感知层安全（RFID安全）

感知层安全（RFID的安全）

感知层层安全，主要介绍RFID安全，包括RFID安全威胁和安全关键技术。

本章重点：RFID安全威胁和防护技术

本节内容：RFID安全威胁分析

1 感知层安全概述


信息处理
信息传输
信息采集
应用层
网络层
感知层
物联网应用
供应链管理
智能交通
工业控制
智能家居
物联网应用支撑子层
公共中间件
信息开放平台
“云计算”平台
服务支撑平台
移动通信网、广电网、互联网和其他专网
异构网融合
资源与存储管理
专用网络
远程控制
下一代承载网
M2M无线接入
移动通信网
互联网
传输层与信息采集层互通
组网与协同信息处理
远距离与近距离数据传输技术
自组织组网技术
协同信息处理技术
信息采集中间件技术
信息采集
传感器
一维/二维条码
RFID
多媒体信息
公共技术
编码技术
标识技术
解析技术
信息服务
安全技术
中间件技术

1 感知层安全概述

- 物联网在感知层采集数据时,其信息传输方式基本是无线网络传输,对这种暴露在公共场所中的信号如果缺乏有效保护措施的话,**很容易被非法监听、窃取、干扰**;而且在物联网的应用中,大量使用传感器来标示物品设备,由人或计算机远程控制来完成一些复杂、危险或高精度的操作,在此种情况下,物联网中的这些物品设备大多都是部署在无人监控的地点完成任务的,那么攻击者就会比较容易地接触到这些设备,从而可以对这些设备或其承载的传感器进行破坏,甚至通过破译传感器通信协议,对它们进行非法操控。
- 目前**感知层**的**两大关键技术**是**RFID技术**和**WSN技术**。
- 这里先介绍RFID系统的安全问题。

RFID技术

RFID（Radio Frequency Identification）技术，又称无线射频识别，是一种通信技术，可通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触。

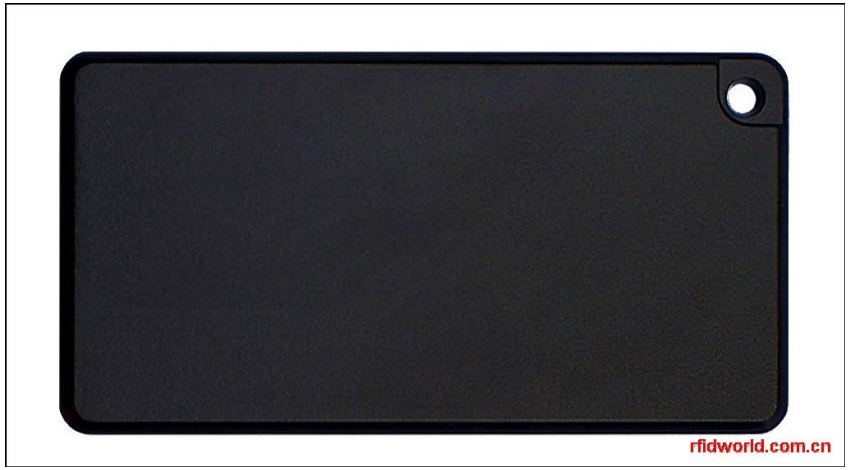
射频标签是产品电子代码（EPC）的物理载体，附着于可跟踪的物品上，可全球流通 并对其进行识别和读写。RFID（Radio Frequency Identification）技术作为构建“物联网” 的关键技术近年来受到人们的关注。

RFID 技术早起源于英国，应用于第二次世界大战中辨别敌我飞机身份，20 世纪 60 年代开始商用。

RFID技术

- 美国国防部规定 2005 年 1 月 1 日以后，所有军需物资都要使用 RFID 标签；
- 美国食品与药品管理局（FDA）建议制药商从 2006 年起利用 RFID 跟踪常 造假的药品。Walmart，Metro 零售业应用 RFID 技术等一系列行动更是推动了 RFID 在全世界的应用热潮。
- 欧盟统计办公室的统计数据表明，2010 年，欧盟有 3%的公司应用 RFID 技术，应用分布在身份证件和门禁控制、供应 链和库存跟踪、汽车收费、防盗、生产控制、资产管理。

认识RFID产品



认识RFID产品

认识RFID产品

图 1-3 RFID 手持阅读器

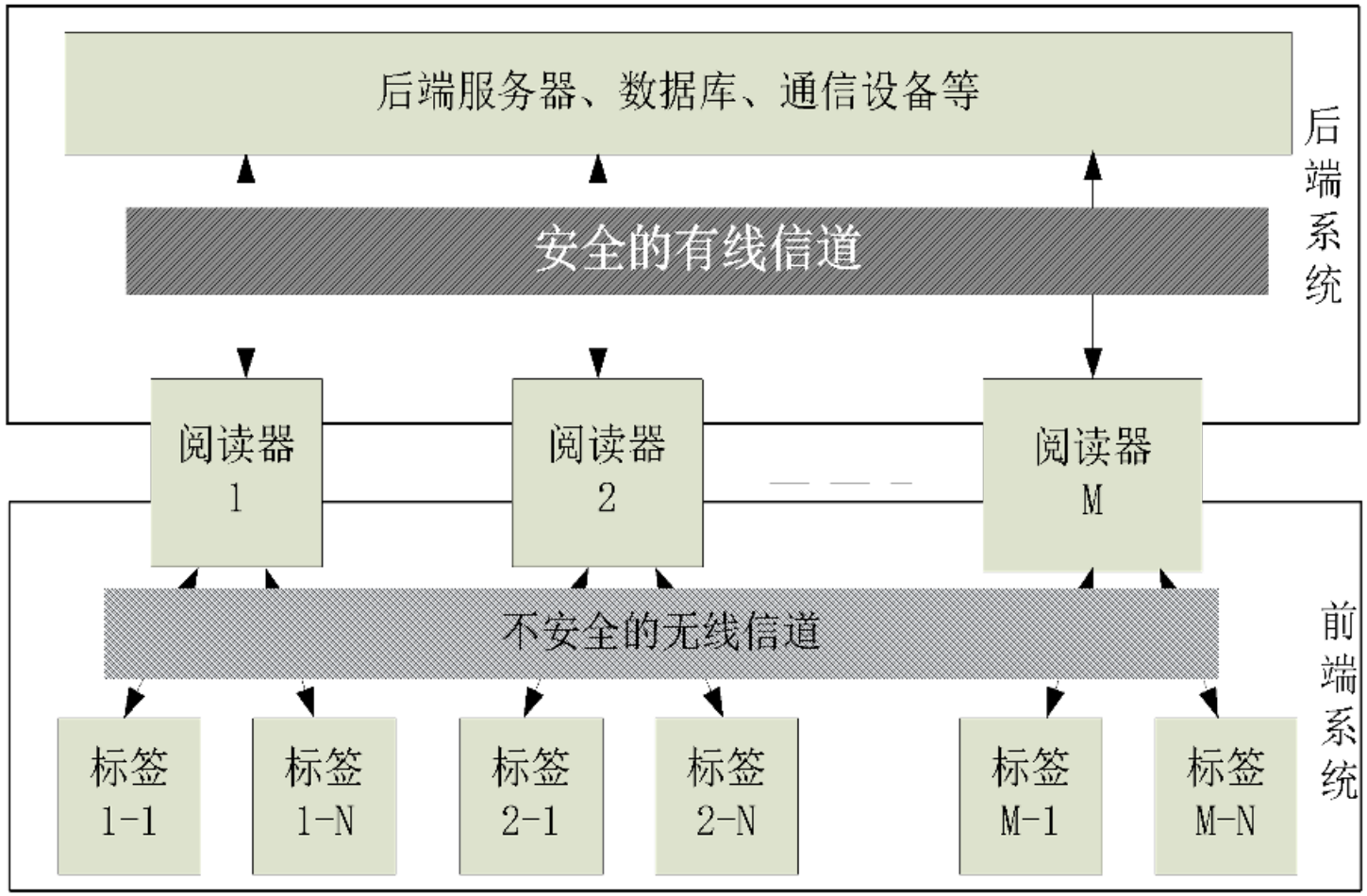
图 1-5 Intermec IF5
固定式 RFID 阅读器

图 1-4 内置天线的 RFID 移动阅读器

认识RFID产品

RFID应用系统构成

RFID技术是互联网、移动通信等技术的结合。RFID 应用系统的组成结构如图



RFID工作流程及原理

RFID系统因应用不同器组成会有所不同，但基本上由三部分组成：标签（Tag）、读写器（Reader）、后端系统。

1.标签：标签又称应答器，放置在要识别的物体上，携带目标识别数据，由耦合元件、调制器、编码发生器、时钟及存储器等微电子芯片组成。标签数据和信息通常要传递到读写器，然后转发至后端系统。后端系统也是通过阅读器和中间通信网络，实现物品（商品）的识别、跟踪和信息交互，以及对物品进行“透明”管理。

RFID工作流程及原理

标签按供电方式分类，主要有三类：

① 无源标签：本身不带电池，依靠读写器发出的电磁能供电，通常需要大功率读写器来提供能源。无源标签的特点是通信距离比较短，有的仅几厘米，但优点是重量轻、体积小、寿命长、成本低。目前，无源标签在购物、物流、购物和健康医疗等领域存在广泛使用。

② 有源标签：自带电池，电池能量可支持标签全部工作，不需读写器供电。有源标签特点是通信距离较长，可达几十米甚至上百米，具有较高的可靠性，但其缺点是为维持供电，需要占用较多的体积和重量，不适合在恶劣环境下工作，当使用时间较长是，传输距离会因电池电力消耗而缩短。同时，价格相对较高，大规模推广使用困难。

③ 半有源标签：自带电池，但电池仅支持数据电路及芯片工作，向读写器发送信号依然需要依靠读写器发出的电磁能。电池可维持几年，甚至可以长达10年，其信号传输范围以及硬件成本介于无源标签与有源标签之间。

RFID工作流程及原理

2.读写器：读写器又称响应器，是用于读或读/写标签数据的装置，由射频模块（发送器和接收器）、控制单元、电藕合单元组成[14][36]。读写器主要功能是获取后端系统命令，盘询标签，读取标签数据，将读取的标签数据发送后端系统，并进行信息交互与共享。读写器工作时通过天线发送射频信号，实现对标签的盘询，读写器通过射频接口来获取标签中的信息，并通过通信接口将其传递给后端系统，再进行相关信息的处理。

后端系统：后端系统包含各类服务器、数据库系统、业务应用系统等，主要用于存储、管理、查询标签信息，完成标签标识检测、读写器定位功能，提供业务应用服务等。后端系统接收来自读写器获得的标签数据，将数据存储到服务器数据库里，实现前端系统和后端系统的交互。

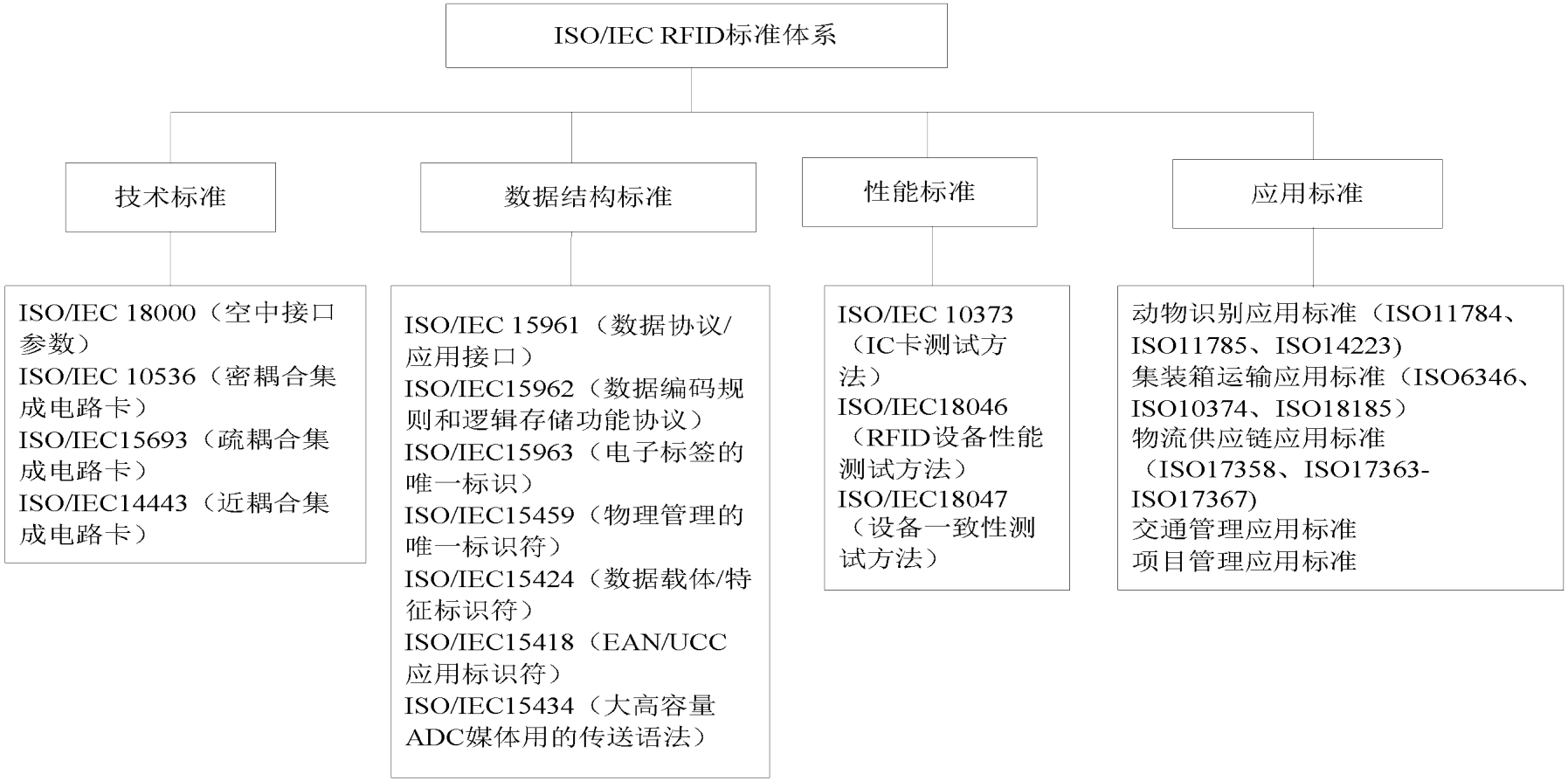
RFID频率

常见的RFID系统电磁信道频段分为低频、高频、超高频和微波

频率	设别距离	传输速率	受方向影响	现使用情况
低频 125-134KHz	<10cm	慢	无	价格便宜，大量使用
高频 156MHZ	<1m	中等	无	价格便宜，大量使用
超高频 433M 860-930MHZ	<10m	快	一般	价格便宜，大量使用
微波 2.45GHZ 5.8GHZ	>10m	很快	一般	价格较高，使用较少

RFID标准

目前主要采用的RFID标准体系有国际标准化组织ISO/国际电工委员会IEC的ISO/IEC标准、EPC标准和日本UID标准



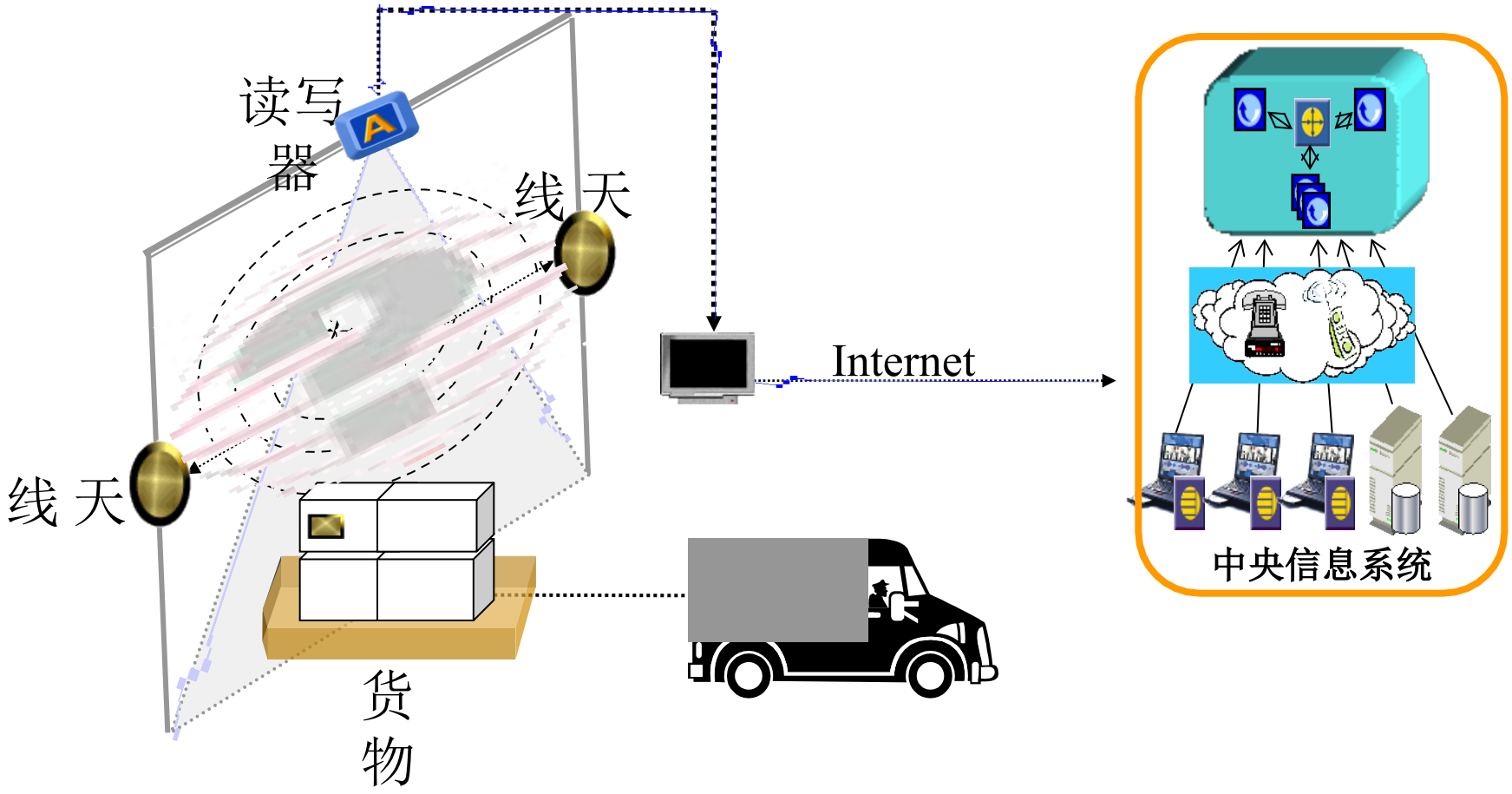
RFID标准

目前主要采用的RFID标准体系有国际标准化组织ISO/国际电工委员会IEC的ISO/IEC标准、EPC标准和日本UID标准

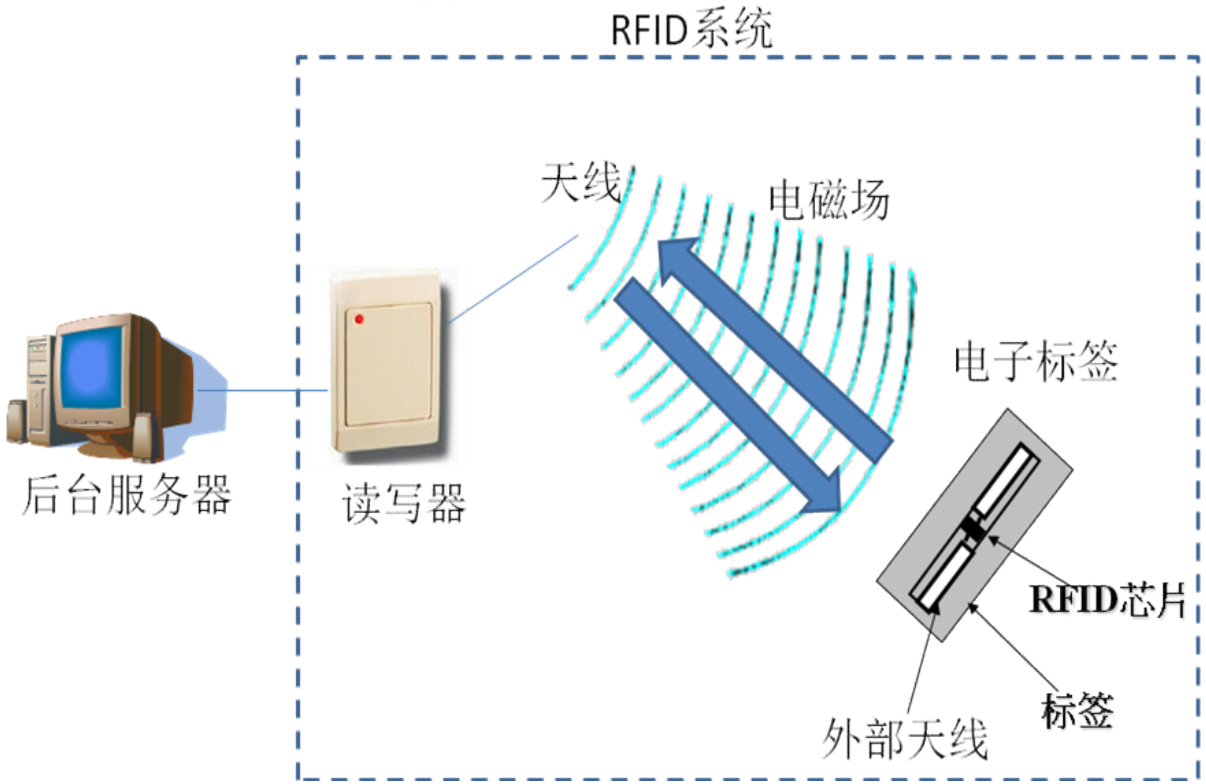
EPC Global是由美国主导，欧美参与制定的，是全球实力最大的物联网RFID标准组织。EPCglobal的RFID标准是一个应用标准，其特点是面向应用，特别是面向物流供应链领域。

EPCglobal标准体系包括数据标准、基础实施标准、物理对象交换标准，由EPCgloba体系框架内相应的具体标准支撑。EPC Global具体标准主要包括EPC 标签数据规范、EPC空中接口协议、EPC读写器数据协议、EPC读写器管理协议、EPCIS 询问接口协议、EPCIS 发现接口协议、标签数据转换框架、用户验证接口协议、物理标记语言PML等[。同时，EPCglobal 制定了标准开发过程规范，EPCglobal 各部门职责以及标准开发的业务流程。

RFID工作流程及原理



RFID工作流程及原理



RFID系统运行时，是后端系统、读写器和标签之间的交互。后端系统和读写器之间的互动与传统网络方式类似，读写器和标签之间的交互是通过读写器的天线与盘绕标签的天线建立的电磁场进行的。读写器和标签就利用这个电磁场进行通信的。读写器和标签之间的交互过程如图所示。

RFID工作流程及原理

- 工作原理
  - 标签进入磁场后，接收读写器发出的射频信号，凭借感应电流所获得的能量发送出存储在RFID芯片中的产品信息（Passive Tag，无源标签或被动标签），或者主动发送某一频率的信号（Active Tag，有源标签或主动标签）；读写器读取信息并解码后，送至中央信息系统进行有关数据处理。
  - 在实际应用中，标签附着在待识别物体的表面。阅读器可无接触地读取并识别电子标签中所保存的电子数据，从而达到自动识别体的目的。通常阅读器与电脑相连，所读取的标签信息被传送到电脑上进行下一步处理。

RFID工作流程及原理

- 工作流程
  - 读写器将无线电载波信号经过发射天线向外发射
  - 当电子标签进入发射天线的工作区域时，电子标签被激活，将自身信息的代码经过天线发射出去
  - 系统的接收天线接收电子标签发出的载波信号，经天线的调节器传输给读写器。读写器对接收到的信号进行解调解码，送往后台的电脑控制器
  - 电脑控制器根据逻辑运算判断该标签的合法性，针对不同的设定做出相应的处理和控制，发出指令信号控制执行机构的动作
  - 执行机构按照电脑的指令动作
  - 通过计算机通信网络将各个监控点连接起来，构成总信息平台，可以根据不同的项目设计不同的软件来完成要实现的功能

RFID系统性能指标

- 电子标签存储容量
- 数据传输速度
- 多标签可读写性
- 读写距离
- 连通性
- 工作温度
- 载码体——天线间的射频载波频率

2 RFID 安全

随着RFID技术应用的不断普及，RFID已经得到了广泛应用。由于**信息安全问题**的存在，**RFID应用尚未普及到**至为**重要的关键任务**中。没有可靠的信息安全机制，就无法有效保护整个RFID系统中的数据信息，如果信息被窃取或者恶意更改，将会给使用RFID技术的企业、个人和政府机关带来无法估量的损失。特别是对于**没有可靠安全机制的电子标签，会被邻近的读写器泄漏敏感信息，存在被干扰、被跟踪等安全隐患**。