供安全保护。**

6.1.2.3 异构网安全接入

本项要求包括：

a) 应建立异构网络的接入认证系统，实现安全的传输控制信息；

b) **应具有拒绝恶意节点的接入能力，保证合法节点不被恶意节点攻击而被拒绝接入，保证网络资源的可使用性。**

6.1.3 应用和数据安全

6.1.3.1 访问控制

本项要求包括：

a） 对远程登陆的用户具有认证功能，确保只有合法用户才能登陆；

b) **对远程登陆的用户服务应覆盖高峰时期的用户访问数量。**

6.1.3.2 数据完整性

应能够检测到感知节点设备生存信息、**鉴别信息、隐私性数据和重要业务数据**在传输过程中完整性受到破坏；

6.1.3.3 数据保密性

应采用密码技术对重要数据（指令控制数据、业务数据）实施机密性保护，确保这些数据在传输中的保密性。

6.1.3.4 数据可用性

本项要求包括：

a) 应保证感知网络实体间通信数据的新鲜性；

b) **应提供重要业务数据的本地备份与重传功能。**

6.2 管理要求

6.2.1 安全建设管理

6.2.1.1 自行研发感知节点设备（包括 RFID）

本项要求包括：

a) 应确保终端感知节点设备、网关节点设备的主要部件（芯片、电池、天线等）参数满足系统功能需求；
b) 应确保研发环境与实际运行环境物理分开；
c) **应制定软、硬件研发管理制度，明确说明研发过程的控制方法和人员行为准则；**
d) 应确保提供软、硬件设计的相关文档**和使用指南**，并由专人负责保管。

6.2.1.2 外包研发感知节点设备（包括 RFID）

本项要求包括：

a) 应根据研发需求检测软、硬件质量；
b) 应确保提供软、硬件设计的相关文档和使用指南；
c) 应在软件安装之前检测软件包中可能存在的恶意代码；
d) **应要求研发单位提供软件源代码，并审查软件中可能存在的后门；**
e) **应要求研发单位提供硬件设计图，并审查硬件设计中可能存在的后门；**
f) 应根据研发单位提供的硬件设计图审查实物与设计是否一致。

6.2.2 安全运维管理

6.2.2.1 感知节点设备（包括 RFID）环境管理

本项要求包括：

a) 应指定人员定期巡视终端感知节点设备、网关节点设备的部署环境，对可能影响终端感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
b) 应记录终端感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关节点设备进行现场维护（除尘、充电、修理等）；
c) 应建立针对终端感知节点设备、网关节点设备部署环境的评估制度，编写可操作评估方法，并由专人完成评估；
d) 应制定终端感知节点设备、网关节点设备管理制度，对终端感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
e) **应加强对终端感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。**

6.2.2.2 感知节点设备（包括 RFID）备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
b) 应规定终端感知节点设备、网关节点设备备份信息的备份方式、备份频度、存储介质、保存期等。
c) **应根据终端感知节点设备、网关节点设备数据的重要性及其对系统运行的影响，制定终端感知节点设备、网关节点设备数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。**

7 第三级基本要求

7.1 技术要求

7.1.1 物理和环境安全

7.1.1.1 终端感知节点设备（包括RFID标签）的物理和环境安全

本项要求包括：

a) 感知节点设备所处的物理环境应该不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应该能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）；

c) **感知节点设备在工作状态所处物理环境应该不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；**

d) **关键感知节点设备应具有可供长时间工作的电力供应；**

e) **关键感知节点设备所处的物理环境应避免信号干扰。**

7.1.1.2 感知网关节点设备（包括RFID读写器）的物理和环境安全

本项要求包括：

a) 网关节点设备所在物理环境应该具备防火、防静电的能力；

b) 网关节点设备所在物理环境应该具备防潮、防水的能力；

c) 网关节点设备的主要部件进行固定，并设置明显的不易除去的标记；

d) **关键网关节点设备应具有持久的，稳定的电力供应能力；**

e) **关键网关节点设备所在物理环境应保证其具有良好的信号收发能力(尽量避免信道遭遇屏蔽)。**

7.1.2 网络和通信安全

7.1.2.1 数据源认证

本项要求包括：

a) 应确保信息来源于正确的感知节点设备；

b) **应确保感知节点设备没有被恶意注入虚假信息。**

7.1.2.2 感知节点设备访问控制

本项要求包括：

a) 应设置传感网入网访问控制，对感知节点设备接入网络资源设置访问控制机制，防止感知网资源被非法访问和非法使用；

b) 远程配置感知节点设备上软件应用时应当提供安全保护；

c) **访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。只有经过授权的软件应用才能被下载到感知节点设备上，只有合法用户可以通过外部接口提交关于感知节点设备的信息更改请求。**

7.1.2.3 异构网安全接入

本项要求包括：

a) 应建立异构网络的接入认证系统，实现安全的传输控制信息；

b) 应具有拒绝恶意节点的接入能力，保证合法节点不被恶意节点攻击而被拒绝接入，保证网络资源的可使用性；

c) **应确保异构网接入时转发数据的完整性和保密性；**

d) **应根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段。**

7.1.3 设备和计算安全

7.1.3.1 终端感知节点设备（包括 RFID 标签）的设备安全

本项要求包括：

a) **应具有对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别的能力；**

b) **应具有对连接的感知节点设备（包括路由节点）进行身份标识与鉴别的能力。**

7.1.3.2 感知网关节点设备（包括 RFID 读写器）的设备安全

本项要求包括：

a) **应控制外部接入网关的连接数量；**

b) **应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识与鉴别的能力；**

c) **应具备过滤非法节点和伪造节点所发送的数据的能力；**

d) **应具备防止非法节点重放合法节点的历史数据的能力。**

7.1.4 应用和数据安全

7.1.4.1 访问控制

本项要求包括：

a) 对远程登陆的用户具有认证功能，确保只有合法用户才能登陆；

b) 对远程登陆的用户服务应覆盖高峰时期的用户访问数量；

c) **应对远程用户的访问进行访问控制管理，严格管理不同用户所能访问的数据、访问权限（读、写、执行、转发）、和访问时效性。**

7.1.4.2 资源控制

应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。

7.1.4.3 在线更新

a) **授权用户应能够在设备使用过程中对关键密钥进行在线更新；**

b) **授权用户应能够在设备使用过程中对关键配置参数进行在线更新。**

7.1.4.4 抗数据重放

a) **应能够鉴别数据的新鲜性，避免历史数据的重放攻击；**
b) **应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。**

7.1.4.5 数据完整性

本项要求包括：

a) 应能够检测到重要数据（指令控制数据、业务数据）在传输过程中完整性受到破坏；
b) **应能够检测到重要数据（指令控制数据、业务数据）在存储过程中完整性受到破坏。**

7.1.4.6 数据保密性

本项要求包括：

a) 应采用密码技术对重要数据（指令控制数据、业务数据）实施机密性保护，确保这些数据在传输中的保密性；
b) **应采用密码技术对重要数据（指令控制数据、业务数据）实施机密性保护，确保这些数据在存储中的保密性。**

7.1.4.7 数据可用性

本项要求包括：

a) 应保证感知网络实体间通信数据的新鲜性；
b) 应提供重要数据的本地备份与重传功能；
c) **应提供关键感知网络节点冗余，保证系统的高可用性。**

7.2 管理要求

7.2.1 安全建设管理

7.2.1.1 自行研发感知节点设备（包括 RFID）

本项要求包括：

a) 应确保终端感知节点设备、网关节点设备的主要部件（芯片、电池、天线等）参数满足系统功能需求；
b) 应确保研发环境与实际运行环境物理分开，**研发人员和测试人员分离，测试数据和测试结果受到控制；**
c) 应制定软、硬件研发管理制度，明确说明研发过程的控制方法和人员行为准则；
d) **应制定传感节点自行研发安全规范，要求研发人员参照规范研发传感节点；**
e) 应确保提供软、硬件设计的相关文档和使用指南，并由专人负责保管；
f) **应确保对软、硬件设计资源库的修改、更新、发布进行授权和批准。**

7.2.1.2 外包研发感知节点设备（包括 RFID）

本项要求包括：

a) 应根据研发需求检测软、硬件质量；
b) 应要求研发单位提供软、硬件设计的相关文档和使用指南；

c) 应在软件安装之前检测软件包中可能存在的恶意代码；
d) 应要求研发单位提供软件源代码，并审查软件中可能存在的后门；
e) 应要求研发单位提供硬件设计图，并审查硬件设计中可能存在的后门；
f) 应根据研发单位提供的硬件设计图审查实物与设计是否一致。

7.2.2 安全运维管理

7.2.2.1 感知节点设备（包括 RFID）环境管理

本项要求包括：

a) 应指定人员定期巡视终端感知节点设备、网关节点设备的部署环境，对可能影响终端感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
b) **应指定部门负责终端感知节点设备、网关节点设备的部署环境的安全**，并配备安全管理人员记录终端感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关节点设备进行现场维护（除尘、充电、修理等）；
c) 应建立针对终端感知节点设备、网关节点设备部署环境的评估制度，编写可操作评估方法，并由专人完成评估；
d) 应制定终端感知节点设备、网关节点设备管理制度，对终端感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
e) 应加强对终端感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录、**工作人员离开现场时应确保作业现场没有包含敏感信息的纸质文档**等。

7.2.2.2 感知节点设备（包括 RFID）监控管理和安全管理中心

本项要求包括：

a) **应对终端感知节点设备、网关节点设备、通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；**
b) **应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；**
c) **应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。**

7.2.2.3 感知节点设备（包括 RFID）备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
b) **应建立备份与恢复管理相关的安全管理制度，**对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c) 应根据终端感知节点设备、网关节点设备数据的重要性及其对系统运行的影响，制定终端感知节点设备、网关节点设备数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法；

d) **应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；**

e) **应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。**

8 第四级基本要求

8.1 技术要求

8.1.1 物理和环境安全

8.1.1.1 终端感知节点设备（包括 RFID 标签）的物理和环境安全

本项要求包括：

a) 感知节点设备所处的物理环境应该不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应该能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域）；

c) 感知节点设备在工作状态所处物理环境应该不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；

d) **感知节点设备**应具有可供长时间工作的电力供应；

e) **感知节点设备**所处的物理环境应避免信号干扰。

8.1.1.2 感知网关节点设备（包括 RFID 读写器）的物理和环境安全

本项要求包括：

a) 网关节点设备所在物理环境应该具备防火、防静电的能力；

b) 网关节点设备所在物理环境应该具备防潮、防水的能力；

c) 网关节点设备的主要部件进行固定，并设置明显的不易除去的标记；

d) **网关节点设备**应具有持久的，稳定的电力供应能力；

e) **网关节点设备**所在物理环境应保证其具有良好的信号收发能力(尽量避免信道遭遇屏蔽)。

8.1.2 网络和通信安全

8.1.2.1 数据源认证

本项要求包括：

a) 应确保信息来源于正确的感知节点设备；

b) 应确保感知节点设备没有被恶意注入虚假信息。

8.1.2.2 感知节点设备访问控制

本项要求包括：

a) 应设置传感网入网访问控制，对感知节点设备接入网络资源设置访问控制机制，防止感知网资源被非法访问和非法使用。
b) 远程配置感知节点设备上软件应用时应当提供安全保护；
c) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。只有经过授权的软件应用才能被下载到感知节点设备上；只有合法用户可以通过外部接口提交关于感知节点设备的信息更改请求。
d) **应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；**
e) **应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。**

8.1.2.3 异构网安全接入

本项要求包括：

a) 应建立异构网络的接入认证系统，实现安全的传输控制信息；
b) 应具有拒绝恶意节点的接入能力，保证合法节点不被恶意节点攻击而被拒绝接入，保证网络资源的可使用性；
c) 应确保异构网接入时转发数据的完整性和保密性；
d) 应根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段；
e) **应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。**

8.1.3 设备和计算安全

8.1.3.1 终端感知节点设备（包括 RFID 标签）的设备安全

本项要求包括：

a) 应具有对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别的能力；
b) 应具有对连接的感知节点设备（包括路由节点）进行身份标识与鉴别的能力。

8.1.3.2 感知网关节点设备（包括 RFID 读写器）的设备安全

本项要求包括：

a) 应控制外部接入网关的连接数量；
b) 应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识与鉴别的能力；
c) 应具备过滤非法节点和伪造节点所发送的数据的能力；
d) 应具备防止非法节点重放合法节点的历史数据的能力。

8.1.4 应用和数据安全

8.1.4.1 访问控制

本项要求包括：

a) 对远程登陆的用户具有认证功能，确保只有合法用户才能登陆；
b) 对远程登陆的用户服务应覆盖高峰时期的用户访问数量；

c) 应对远程用户的访问进行访问控制管理，严格管理不同用户所能访问的数据、访问权限（读、写、执行、转发）、和访问时效性。

8.1.4.2 资源控制

本项要求包括：

a) 应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用；

b) **应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。**

8.1.4.3 在线更新

a) 授权用户应能够在设备使用过程中对关键密钥进行在线更新；

b) 授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

8.1.4.4 抗数据重放

a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

b) 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

8.1.4.5 抗功耗攻击

应采取措施避免功耗攻击。

8.1.4.6 设备工作状态信息保护

应采取措施避免设备工作状态信息被泄露。

8.1.4.7 数据完整性

本项要求包括：

a) 应能够检测到重要数据（指令控制数据、业务数据）在传输过程中完整性受到破坏；

b) 应能够检测到重要数据（指令控制数据、业务数据）在存储过程中完整性受到破坏。

8.1.4.8 数据保密性

本项要求包括：

a) 应采用密码技术对重要数据（指令控制数据、业务数据）实施机密性保护，确保这些数据在传输中的保密性；

b) 应采用密码技术对重要数据（指令控制数据、业务数据）实施机密性保护，确保这些数据在存储中的保密性。

8.1.4.9 数据可用性

本项要求包括：

a) 应提供重要数据的本地备份与重传功能；

b) 应提供关键感知网络节点和**通信线路冗余**，保证系统的高可用性；

c) 应保证感知网络实体间通信数据的新鲜性。

8.2 管理要求

8.2.1 安全建设管理

8.2.1.1 自行研发感知节点设备（包括 RFID）

本项要求包括：

a) 应确保终端感知节点设备、网关节点设备主要部件（芯片、电池、天线等）参数满足系统功能需求；
b) 应确保研发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
c) 应制定软、硬件研发管理制度，明确说明发过程的控制方法和人员行为准则；
d) 应制定终端感知节点设备、网关节点设备自行研发安全规范，要求研发人员参照规范研发传感节点；
e) 应确保提供软、硬件设计的相关文档和使用指南，并由专人负责保管；
f) 应确保对软、硬件设计资源库的修改、更新、发布进行授权和批准；
g) **应确保终端感知节点设备、网关节点设备的研发人员为专职人员，开发人员的开发活动受到控制、监视和审查。**

8.2.1.2 外包研发感知节点设备（包括 RFID）

本项要求包括：

a) 应根据研发需求检测软、硬件质量；
b) 应在软件安装之前检测软件包中可能存在的恶意代码；
c) 应要求研发单位提供软、硬件设计的相关文档和使用指南；
d) 应要求研发单位提供软件源代码，并审查软件中可能存在的后门**和隐蔽信道；**
e) 应要求研发单位提供硬件设计图，并审查硬件设计中可能存在的后门**和隐蔽信道；**
f) 应根据研发单位提供的硬件设计图审查实物与设计是否一致。

8.2.2 安全运维管理

8.2.2.1 感知节点设备（包括 RFID）环境管理

本项要求包括：

a) 应指定人员定期巡视终端感知节点设备、网关节点设备的部署环境，对可能影响终端感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
b) 应指定部门负责终端感知节点设备、网关节点设备的部署环境的安全，并配备安全管理人员记录终端感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关节点设备进行现场维护（除尘、充电、修理等）；
c) 应建立针对终端感知节点设备、网关节点设备部署环境的评估制度，编写可操作评估方法，并由专人完成评估；
d) 应制定终端感知节点设备、网关节点设备管理制度，对终端感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；

e) 应加强对终端感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录、工作人员离开现场时应确保作业现场没有包含敏感信息的纸质文档等；

f) 应对终端感知节点设备、网关节点设备的部署环境和办公环境实行统一策略的安全管理，**对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。**

8.2.2.2 感知节点设备（包括 RFID）监控管理和安全管理中心

本项要求包括：

a) 应对终端感知节点设备、网关节点设备、通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；

b) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；

c) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

8.2.2.3 感知节点设备（包括 RFID）备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c) 应根据终端感知节点设备、网关节点设备数据的重要性及其对系统运行的影响，制定终端感知节点设备、网关节点设备数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法；

d) 应建立控制数据备份和恢复过程的程序，记录备份过程，**对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场，**所有文件和记录应妥善保存；

e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；

f) **应根据终端感知节点设备、网关节点设备的备份技术要求，制定相应的灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。**

附 录 A
（规范性附录）
与 GB/T 22239.1-XXXX 的关系

采用物联网技术的信息系统首先应实现 GB/T 22239.1-#### 《信息安全技术 信息安全等级保护基本要求：第 1 部分 安全通用要求》提出的对信息系统的通用安全要求，在此基础上进一步实现本部分提出的扩展安全要求。

本部分与GB/T 22239.1-####的关系如下表。

类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	/	继承	继承	继承
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
	终端感知节点（包括 RFID 标签）	增加	增加	增加	增加
	感知层网关节点（包括 RFID 读写器）	增加	增加	增加	增加
网络和通信安全	网络架构	继承	继承	继承	继承
	通信传输	继承	继承	继承	继承
	边界防护	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	入侵防范	/	继承	继承	继承
	恶意代码防范	/	/	继承	继承
	安全审计	/	继承	继承	继承
	集中管控	/	/	继承	继承
	数据源认证	增加	增加	增加	增加
	异构网安全接入	增加	增加	增加	增加
	感知设备访问控制	/	增加	增加	增加
	组认证	/	/	增加	增加
设备和计算安全	身份鉴别	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	安全审计	/	继承	继承	继承
	剩余信息保护	/	/	继承	继承

类	子类	第一级	第二级	第三级	第四级
	入侵防范	继承	继承	继承	继承
	恶意代码防范	继承	继承	继承	继承
	资源控制	/	继承	继承	继承
	集中管控	/	/	继承	继承
	终端感知节点（包括 RFID 标签）的设备安全	/	/	增加	增加
	感知网关节点（包括 RFID 读写器）的设备安全	/	/	增加	增加
应用和数据安全	身份鉴别	继承	继承	继承	继承
	访问控制	增加	增加	增加	增加
	安全审计	/	继承	继承	继承
	软件容错	继承	继承	继承	继承
	资源控制	/	继承	增加	增加
	数据完整性	增加	增加	增加	增加
	数据保密性	/	增加	增加	增加
	数据备份恢复	继承	继承	继承	继承
	剩余信息保护	/	继承	继承	继承
	个人信息保护	/	继承	继承	继承
	数据生命周期保护	/	继承	继承	继承
	数据可用性	增加	增加	增加	增加
	数据可用性	增加	增加	增加	增加
安全策略和管理制度	安全策略	/	/	继承	继承
	管理制度	继承	继承	继承	继承
	制定和发布	继承	继承	继承	继承
	评审和修订	/	继承	继承	继承
安全管理机构和人员	岗位设置	继承	继承	继承	继承
	人员配备	继承	继承	继承	继承
	授权和审批	继承	继承	继承	继承
	沟通和合作	/	继承	继承	继承
	审核和检查	/	继承	继承	继承
	人员录用	继承	继承	继承	继承
	人员离岗	继承	继承	继承	继承
	安全意识教育和培训	继承	继承	继承	继承
	外部人员访问管理	继承	继承	继承	继承
系统安全建设管理	系统定级和备案	继承	继承	继承	继承
	安全方案设计	继承	继承	继承	继承
	产品采购和使用	继承	继承	继承	继承
	自行软件开发	/	继承	继承	继承
	外包软件开发	继承	继承	继承	继承
	工程实施	继承	继承	继承	继承

类	子类	第一级	第二级	第三级	第四级
	测试验收	继承	继承	继承	继承
	系统交付	继承	继承	继承	继承
	等级测评	/	继承	继承	继承
	服务供应商选择	继承	继承	继承	继承
	供应链管理	/	继承	继承	继承
	自行研发感知设备（包括 RFID）	增加	增加	增加	增加
	外包研发感知设备（包括 RFID）	增加	增加	增加	增加
系统安全运维管理	环境管理	继承	继承	继承	继承
	资产管理	/	继承	继承	继承
	介质管理	继承	继承	继承	继承
	设备维护管理	继承	继承	继承	继承
	漏洞和风险管理	继承	继承	继承	继承
	网络和系统安全管理	继承	继承	继承	继承
	恶意代码防范管理	继承	继承	继承	继承
	配置管理	/	继承	继承	继承
	密码管理	/	继承	继承	继承
	变更管理	/	继承	继承	继承
	备份与恢复管理	继承	继承	继承	继承
	安全事件处置	继承	继承	继承	继承
	应急预案管理	/	继承	继承	继承
	外包运维管理	/	继承	继承	继承
	监控和审计管理	/	继承	继承	继承
	感知设备（包括 RFID）环境管理	增加	增加	增加	增加
	感知设备（包括 RFID）监控管理和安全管理中心	/	增加	增加	增加
	感知设备（包括 RFID）备份与恢复管理	增加	增加	增加	增加

附 录 B
（规范性附录）
安全要求的使用

本部分中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为A）；其他通用安全保护类要求（简记为G），所有管理安全要求均为通用安全保护类要求。具体见表B。

表 B 安全要求及属性标识

技术/管理	分类	安全控制点	属性标识
技术要求	物理和环境安全	终端感知节点设备（包括RFID标签）的物理和环境安全	G
		感知网关节点设备（包括RFID读写器）的物理和环境安全	G
	网络和通信安全	数据源认证	S
		感知节点设备访问控制	S
		异构网安全接入	S
	设备和计算安全	终端感知节点设备（包括RFID标签）的设备安全	S
		感知网关节点设备（包括RFID读写器）的设备安全	S
	应用和数据安全	访问控制	S
		资源控制	A
		在线更新	S
		抗数据重放	G
		抗功耗攻击	A
		设备工作状态信息保护	A
		数据完整性	S
		数据保密性	S
		数据可用性	A
管理要求	安全建设管理	自行研发感知节点设备（包括RFID）	G
		外包研发感知节点设备（包括RFID）	G

技术/管理	分类	安全控制点	属性标识
	安全运维管理	感知节点设备（包括RFID）环境管理	G
		感知节点设备（包括RFID）监控管理和安全管理中心	G
		感知节点设备（包括RFID）备份与恢复管理	G

参 考 文 献

[1] GB/T 22239-2008信息安全技术网络安全等级保护基本要求