

5 电子标签在一体化管理应用中的核心技术分析

将具有无线射频识别功能的电子标签有效应用到实体档案馆和数字档案馆档案安全中是一个复杂的过程。课题组认为需要在如下核心技术领域开展相关研究,从而有效推进实体档案与数字档案安全一体化管理系统的建设。

5.1 信息的传递

射频识别系统通常是由电子标签、读写器和天线、中间件以及计算机数据处理系统组成。射频识别系统的基本工作流程如下:

- (1) 读写器将无线电载波信号经过发射天线向外发射;
- (2) 当电子标签进入发射天线的工作区时,电子标签被激活,将自身信息的代码经天线发射出去;
- (3) 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,送往后台的计算机控制器;
- (4) 计算机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;
- (5) 执行机构按照计算机的指令动作;
- (6) 通过计算机通信网络将各个监控点连接起来,构成总控信息平台,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。

由上可见,在 RFID 系统中,信息的传递存在于两个环节,即读

写器和电子标签之间、以及读写器和计算机系统之间。如图 5-1 所示：

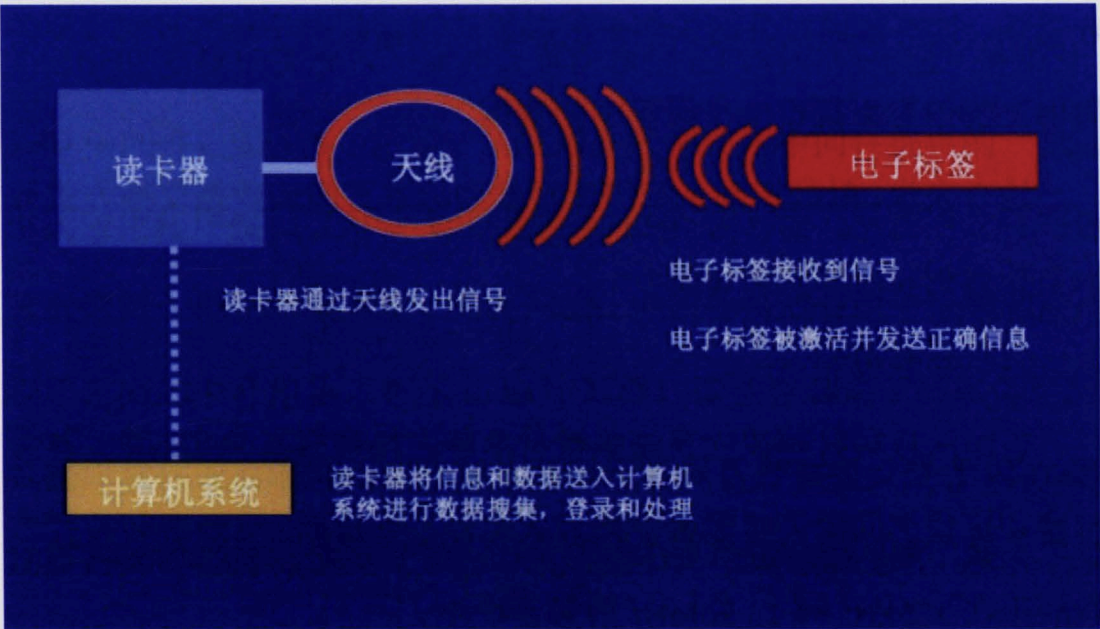


图 5-1 射频识别系统中的信息传递

5.1.1 读写器和电子标签之间的信息传递

在上文阐述射频识别技术的原理时，提到 RFID 技术利用电磁波进行信息传递和交流。读写器与电子标签通过各自的天线产生电磁场区。天线产生的电磁场区根据频率和电线的尺寸划分成两个部分：近场区与远场区。天线进场区是指引起空间中电场传输的天线附近的电磁区域，辐射场的角度分布与距离天线口径的距离有关。远场区是指电磁场和天线分离开来，以平面波的方式在空间传播。

电子标签和读写器之间的数据必须在可靠的方式下通信，可靠通信首先是对数据进行编码，其次是对信号的调制，然后接受信号并对信号进行解调。

读写器向一个或一个以上的电子标签发送信息，发送方式是采用

无线通信的方式调制射频载波信号。标签通过相同的调制射频载波接收功率。读写器通过发送未调制射频载波和接收电子标签反射（反向散射）的信息来接收电子标签中的数据。

综合来说，射频识别系统的读写器和标签之间的数据交换方式分为负载调制和反向散射调制。

（1）负载调制

近距离低频射频识别系统是通过准静态场的耦合来实现的。其读写器和标签之间的天线能量交换方式类似于变压器，负载调制方式广泛应用在 125KHz 和 13.56MHz 射频系统中。

（2）反向散射调制

在典型的远场，如 915MHz 和 2.45GHz 的射频识别系统中，阅读器和电子标签之间的距离有几米，而载波波长仅有几到几十厘米。阅读器和电子标签之间的能量传递方式为反向散射调制。

反向散射调制技术是指无源 RFID 电子标签将数据发送回读写器所采用的通信方式，是采用反射电磁波能量的方式完成通信的。电子标签平时处于匹配状态，它从读写器发射来的电磁场中获取能量和信息。而当电子标签发送数据时，微控器根据数据的不同改变 RFID 电子标签天线的负载电阻值，从而改变天线的散射面积。这样就会使读写器天线接受到的电磁波能量随数据的变化而变化，最终完成电子标签与读写器的通信。

5.1.2 读写器和计算机系统之间的信息传递

RFID 系统中实现读写器和计算机系统之间的信息传递，离不开 RFID 中间件，如图 5-2 所示，从应用程序端使用中间件提供的一组通用的应用程序接口（API）即能连接到 RFID 读写器，从而通过读写器读取或写入电子标签数据。因此，RFID 中间件扮演着电子标签和应用程序之间的中介角色。有了 RFID 中间件，即使存储电子标签信息的数据库软件或后端应用程序增加或改由其他软件取代，或者 RFID 阅读器种类的增加等情况发生时，应用端不需修改也能处理，解决了多对多连接的维护复杂性问题。

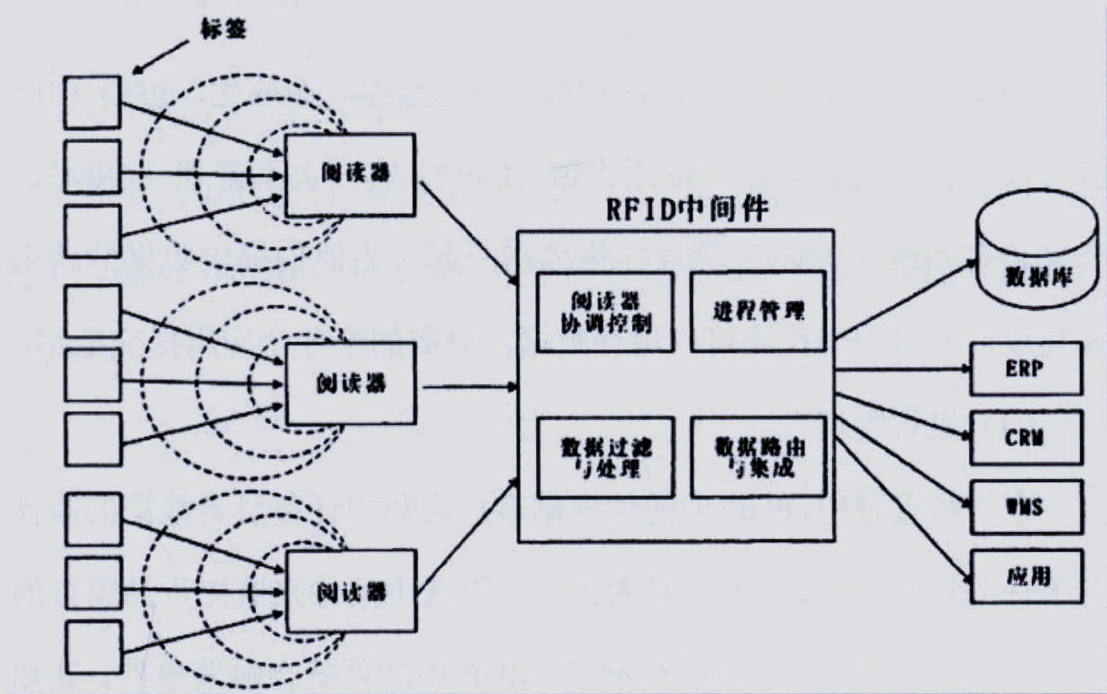


图 5-2 RFID 中间件

RFID 中间件主要包括以下 4 个功能：

(1) 阅读器协调控制

终端用户可以通过 RFID 中间件接口直接配置、监控以及发送指

令给阅读器。例如终端用户可以配置阅读器,使得当频率碰撞发生时,阅读器自动关闭。一些 RFID 中间件开发商还提供了支持阅读器即插用的功能,使终端用户新添加不同类型的阅读器时不需要增加额外的程序代码。

(2) 数据过滤与处理

当标签信息传输发生错误或有多余数据发生时,RFID 中间件可以通过一定的算法纠正错误并过滤掉多余的数据。RFID 中间件可以避免不同的阅读器读取同一电子标签的碰撞,确保了高于阅读器水平的数据准确率。

(3) 数据路由与集成

RFID 中间件能够决定采集到数据传递给哪一个应用。RFID 中间件可以与企业现有的企业资源计划(ERP)、客户关系管理(CRM)、仓储管理系统(WMS)等软件集成在一起,为他们提供数据的路由和集成,同时中间件还可以保存数据,分批的给各个应用提交数据。

(4) 进程管理

在进程管理中,RFID 中间件根据客户定制的任务负责数据的监控与事件的触发。例如,在仓储管理中,设置中间件来监控货品库存的数量,当库存量低于设置的标准时,RFID 中间件就会触发事件,通知相应的软件。

当前许多公司正在开发有效的平台来更好地管理和利用 RFID 数据,通过开发性能良好的中间件来提高存储和查询效率。中间件可放置在 RFID 网络的端点上,也可以放置在中心服务器,加快数据的采

集、存储和查询。中间件可看作是 RFID 系统运作的中枢，独立并介于 RFID 阅读器与后端应用程序之间，能够与多个阅读器及后端应用程序连接以减轻构建与维护 RFID 系统的复杂性。除此以外，中间件还与其他应用层协同工作，读取数据并将数据送到数据库系统，许多中间件还解决 RFID 系统的数据安全性问题。中间件扮演者“控制中心”的角色，能够提高数据存储、查询和运行效率，并使整个运作流程有着更高的可视性和控制。

5.2 存储

5.2.1 标签数据存储

对于每个厂商生产的电子标签，其存储器的结构是相同的，但会存在容量大小的差别。在逻辑上来说，一个电子标签分为四个存储体，每个存储体可以由一个或一个以上的存储字组成，其存储逻辑如图 5-3 所示：

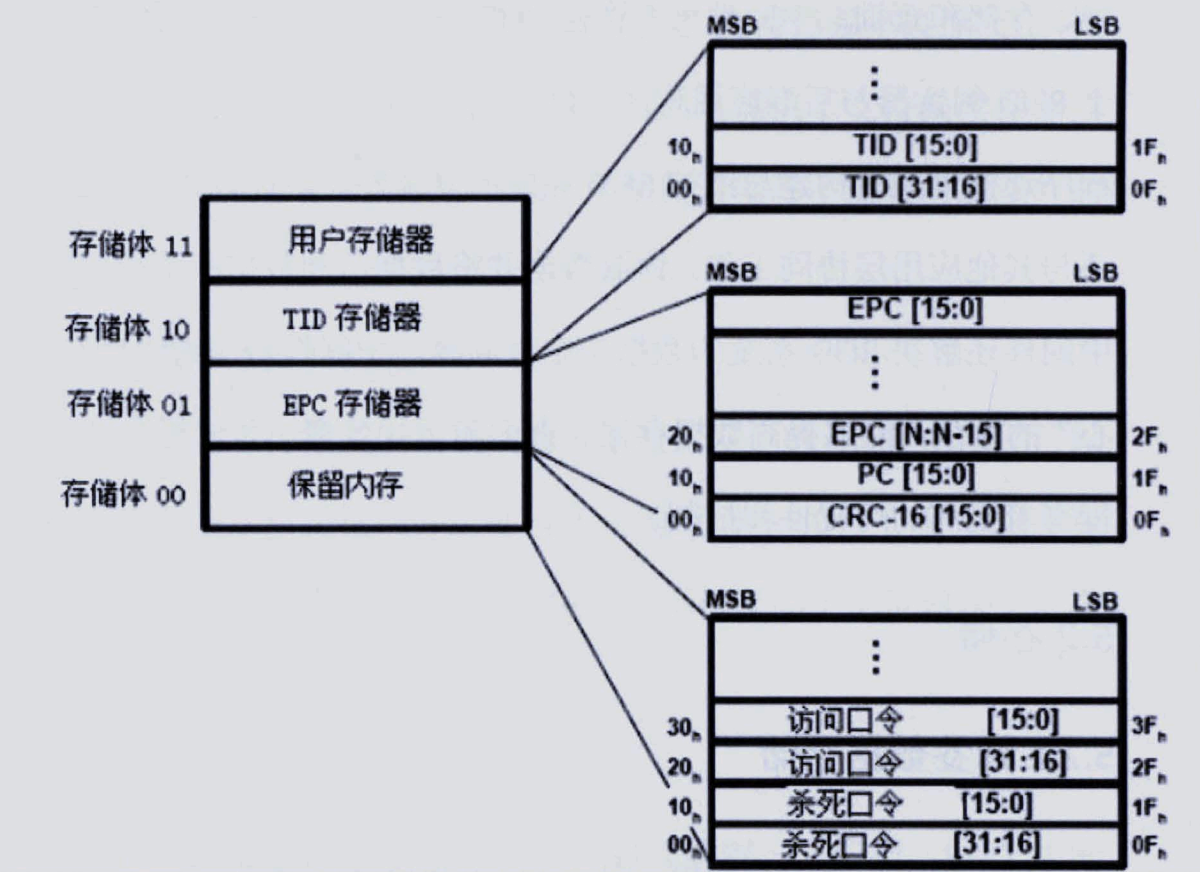


图 5-3 电子标签存储器结构图

从以上结构图中可以看到，一个电子标签的存储器分成四个存储体，分别是：

- ✧ 存储体 0：保留内存（Reserver）
- ✧ 存储体 1：EPC 存储器
- ✧ 存储体 2：TID 存储器
- ✧ 存储体 3：用户自定义存储器

（1）保留内存。保留内存为电子标签存储密码（口令）的部分。包括灭活口令和访问口令。灭活口令和访问口令都为 4 个字节。

（2）EPC 存储器。EPC 存储器用于存储电子标签的 EPC 号、PC（协

议-控制字)以及这部分的 CRC-16 校验码。其中, CRC-16 为本存储体中存储内容的 CRC 校验码。PC 表明本电子标签的控制信息。EPC 号为识别标签对象的电子产品码,该 EPC 号长度在以上 PC 值中来指定。每类电子标签(不同厂商或不同型号)的 EPC 号长度可能会不同。用户通过该存储器内容命令读取 EPC 号。

(3) TID 存储器。该存储体是指电子标签的产品类识别号,每个生产厂商的 TID 号都会不同。用户可以在该存储区中存储其自身的产品分类数据及产品供应商的信息。一般来说, TID 存储区的长度为 4 个字, 8 个字节。但有些电子标签的生产厂商提供的 TID 区会为 2 个字或 5 个字。

(4) 用户存储器。该存储区用于存储用户自定义的数据。用户可以对该存储区进行改、写操作。该存储区的长度由各个电子标签的生产厂商确定。每个生产厂商提供的电子标签,其用户存储区的长度会不同。

由电子标签供应商提供的标签为空白标签,用户首选会在电子标签的初始化时,通过读写器将相关数据存储在电子标签中(初始化)。然后在标签的流通使用过程中,通过读取标签存储器的相关信息,或将某状态信息写入到电子标签中。

对于电子标签的四个存储区,读写器提供的存储命令都能支持对其的读写操作。但有些电子标签在出厂时就已由供应商设定为只读,而不能由用户自行改写。

对一般的 RFID 系统来说,使用电可擦可编程只读存储器

(EEPROM) 来存储数据是主要方法。对微波系统来说, 还使用静电随机存取存储器 (SRAM), 存储器能很快写入数据。为了永久保存出具, 需要用辅助电池作不中断的供电。

江苏省太仓市档案馆 RFID 档案实时追踪管理系统选用的电子标签拥有 128bit 的用户内存以及 496bit 的 EPC 内存, 扩大的用户内存提供可随标签移动的便携但专用的数据库, 支持不能进行可靠数据库连接的应用。扩展的 EPC 内存符合需要大于 96 比特 EPC 码的要求。

5.2.2 数据库数据存储

江苏省太仓市档案馆 RFID 档案实时追踪管理系统采用 Oracle 10g 数据库。Oracle 是目前最流行的关系型数据库管理系统, 被越来越多的用户在信息系统管理、企业数据处理、Internet、电子商务网站等领域作为应用数据的后台处理系统。其突出的优点包括: 支持多用户、大事物量的事物处理; 数据安全性和完整性的有效控制; 支持分布式数据处理; 可移植性很强。

数据库的存在一定需要有永久性存储方式和介质。Oracle 自然也不例外, 在 Oracle10g 中, 有 4 种存储形式, 分别是操作系统文件、裸分区、自动存储管理和集群系统 OCFS (RAC)。下面分别说一下这 4 种存储形式。

(1) 操作系统文件。这种是大家最常用的方式, 也是非商业运行模式 (比如开发或者开发阶段的测试环境) 下最常用的形式。当安装 Oracle 的时候, 如果选用了操作系统文件的存储形式, 那么就会把

Oracle 的数据存储在操作系统中，以文件的形式存在。用文件形式存储数据，带来的优点就是易于数据库移动。比如把 Oracle 的数据文件直接复制到一台电脑上，就可以很快复制出一个一样的数据库系统出来。在文件的读写的时候，操作系统通常会提供缓存形式进行读写，避免过多读写硬盘对磁盘造成很大伤害。所以用操作系统文件形式存储数据，等于先天性获得了操作系统的缓存功能。

(2) 裸分区。裸分区就是把数据库直接写在磁盘上，不再经过操作系统这一层，Oracle 专门来对这个分区进行读写。因为有了操作系统这一层，所以读写起来的速度和性能是质一般的飞跃的，在某些对 Oracle 读写非常频繁的数据库应用中，采用裸分区形式存储数据甚至可以提高 30% 以上的性能。

(3) 自动存储管理。自动存储管理通常也被称为 ASM，是在 Oracle 10g 以后才提供的一种新的存储形式。这种存储形式似乎是前两种存储形式的折中。既不是用的 host 操作系统的文件系统，也不是裸分区的形式直接由 Oracle 读写。而是可以看作是一种 Oracle 特有的文件系统形式。在 ASM 上可以存储数据文件，控制文件、日志文件等等，在 ASM 中，这些也是以文件的形式存在的，只不过这个时候的文件格式是 Oracle 自有的 ASM 形式。

(4) 集群系统 OCFS (RAC)。RAC 的全称是 Real Application Cluster，是一种在集群的环境下实现共享的一种数据库存储形式。OCFS 是一种无断点恢复的存储形式，在整体给人的感觉就是每台数据服务器都有自己的文件系统，但是这些文件系统又仿佛只是同一个文件系统，

因为数据更新或者其他的操作都是很统一的。即使某台电脑出了问题，其余的服务器照样运行，不会出现数据库的异常，而如果想新加入一台服务器也是很简单的事。特别适合于商用的 7X24 这种服务形式。

在该项目中，数据库数据的存储形式采用的是最常用的操作系统文件形式。

5.3 安全保密

随着 RFID 技术市场走过了初级阶段，与之相关的 RFID 系统的安全性问题也随之产生，即在使用 RFID 系统过程中如何确保其安全性和隐私性，不至于导致个人信息、业务信息和财产等丢失或被他人盗用。

由于集成的 RFID 系统实际上是一个计算机网络应用系统，因此安全问题类似于计算机和网络的安全问题，但它仍然有两个特殊的特点：首先，RFID 标签和后端系统之间的通信是非接触和无线的，使它们很易受到窃听；其次，标签本身的计算能力和可编程性，直接受到成本要求的限制。一般地，RFID 的安全威胁除了与计算机网络有相同之处外，还包括以下三种类型：

(1) 标签中数据的安全威胁

由于标签本身的成本所限，标签本身很难具备能够足以保证安全的能力。这样，就面临了很大的问题。非法用户可以利用合法的阅读器或者自构一个阅读器，直接与标签进行通信。这样，就可以很容易

地获取标签内所存数据。而对于读写式标签，还面临数据被篡改的风险。

(2) 通信链路上的安全威胁

当标签传输数据给阅读器，或者阅读器质询标签的时候，其数据通信链路是无线通信链路，无线信号本身是开放的。这就给非法用户的侦听带来了方便。实现的常用方法包括：非法截取通信数据；非法用户通过发射干扰信号来堵塞通信链路；利用冒名顶替标签来向阅读器发送数据，真实的数据则被隐藏；通过发射特定电磁波破坏标签等。

(3) 阅读器协议的安全威胁

阅读器协议的安全威胁主要有三个方面：物理攻击，通过物理方式侦测或者修改读写器；修改配置文件或者特征配置文件；窃听、修改和干扰读写器和 HOST(与 EPC 兼容的应用程序)之间交换的数据。

RFID 所遇到的安全问题，要比通常的计算机网络安全问题要复杂的多。通过分析 RFID 系统的安全威胁，受到非授权攻击的数据可能保存在标签中、阅读器中，或者当数据在各个组件之间传输时，我们必须采取相应的对策解决。

5.3.1 标签中数据安全对策

为了防止 RFID 标签泄露私密信息，人们从技术上提出了多种方案。如下表所示：

方法名称	描述
Kill 标签	物品交付给最终用户时，通过 Kill 指令杀死标签，标签无法再次被激活

法拉第网罩	将贴有 RFID 标签的物品放入由金属网罩或金属箔片组成的容器中，从而阻止标签和阅读器的通信
主动干扰	用户使用能够主动广播干扰信号的设备，干扰对受保护标签的读取
智能标签	增加标签的处理能力，利用加密技术进行访问控制，保护标签信息
阻止标签	使用一个特殊的标签（称为阻止标签）对阅读器的读取命令总应答相同的数据，从而保护用户标签
Hash 锁	通过简单的 hash 函数，增加闭锁和开锁状态，对标签与阅读器之间的通信进行访问控制
辅助标签	当 RFID 标签被无线方式修改难以识别时，利用条形码、十进制码或产品标志等，可增加辅助识别。
用户密码	用户需要了解产品的附属性能和跟踪信息时，通过用户密码获取
解码器	通过在解码器内产生一个高压脉冲信号，使标签内的电容击穿，从而解码失效
阻塞器标签	一种内置在购物袋中的专门设计的 RFID 标签，能发动 DoS 攻击，防止 RFID 阅读器读取袋中所购货物上的标签
软阻塞器标签	（阻塞器标签的改进）在销售点通过会员卡可看到隐藏的信息，购买后，销售点更新隐私信息，提示某些阅读器如供应链阅读器不要读取该信息

当然还可以使用各种认证和加密手段来确保标签和阅读器之间的数据安全。比如，直至阅读器发送一个密码来解锁数据之前，标签的数据一直处于锁定状态。更严格的还可能同时包括认证和加密方案。但是标签的成本直接影响到其计算能力以及采用的算法的强度。在现实生活中选择射频识别系统时，应该根据实际情况考虑是否选择有密码功能的系统。因此，一般来说，在高端 RFID 系统(智能卡)和高价值的被标签物品场合，可以采用这种方式。

最新的 RFID 标准重新设计了 UHF(超高频)空中接口协议，该协议用于管理从标签到读卡器的数据的移动，为芯片中存储的数据提供了一些保护措施。新标准采用“一个安全的链路”，保护被动标签免于受到大多数攻击行为。当数据被写入标签时，数据在经过空中接

口时被伪装。从标签到读卡器的所有数据都被伪装，所以当读卡器在从标签读或者写数据时数据不会被截取。一旦数据被写入标签，数据就会被锁定，这样只可以读取数据，而不能被改写，就是具有我们常说的只读功能。

5.3.2 各组件通信链上数据安全对策

(1) 限制标签和阅读器之间的通信距离。采用不同的工作频率、天线设计、标签技术和阅读器技术可以限制两者之间的通信距离，降低非法接近和阅读标签的风险，但是这仍然不能解决数据传输的风险，还以损害可部署性为代价。

(2) 实现专有的通信协议。在高度安全敏感和互操作性不高的情况下，实现专有通信协议是有效的。它涉及到实现一套非公有的通信协议和加解密方案。基于完善的通信协议和编码方案，可实现较高等级的安全。但是，这样便丧失了与采用工业标准的系统之间的 RFID 数据共享能力。当然，还可以通过专用的数据网关来进行处理。

(3) 为 RFID 标签编程，使其只可能与已授权的 RFID 阅读器通信。解决办法是，确保网络上的所有阅读器在传送信息给中间件(中间件再把信息传送给应用系统)之前都必须通过验证，并且确保阅读器和后端系统之间的数据流是加密的。部署 RFID 阅读器时应采取一些非常切合实际的措施，确保验证后方可连入网络，并且不会因为传输而被其他人窃取重要信息。

5.3.3 保护阅读器中数据安全对策

在 RFID 系统中，阅读器只是一个简单的读写设备没有太多的安全功能，因此阅读器中数据采集的安全问题必须依靠中间件来解决。中间件的安全对策与计算机网络系统有相同之处这里不再赘述。攻击者要想对阅读器进行攻击，多数情况是必须至少得和阅读器接触，所以保护数据安全除了不断推进加密技术来应对之外，还要依靠安全的管理制度，完备的数据管理模式，依靠数据的管理者持续的工作来保持数据的安全性，所以保密是一个过程。

5.3.4 数据库数据安全对策

随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为如今关注的一个话题。

信息安全中，安全策略主要是维护数据信息的完整性、保密性和可用性。因此，数据库的安全策略将主要围绕这三点进行，包括物理安全、访问控制、数据备份和应急响应等。

(1) 物理安全

保证物理安全是安全防范的基本。这主要是指保证数据库服务器、数据库所在环境、相关网络的物理安全性。比如：是否能够保证服务器所在网络的网线、交换机等环境的物理安全；是否只有数据库管理员能够在物理上接触数据库服务器；是否能够确保避免通过社会工程学的手段来欺骗或者诱导从而能获得物理上的访问能力等等。

（2）访问控制

访问控制是基本安全性的核心。它包括了帐号管理、密码策略、权限控制、用户认证等方面，主要是从与帐号相关的方面来维护数据库的安全性。访问控制策略主要包括：

- ◇ 避免帐号被人列举。比如，非管理员获得所有数据库用户帐号列表。

- ◇ 最小化权限原则。数据库管理员仅仅分配帐号的足够使用权限。比如，如果一个用户只需要进行数据库的查询工作，那么这个用户使用的权限就只能局限于 `select` 语句，而不能有 `delete`、`update` 等语句的使用权限。权限的扩散以及超越应用范围的访问是访问控制的一大威胁。

- ◇ 最高权限最小化原则。确保不会分配多余的管理员权限帐号。管理员帐号的数量和安全危险性是成正比的。

- ◇ 帐号密码安全原则。分配帐号的密码必须符合密码安全原则的要求。基本密码安全要求包括：密码长度（8 位以上）、密码复杂性（必须同时包括字母、数字和符号）、密码结构非连续性（密码构成内容必须是在键盘上分别隔离的元素，1234%qwerty 这样的密码结构

就是不符合要求的)等。有条件的或者有非常高安全要求的环境甚至可以采用一次性密码。密码的安全性是访问控制的主要威胁,特别是最高管理员,比如 system 帐号的密码。

✧ 用户认证是否足够安全。密码是否经过加密,确保认证过程的密码安全性,用户认证过程是否有日志记录。Oracle 默认情况下,数据的传输是明文的,包括密码(只是经过非常简单的编码),因此,有必要情况下必须采用比如 SSL 加密。

✧ 详尽的访问审核。访问审核能够为损害等提供可查依据。Oracle 提供了详尽的审核功能,比如:SQL 语句、角色添加删除、表空间维护、登录事件的成功失败、对象的使用、语句权限的使用、密码更改、数据库事件、锁事件、存储过程事件以及服务关闭启动等等。Oracle 数据库提供了 SQL 事件探查器,可以用来监视这些事件等。

✧ 文件的访问控制。确保文件不会被人修改、删除。这些文件包括数据库系统文件、数据库文件、日志文件以及备份文件等。

(3) 数据备份

定期的进行数据备份是减少数据损失的有效手段,能让数据库遭到破坏(恶意或者误操作)后,恢复数据资源。这也是数据库安全策略的一个重要部分。Oracle 备份和还原组件为存储在 Oracle 数据库中的关键数据提供重要的保护手段。可以从多种故障中恢复,包括:媒体故障,用户错误,服务器永久丢失。

制订适合自己的数据库备份策略,必须确定数据的可用性要求。总体备份策略包括备份的类型和频率以及所需的硬件特性和速度。最好能

够测试备份和恢复过程，有助于确保拥有从各种故障中恢复所需的备份，并且当真正的故障发生时可以快速平稳地执行恢复过程。

制订过程中需要根据自己的实际情况来确定备份周期等，比如：服务器故障时间将造成多大的经济损失；重新创建丢失的数据的难易程度如何；如果遇到媒体故障，如磁盘驱动器发生故障，可接受的故障时间是多长；一旦发生灾难，如因火灾丢失服务器，可接受的故障时间是多长；什么时候大量使用数据库，导致频繁的插入和更新操作，等等。

（4）应急响应

正确的事件响应机制应是总体安全策略和降低风险战略的不可分割的一部分。对安全事件及时做出响应有直接的好处，这是很显然的。当然完全防止所有安全问题的发生是不可能的，所以当安全问题出现的时候，需要确保它能造成的损失和影响最小。可以采取这样的措施使安全问题的数量和影响最小化。这就包括：

✧ 明确地建立并实施所有策略和步骤。许多安全问题是人为无意间造成的，可能是因为没有遵守或不理解更改管理过程，或者对安全设备配置不当。

✧ 建立安全事件响应小组。小组成员负责处理所有安全事件。每个成员都应有明确定义的职责，以确保能对每一个问题做出及时响应。

✧ 收集整理出所有相关人员或者公司的通讯信息。应确保有他们的联系人姓名和电话号码，比如事件响应小组成员的通讯信息。甚至

需要地方和国家执法机关的详细信息，有助于确保知道通过什么步骤通报事件和收集证据。当应急情况发生的时候，可以按照下面这些步骤由应急小组成员或者管理员指定：

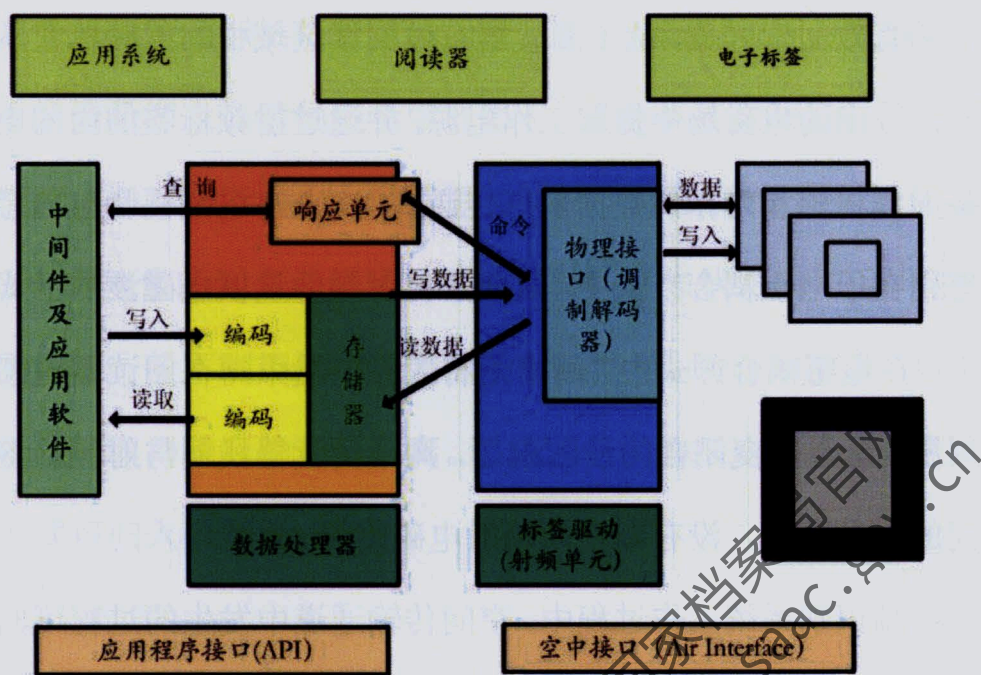
- 作出初步评估，并通报发生的事件
- 立刻控制损失/将风险减到最小，并确定破坏的类型和严重程度
- 保护证据，并通知其他机构等
- 恢复系统
- 编写和整理事件记录资料，评估事件的破坏和损失代价
- 总结响应过程并更新策略。

6 实体档案与数字档案一体化管理模型分析及应用

6.1 无线射频电子标签管理功能模型

射频识别技术实际上是自动识别技术（AEI, Automatic Equipment Identification）在无线电技术方面的具体应用与发展。该项技术的基本思想是，通过采用一些先进的技术手段，实现人们对各类物体或设备（人员、物品）在不同状态（移动、静止或恶劣环境）下的自动识别和管理。

典型的射频识别系统通常是由电子标签、读写器和天线、中间件以及计算机数据处理系统（应用软件）4个部分组成，一般我们把中间件和应用软件统称为应用系统。射频识别系统的基本功能模型如图3-1所示：



无线射频识别系统的基本功能模型

在介绍射频识别系统的工作原理时，提到射频识别系统工作过程中，空间传输通道中发生的过程可归结为三种事件模型，下面就以此三种事件模型的描述来介绍射频识别系统典型的工作方式与工作流程，从而进一步勾勒出射频识别系统的基本功能模型。

射频标签与阅读器（读写器）之间通过两者的天线架起空间电磁波传输的通道。细分射频标签与阅读器之间的电磁耦合，包含两种情况：即近距离的电感耦合与远距离的电磁耦合。在电感耦合方式中，阅读器一方的天线相当于变压器的初级线圈，射频标签一方的天线相当于变压器的次级，因而也称电感耦合方式为变压器方式。电感耦合方式的耦合中介是空间磁场，耦合磁场在阅读器线圈初级与射频标签次级之间构成闭合回路。电感耦合方式是低频近距离无接触射频识别系统的一般耦合原理。在电磁耦合方式中，阅读器的天线将阅读器产生的读写射频能量以电磁波的方式发送到定向的空间范围内，形成阅读器的有效阅读区域，位于阅读器有效阅读区域中的射频标签从阅读器天线发出的电磁场中提取工作电源，并通过射频标签的内部电路及标签天线将标签内存的数据信息传送到阅读器。电磁耦合与电感耦合的差别在于电磁耦合方式中，阅读器将射频能量以电磁波的形式发送出去；在电感耦合方式中，阅读器将射频能量束缚在阅读器电感线圈的周围，通过交变闭合的线圈磁场，沟通阅读器线圈与射频标签线圈之间的射频通道，没有向空间辐射电磁能量。

射频识别系统工作过程中，空间传输通道中发生的过程可归结为三种事件模型，如图 3-2 所示：

- (1) 数据交换是目的；
- (2) 时序是数据交换的实现方式；
- (3) 能量是时序得以实现的基础。

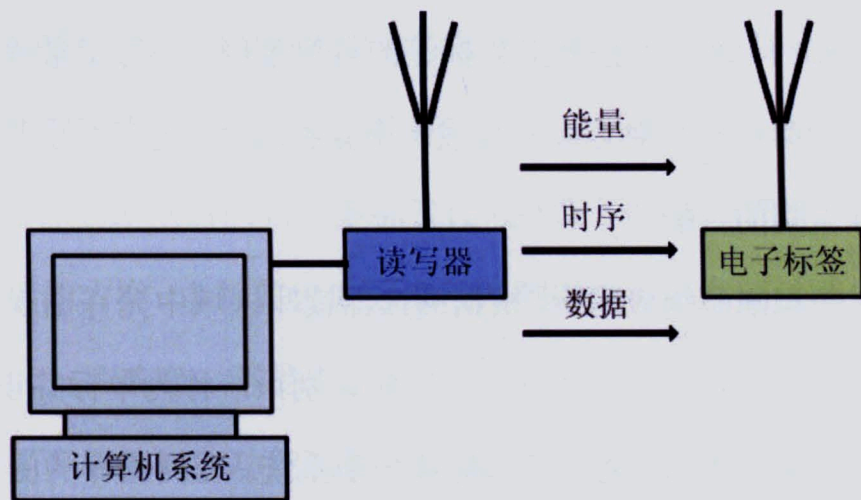


图 3-2 射频识别系统的三种事件模型

下面以此三种事件模型的描述来详细介绍射频识别系统的典型工作方式与工作流程。

(1) 能量

阅读器向射频标签供给射频能量。对于无源射频标签来说，其工作所需的能量即由该射频能量中取得（一般由整流方法将射频能量转变为直流电源存在标签中电容器里）；对于有源或半有源射频标签来说，该射频能量的到来起到了唤醒标签转入工作状态的作用。完全有源射频标签一般不利用阅读器发出的射频能量，因而阅读器可以较小的能量发射取得较远的通信距离。移动通信中的基站与移动台之间的通信方式可归入该类模式。

(2) 时序

对于双向系统（阅读器向射频标签发送命令与数据、射频标签向

阅读器返回所存存储的数据)来说,阅读器一般处于主动状态,即阅读器发出询问后,射频标签予以应答,称这种方式为阅读器先讲方式。另外一种情况是射频标签先讲方式,即射频标签满足工作条件后,首先自报家门,阅读器根据射频标签的自报家门,进行记录或进一步发出一些询问信息与射频标签构成一个完整对话,达成阅读器对射频标签进行识别的目的。

射频识别系统应用中,根据阅读器读写区域中允许出现单个射频标签或多个射频标签的不同,将射频识别系统称为单标签识别系统,或简称为射频识别系统,与多标签识别系统。在阅读器的阅读范围内有多个标签时,对于具有多标签识读功能的射频识别系统来说,一般情况下,阅读器处于主动状态,即阅读器先讲方式。阅读器通过发出一系列的隔离指令,使得读出范围内多个射频标签逐一或逐批地被隔离出去(令其睡眠),最后保留一个处于活动状态的标签与阅读器建立无冲撞的通信。通信结束后将当前活动标签置为第三态(可称其为休眠状态,只有通过重新上电,或特殊命令,才能解除休眠),进一步由阅读器对被隔离(睡眠)的标签发出唤醒命令唤醒一批(或全部)被隔离的标签,使其进入活动状态,再进一步隔离,选出一个标签通信。如此重复,阅读器可读出阅读区域内的多个射频标签信息,也可以实现对多个标签分别写入指定的数据。

实现多标签的读取,现实应用中也有采用标签先讲方式的应用。多标签读写问题是射频识别技术中面临的一个较为复杂的问题,目前已有多种实用方法解决这一问题。解决方案的评级一句,一般考虑以

下三个因素：

- a. 多标签读取时待读标签的数目；
- b. 单位时间内识别标签数目的概率分布；
- c. 标签数目与单位时间内识读标签数目概率分布的联合评估。

理论分析表明，现有的方法都有一定的适用范围，需根据具体情况，结合上述三点因素对多标签读取方案给出合理评价，选出适合具体应用的方案。多标签读取方案涉及到射频标签与阅读器之间的协议配合，一旦选定，不易更改。

对于无多标签识读功能的射频识别系统来说，当阅读器的读写区域内同时出现多个标签时，由于多标签同时响应阅读器发出的询问指令，会造成阅读器接收信息相互冲突而无从读取标签信息，典型情况是一个标签信息也读不出来。

（3）数据传输

射频识别系统所完成的功能可归结为数据获取的一个便利手段，因而国外也有将其归为自动收集数据 ADC（Automatic Data Capture）技术范畴。射频识别系统中的数据交换包含两个方面的含义：

- a. 从阅读器向射频标签方向的数据交换；
- b. 从射频标签到阅读器方向的数据交换。

根据具体实现系统的不同，以及理解层面的不同，上述两个方面的含义会有不同的理解和解释，下面分别给予简单讨论。

6.1.1 从阅读器向射频标签方向的数据交换

从射频识别系统实现过程中的纯技术层面来说,如果将注意力放在射频标签中存贮信息的注入方式来说,阅读器向射频标签方向的数据交换可分为两种情况,即有线写入和无线写入方式。具体采用何种方式,需结合应用系统需求、代价,技术实现的难易程度等因素来定。在有线写入方式下,阅读器的作用是向射频标签(中的存贮单元)写入数据信息。阅读器更多地被称为编程器。根据射频标签存贮单元及编程写入控制电路的设计情况,写入可以是一次性写入不能修改,也可以是允许有线多次改写的情形。另外一种写入情形是,在绝大多数通过射频识别系统应用中,每个射频标签要求具有唯一的标识。这种唯一的标识被称为射频标签的 ID 号,通常在标签出厂时已被固化在射频标签内,用户无法修改。ID 号的固化过程可以在射频标签芯片生产过程中完成,也可以在射频标签应用指定后的初始化过程中完成。无论在何时完成,都是以有线(接触)方式实现 ID 号的写入。

对于声表面波 SAW 射频标签以及其他无芯片射频标签来说,一般均在标签制造过程中将标签 ID 号固化到标签记忆体中。

无线写入方式是射频识别系统中阅读器向射频标签方向数据交换的另外一种情况。根据射频识别系统实现技术方面的一些原因,一般情况下应尽可能地不要采用无线写入方式,尤其是在射频识别系统工作过程中。这种建议的主要原因有以下几点:

(1) 具有无线写入功能的射频识别系统属于相对复杂的系统,能够采

用简单系统解决应用问题即采用简单系统是一般的工程设计原理。其背后隐含着简单系统较复杂系统成本更低、可靠性更高、培训、维护成本更低。

(2) 采用集成电路芯片的射频标签写入信息要求的能量比读出信息要求的能量要大得多, 可以 10 倍的量级进行估算。这就造成射频标签无线写入过程花费的时间要比从中读取等量数据信息花费的时间要长许多。

(3) 无线写入后一般均应对写入结果进行检验, 检验的过程是一个读取过程, 因而造成写入过程所需时间进一步增加。

(4) 写入过程花费时间的增加非常不利于射频识别在鉴别高速移动物体方面的应用。这很容易理解, 阅读器与射频标签之间经空间传输通道交换数据过程中, 数据是一位一位排队串行进行的, 其排队行进的速度由射频识别系统设计时决定。将射频标签看作数据信息的载体, 数据信息总是以一定长度的数据位组成, 因而读取或写入这些数据信息位要花费一定的时间。移动物体运动的速度越高, 通过阅读区所花费的时间就越少。当有无线写入要求时, 必将限制物体的运动以保证有足够的时间用于写入信息。

(5) 无线写入过程面临着射频标签信息的安全隐患。由于写入通道处于空间暴露状态, 这给蓄谋攻击者提供了改写标签内容的机会。

另一方面, 如果将注意力放在阅读器向射频标签是否发送命令方面, 也可分为两种情况, 即射频标签只接受能量激励和既接受能量激励也接受阅读器代码命令。

射频标签只接受能量激励的系统属于较简单的射频识别系统。这种射频识别系统一般不具备多标签识别能力。射频标签在其工作频带内的射频能量激励下，被唤醒或上电，同时将标签存贮的信息反射出来。目前在用的铁路车号识别系统即采用这种方式工作。

同时接受能量刺激和阅读器代码命令的系统属于复杂射频识别系统。射频标签接受阅读器的指令无外乎是为了做两件事，即无线写入和多标签读取。

6.1.2 从射频标签向阅读器方向的数据交换

射频标签的工作使命即是实现由标签向阅读器方向的数据交换。其工作方式包括：

(1) 射频标签收到阅读器发送的射频能量时，即被唤醒并向阅读器反射标签存贮的数据信息；

(2) 射频标签受到阅读器发送的射频能量被激励后，根据接收到的阅读器的指令情况转入发送数据状态或“睡眠/休眠”状态。

从工作原理上来说，第一种工作方式属单向通信，第二种工作方式为半双工双向通信。

6.2 电子标签在档案管理中的应用分析

6.2.1 技术可行性

从 20 世纪 90 年代起，RFID 技术开始用于商业领域并逐渐深化。RFID 技术本身也日趋成熟，经过长时间以来，人们对 RFID 技术、产

品和应用坚持不懈的研究和实践，并在这些研究成果的基础上形成了现在广为人知的一系列 ISO 标准和 EPC Gen2 标准。RFID 技术在一系列实践领域的应用尝试取得喜人成绩后，开始进入档案管理领域。

RFID 应用于档案管理，在技术上有以下突出优势：

(1) 非接触式数据采集。RFID 技术极大地增强了管理员对库房档案的信息收集、交换与跟踪能力。管理员无需打开档案盒，只需将粘有 RFID 标签的档案盒在阅读器前经过，就可以在电脑屏幕上显示出盒内档案的具体名目、数量、档案摘要等信息，缩减了管理员的作业环节，提高了作业效率，从而有助于管理者实施库存档案的动态化管理。

(2) 快速扫描，且一次性数据处理量大。RFID 读写器可以同时从多个射频标签中快速读取包括位置信息、档案内容摘要信息等多项相关数据信息。如一些读写器可以每秒读取 200 个标签的数据，这比传统扫描方式要快超过 100 倍。

(3) 标签信息容量大，使用寿命长，可重复使用。和传统的条形码、磁卡等数据存储介质相比，RFID 标签可存储的数据量大大增加，可达 1K 甚至更大的容量；标签的内容可以反复被擦写，而不会损害标签的功能，从而可实现标签的重复使用。

(4) 安全性高。标签的数据存取具有密码保护，识别码独一无二，无法仿造，这种高度安全性的保护措施使得标签上的数据不易被伪造和篡改。

(5) 抗污染性能强和耐久性。传统条形码的载体是纸张，因此

容易受到污染，但 RFID 对水、油和化学药品等物质具有很强抵抗性。此外，由于条形码是附于塑料袋或外包装纸箱上，所以特别容易受到折损；RFID 卷标是将数据存在芯片中，因此可以免受污损。

(6) 体积小小型化、形状多样化。RFID 在读取上并不受尺寸大小与形状限制，不需为了读取精确度而配合纸张的固定尺寸和印刷品质。此外，RFID 标签更可往小型化与多样形态发展，以应用于不同档案。

(7) 可重复使用。现今的条形码印刷上去之后就无法更改，RFID 标签则可以重复地新增、修改、删除 RFID 卷标内储存的数据，方便信息的更新。

(8) 穿透性和无屏障阅读。在被覆盖的情况下，RFID 能够穿透纸张、木材和塑料等非金属或非透明的材质，并能够进行穿透性通信。而条形码扫描机必须在近距离而且没有物体阻挡的情况下，才可以辨读条形码。

(9) 标签具有 EAS 防盗功能。配合门型通道天线，可以很好的防止档案丢失，实现非法取走报警功能。

6.2.2 经济可行性

RFID 技术现在正值高速发展期，各种应用系统层出不穷，应用潜力也十分巨大，将对工业化、信息化的发展作出巨大的贡献。而 RFID 与档案馆的结合使用，展现了一个新的应用领域。虽然 RFID 系统的应用中仍碰到价格的阻力，但是综合分析，射频识别技术应用于档案

馆在经济上是完全可行的。

(1) RFID 标签成本

成本价格是制约 RFID 发展的最主要因素之一。与过去几年相比, RFID 标签的价格已经有了较大幅度的降低, 国外已实现每个标签 5 美分 (不需要大批量购买), 国内的最低价格是每个 7 角人民币。尽管如此, 对大规模推广来说, RFID 标签与条码极低的成本相比仍显得过高, 这将成为阻碍 RFID 技术在图书管理中应用的最关键性因素。

随着技术的进步和使用数量的不断增加, 芯片的价格会不断下降, 而体积会不断变小, 存储量会不断增长; 另外 RFID 标签的使用年限长, 并可重复使用, 相对现在的防盗磁条以及条形码技术的使用寿命来说, 可获得质的提升, 因此随着 RFID 技术的发展成熟, 其必然将会在档案馆领域中得到广泛应用和推广。

(2) RFID 平台的建设

为了推出基于 RFID 技术的档案馆自动化管理业务, 需要建设一个能给予该业务支持的软件平台。该平台应具有能实现多个用户共同使用的功能; 具有读写器和后台的信息支撑系统、认证系统、安全系统; 能适应大通信量的支持读取, 如成千上万个标签, 并进行验证。这一系统平台只需充分利用原来的信息化管理系统, 新开发的部分并不多, 而且是一次性投入。

(3) RFID 阅读器的成本

RFID 的阅读器产品丰富, 技术相对较成熟, 市场价格在 8000-16000 元人民币左右, 而且档案馆应用所需的读写器数量不多,

因此投入不大。

总的来说,目前 RFID 技术的应用成本随着科技日新月异的进步,不断下降,使它在档案馆领域中的实际应用越来越得到普及和推广,真正实现档案馆自动化智能化管理。

6.2.3 管理可行性

基于 RFID 技术的档案管理系统能够为用户提供更为直接、简洁的操作流程以满足用户在档案的收集、整理、保存、统计、检索、利用和追踪防盗的各个环节工作需求。以前的管理模式大部分是由手工操作,需要大量的劳动力与工作量,而且由于人为的原因容易造成一些错误。将 RFID 技术应用于档案管理,可以大大改进管理方式、提高工作效率。

(1) 提高档案流通效率。随着知识经济时代,人们对于档案的需求不断提高,档案馆的馆藏量不断增加,档案馆的档案借阅量随之增加。现行的条形码方式在借还档案业务操作时,需要对每份档案的条形码逐条扫描,从而使借还档案处理时间长,这无疑增加了档案馆的档案管理的难度,降低了档案馆的服务效率。而采用 RFID 技术的档案馆则可以对批量借阅或归还的档案进行处理,可以实现瞬间、非接触完成,现有技术最大距离已经可以大于 10 米,从而大大提高档案流通效率。

(2) 简化档案清点和整理工作。目前,我国档案馆馆藏量较大,清点、盘库面临着巨大的工作量,现行的技术无法有效地解决这一问

题；由于馆藏量大，借阅数多，整理时需要耗费很大的人力。采用 RFID 技术后可一次读取数本贴有 RFID 标签的档案资料，大大简化盘点工作；利用 RFID 技术的手持式阅读器很容易查找不在架上或者乱架的档案，使得档案整理工作更简易。

（3）提高档案安全防盗性能。档案馆和图书馆界目前普遍使用的安全防盗系统是采用磁针检测技术和条形码识别技术，由于磁条的使用寿命和电磁状态难以确保正常、稳定。使得安全系统不可靠；而 RFID 技术的灵敏度、准确性远远高于磁性检测报警器。档案馆如果引进和应用 RFID 系统，能更有效防止未借出档案资料被带离档案馆，且 RFID 电子标签的数据存储有密码保护，不易被伪造和更改，另外，还可以实现对附有 RFID 标签的档案进行追踪定位，防止档案丢失。

6.2.4 所面临的问题

采用 RFID 技术虽然很大程度上提高了档案馆的工作效率和档案的安全性，但是也有以下一些问题需要慎重考虑：

（1）信号不稳定性问题

如果 RFID 标签被厚实的包裹物或其他较厚的物体挡住时，其射频信号会减弱很多。同时，如果两个 RFID 标签相向放在一起，其中一个的射频信号可能会覆盖另一个的射频信号，影响信号的正常传输。

（2）信号泄密问题

目前存储在 RFID 标签中的数据主要有：①物品 ID、标识码或条

形码信息；②流通状态信息；③附加的数据，如物品的存放位置、档案名等信息。如果 RFID 标签中仅存储“物品 ID”，这一信息即使经由其他的企图窃取信息的扫描器识别，但是由于借阅资源和借阅者之间的数据关联存储在档案馆综合管理系统的后台数据库中，所以泄漏出去也不会存在安全隐患。如果“流通状态信息”和“附加的数据”也存储在 RFID 标签内，由于这些信息可能涉及到借阅资源的借阅状态和借阅者的信息，如果一旦被窃取，则存在较大的安全隐患，侵犯隐私的可能性也较大。因此，必须要求 RFID 标签在一个有限的距离范围内才能够被阅读器识别，这样才能够保证存储在 RFID 标签中的信息不会被泄露出去。

（3）与现有系统的整合问题

档案馆综合管理系统在设计时是以条码技术和磁条技术为基础的，RFID 系统则是以 RFID 标签技术为基础，二者在通信协议、接口的方面需要整合，如果没有一定的技术力量很难完成这方面的工作，RFID 系统和现有档案馆综合管理系统的整合难度较大。

（4）同一标准化问题

到目前为止，包括 ISO（国际标准组织）和 CEN（欧洲标准委员会）在内的 10 多个国家或国际机构颁发了有关 RFID 的技术标准，彼此并不完全兼容。在物流领域，RFID 技术存在两种编码体系：日本 UID 标准和欧美的 EPC 标准，这两个标准适用的无线频段、信息位数和应用领域等存在着不同程度的差异。由于 RFID 在国际上还没有一个成熟的技术标准及行业使用规范，各个厂家推出的 RFID 产品

互不兼容，这对 RFID 产品互通和发展以及在档案馆的应用造成了一定的障碍。

（5）兼容问题

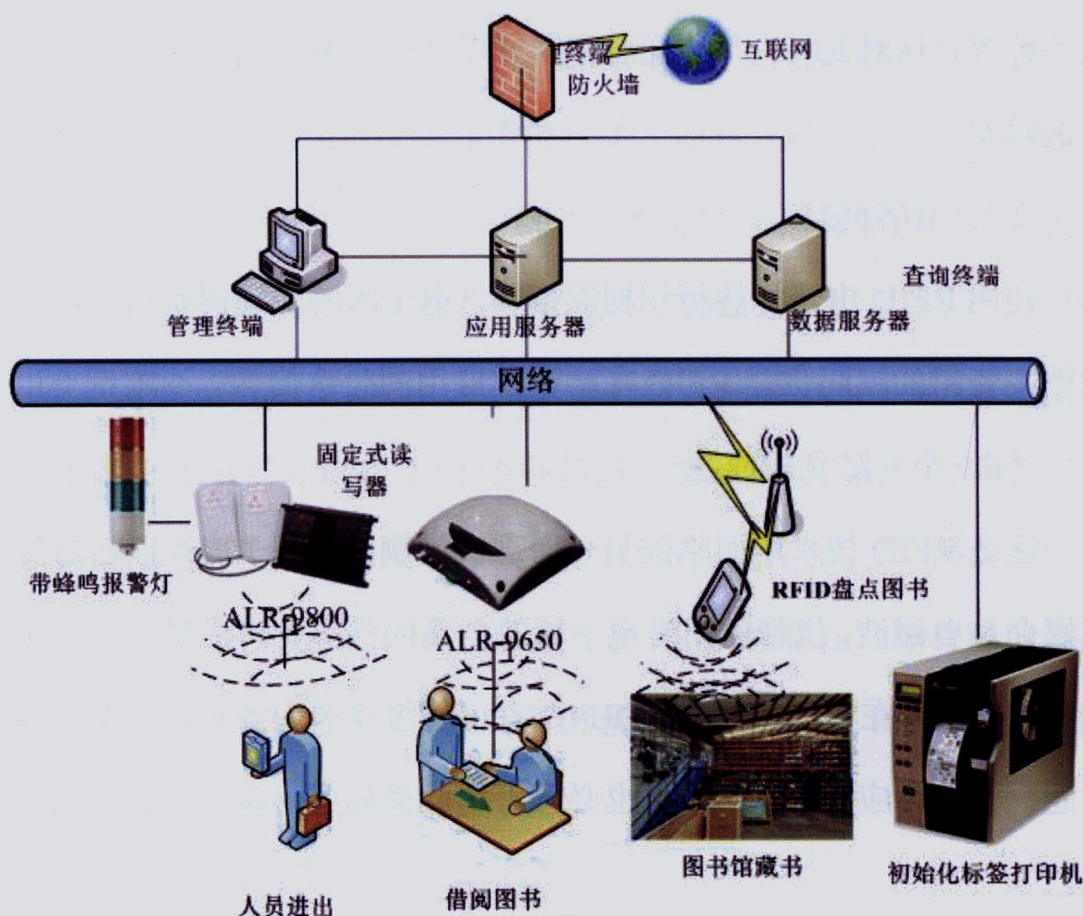
使用 RFID 电子标签标识档案资料，电子标签的编码是否兼容原有档案资料的编码也是 RFID 在档案馆应用的一个问题。

（6）个人隐私权问题

这是 RFID 技术所面临的另一个现实问题。由于 RFID 识别的信息媒介是电磁波，携带着附有电子标签档案的借阅者有遭到追踪的潜在威胁，所以在档案领域使用 RFID 有可能涉及个人隐私权遭受侵害问题，档案馆应用 RFID 技术也必须考虑此类问题，避免不必要的麻烦。

6.3 实体档案和数字档案一体化管理应用分析

基于对目前无线射频识别功能模型的基本认识，结合太仓市智能化档案新馆的建设目标以及档案馆的实际情况，课题组提出了如下功能模型：



基于无线射频识别技术的智能化档案新馆功能模型

6.3.1.1 基本功能

建设基于 RFID 技术的档案实时安全管理系统网络环境并部署相应的 RFID 硬件设备。用来识别、追踪和保护档案馆的所有资料。通过 RFID 系统实现档案借还、顺架、查找、馆藏盘点等功能。

6.3.1.2 系统构成

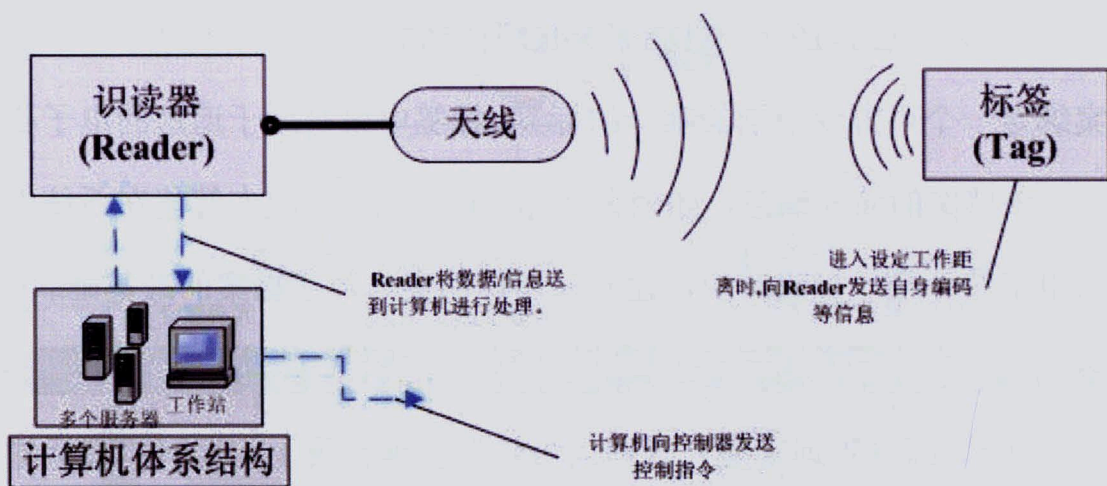
系统包含 5 个功能模型：大屏幕实时监控模型，移动终端管理模型，短信管理模型，五级预警机制，视频、温湿度联动模型，具体可实现：

(1) 信息识别。一旦档案被收藏在档案室，就需要为每一件档案绑定一个可方便识别的唯一的标签，标签中带有用于追踪的电子芯片。该档案的简要信息，如档案名称、存放位置，状态等能在系统中与电子芯片唯一号码对应，建立起实体档案与数字档案的最基础联系。

(2) 标签管理功能。管理人员能在管理系统上实现对档案标签的管理，包括修改标签信息比如档案名称、存放位置、档案出入库情况等；由于档案报废销毁而删除标签。

(3) 实体管理功能。若需要将档案带离档案室，则需要办理借出登记，记录必要信息，且信息将显示在终端系统上。只有办理完毕借出登记，档案方可被安全带出档案室，且不会触发报警系统。若需要将档案还回档案室，同样需要办理还回登记，记录必要信息，且信息将显示在终端系统上。

(4) 异常情况分级报警功能。人员携带档案经过进出入口通过固定式读写器对档案上粘贴的电子标签进行识读。通过后台比对，如合法无动作，非法则通过读写器控制触发报警。在未经授权的档案调用或是疑似偷盗行为发生时，系统能立即发出警报并显示被偷窃档案信息，通知安保人员立即处理。

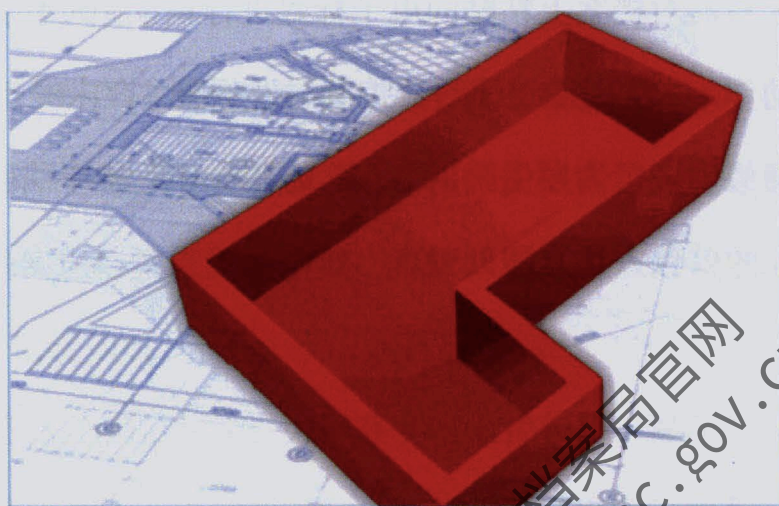


含电子标签的档案触发安全报警模型

在此基础上,江苏省太仓市档案局创新推出了五级颜色预警的安全管理机制,针对不同情况的异常信息,采用不同级别的报警机制。

a.红色预警

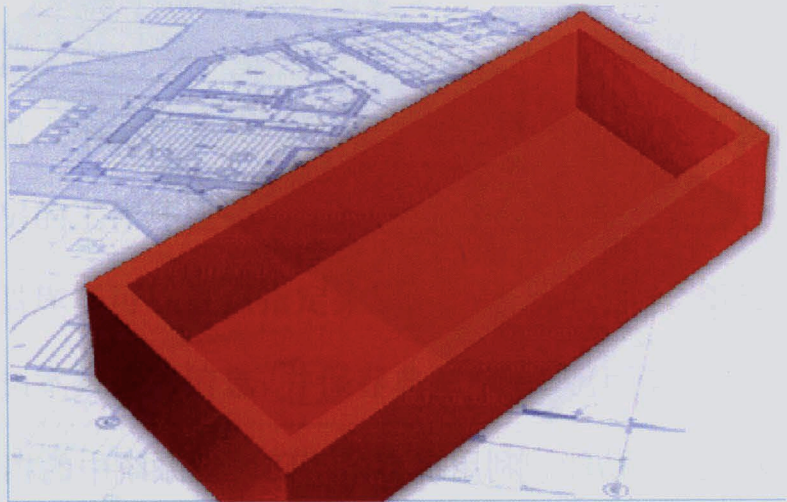
即最高级别预警,实体档案非正常出馆、重点档案非正常出库(馆)时触发。系统会弹出红色警示图片,进行预警。该事件会被记录在系统中,报警需负责人员确认事件得到处理后方能被停止。报警颜色如图所示:



b.橙色预警

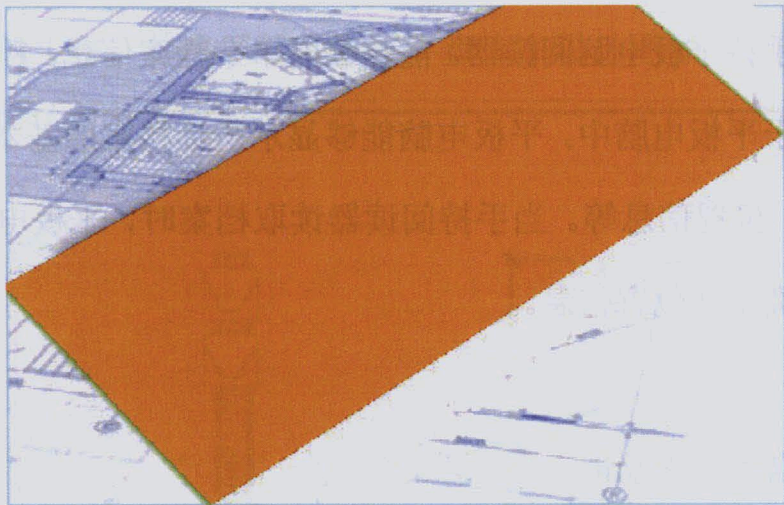
第二级别预警,实体档案非正常出库、调卷多调时触发,系统会

弹出橙色警示图片，进行预警。橙色预警图片如下：



c.黄色警报

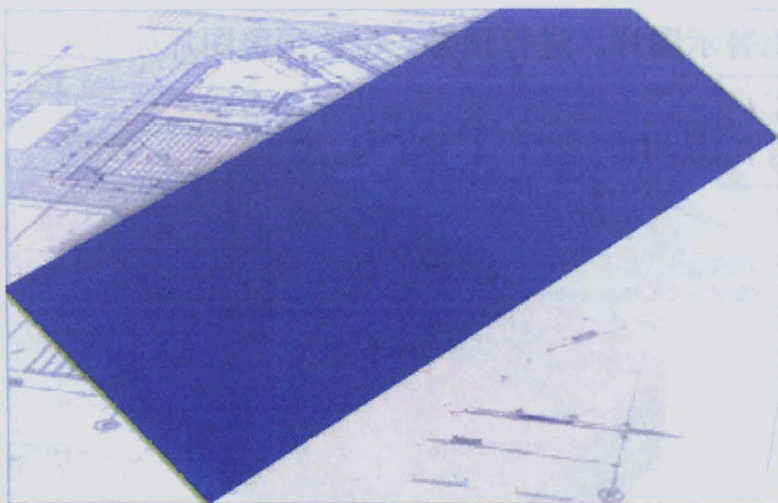
第三级别预警，调卷漏调、还卷多还，重点档案到期未还时触发，系统弹出黄色警示图片，进行预警。黄色预警图片如下：



d.蓝色预警

第四级别预警也是最低级别的预警，普通档案到期未还时触发，。系统会弹出蓝色警示图片，进行预警，提醒管理员对借阅人员进行催还。蓝色预警图片如下：

国家档案局官网
WWW.SAAC.GOV.CN



(5) 区域定位功能。利用现有条形码管理系统中的档案位置信息，构建档案追踪表和定位表，实现实体档案的区域追踪，和案卷的库房、列、架、格、盒五级定位。

(6) 手持移动读取功能

通过手持平板电脑阅读器，能够读取单个档案信息。档案的基本信息预存于平板电脑中，平板电脑能够显示所读档案的基本信息，包括：标题、位置信息等。当手持阅读器读取档案时，平板电脑直接显示标题、类别和位置信息。

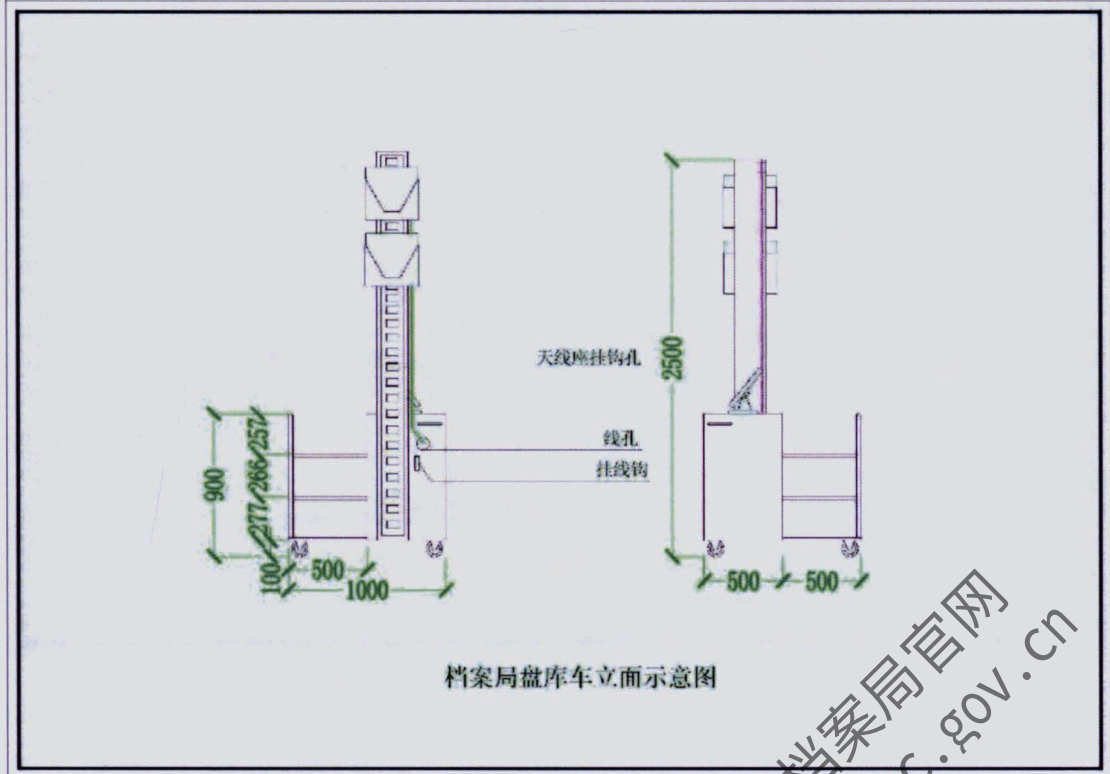
(6) 自动盘库功能

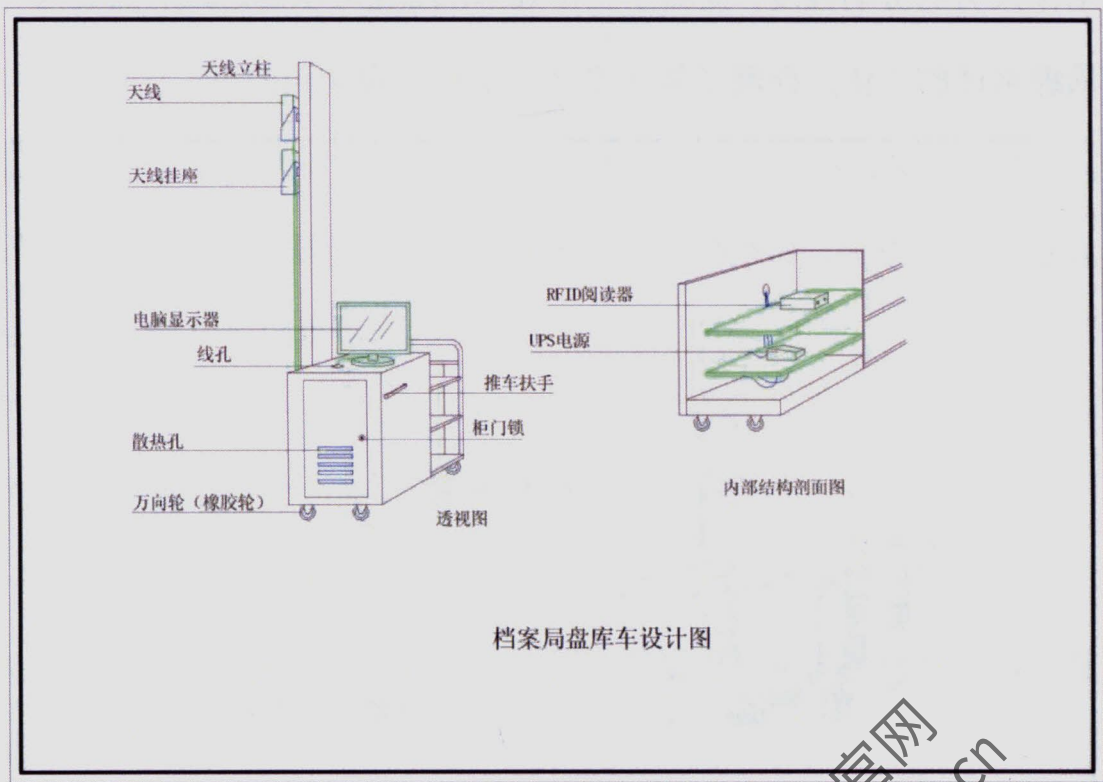
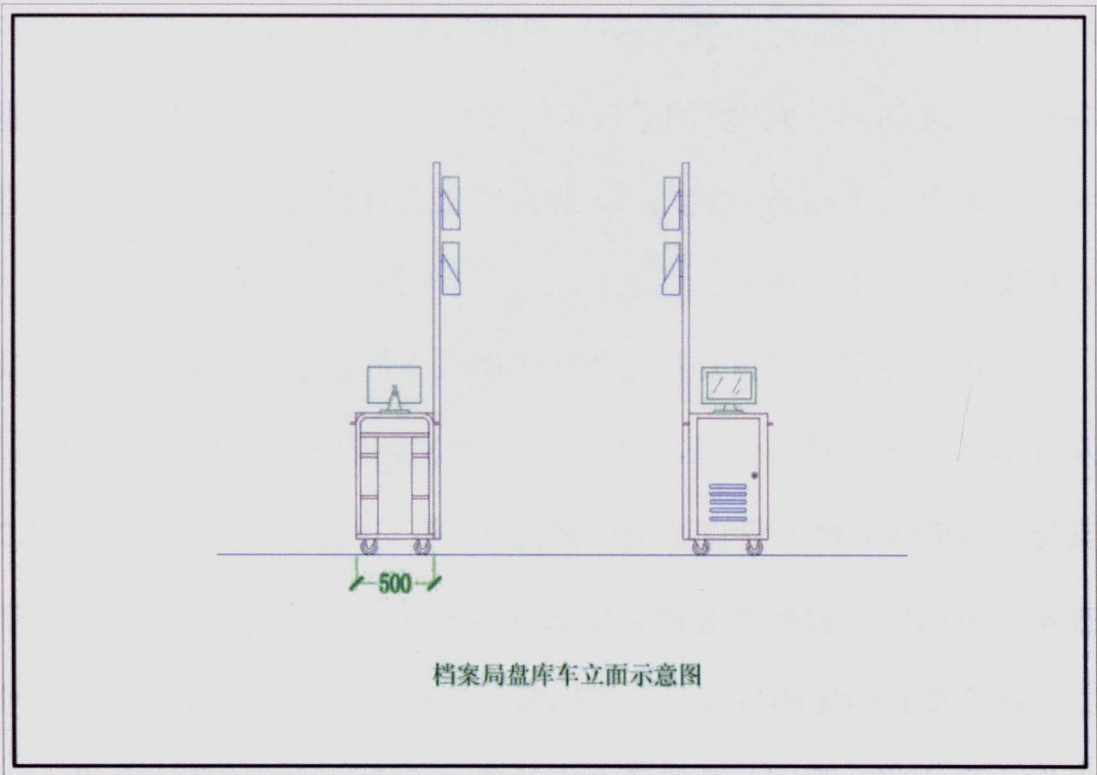
由于档案馆一般档案都比较多，盘库工程耗费人工多、时间长，出错的几率也比较大。鉴于以上原因，研制出推车式移动盘库车进行自动盘库。

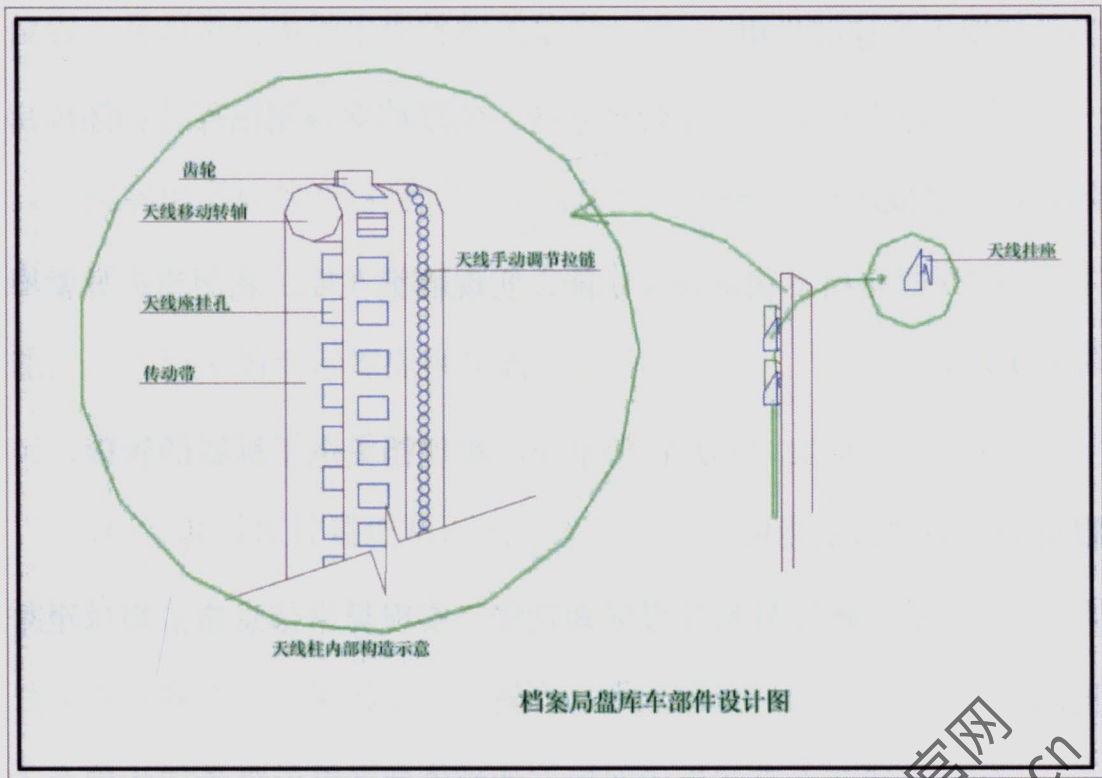
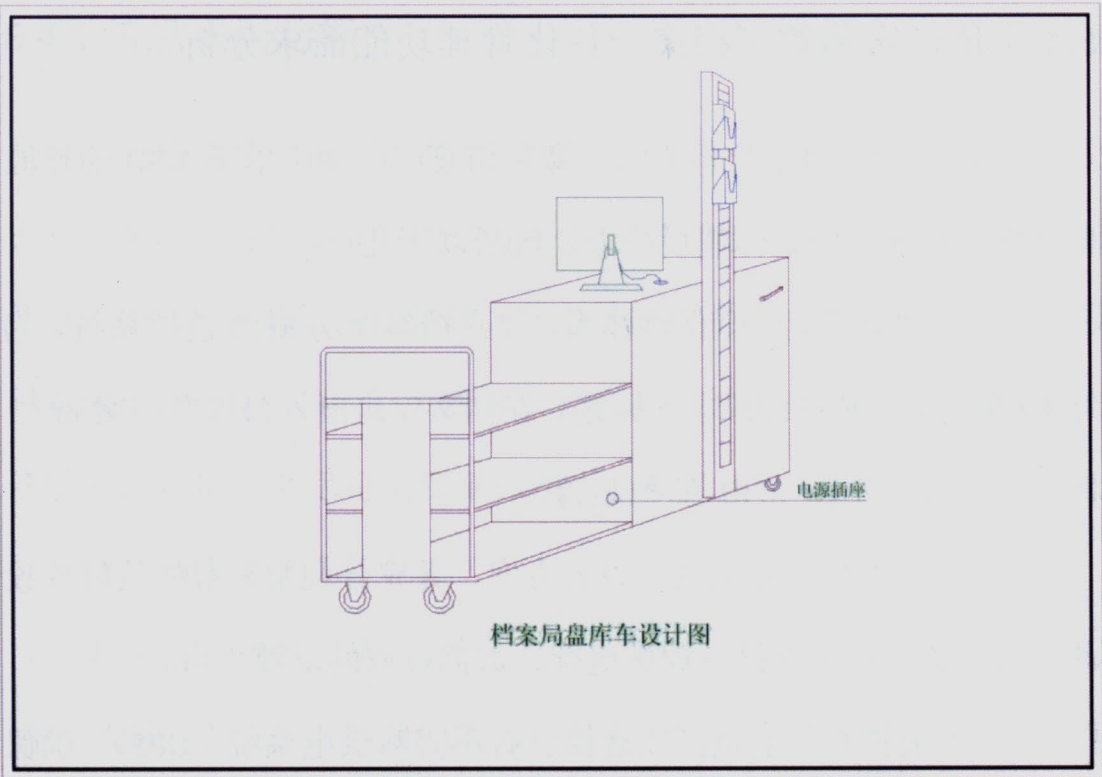
机盘库车通过采用 UHF 频段 RFID 技术，充分满足了盘点速度快、盘点准确率高的要求。通过采用无线传输技术使得产品脱离了网线的束缚。采用蓄电池供电的方法使得产品又脱离了电线的束缚。车身下

的万向轮使得产品能够自由移动. 纤细型车身使其能够方便地出入于各种书架之间。可以折叠的手持天线和可以自由伸缩的射频线使得能够方便地盘点不同高度的档案。触摸屏交互方式简化了操作，完全适合档案库房的工作环境。

通过盘库车可以盘点指定架标. 层标下的在架、错架、不在架以及外借的档案数量与信息, 并保存典藏结果, 也可保存中间盘点结果, 支持复盘功能, 保证盘点结果正确无误。推车式移动盘点车通过 RFID 技术, 可以同时读取多卷档案信息, 这就不需要从档案架上取下档案. 就能找到档案的位置, 了解档案的信息。这样不但极大地减轻了工作人员的劳动强度, 提高了工作效率, 而且可以使馆藏清点成为一项经常性的工作, 提高了管理水平。盘库车设计图如下:







国家档案局官网
www.saac.gov.cn

6.4 实体档案和数字档案一体化管理功能需求分析

通过科学的需求分析方法，课题组总结归纳出基于 RFID 的智能化档案管理项目的整体建设需求，包括以下几点：

(1) 加强档案安全保障体系，建立档案库房 RFID 监控系统。为每本/卷档案安装 RFID 电子标签。在档案库房出入口以及档案局大楼门厅出入口安装 RFID 监控装置。

(2) 合理配置相关硬件设备方案，并充分利用现有的软硬件设备。为业务软件系统提供业务运行、数据存取的支撑平台。

(3) 监控系统的电源需连接已有不间断供电系统（UPS），确保异常情况下的连续供电。

(4) 建立档案出入库管理系统，实现档案调用出库，归还库房的登记，审批和统计功能。

(5) 建立档案状态统计功能，实现档案在库、利用率、异常率等相关统计。

(6) 建立档案 RFID 管理系统，实现档案电子标签的管理，可视化的监控和跟踪功能。

(7) 建立档案异常警报通知功能，实现异常信息定点报送至个人。

(8) 上述两个系统集成在现有的档案局业务系统中，实现单点登录和权限控制，提高办事效率。

(9) 建立数据存储备份系统，制定相应的安全策略、保障档案资源的原始性、安全性、可靠性、可用性。

6.4.1 信息识别功能

一旦档案被收藏在档案室，就需要为每一件档案绑定一个可方便识别的唯一的标签，标签中带有用于追踪的电子芯片。该档案的简要信息，如档案名称、存放位置，状态等能在系统中与电子芯片唯一号码对应。RFID 标签应被妥善地装贴在档案卷轴中，不影响卷轴中文件的阅读使用，并尽可能保证标签不会被撕毁。

(1) 档案电子标签创建

为新建的档案创建/初始化电子标签时，系统应提供电子标签初始化界面。方便输入档案的编号，名称，主要内容，类别，存放库房位置，是否需要审批出库等相关信息。

(2) 档案电子标签注销

档案电子标签在自身受损或档案被销毁时应能在系统中被注销。电子标签在不正当使用的情况下会受损，系统提供电子标签注销的功能，并为档案的新标签提供初始化服务。

(3) 档案电子标签的读取

当档案通过监控通道从而出入库房的情况出现时，系统应能准确读取档案信息，并记录该事件的详细情况，包括时间，档案信息，是否是非法操作。如果属于非法操作，系统应及时发出警报，并通知相关人员及时处理该异常事件。

6.4.2 标签管理功能

管理人员能在管理系统上实现对档案标签的管理，包括修改标签

信息比如档案名称、存放位置、档案出入库情况等；由于档案报废销毁而删除标签。

6.4.3 档案电子标签信息修改

当档案存放位置，档案名称或其它档案信息发生变化时。档案所对应的电子标签应对相应修改。系统应提供便捷的修改界面，并保证修改情况被记录在系统中用作审核、校对。

6.4.4 记录借还功能

若需要将档案带离档案室，则需要办理借出登记，记录必要信息，且信息将显示在终端系统上。只有办理完毕借出登记，档案方可被安全带出档案室，且不会触发报警系统。若需要将档案还回档案室，同样需要办理还回登记，记录必要信息，且信息将显示在终端系统上。

(1) 档案出库

对于不存在或尚不存在电子档的实体档案，如果个人或单位申请调用出库，系统应登记该调用请求，并针对不同安全类别的档案进行审批。通过审批的调档请求将在系统中自动记录该调档事件，并更新对应档案电子标签的状态从而在档案取出库房时不会触发系统报警机制。系统需详细记录对档案进行调用的组织和个人的证件、借阅时间、归还日期等信息。

(2) 档案入库

档案调用完毕后，调用人员归还档案。系统能在无需任何人工操作

的情况下自动完成档案调用情况的更新和对相应电子标签状态的更新。当档案被桌面 RFID 读取器读取到后，上述操作应能自动完成。

(3) 档案催还

对于到期没有归还的档案，系统应能发出催还通知给档案调用人员以及档案馆负责人员。通知发出的频率随着拖延的日期延长而增加。

(4) 档案统计

通过利用统计功能，能够自动实现一定时间范围内各种档案类型的借阅卷次、借阅人数、借出卷次、借出人次、卷次总计、人次总计等统计信息，为档案管理人员更好的档案管理以及档案利用提供数据依据。同时能精确实现档案在库、利用率、异常率等相关统计。

6.4.5 报警功能

在未经授权的档案调用或是疑似偷盗行为发生时，系统能立即发出警报并显示被偷窃档案信息，通知安保人员立即处理。

(1) 库房报警

档案未经审批同意调用而被带出库房，库房门禁会有报警。该事件会被记录在系统中，报警需负责人员确认事件得到处理后方能被停止。

(2) 保安人员报警

在档案出现非法调用情况时，保安人员特别是保安室会得到及时通知。

(3) 负责人报警

在档案出现非法调用情况时，档案局相关负责人会在其工作电脑上收到即时通知，在其手机上收到相关文字信息告知该紧急情况。

6.4.6 人员管理功能

系统中应提供档案调动审批人员管理，档案安全负责人员管理以及档案出入库登记人员管理模块。

(1) 审批人员管理

部分重要档案需要审批同意才能借阅的，需通过指定档案局负责人员审批。系统应提供便捷的后台管理界面，支持审批人员的新增，更改和删除操作。

(2) 档案安全负责人员管理

档案出入库房出现非法事件时，安全负责人员需处理该事件，并把处理结果记录在系统中。系统应提供便捷的后台管理界面，支持安全人员的新增，更改和删除操作。

(3) 档案出入库登记人员管理

档案出库，入库的登记工作由档案大厅服务人员负责，具体的调用情况比如调用人，借出归还日期，调用事由，审批情况等均需登记人员负责记录在系统中。登记人员名单管理应和上述安全负责人和审批人类同。