文章编号：2095-2163(2021)01-0024-04 中图分类号：TP393.08 文献标志码：A

# 校园一卡通系统安全模型的构建及应用

吴文晖
（南京农业大学，南京 210095）

**摘 要：** 校园一卡通系统在高校的应用经历了高速发展的过程，给学校和师生带来便捷的同时，也呈现出纷繁复杂的安全问题。多数校园一卡通系统是从食堂收费系统发展而来，缺少必要的顶层设计和标准规范，其组成模式基本采用搭积木方式整合而成。经多年使用，目前系统的安全不仅牵涉到硬件故障、软件缺陷，还涉及管理问题。本文通过对校园一卡通系统安全模型的构建和对风险来源的分析，在实践的基础上，提出规避风险的应用策略。

**关键词：** 一卡通系统；安全模型；风险来源；应用策略

## Construction and application of the security model of campus card system

WU Wenhui
（Nanjing Agricultural University, Nanjing 210095, China）

**【Abstract】** The application of the campus all-in-one card system in colleges and universities has undergone a rapid development process, which brings convenience to schools, teachers and students, but also presents numerous and complicated safety problems. Most campus all-in-one card systems are developed from the mess-hall charging system, lacking the necessary top-level design and standard specifications, and their composition mode is basically integrated by building blocks. After years of use, the current system security not only involves hardware failures and software defects, but also management problems. Based on the construction of the security model of the campus all-in-one card system and the analysis of risk sources, this paper proposes application strategies to avoid risks on the basis of practice.

**【Key words】** all-in-one card system; security model; source of risk; application strategy

## 0 引 言

目前，针对校园一卡通系统安全问题的研究通常基于数据存储、卡安全和病毒防范等单一层面，忽略了校园一卡通系统的自身缺陷、布线环境和缺乏可行的管理制度等带来的综合风险。这些问题均可引发故障，造成危害。随着高校的高速发展，一卡通系统的需求范围不断扩大，业务功能日益丰富，专业应用持续深入，由此带来的流量也急剧上升，数据交换频率和系统集成的复杂程度都超出原有设计要求，应用系统经常处于临界运行状态。虽然系统不断采取修补式升级，但安全风险还是频现。

## 1 校园一卡通系统概念

校园一卡通系统是在学校专用网络基础上，以使用 RFID 和 IC 技术封装的智能卡片或虚拟卡技术集成应用的手机为载体，利用终端采集数据，经应用系统管理主机分类，实时上传至服务器处理，再将处理后的数据回传主机和终端，完成身份认证，实现教学服务、生活服务和校园收支等数字化管理。

### 1.1 平台架构

校园一卡通系统实施统一管理，分级运用综合性平台架构，通过系统的模块化结构设计，按需配置功能，实现数据共享，提高运行效率。并预留接口方便其后的扩展。校园一卡通系统的平台架构如图 1 所示。

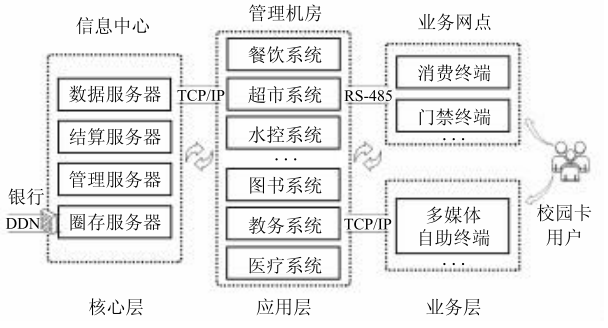


**图 1 校园一卡通系统的平台架构**

**Fig. 1 Platform architecture of campus card system**

### 1.2 业务模块

具体功能包括：数据收发（对食堂、超市、浴室、洗衣房等的消费数据实时处理）；卡务中心（含发卡、销户、挂失、解挂等业务功能）；结算中心（负责

**作者简介：** 吴文晖（1969 -），男，本科，技师，主要研究方向：计算机应用系统安全技术。自 1994 年迄今，先后参与哈尔滨“新中新”、南京“鑫三强”、北京“北大青鸟”、南京“理达”和郑州“新开普”校园卡系统在本校的建设、管理与维护。

**收稿日期：** 2020-11-26

销售报表和管理报表的生成与审计）；管理中心（负责教务系统、图书系统、医疗系统、圈存系统各主机与服务器的对接、设备授权和系统升级）；数据处理服务（运行于服务器端，完成数据监控、采集和存储）；多媒体自助圈存服务（含自助查询、充值、报名与综合缴费等业务功能）；自动唤醒服务（当系统进程掉线时自动重启程序）。

## 2　校园一卡通系统的安全

校园一卡通系统的安全是指在相对封闭的专用网络中，系统的硬件、软件、网络、管理环境及所发生的业务资源受到保护，不因意外或恶意原因遭受损毁、更改和泄露，系统能够可靠地运行，网络连接不间断，数据收发和管理信息交换持续，满足校园用户的正常业务需求。

### 2.1　安全模型的构建

校园一卡通系统安全模型由实体和虚拟两类共五层组成[1-2]，见图 2。其中，实体层的第一层、即核心层由服务器群组成，通过 TCP/IP 协议与主机通信，同时圈存服务器通过 DDN 专线与银行前置机通信。第二层、即应用层由主机及一卡通应用系统组成。第三层、即业务层由终端群组成。消费终端和门禁终端以 RS485 协议与管理主机互联。多媒体自助终端以 TCP/IP 协议与圈存服务器联接。第四层、即网络层由各级网络关口、通信线路和网络设施组成。数据通过网络层上传下达。第五层为虚拟的，即管理层。由管理人员、操作人员和管理制度组成。负责细则的制定和人员落实，强化安全意识。

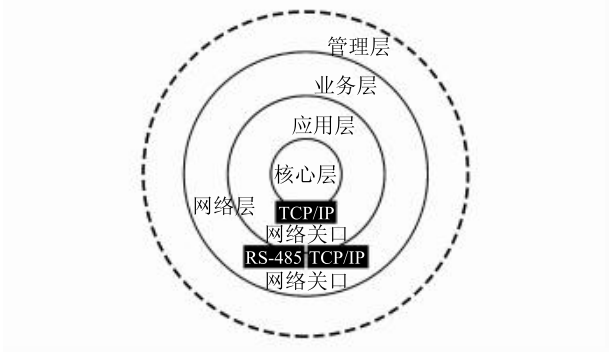


**图 2　校园一卡通系统安全模型**

**Fig. 2　Security model of campus card system**

### 2.2　安全模型的内容

（1）核心层。由信息中心数据服务器负责控制整个系统数据的采集与交换，最终存储原始数据。结算服务器通过原始数据的统计与分析生成财务报表，汇总出所有数据源供应用层调用。管理服务器负责应用层统一管理、身份验证、行为审计、权限下发、系统设置，实现对应用系统的部署和数据的组织、调用。圈存服务器负责学校与银行间财务数据的交换与结算。

（2）应用层。由赋予一卡通系统应用功能的主机群实施。在行使数据收发、卡务管理、餐饮管理、水控管理、图书管理、教务管理和医疗管理的同时，履行数据上传、日常查询、卡务办理和报表打印等具体作业的功能。

（3）业务层。属于窗口业务网点，面向校园卡最终用户。消费终端和门禁终端自身采用 EPROM 存储芯片，可存储 2 000 笔本机交易数据和 10 批次黑名单数据，网络中断时可比对黑名单脱机使用。多媒体自助终端提供人机交互服务。

（4）网络层。由服务器通过光纤连接至各管理机房主机组成一级主干网，由主机连接多媒体自助终端组成二级子网，由主机连接消费终端和门禁终端组成三级子网。这些都是连接核心层、应用层和业务层的桥梁。

（5）管理层。是虚拟的逻辑层。安全问题多由系统内部引起。缺乏相应的规章制度、制度不落实及权责不明都可引发风险。因此建立和完善一套行之有效的安全管理规章制度十分必要。同时对从业人员要强化责任意识和专业技能培训。为预防突发事件，还应制订对应的应急工作预案。

### 2.3　安全模型的作用

安全模型的建立，简洁明了地展现校园一卡通系统各个层次的安全节点，有利于厘清各方关系，专注其风险控制，配合管理制度的有效实施，可以积极保障系统的持续安全运行。

## 3　校园一卡通系统安全风险来源

根据安全模型的构建，可将校园一卡通系统风险的来源归纳为软件、硬件和安全管理三个方面。对此展开的研讨分述如下。

### 3.1　软件安全风险

这类风险来自于操作系统、数据库系统、应用系统等软件。其中，操作系统应定期安装补丁程序，才能避免相关安全风险。应用系统包含服务器应用、主机应用和终端单片机应用软件。数据服务器与消费终端进行数据交换时，或结算服务器、自助圈存终端与银行前置机进行数据交换时，因软件自身缺陷或病毒侵入，即可引发数据安全风险。服务器的初期配置主要为校园生活业务服务，完全能够支持一

卡通系统的正常运作。随着高校人数逐年增长,以及各项业务的逐步展开,服务器群的负载越来越重,系统陈旧数据也越积越多,业务流量经常瞬间超负荷即会造成服务器系统崩溃,引起连锁反应。

### 3.2 硬件安全风险

这类风险主要来自通信线路(含交换机等网络设备)和电源线路(包括机房 UPS 及其电池组)。此外,主机、终端也会因故障引发一定风险,但一经发现可用备件更换。服务器与主机、多媒体自助终端间连接的光纤网络是串联整个系统的主线,但线路的铺设常非一次完成,欠规范;且因校园施工、维修等因素常易受到损坏。主机采用 RS485 协议与消费终端、门禁终端连接,接头各异,导致节点故障频率也较高。某一节点发生短路或间歇故障时,即可引起子网线路整体瘫痪。

### 3.3 安全管理风险

这类风险来自管理制度和从业人员。例如:管理员对服务器运行异常警惕性低,当银行前置机传入蠕虫病毒并在专网的主机内互相感染时未能及时发现;操作员密码泄露,造成校园卡被恶意退费致商户损失;意外停电时起应急作用的 UPS 系统因疏于专业维护,未发现个别电池失效,导致系统无法运行;厂方维护员使用带病毒 U 盘升级应用系统,使主机感染中毒。

## 4 校园一卡通系统的安全应用

依照"统一规划、分步实施"的原则,校园一卡通系统的安全应用应形成专门体系,整合学校技术和管理方面的优势,建立有效的更新机制,并在实践中逐步完善[3-4]。

### 4.1 服务器

服务器是校园一卡通系统的核心,宜采用新版 Windows Server 操作系统和 Oracle 数据库系统实现数据存储和管理功能。对服务器应分类管理,通过本机 RID3 模式进行一级备份,外置二级备份作为冗余手段,以保证原始数据安全。对一卡通系统在数据收发等过程中自身导致的错误,要及时将消费终端底层的保留数据进行比对校正,保持卡账平衡。圈存服务器是校园专网与银行外网间数据通信的唯一网络关口,应配置硬件防火墙作安全防护,对业务请求加以实时过滤,外来敏感数据则做到有效隔离,防止蠕虫类病毒感染、传播和破坏。根据校园一卡通系统发展和使用的需求,提前做好服务器更换或升级规划,对系统、数据的迁移和测试宜安排在寒暑假期间,预留充分时间处理突发问题。

### 4.2 主机

主机负责各业务部门功能的实施。主机应采用授权方式打开应用管理系统,厂方维护员和校方从业人员均需按各自用户名及密码登录行使工作权限,人员离开即时注销。发现问题凭操作日志或工作记录来进行追溯。针对主机操作系统及应用软件故障或病毒感染问题,应提前做好防护及备份工作。操作系统安装与设置用时较长,一卡通系统安装要求更为复杂,需绑定计算机名、用户名并以 IP 地址验证的方式连接服务器调试参数。在软件安装调试结束后,应立即用 PE 系统启动主机,调用 Acronis True Image 软件,将上述系统备份至专门分区保存,再调用 Disk Genius 工具将备份分区设为隐藏加以保护,需要时可快速恢复,见图 3。

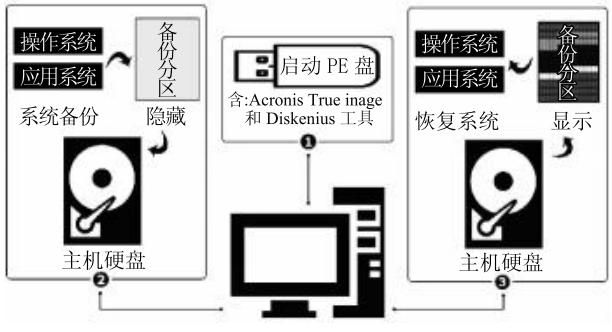


**图 3 硬盘分区备份与恢复示意**

**Fig. 3 How to back up and restore hard disk partitions**

### 4.3 终端

终端故障主要以键盘、通信芯片和接头为主。一般现场更换备件,在油污、水气侵蚀严重的食堂、水房和浴室等区域,接头应选用防水接头;键盘主要采用加贴硅胶保护套及终端整体覆膜保护。更换终端时要在正面标记序号和机号,避免数据错乱。应建立设备日常保养制度,以检查、培训手段促进长效管理。对终端更新系统码、黑名单等引起的网络数据阻塞,应在零点后、早餐前进行。

### 4.4 网络

网络中最重要的是通信线路安全。光纤线路及网络关口发生问题时,应先用智能寻线仪探查配线架和光交换机模块。若因跳线接触不良或设备故障,同型号备件更换;否则需用可视故障探测仪分段检查光纤线路,逐步缩小范围查明断点,熔接修复。

食堂、水房和浴室等单位的三级子网均以 RS485 协议上连主机、下接消费终端,承载着底层数据传输的作用,最易发生电线与通信线的短路风险,引发线路损毁。依据综合布线可靠性原则,在环境

复杂和终端集中布设的重要部门，推荐采取间隔冗余布线方案。在每个机位下方分别设立强电、弱电两只分线盒连入终端，一路线接单号机，另一路线接双号机，详见图 4。故障发生时，即可保证每个营业点内都有一台终端可用，避免因线路故障产生营业损失，也给抢修和设备维护带来了便利。

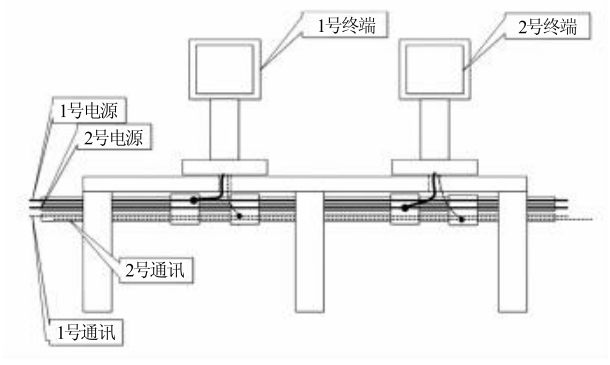


**图 4　间隔冗余布线法**

**Fig. 4　Interval redundant wiring method**

### 4.5　管理方面

管理策略首先要在制度建设的基础上，弥补缺乏顶层设计带来的缺陷，逐步完善一卡通系统的管理措施和人员管理，使其既符合技术规范要求，又能充分发挥业务功能。校园一卡通系统发展到现在，欲达到优化管理的目标，必须充分发挥学校各部门的优势，联合厂方共同做好安全保障工作。

建议学校以信息部门牵头组建一卡通管理中心，负责系统的规划、维护和日常服务管理。校财务部门负责银行、师生间账务业务，代表学校监管圈存、缴费资金。将校园的生活业务和医疗业务归属后勤部门。图书馆负责图书系统的工作。教务部门负责选课、报名考试、缴费等功能的管理。做到规范划分，分工明确，各司其职。

学校对校园一卡通从业人员应统一管理，制定岗位职责、技能要求及考核内容。从机房每日工作要点、维修流程、应急预案等细节入手，不断改进管理措施。梳理日常故障案例，总结维护经验，定期组织管理人员和操作人员进行专业技能和安全知识的培训。

## 5　结束语

校园一卡通系统安全性的建立，是一个系统工程，从设计之初、施工过程到应用期间都需不断总结经验，加以完善。一卡通已不再是学校某部门的单一应用，而是具有汇聚全校行政管理功能、教学与生活业务功能和数字收付功能的三重属性。面对智慧校园的创新发展和大数据的综合运用，业务开放性和数据共享性将使系统安全受到进一步挑战。如何保证系统的安全，体现了高校信息化管理水平再上一个台阶，则亟待后续的深入研究及探讨。

## 参考文献

[1] 田爱宝，董增华. 校园一卡通网络安全设计与实现[J]. 微型电脑应用，2016，32(7)：68-70.

[2] 王永建，郎丰凯，王迅，等. 智慧校园一卡通系统安全研究[J]. 信息安全研究，2016，2(5)：454-461.

[3] 陈晓红. 校园一卡通系统安全方案设计[J]. 武汉职业技术学院学报，2008，7(1)：79-82，86.

[4] 鄢翔. 基于安全等级保护 2.0 的高校一卡通应用系统安全方案设计[J]. 电子技术与软件工程，2019 (1)：192-195.

(上接第 23 页)

路跟踪效果较好；最大航向偏差约为 1rad，此时车道保持系统控制下转向系统输出转角值约为 23°，能及时帮助驾驶员纠正车辆的偏离动作。通过对该算法的上述仿真测验可知，基于 LQR 算法搭建的车道保持控制模型具有较好的实时性和鲁棒性。由图 7 可知，所搭建的车道偏离预警模型适用性和有效性较好。

## 4　结束语

本文研究的车道偏离预警技术和车道保持控制技术是车辆智能辅助驾驶系统的重要组成部分，通过仿真实验与实车测验可知该模型具有一定的实用价值与应用前景。

## 参考文献

[1] 李晗. 基于机器视觉的高速车道标志线检测算法的研究[D]. 沈阳：东北大学，2006.

[2] 余天洪. 基于机器视觉的车道偏离预警系统的研究[D]. 长春：吉林大学，2006.

[3] MAMMAR S，GLASER S，NETTO M. Time to line crossing for lane departure avoidance：A theoretical study and an experimental setting [J]. IEEE Transactions on Intelligent Transporation Systems，2006，7(2)：226-241.

[4] MAMMAR S，MINOIU-ENACHE N M，GLASER S，et al. Lane keeping automation at tire saturation[C]// Proceeding of the American Control Conference. Baltimore，Maryland：IEEE，2010：6466-6471.