ICS 35.240.50
L 67

中华人民共和国国家标准

GB/T 28847.3—2012

建筑自动化和控制系统
第3部分:功能

Building automation and control systems—
Part 3:Function

(ISO 16484-3:2005,Building automation and control systems(BACS)—Part 3:Functions,NEQ)

2012-11-05 发布　　2013-02-15 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

GB/T 28847《建筑自动化和控制系统》分为七个部分：

——第 1 部分：概述；

——第 2 部分：硬件；

——第 3 部分：功能；

——第 4 部分：应用；

——第 5 部分：数据通信协议；

——第 6 部分：数据通信一致性测试；

——第 7 部分：工程实现。

本部分为 GB/T 28847 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法参考 ISO 16484-3:2005《建筑自动化和控制系统　第 3 部分：功能》编制，与 ISO 16484-3:2005 的一致性程度为非等效。

本部分由住房和城乡建设部提出。

本部分由全国智能建筑及居住区数字化标准化技术委员会(SAC/TC 426)归口。

本部分起草单位：住房和城乡建设部信息中心、中外建设信息有限责任公司、北京交通大学、机械工业仪器仪表综合技术经济研究所、住房和城乡建设部 IC 卡应用服务中心、深圳达实智能股份有限公司、广州市聚晖电子科技有限公司、松下电器研究开发(中国)有限公司、深圳鹰锐通电器制造有限公司、北京复旦微电子技术有限公司、上海宸新智能系统集成有限公司、深圳市赛为智能股份有限公司、青岛海尔智能家电科技有限公司、上海长江新成计算机系统集成有限公司、吉林省一夫智能科技有限公司、国家电网公司四川德阳电业局。

本部分主要起草人：王辉、周欣、杨辉、周波、张永刚、陈列、尚治宇、马虹、申绯斐、王毅、程卫东、王春喜、林木青、贾东耀、黄吉文、肖明超、王宝鹏、杨硕、林必毅、顾清坤、胡龙、顾国矛、廖学静。

建筑自动化和控制系统
第3部分:功能

1 范围

GB/T 28847的本部分规定了建筑自动化和控制系统功能框架、基本功能,以及机电设备监控系统、火灾自动报警及消防联动控制系统和安全防范系统的功能要求。

本部分适用于建筑自动化和控制系统的功能设计和实施。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 4715 点型感烟火灾探测器

GB 4716 点型感温火灾探测器

GB/T 4718 火灾报警设备专业术语

GB 14003 线型光束感烟火灾探测器

GB 15631 特种火灾探测器

GB 16280 线型感温火灾探测器

GB 16796 安全防范报警设备安全要求和试验方法

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 18336.1 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

GB/T 18336.2 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求

GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求

GB 20815 视频安防监控数字录像设备

GB/T 28847.1 建筑自动化和控制系统 第1部分:概述

GB 50016 建筑设计防火规范

GB 50045 高层民用建筑设计防火规范

GB 50067 汽车库、修车库、停车场设计防火规范

GB 50098 人民防空工程设计防火规范

GB 50116 火灾自动报警系统设计规范

GB 50166 火灾自动报警系统施工及验收规范

GB 50189 公共建筑节能设计标准

GB/T 50314 智能建筑设计标准

GB 50348 安全防范工程技术规范

GB/T 50378 绿色建筑评价标准

GB 50394 入侵报警系统工程设计规范

GB 50395 视频安防监控系统工程设计规范

GB 50396 出入口控制系统工程设计规范

GB 50411 建筑节能工程施工质量验收规范

GB 50464　视频显示系统工程技术规范
GBZ 122　离子感烟火灾探测器放射防护标准
GA/T 72　楼宇对讲系统及电控防盗门通用技术条件
GA/T 74　安全防范系统通用图形符号
GA/T 75　安全防范工程程序与要求
GA/T 269　黑白可视对讲系统
GA 308　安全防范系统验收规则
GA/T 367　视频安防监控系统技术要求
GA/T 368　入侵报警系统技术要求
GA/T 394　出入口控制系统技术要求
JGJ 176　公共建筑节能改造技术规范

3　术语和定义

GB/T 28847.1界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 28847.1中的某些术语和定义。

3.1

三触点控制　3 point control

具有三个位置输出的控制功能。这三个输出是零和两个符号相反的数，是通过两个二进制信号表示的三种控制状态。这些输出用于定位。

3.2

闭环控制　closed loop control

被控的输出以一定方式返回到作为控制的输入端，并对输入端施加控制影响的一种控制关系。

3.3

节点　node

在BACS中，指可寻址设备连接到通信介质的点。

3.4

点地址　point address

在BACS中，指系统访问点信息的唯一的数据点标识符。

3.5

脉冲信号　pulsed signal

时间上不连续的信息特征信号。

3.6

站点　site

在建筑物内，为安装设备而明确界定的区域。

4　缩略语

下列缩略语适用于本文件。

BACS：建筑自动化和控制系统(Building Automation And Control System)
BACS PL：建筑自动化和控制系统点表(Building Automation And Control System Points List)
I/O：输入/输出(Input/Output)
MCU：微控制单元(Micro Control Unit)

MOU:监视和操作单元(Monitoring And Operator Unit)

5 总则

5.1 BACS 框架

系统框架图如图 1 所示。

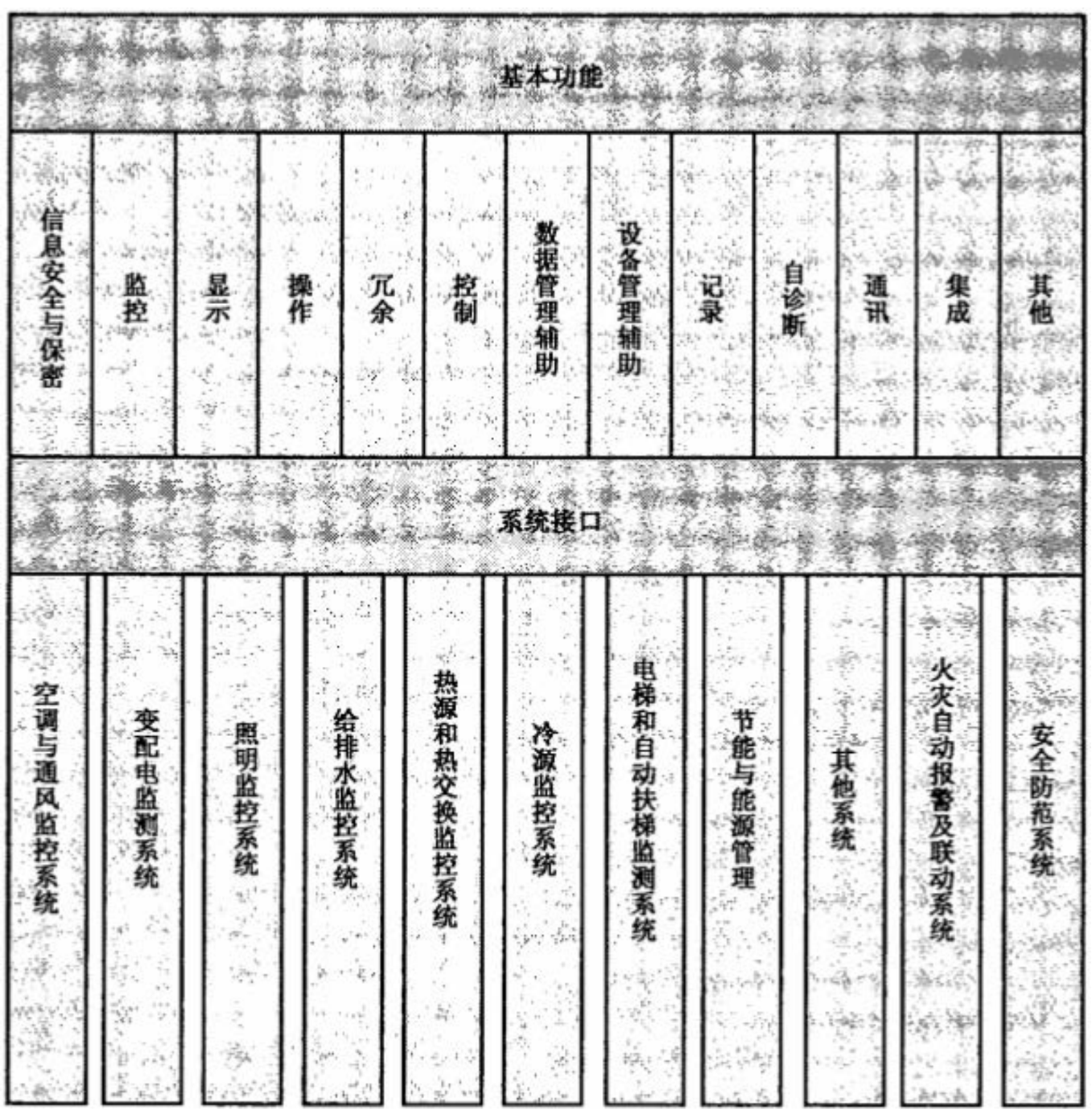


图 1 BACS 框架图

5.2 基本功能

5.2.1 一般规定

系统应具有信息安全与保密、监测功能、显示功能、操作功能、冗余功能、控制功能、数据管理功能、设备管理功能、记录功能、自诊断功能、通信功能、集成功能和其他功能等。

系统功能配置管理参见附录 A。

5.2.2 要求

5.2.2.1 信息安全与保密

5.2.2.1.1 信息安全

信息安全要求包括:

a) 一般规定:

- 对涉及人身安全的信息设备，应具有主管部门颁发的3C认证标志；
- 信息系统安全应符合GB 17859、GB/T 18336.1、GB/T 18336.2和GB/T 18336.3的要求；
- 保障运营服务信息系统的安全，保证运营服务系统不会对用户造成信息安全损害。

b) 基本安全活动：

- 根据信息系统特点和服务对象的需求，基于风险分析的结果，确定信息系统的安全等级；
- 具有安全策略的制定、发布、培训、评价、修正等功能；
- 确定信息系统中的关键信息资产，并进行资产分类管理；
- 根据信息系统的安全等级，具有相应的物理和环境安全保护体系；
- 根据信息系统的安全等级，具有相应的信息安全技术保障体系；
- 针对信息系统和普通用户，具有应急响应体系、安全基础设施服务体系、定期的安全风险评估体系等；
- 根据信息系统的安全等级，具有对相应的信息系统承包商、信息软硬件产品进行安全资质审查、实施过程的质量监督和控制等功能；
- 根据信息系统的安全等级，具有对系统运行过程中可能发生的升级、完善等活动做好安全规划，对系统的拆除提前做好规划和处理等功能。

c) 风险分析与评估：

- 应对信息系统进行风险分析，并将风险分析结果作为确定相应系统安全等级的主要依据；
- 应具有定期和不定期风险评估的机制；
- 信息系统的安全风险分析与评估，宜由有相应资质的机构完成；
- 风险分析与评估宜采用适用的方法，对每一个识别出的信息资产，按照资产的“保密性”“完整性”“可用性”和“可控性”四个最基本的安全要求，分析可能受到的威胁和后果，提出相应的安全需求建议。

d) 安全策略：

- 物理安全策略：确定在物理访问、保护方面的安全规定；
- 访问控制策略：规定内部网与外部网之间，以及内部网段之间的访问规定和策略要求；
- 安全检测策略：规定对系统安全实施定期检查的周期、方法等；
- 审计与监控策略；
- 网络防病毒策略；
- 备份与灾难恢复策略。

e) 安全体系：

- 具有明确的信息安全体系，包括明确的安全策略、网络系统配置安全服务和安全机制运行说明，指明在哪些部位必须配置哪些安全服务和安全机制，以及规定如何进行安全管理；
- 采取措施保护局域网；
- 采取措施保护基础通信设施；
- 采取措施保护边界；
- 配置或依托公共信息安全基础设施；
- 根据系统的实际情况，确定具体的安全措施。

f) 本地计算环境：

- 计算环境涉及的局域网络、主机设备、操作系统、应用支撑系统(包括WEB系统、数据库系统等)和应用系统，都应该采取相应的措施保护在计算环境内存储、传输和处理的数据的保密性。
- 计算机环境涉及的局域网络、主机设备、操作系统、应用支撑系统和应用系统，都应采取相

应的措施保护本地计算环境内存储、传输和处理的数据的完整性，以及系统的完整性。系统完整性措施包括主机漏洞扫描、防病毒和补丁管理等。

- 确保本地计算环境内的网络平台、操作系统、应用支撑系统以及应用系统正常地运行，并使授权用户得到所需的系统和应用服务。
- 具有足够的防止内外人员进行违规操作和攻击的能力。

g) 网络基础设施：

- 具有机房和通信缆线的物理环境保护措施；
- 具有保护网络基础设施的可用性，保证基础设施所支持的业务应用的可用性的功能；
- 具有保护网络基础设施控制信息，保护网络基础服务系统的保密性和完整性的功能；
- 根据用户需求提供物理隔离或逻辑隔离的网络体系。

h) 边界：

- 具有网络访问控制体系，划分虚拟子网或安装网络防火墙；
- 根据安全需求，在网络边界之间建立安全的通信连接，以保护通过边界传输数据的保密性；
- 所有的边界节点都是合法的，并在有效的安全管理控制之下；
- 宜考虑边界的冗余配置、容错和负载均衡机制，以及加强边界设备自身安全保护，保证通过边界的通信的连续性；
- 具有系统远程访问安全系统，以保护系统边界远程访问的安全；
- 具有基于网络的入侵检测系统，以防止入侵者的攻击；
- 具有基于网络的防病毒系统，以防止病毒入侵；
- 具有漏洞扫描系统以改进系统的配置和功能设置。

i) 支撑性安全基础设施：

- 公共密钥基础设施；
- 密钥管理系统；
- 安全管理系统；
- 应急响应体系。

5.2.2.1.2 监测功能

系统信息安全与保密的监测功能应具有以下要求：

——状况监测：对数字和模拟管理点的状况进行监测。定期更新数据，并可将该数据随时显示在监视器上。

——警报发生监测：发生警报时，自动执行警报发生信息显示和强制画面显示，并在鸣响警报铃的同时，显示出警报和未确认警报指示器。对每一管理点可进行警报级别以及画面强制显示级别、警报声音信息等的设定，并且还可设定每一警报级别的警报铃声。

——启动/停止失败监测：在输入启动/停止指令并经过一段时间后，设备状况仍然与输出状况不一致，则被视为启动/停止失败(异常停止/启动)而发出警报。

——计测值上下限监测：对计测值进行上下限设定，当计测值大于设定值时，则执行警报判断操作。

计测值偏差监测：对计测值进行偏差设定，当控制标准值和计测值的偏差大于该设定值时，则执行警报判断操作。

连续运转时间监测：当设备的连续运转时间大于设定值时，则发出警报。

运转时间累计：依据设备的运转状况累计运转时间，作为维修和检查的指南。

——启动/停止次数累计：累计设备的启动/停止次数，作为维修和检查的指南。

监视器使用范围指定：可分别指定监视器、打印机、警报铃等的使用范围。当其中的一台监视器发生故障时，另一台监视器将会自动切入，或按照备份用的设定使用范围进行监测。

5.2.2.2 显示功能

系统显示功能包括：

——监视器系统图显示：以图表显示每一个系统的控制和管理内容，应显示设备的实际运转状况以及各种数据，并定时刷新。系统间重叠画面的转移和对图表全排列画面的切换，应以单触点操作完成，并显示出设备时间表中的时间。

——动画显示：以符号形状、颜色变化产生的动画来表示设备运行情况和计测值。

——多窗口显示：包括监视器系统图显示在内，可以同时显示出多种一览表，以及数幅控制画面。

——画面移动显示：当所有的数据无法一次显示在画面上时，可以利用滚动条移动画面以显示出剩余数据。

单管理点的详细画面显示：可从系统中调出单管理点的详细画面，应显示有该管理点 48 h 间隔内的趋势图，并可对该管理点进行名称变更等的操作。

——趋势图、长条图显示：以最大 48 h 间隔的时间数列方式，每隔 1 min 将计测值记录，并且每隔 30 min 或 1 h 将累计值分别显示在趋势图、长条图、累计图、组合图上。

日历显示：在监视器画面应显示有年月日、星期、时间等，也可依据指定条件解除该显示。

——警报一览表显示：以一览表方式显示出系统中所发生的警报，也可执行报表列印输出操作，并可利用警报级别和管理点名称等进行检索操作。

未确认警报一览表显示：以一览表方式显示出系统中尚未经过确认的警报。警报确认操作可以汇总或个别被执行，也可执行报表列印输出操作，并可利用警报级别和管理点名称等进行检索操作。

维修登录一览表显示：以一览表方式显示出维修登录管理点。可执行报表列印输出操作，也可利用管理点号码和管理点名称等进行检索操作，并可解除维修操作状态。

——设备一览表显示：以一览表方式显示出计测点、累计点、运转中的设备、停止运转中的设备、设备状况等的信息。可执行报表列印操作，并可利用管理点号码和管理点名称等进行检索操作。

——程序一览表显示：根据每一程序的类型，以一览表方式显示出日历、时间程序、联动程序、趋势图、长条图显示等各种程序的名称。

日报/月报/年报显示：以日报(时间单位)、月报(日单位)、年报(月单位)的格式显示出所指定的计测值和计量值，画面显示数据可被列印输出。

——预约画面显示：可进行预约画面设定、显示。

——履历的显示：可调出被监视器上删除的最后 20 幅中的画面。

——选择显示：可跳过显示中的画面直接显示出所需的画面。

——警报指示显示：在警报发生时，可显示有处理程序以及紧急联络地址的画面。

5.2.2.3 操作功能

系统操作功能包括：

——手动启动/停止(切换)：可在系统中对特定设备进行手动启动/停止(切换)操作；

程序设定值变更：更改时间、标准值、控制参数、登录管理点等的程序设定值；

——许可/禁止指定：以管理点和程序为单位，可执行暂停控制操作；

——维修登录/解除：以管理点为单位，可执行暂停控制操作和警报判断；

——鼠标操作：利用鼠标可以选择画面和进行操作；

操作密码设定：在执行某一操作时，可设定操作许可级别/操作设备范围。

5.2.2.4 控制功能

系统控制功能包括：

——日历功能：使用自动判断闰年、大月、小月的万用日历，应可设定 12 个月份中的指定节假日；

——系统计时：

- 内部/外部时钟要求；
- 外部时钟的种类要求；
- 系统时钟的精度要求；
- 整个系统的时间同步要求；
- 本地数据处理设备或服务站的时间与日期变化要求；
- 网络和单机设备的时间与日期变化要求。

——时间程序：将动力设备等登录于时间程序中，即可自动驱动该设备的定时开/关动作。时间程序根据 7 天 2 假日的周期，可对各设备的启动/停止时间进行多次设定。不论是星期几均可在 7 天以内（包含当日）变更各设备的启动/停止时间（时间表的临时变更处理），最小可以 1 min 为单位设定时间程序。

——联动程序：以管理点的状况变化、警报发生等为设定条件，可驱动预先设定的对象动作。

火灾意外事故程序：发生火灾时，可联动停止空调器等相关设备的运作。在触发火灾信号时，火灾画面应显示在监视器上，并可由人工触发。

——停电处理：断电时（在没有备用电源的场合），只有火灾意外事故程序和手动操作可以执行输出操作。

——自备发电时的强制驱动控制：当进行自备发电时，应自动记录设备的工作参数。

恢复供电程序：恢复供电后，遵照自动或手动的恢复供电指令操作，并依照自备发电时的强制驱动控制让运转设备停止运作，参照时间表让停电瞬间正在运转（闭路）中的设备重新启动（投入）。

——最佳启动/停止控制（预冷预热控制）：根据温度的上升、下降特性的预测判断，控制空调器的最佳启动/停止时间。

室外空气引入控制：在季节过渡期间，使用室外空气当作冷循环使用时，本控制系统将有效地控制引入室外空气。

——远程设定值的时间控制：在规定时间内对预先设定好的指定时间进行自动变更管理。

——简易运算控制：可执行加、减、乘、除、与、或等运算的设定。

注 1：最佳启动/停止时间基于时间程序、室温、室温增益（变化趋势）等理论，以人工智能控制方式推算而得。

注 2：室外空气的引入根据室外空气和循环空气（室内）的比例，与其室内温度的比较运算值来判断。

5.2.2.5 数据管理功能

系统数据管理功能包括：

——数据使用和存储：I/O、处理和其他管理功能的状态变化和数值的改变应以包含时间戳方式存储，用于事后分析。

——趋势数据的再显示功能：以月为单位，按时将趋势/长条图显示、高速趋势图显示、日报/月报/年报显示、警报记录、操作/状况变化记录等所搜集、累积的数据保存于存储设备之中。必要时也可再显示、列印出存储数据。

用户数据处理辅助功能：可将指定计测值、累计值、趋势数据等输出于各种存储设备中，并可在常用软件中使用这些累积数据。

——警报记录：将累积的警报发生和复位等数据，以图表方式显示、列印输出。

——操作/状况变化记录：将累积的操作指令和设备的状况变化等数据，以图表方式显示、列印输出。

——数据归档：历史功能数据库所收集的数据和其他的系统数据可使用数据归档方法永久归档。

——数据的导入导出：数据处理装置或服务器应具有导入导出数据的能力，数据格式应予以规定。

——备份和存储：提供备份软件、备份方式、恢复所有功能及其配置的方法和使用的备份介质。

——备份与存储要求提供完成系统备份和系统恢复所需的时间。

——数据导入导出应至少提供数据处理装置或服务器的数据导入格式、传送到控制器/自动化站的数据导入格式和从控制器/自动化站传出数据的导出格式。

5.2.2.6 设备管理功能

系统设备管理功能包括：

——设备登记簿/记录履历管理；

——设备运转工况记录管理；

——设备操作人员情况登记管理；

——安全保障时间表管理。

5.2.2.7 记录功能

系统记录功能包括：

a) 信息打印：

- 执行警报记录；
- 正常复位记录；
- 启动/停止失败记录；
- 计测值上下限警报记录；
- 日报变化记录；
- 停电/恢复供电记录；
- 火灾时间记录；
- 操作记录；
- 状况变化记录。
- 警报发生时以红字，警报复位时以蓝字，其他状况时则以黑字进行列印。

b) 报表打印：

- 以指定的日、月、年使用量总计值为列印单位，或是手动输入日、月、年以列印日报、月报、年报；
- 可打印出极大值、极小值、平均值等的计算值；
- 可根据任意设定管理点、标题、检验章栏的有无等以格式化方式来列印日报、月报、年报。

c) 拷屏彩色打印：

- 对显示于监视器上的画面进行拷贝记录，并在拷贝时进行彩色输出。

5.2.2.8 自诊断功能

系统自诊断功能包括：

——传送系统故障监控：当远程装置传送异常时，实施警报显示；

系统异常状况自行监控：监控系统中的各块模块状况、通信状况，以便在发生异常状况时列印信息；

——诊断功能应至少提供存储器和系统资源使用要求、所有系统网络通信活动的失效率要求、系统

故障的原因要求。

5.2.2.9 冗余功能

规定可使用多重硬件自动克服任何设备失效的能力，系统可配置对电源供应、处理单元、输入输出单元、网络接口与访问单元、硬盘、主存储器、显示器、键盘、鼠标和其他定位设备、打印机失效/缺纸等设备冗余。

5.2.2.10 通信功能

系统通信功能包括：

——通话功能：利用鼠标器选择远程子机电话，进行呼叫和互相通话；

音频监控功能：利用鼠标器选择远程子机电话，监控附近的声音；

数据传输通信功能：实现各系统设备之间的数据通信，以及与系统外设备数据的通信。

5.2.2.11 集成功能

系统集成功能包括：

系统内不同设备之间的数据通信、功能联动、数据库共享、系统报表的集成管理；

——与火灾自动报警系统、安全防范报警系统之间的功能联动、数据库共享、系统报表的集成管理；

与其他系统的功能联动、数据共享、报表的集成管理；

5.2.2.12 其他功能

其他功能包括：

——节能设备应用；

——能源管理与节能控制管理；

——其他管理。

6 机电设备监控系统

6.1 一般规定

机电设备监控系统用于对建筑物或建筑群内的空调与通风、照明、给排水、热源和热交换、冷源等设备进行集中监视、控制及自动化管理，对变配电、电梯和自动扶梯等设备进行集中监测及自动化管理。

机电设备监控系统可分为空调与通风监控、变配电监测、照明监控、给排水监控、热源和热交换监控、冷源监控、电梯和自动扶梯监测，以及其他应用子系统。各子系统应满足下列要求：

BACS PL 参见附录 B；

——应用子系统设计应符合 GB/T 50314、GB 50189、GB 50411、GB/T 50378 和 JGJ 176 的要求。

6.2 要求

6.2.1 空调与通风监控系统

空调与通风监控系统应符合下列要求：

a) 压缩式制冷机系统和吸收式制冷系统的运行状态监测、监视、故障报警、启停程序配置、机组台数或群控控制、机组运行均衡控制及能耗累计；

b) 蓄冰制冷系统的启停控制、运行状态显示、故障报警、制冰与溶冰控制、冰库蓄冰量监测及能耗累计；

c) 空调机组中冷冻水及冷却水相关状态：

- 冷冻水供、回水温度；
- 压力与回水流量监测；
- 冷冻泵启停控制(由制冷机组自备控制器控制时除外)和状态显示；
- 冷冻泵过载报警；
- 冷冻水进出口温度；
- 压力监测；
- 冷却水进出口温度监测；
- 冷却水最低回水温度控制；
- 冷却水泵启停控制(由制冷机组自带控制器时除外)和状态显示；
- 冷却水泵故障报警；
- 冷却塔风机启停控制(由制冷机组自带控制器时除外)和状态显示；
- 冷却塔风机故障报警。

d) 空调机组运行状态显示：

- 机组启停控制；
- 过载报警监测；
- 送、回风温度监测；
- 室内外温、湿度监测；
- 过滤器状态显示及报警；
- 风机故障报警；
- 冷(热)水流量调节；
- 加湿器控制；
- 风门调节；
- 风机、风阀和调节阀连锁控制；
- 室内 CO_2 浓度或空气品质监测；
- 防冻控制(寒冷地区)；
- 送回风机组与消防系统联动控制。

e) 对变风量系统实现节能运行方式：

- 变风量系统的总风量调节；
- 送风压力监测；
- 风机变频控制；
- 最小风量控制；
- 最小新风量控制；
- 加热控制；
- 变风量末端自带控制器时应与建筑设备监控系统联网。

f) 风机的相关控制：

- 对通风用的送风机/排风机的运行状态进行监测和控制，并可按空气环境参数要求自动控制启停，风机与消防系统联动控制；
- 风机盘管机组的室内温度测量与控制；
- 冷(热)水阀开关控制；
- 风机启停及调速控制；
- 能耗分段累计。

6.2.2 变配电监测系统

变配电监测系统应满足：

a) 对变配电系统进行电压、电流、有功功率、功率因数、用电量等参数的测量与记录；

b) 对高、低压开关柜、直流电源柜、变压器、自备发电系统的工作状态和故障进行监视；

c) 供配电系统相关状态检测：

- 中压开关与主要低压开关的状态监视及故障报警；
- 中压与低压主母排的电压和电流及功率因数测量；
- 电能计量；
- 变压器温度监测及超温报警；
- 备用及应急电源的手动/自动状态、电压、电流及频率监测；
- 主回路及重要回路的谐波监测与记录。

6.2.3 照明监控系统

照明监控系统应满足：

a) 按照照度或预设时间表对公共照明设备包括开关、调光、场景等进行控制；

b) 系统根据房间每天不同时间的亮度情况，自动优化调节灯具的亮度，节约电能；

c) 照明设施的相关控制及故障报警：

- 大空间、门厅、楼梯间及走道等公共场所的照明按时间程序控制(值班照明除外)；
- 航空障碍灯、庭院照明、道路照明按时间程序或按亮度控制和故障报警；
- 泛光照明的场景；
- 亮度按时间程序控制和故障报警；
- 广场及停车场照明按时间程序控制。

d) 根据需要对公共照明的回路进行状态检测和故障报警。

6.2.4 给排水监控系统

给排水监控系统应满足：

a) 对给排水系统的运行状态与故障状态实行监控和记录，自动调整投运水泵台数；

b) 对中水系统的运行状态与故障状态进行监控；

c) 给水系统的运行状态显示：

- 水泵自动启停控制；
- 水泵故障报警；
- 水箱液位监测；
- 超高与超低水位报警。

d) 污水处理系统的运行状态显示：

- 水泵启停控制；
- 水泵故障报警；
- 污水集水井；
- 中水处理池监视；
- 超高与超低液位报警；
- 漏水报警监视。

6.2.5 热源和热交换监控系统

热源和热交换监控系统应满足：

a) 对热源和热交换设备运行状态、故障等进行监视、记录与报警；
b) 系统的负荷调节、预定时间表自动启停和节能优化控制；
c) 对热源和热交换系统设备的联动控制；
d) 对供回水压差或供回水温度的自动控制；
e) 热力系统的运行状态监视：
   - 台数控制；
   - 燃气锅炉房可燃气体浓度监测与报警；
   - 热交换器温度控制；
   - 热交换器与热循环泵连锁控制及能耗累计。

6.2.6 冷源监控系统

冷源监控系统应满足：

系统的负荷调节、预定时间表自动启停和节能优化控制；

——系统设备的联动控制；

对系统运行参数、状态、故障等的监视、记录与报警；

对供回水压差或供回水温度的自动控制。

6.2.7 电梯和自动扶梯监测系统

电梯和自动扶梯监测系统应满足：

对电梯和自动扶梯系统运行状态和故障进行监测；

电梯及自动扶梯的运行状态显示及故障报警。

6.2.8 节能与能源管理系统

节能与能源管理系统应满足：

对空调输配系统、照明系统、给排水系统、热源和热交换系统、冷源系统等部分的节能和能源进行监测；

对空调输配系统、照明系统、给排水系统、热源和热交换系统、冷源系统等部分的节能实现分项和分区域计量；

6.2.9 其他系统

实现其他监测或控制功能。

7 火灾自动报警及消防联动控制系统

7.1 一般规定

火灾自动报警及消防联动控制系统由火灾探测器、火灾报警控制器、消防设施的联动控制三部分组成。相关部分应符合下列要求：

——对于重要的建筑物，火灾自动报警系统的主机宜设有热备份，当系统的主用主机出现故障时，备份主机能及时投入运行；

——应配置带有汉化操作的界面，操作软件的配置应简单易操作；

应预留与建筑设备管理系统的数据通信接口，接口界面的各项技术指标均应符合相关要求；

宜与安全技术防范系统实现互联，安全技术防范系统作为火灾自动报警系统有效的辅助手段；

消防监控中心机房宜单独设置，当与建筑设备管理系统和安全技术防范系统等合用控制室时，

应符合 GB/T 50314 和 GB 50116 的要求；

——系统应符合 GB 50166、GB 50045 和 GB 50016 的要求。

7.2 要求

火灾自动报警及消防联动控制系统要求包括：

——防空工程、汽车库、停车场防火规范应符合 GB 50098 和 GB 50067 的要求；

——火灾探测器应符合 GB 4716、GB 4715、GB 14003、GB 16280、GB 15631 和 GBZ 122 的要求；

——系统相关设备名称应符合 GB/T 4718 的要求。

8 安全防范系统

8.1 一般规定

安全防范系统主要由视频安防监控系统、入侵报警系统、出入口控制(门禁)系统、电子巡更系统、汽车停车场管理系统及访客对讲系统等组成。

注：出入口控制(门禁)系统设计见附录 C。

8.2 要求

安全防范系统应符合下列要求：

——系统应符合 GB 16796、GB 50348、GA/T 75、GA 308 和 GA/T 74 的要求；

——视频安防监控系统的设计应符合 GB 20815、GB 50395、GB 50464 和 GA/T 367 的要求；

——入侵报警子系统的设计应符合 GB 50394 和 GA/T 368 的要求；

——出入口控制子系统的设计应符合 GB 50396 和 GA/T 394 的要求；

——可视对讲系统应符合 GA/T 269 的要求；

——语音对讲系统应符合 GA/T 72 的要求。

附 录 A
（资料性附录）
系统功能配置

A.1 系统功能的一般描述

本附录描述在 BACS 各部分进行配置的过程中所实现的功能，执行的任务与特定系统相关。系统工程至少应包括硬件配置、控制策略配置、管理功能配置、调试和文件编制。

工程过程管理应满足工程工具和操作功能并存，系统许可证包括的工程工具。通过 MODEM、LAN、WAN 等的远程管理，自动生成文档。

A.2 硬件配置

硬件配置至少应包括：

控制原理图或系统和仪表图；

带有 I/O 功能部分和处理功能部分的数据点表，I/O 功能部分用来配置物理 I/O，处理功能部分用来估算处理器的性能和存储器的大小；

——系统和网络描述；

设备清单；

仪表图；

— 布线进度表（现场连接图）；

设备标签。

硬件配置应满足的要求至少应包括：

相同数据需要进入系统不同部分的次数；

——自动核实；

地址复制；

点名称复制；

设备的正确使用；

——进入信息的正确性。

A.3 控制策略配置

控制策略配置是将相关企业和用户的要求作为输入生成一个和多个控制策略，并下载到控制器。

控制策略配置至少应包含以下内容：

下载控制策略文件；

——列出/画出控制策略蓝图；

默认参数设置；

——带有处理和操作功能完善的 BACS PL。

控制策略配置应满足的要求如下：

a) 编程方法：

- 基于文本（程序设计语言）；

- 基于图形(功能块方法)；
- 面向对象型。

b) 可用的应用库函数的数目和类型；

c) 支持下载的类型：

- 用一条命令下载所有的控制器和自动化站软件；
- 部分下载到一个控制器/自动化站中；
- 部分下载程序段的能力，下载程序段时不中断控制器/自动化站运行的功能，也不中断网络上的其他功能运行；
- 下载所需时间。

d) 配置上传能力：

- 将配置上传到编程工具的能力；
- 源程序再生的能力；
- 源程序布局和注释再生的能力；
- 上传程序和源代码比对的能力。

A.4 管理功能配置

管理功能配置是利用相关企业和用户的要求作为输入而定义的要求来生成管理功能。

管理功能配置应包含以下内容：

——带有连接到点信息动态项的示意图；

包含组、类和过滤识别的报警；

用户访问权限；

报告格式和相关的对数据点的连接；

——系统时间表；

BACS PL 包括 I/O 功能、处理功能、管理功能和操作功能。

管理功能配置应满足的要求如下：

——根据第三方应用产生输入图的能力；

支持的资料库；

基本 HVAC(供热通风与空气调节)符号；

——HVAC(供热通风与空气调节)系统项目；

——建筑模型模板；

报告模板；

使用先前工程过程形成的能力，例如：用户地址/助记符；

——时间表项；

基于文本；

——基于图形；

——基于日志；

拷贝设施。

A.5 调试工具功能

A.5.1 一般规定

调试工具应能支持以下任务：

现场设备和硬件的连接检查；

——通信系统测试和协议分析；

——控制策略仿真和验证；

——控制策略下载和参数的初始化；

——通过设备操作和连锁仿真得到的功能性验证；

——系统优化和协调。

调试工具功能应满足的要求包括：

——策略中暂时超驰值的能力；

——观察单个程序周期中系统行为的能力。

闭环控制的处理功能主要包括处理 I/O 和实现虚拟功能，其他功能类型都可使用此功能的结果。闭环控制由诸如 P、PI、PID 之类的算法形成，从受控媒体反馈。每个闭环控制环路均包含一个设置点。

为了在 BACS PL 中定义完整的控制环路，P 控制环路或 PI/PID 控制环路功能和至少有一个控制环路输出功能的组合是必不可少的，其他功能可按需要组合。对于级联控制，过程值通过主控环路功能和从控环路功能来控制。主控环路的输出信号用作从控环路的设置点输入。

在 BACS PL 中，开/关控制器需要一种处理功能 P/PI 控制环路，并增加一个比例到开关转换功能上。三触点控制则需要两个比例到开/关转换功能，设置点参数可经 M●U 在线更改。

A.5.2 闭环控制

A.5.2.1 P 控制环路

比例控制提供的输出比例于设置点和输入信号之间的偏差，输出级别取决于“P”的值。

P 控制环路功能包括固定设置点和关联参数，它至少要与一个输出功能相结合。

A.5.2.2 PI/PID 控制环路

比例和积分控制算法与 P 算法基本相同，但具有时间相关功能的波动，该波动以比例于输入信号和设置点之间的偏差的速率改变输出信号。

比例、积分和微分控制算法在操作上与 PI 算法基本相同，但在由于输入信号的变化率而确定的输出上增加了波动。

PI/PID 算法控制环路功能包括相关参数，并至少与一个输出功能相结合。

A.5.2.3 滑动/曲线设置点

滑动/曲线设置点功能在闭环控制中使用。实际设置点值由输入信号幅度、计算功能来定义。

示例 1：滑动设置点，夏季补偿。该功能是为避免对建筑占据者和节省能源造成热冲击提供一种方法。室内温度设置点线性增加，从预定的室外温度值(起点)开始。

示例 2：曲线设置点，冬季补偿。该功能是为改变室内温度提供一种方法。这种改变取决于室外温度。水流温度的当前设置点可以通过复位时间表来计算或定义。

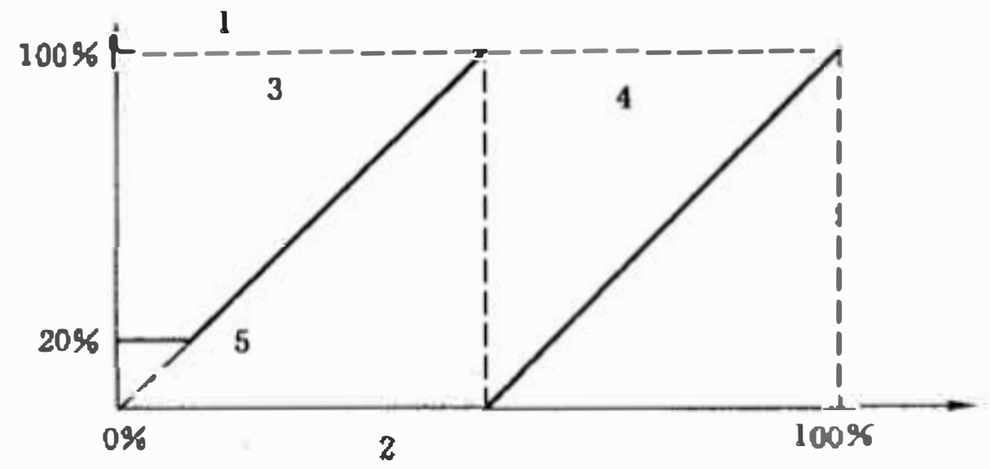
设置点参数和/或复位时间表曲线的形状经 MOU 可以同时在线改变。设置点的极限值必须由分开的设置点/输出极限功能来定义。

滑动/曲线设置点的要求应满足：复位清单的步骤数、计算设定点。

A.5.2.4 比例输出等级

当负载排序需要时，比例输出等级功能将控制器的输出转化为 n 个虚拟值。一个输出功能可分裂为两个或多个输出，并具有定义的幅度和关联参数。输出值必须与 I/O 功能相结合。每个输出等级都应该在 BACS PL 中指出。

比例输出等级的图形功能实例见图 A.1 和图 A.2。



说明：

1——调节器位置；

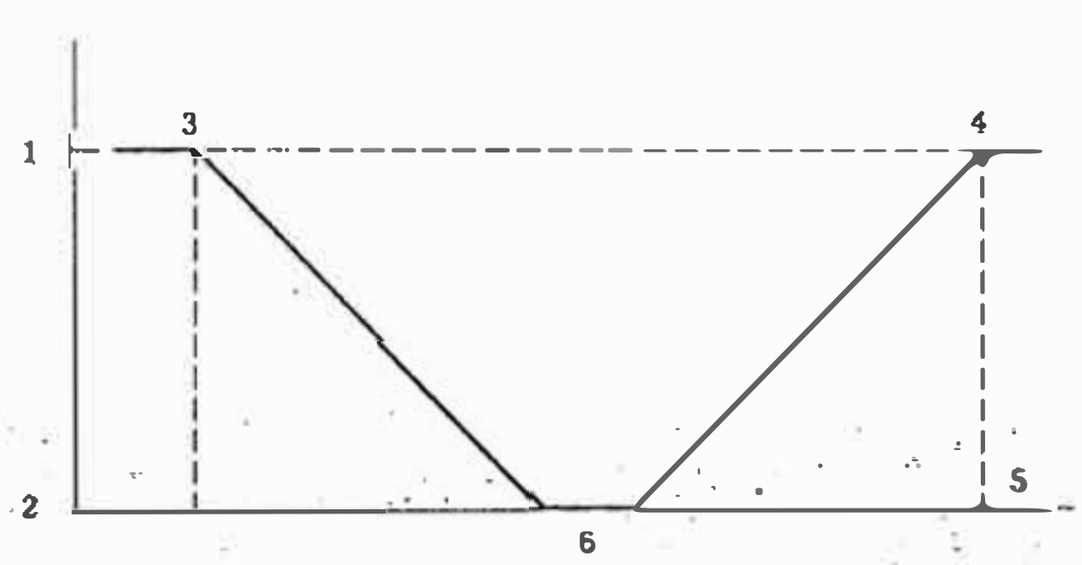
2——控制环路算法输出值；

3——输出等级 1；

4——输出等级 2；

5——输出限制值。

图 A.1　节气门和阀门序列的比例输出等级功能



说明：

1——开始；

2——关闭；

3——制冷阀门位置；

4——加热阀门位置；

5——输出百分数；

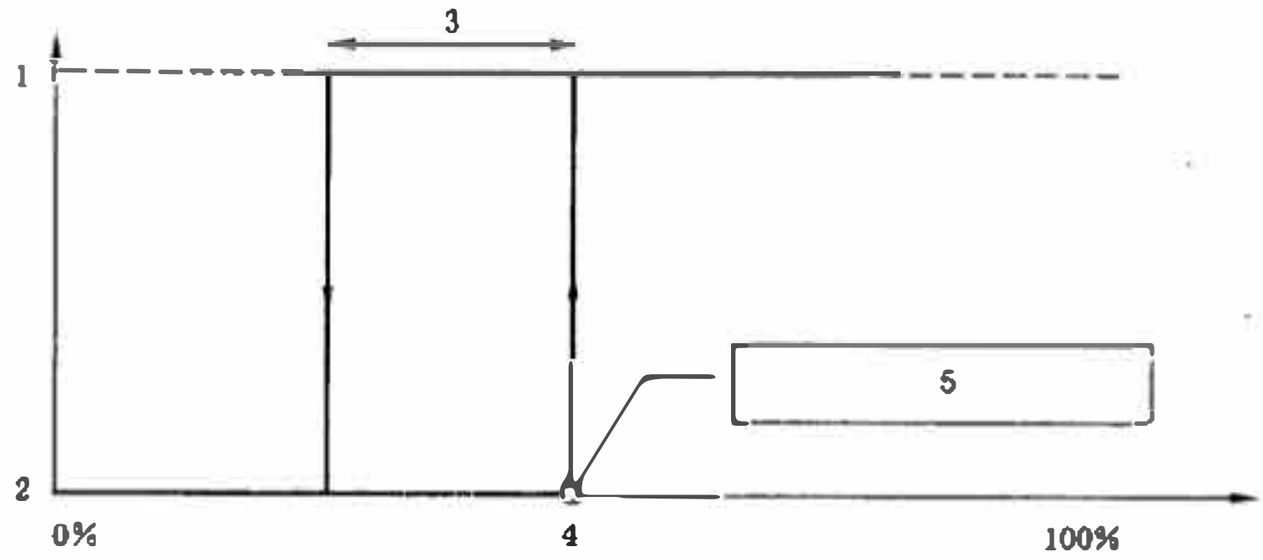
6——控制环路算法输出值。

图 A.2　制冷/加热序列的比例输出等级功能

A.5.2.5　比例到 on/off 转换

比例到 on/off 转换功能将控制器的比例输出转换为 on/off 输出。转换的执行取决于设置点和滞后值，并用于逻辑、物理和通信输出功能。

比例到 on/off 转换的图形功能实例见图 A.3 和图 A.4。



说明：

1——开；

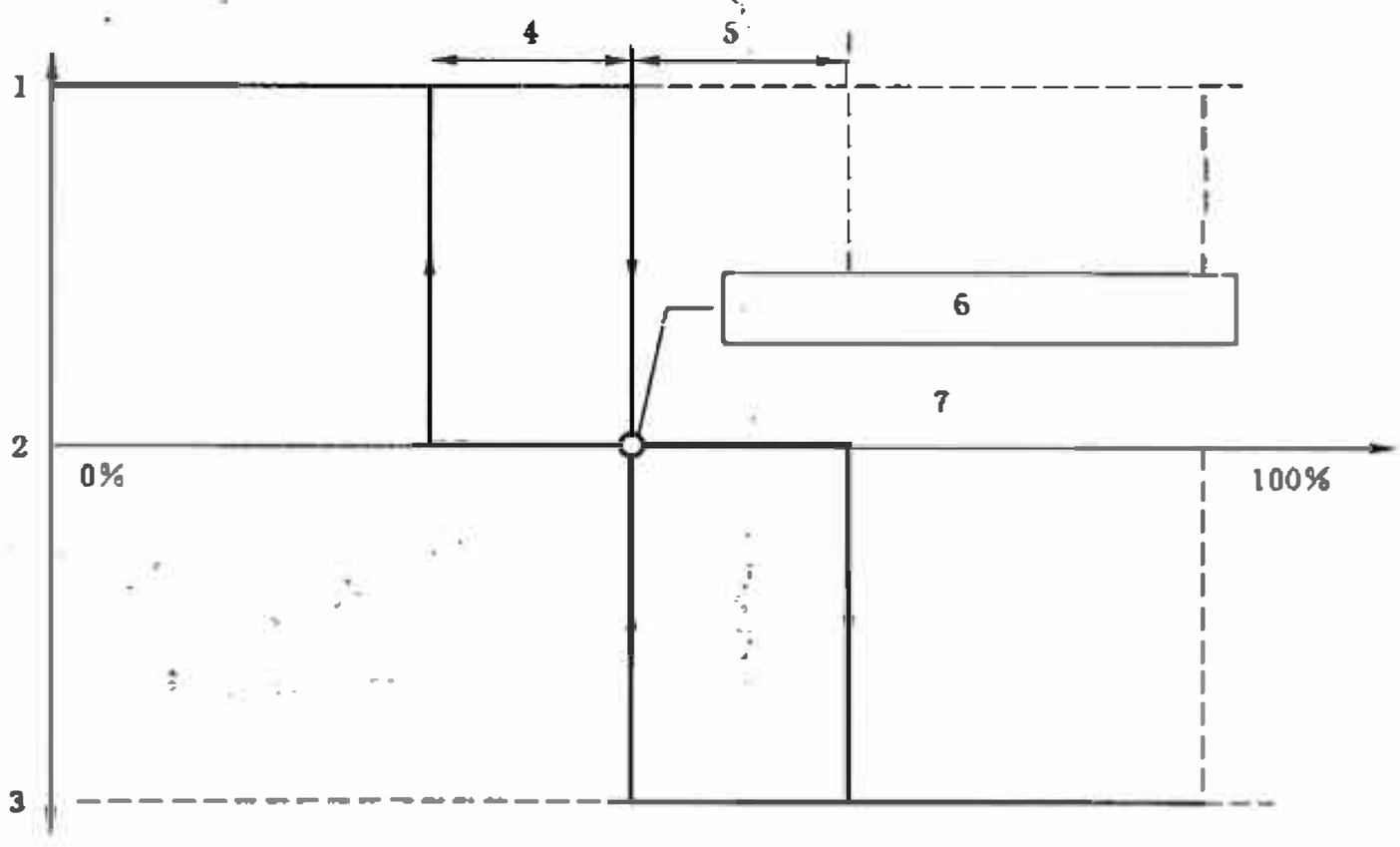
2——关；

3——滞后；

4——控制器输出值；

5——转换设置点。

图 A.3 on/off 转换



说明：

1——开 1；

2——关；

3——开 2；

4——滞后 1；

5 滞后 2；

6——转换设置点；

7——控制环路算法输出值。

图 A.4 三触点控制的 on/off 转换

A.5.2.6 比例到脉冲宽度调制

比例到脉冲宽度调制功能将 P、PI 或 PID 控制环路功能转换为带有可变标记/空格比值的脉冲，该比值取决于输入值的幅度。

A.5.2.7 设置点/输出限制

设置点和/或输出限制功能用来将信号限制到两个限制值之间的值，该功能可由安全功能超驰。每个设置点/输出限制通过在 BACS PL 中录入限制量来规定。

A.5.2.8 参数的切换

参数切换功能用来修改控制环路参数，以优化控制工作。

A.5.3 计算/优化功能

A.5.3.1 一般规定

计算功能用来计算引出的值，向用户或向另一种类型的功能提供复杂的数据，以便具有随之发生的决策功能。

跨设备/系统优化功能用于能量管理，降低能耗和费用。它们以预配置的标准功能来实现，不需要特定项目的编程。为了适配不断变化的需要，它们提供必须带有可调的参数，以给出处理各种类型建筑结构的灵活性，标准的监视、互锁和控制功能。

A.5.3.2 h,x-直接控制

在 h、x 直接控制功能的情况下，所用策略确定调节室外空气的优化方法，以便对规定的房间温度和相对湿度获得所需要的供空气的值。规定的温度和湿度，在舒适现场根据 h，x 图或用温度图表定义。该功能应在 BACS PL 中的与对应输入数据点的同一行列出，以指示专门用于对应的/受控的设备。

A.5.3.3 算术运算

算术运算功能提供任何数目的输入变量算术组合的输出，该输出可用于其他功能。

算术运算功能在 BACS PL 中与对应输入数据点同一行中列出，指示它们专门用于对应的/受控的设备项。计算结果呈现给虚拟数据点，这些虚拟点有自身的数据点地址；对应的备注列可用来指示所关联的输入功能。

A.5.3.4 事件切换

事件切换功能在预定事件发生时提供逻辑输出，该事件可由逻辑、物理或通信输入启动。

在 BACS PL 中的与对应/受控设备具有处理功能，事件切换功能应在其设备控制的同一行上列出，或作为对应的/受控的设备/部件的输出功能切换。BACS PL 应根据输出地址指示事件切换功能。

A.5.3.5 时间表

当设定时间和实际事件匹配时，时间表功能将提供一个逻辑输出。当实际时间与异常日期数据匹配时，则禁止输出，把结果分配给输出功能。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，所说明的数值表示每个指定时段内专用开/关的周期。

时间表应满足的要求包括：时间表的类型，例外天数。

A.5.3.6 优化启/停

A.5.3.6.1 一般规定

根据时间表功能的输入计算出打开/关闭设备的某个项目的最优时间，优化启/停功能将提供一个

逻辑输出。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行。

A.5.3.6.2 占空度

当算法计算出设备的某个项目为节能而关闭时，占空度功能将提供一个逻辑输出。设备运行时间的减少将是输入的温度和状态的结果。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.7 夜间冷却功能

当算法计算出内部温度高于居住期间所需温度时，夜间冷却功能将提供一个逻辑输出，还得考虑夜间室外温度。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.8 房间温度限制

房间温度限制功能作用是防止居住期间室温低于或高于可接受的限值，防止霜冻和露水侵害。当指示的室温达到限值时，HVAC 循环设备开启或关闭，有效地把室温维持在设定限值内。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.9 能量还原

能量还原功能是一种适用于还原加热/冷却/湿度的操作策略，它依据所控区域的能量要求和该区域内空气的可用能源。此功能依据焓计算，包括室外空气与回流空气焓值(或温度)的比较。由此可以以最小能量值达到所需的空间舒适条件。

当依靠焓值的差异切换调整输出时，则可提供一个可选择的功能。在使用此功能前，应确保最低限度的新生空气供应量。能量还原计算的结果是触发逻辑输出功能切换和/或定位。

应将能量还原功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.10 备用电源操作

当备用电源处于运行状态，应提供可用于切换设备的项目的逻辑输出(与可用电源能力相关)，应对设备中的各项排列优先次序。

备用电源操作一般是全系统范围的功能。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

注：在主电源恢复时，正常操作的恢复可通过主电源恢复程序功能来完成。

A.5.3.11 主电源恢复程序

主电源恢复程序触发一系列导致设备中项目的事件，可使用时间延迟和优先级。

主电源恢复程序一般是全系统范围的功能。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.12 峰值负载限制

峰值负载限制功能提供一个输出，该输出是在规定时段内能量达到最大值趋势计算的结果。对设

备中的各项按预定义的优先级次序依次关闭，这样就不会超出最大能量值，任意瞬间使用的能量值通常由物理计数输入提供。可根据供电约定以多种方式决定计算能量等级所对应的时段。

峰值负载限制一般是全系统范围的功能。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

A.5.3.13 随能源价格切换

随能源价格切换是一个取决于能量价格成本的处理功能，能量价格成本每小时、每天和/或每周、每季都会变化。能源成本较高时，低优先级的设备会被禁用或减少使用。当随能源价格切换实现的情况下，可以依据价格情况、价格成本以及设置的优先级，触发输出功能切换。该功能主要应用于多种电能价格分配的情况。

随能源价格切换是全系统范围的功能。应将该功能列于 BACS PL 中，其位置处于相应设备/受控设备的处理功能设备控制的同一行，或者当需要的情况下，则对应于相应设备/受控设备的输出功能切换。

附 录 B
（资料性附录）
建筑自动化和控制系统功能

B.1 BACS PL 的使用

B.1.1 BACS PL 中的功能

BACS PL 是一种工具，用来确定和增加特定项目的功能。把 BACS PL 作为电子数据表计算格式添加功能，这些功能包括整个设备项目功能的所有软件和项目工程/调试/文件编制。处理功能用来监视、控制和优化电动设备和机械设备，所有的处理功能是复杂程序的组成部分，它们基于分配的物理功能或通信功能，并包含必要的参数、S.I. 单元和文本。

B.1.2 BACS PL 的结构

BACS PL 被分为四个主要部分来制定设备的特殊功能，主要包括：

I/O 功能，分为物理输入输出和共享输入输出；

处理功能，分为监控、内联、闭环控制，计算和跨设备/系统优化；

——管理功能，分为通信和历史数据；

——操作功能，分为可视显示和其他消息传送功能。

BACS PL 工作的基础是设备控制原理图/控制流程图，宜使用的方法是沿着原理图中主要介质的走向，把控制相关设备项目填入这些输入输出行中。

BACS PL 的首列示出分配到所需各功能的点描述。备注栏用于对相关内容做进一步说明，当有必要时，则在单独的纸上予以说明，原则上应以面向对象的方式在一个行内结束，这样相应功能均在同一行显示。

B.1.3 通过 BACS PL 实现应用程序描述

为描述设备控制，可通过 BACS PL 描述应用程序实现。处理功能应通过在 BACS PL 中将填入的合适行和列的序号相结合，数据点功能取决于大量的所需功能，为了传送一组功能中所需的特定应用功能，可能需要使用若干列。应说明的是，不可把优化功能理解为互锁或循环功能。

当 BACS PL 不能完整地描述所需的控制方法（尤其是复杂的优化控制或附加的非标准功能）时，应准备附加的文件。这些将与相关的功能一起在 BACS PL 行中列出。为了标识通过该附加的或增强的功能所处理的数据点，应将该参考登入该数据点的行中。

B.1.4 通过 BACS PL 功能描述系统集成

当系统与共享数据点集成时，必须定义数据的客户机和服务器。BACS PL 可指示数据点对象的具体角色。

附 录 C
（资料性附录）
建筑及居住区门禁系统

C.1 门禁系统概述

C.1.1 系统构成

基于非接触式 IC 卡的门禁系统的密码应用涉及应用系统、密钥管理及发卡系统，如图 C.1 所示。

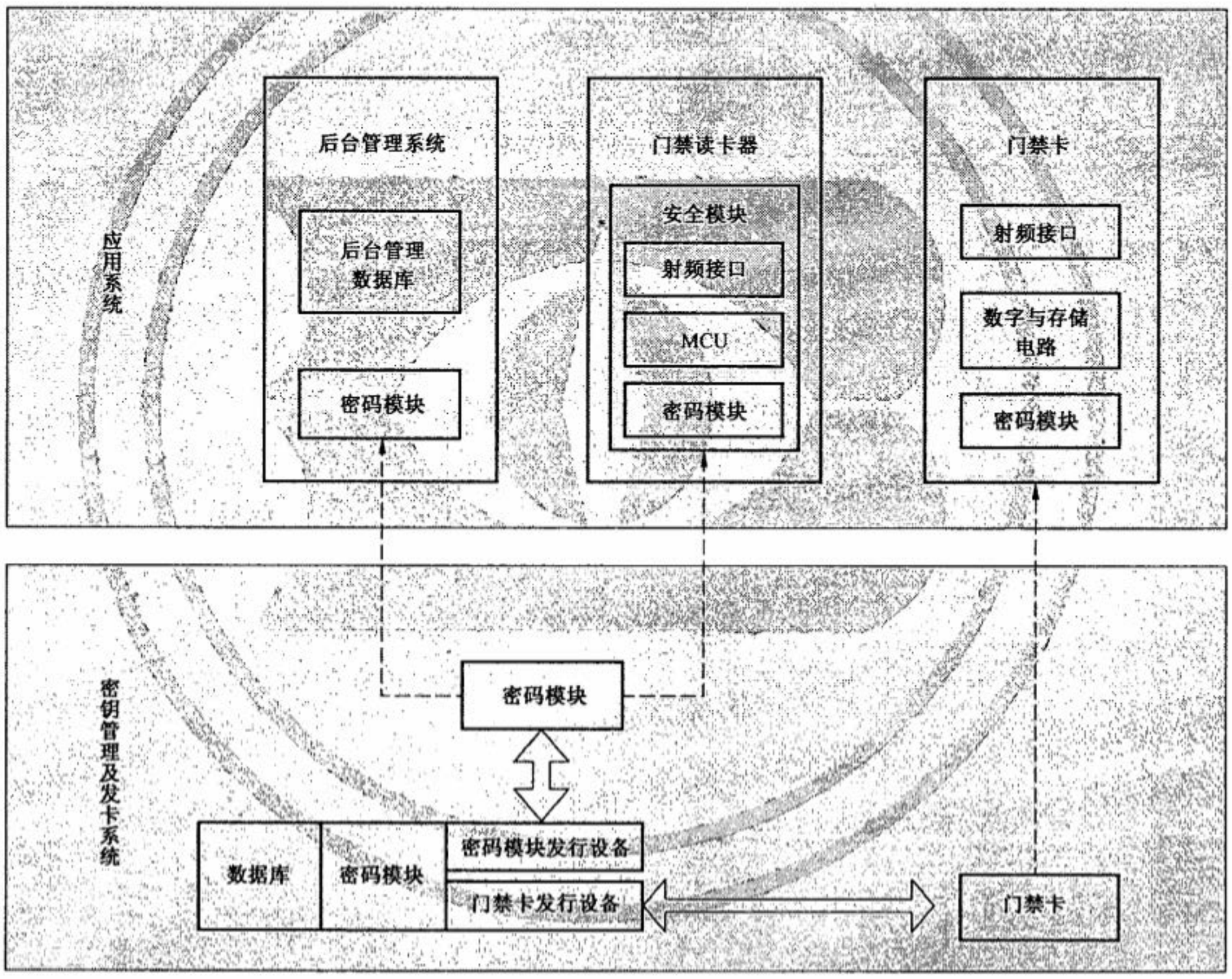


图 C.1 门禁系统中密码应用结构图

C.1.2 应用系统

一般由门禁卡、门禁卡读卡器和后台管理系统构成，通过各设备内的密码模块对系统提供密码安全保护。其中，门禁卡内的密码模块包含：

——用于门禁读卡器或后台管理系统对门禁卡进行身份鉴别时（鉴别门禁卡是否合法）提供密码服务（如计算鉴别码）；

门禁读卡器/后台管理系统内的密码模块；

——用于对门禁卡进行身份鉴别/安全报文传输时提供密码服务（如密钥分散、验证鉴别码等）。

在门禁系统的具体方案设计时，应在门禁读卡器和后台管理系统内配用密码模块。

C.1.3 密钥管理及发卡系统

密钥管理及发卡系统的功能是为了门禁系统的密码应用生成密钥，并通过密码模块发行设备发行（初始化和注入密钥）密码模块，通过发卡设备对门禁卡发卡（初始化、注入密钥和写入应用信息）。系统中的密码设备提供密钥生成、密钥分散及对门禁卡发卡时的身份鉴别等密码服务。

C.2 与密码相关的安全技术要求

C.2.1 密码应用安全技术要求

基于非接触式 IC 卡的门禁系统中的密码应用方案应符合 C.5 的要求。

C.2.2 密码设备安全技术要求

基于非接触式 IC 卡的门禁系统中的密码设备包括：应用系统密码模块、密钥管理及发卡系统密码模块，具体密码设备的配用见图 C.1。

C.2.3 密码算法安全技术要求

在门禁系统中所配用的密码算法应符合国家相关要求。

C.2.4 密码协议安全技术要求

在门禁系统中，应实现门禁读卡器对门禁卡的身份鉴别，以及对鉴别数据的安全传输。

C.3 密钥管理安全技术要求

C.3.1 密钥生成

密钥的生成应使用国家密码管理部门认可的密钥管理系统。

C.3.2 密钥注入

门禁卡发卡和密码模块发行时的密钥注入应注意以下两点：

——密钥注入过程中不得泄露明文密钥的任何组成部分；

——在密码设备、接口和传输信道未收到任何可能导致密钥或敏感数据泄露、篡改的状况下，可以将密钥加载到密码设备中。

C.3.3 其他要求

在密钥生成、注入、更新和存储等的整个过程中，应保证密钥不被泄露。

C.4 其他应考虑的安全因素

除对密码应用的安全要求外，从系统整体的安全性出发，应考虑以下因素：

——后台管理系统的管理要求；

——其他与密码安全机制无关的管理及技术措施，如口令识别、生物特征识别、人员值守等。

在系统方案设计及应用时，宜针对具体应用情况在密码安全保障的基础上采取其他适当的管理和

技术措施，以增强门禁系统的安全性。

C.5 基于SM1算法的非接触式CPU卡方案

C.5.1 系统构成

本方案采用基于SM1算法的非接触CPU卡和基于SM1算法的安全模块，系统构成示意图如图C.2所示。

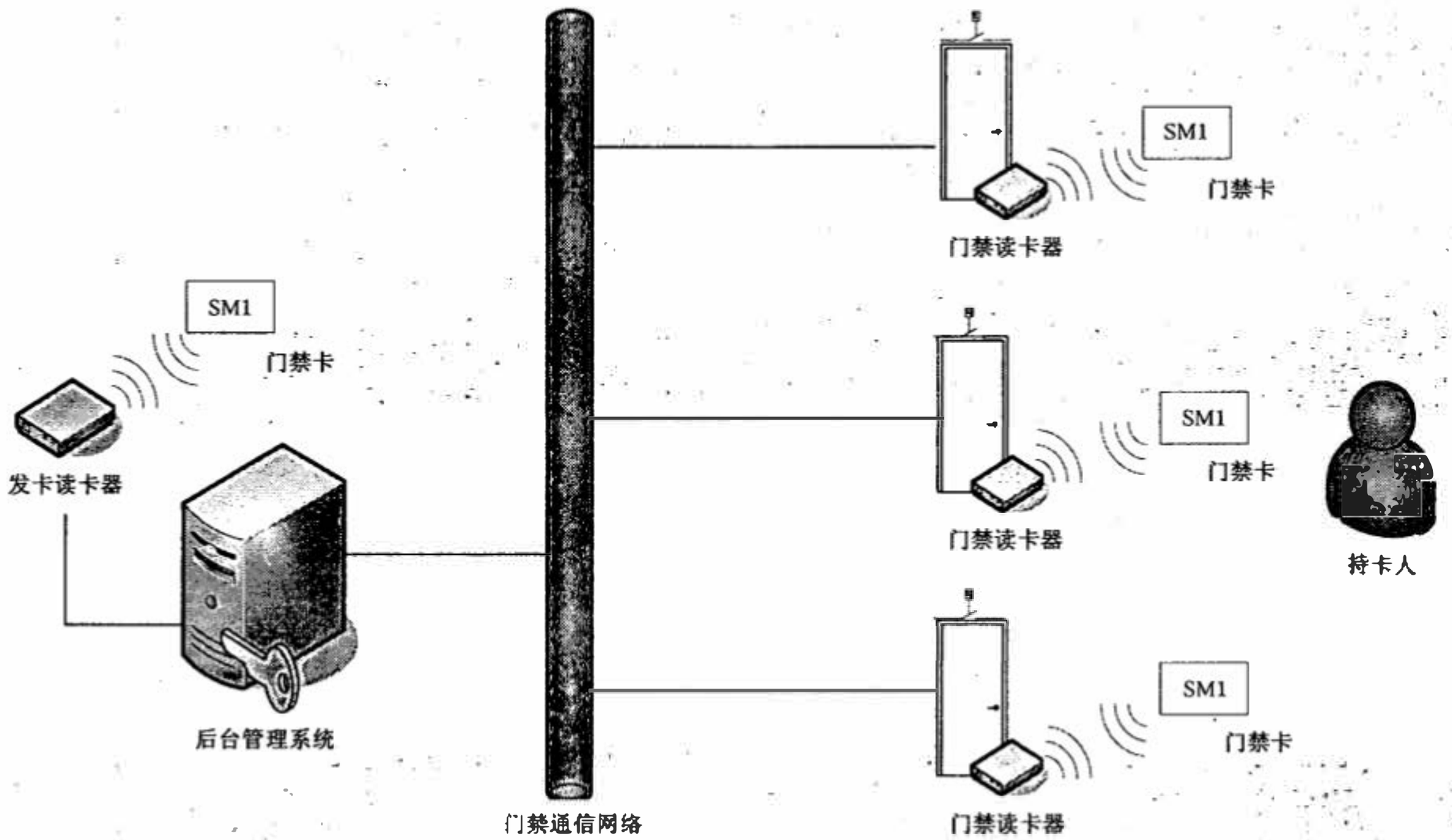


图 C.2 门禁卡的系统示意图

C.5.2 原理

该方案中门禁卡采用SM1算法的CPU卡，卡内存放安全认证码、发行信息和卡片密钥，并具有符合相关标准的片上操作系统。门禁卡与非接读卡器之间采用SM1算法进行身份鉴别和安全报文传输，在发卡系统中和读写器中的安全模块同样采用SM1算法进行门禁卡的密钥分散，实现一卡一密。

方案原理图如图C.3所示。

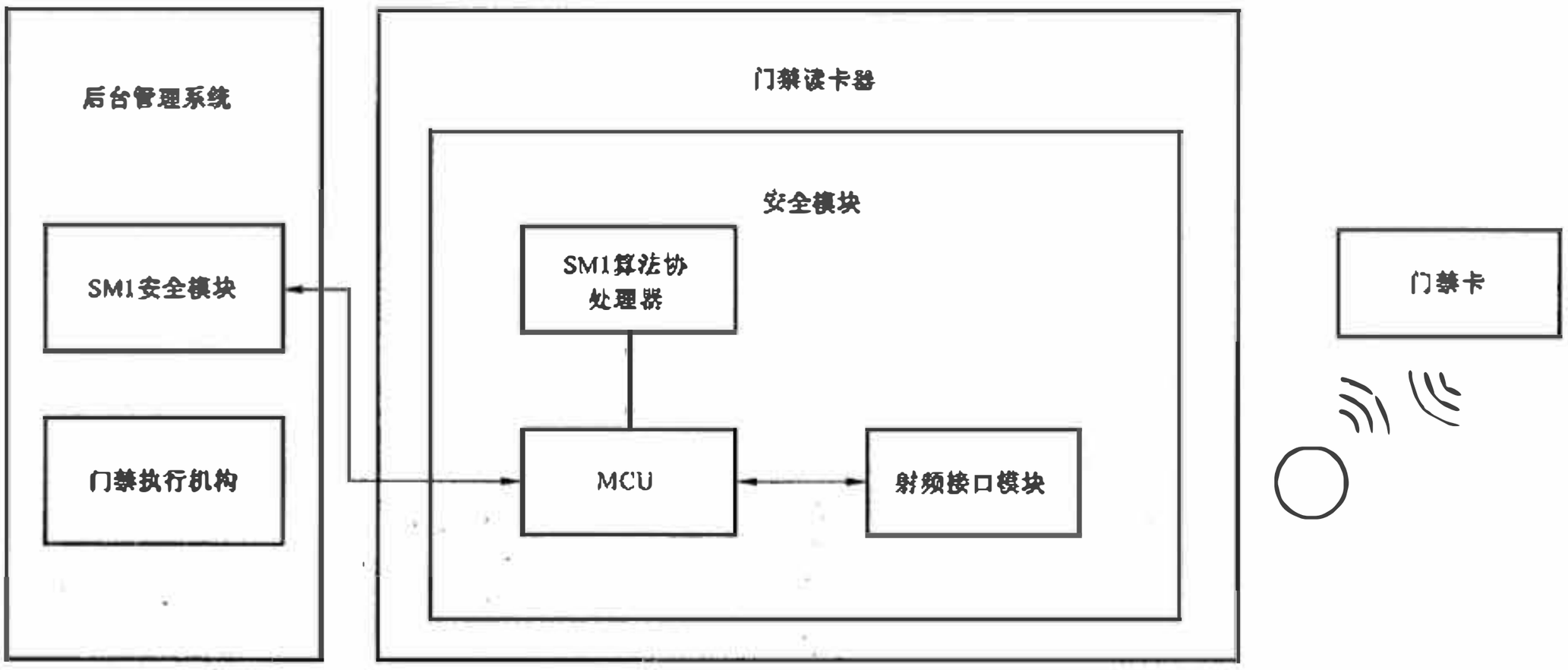


图 C.3 原理图

读卡器负责门禁卡的合法性鉴别，同时将获得的门禁卡身份鉴别信息以安全报文的方式反馈给门禁控制后台管理系统，由后台管理系统的 SM1 算法的安全模块进行双重鉴别门禁卡的合法性，并控制门禁执行机构完成门禁操作，同时门禁服务器还负责门禁读卡器的管理工作。

SM1 算法安全模块集成 MCU 和射频接口功能，所有的处理过程都在安全模块中实现。射频接口模块负责读卡器与门禁卡间的射频通信；MCU 控制射频接口模块与门禁卡的通信，负责实现读卡器内部的数据加密传送及与后台管理系统的通信功能。

C.5.3 密码安全应用流程

C.5.3.1 发卡系统

分为门禁卡发卡、门禁读写器安全模块发行、后台管理系统安全模块发行。

C.5.3.1.1 门禁卡发行

后台管理系统使用 SM1 算法对系统根密钥进行分散，实现一卡一密；通过发卡读卡器对卡片利用过程密钥采用 SM1 算法进行卡片身份鉴别，应用目录、文件系统等数据结构初始化并完成卡片密钥的下载，以及对卡片进行持卡人信息与签发单位信息的写入，该过程使用 CPU 卡的发卡流程保证信息写入的安全性、数据的机密性。

C.5.3.1.2 安全模块发行

门禁后台管理系统使用密钥管理系统成门禁系统根密钥，应安全导入安全模块。

C.5.3.2 门禁卡控制

门禁读卡器应直接对门禁卡做身份鉴别，同时对鉴别数据加密后送给后台管理系统控制门禁功能的执行，不仅保证身份鉴别的真实性，还能保证信息传输过程中的机密性。

具体方法如下：

——门禁读卡器读取门禁的安全识别码，作为卡片一卡一密的分散因子；

门禁读卡器发送一个内部认证命令给门禁卡（门禁安全模块产生随机数），门禁卡内部用存在的卡片中的一卡一密密钥 KEYC 对该随机数用 SM1 算法做加密运算，得到 RA′ = ENK (KEYC,RA)并回发给门禁读卡器；

门禁读卡器首先用安全模块中的根认证密钥 KEYR 用 SM1 算法对安全识别码进行分散得到 KEYC，再对随机数 RA 做加密运算得到 RA″，如果 RA′＝RA″，则卡片的身份鉴别正确，否则鉴别不通过；

——身份鉴别通过后，门禁读卡器安全模块使用加密密钥 KEY 对鉴别信息进行安全报文计算后传送给后台管理系统，后台管理系统用后台安全模块中对应的解密密钥 KEY 对安全报文进行认证。当认证通过后，与后台数据库对比门禁卡合法性执行开门操作。

身份鉴别过程如图 C.4 所示。

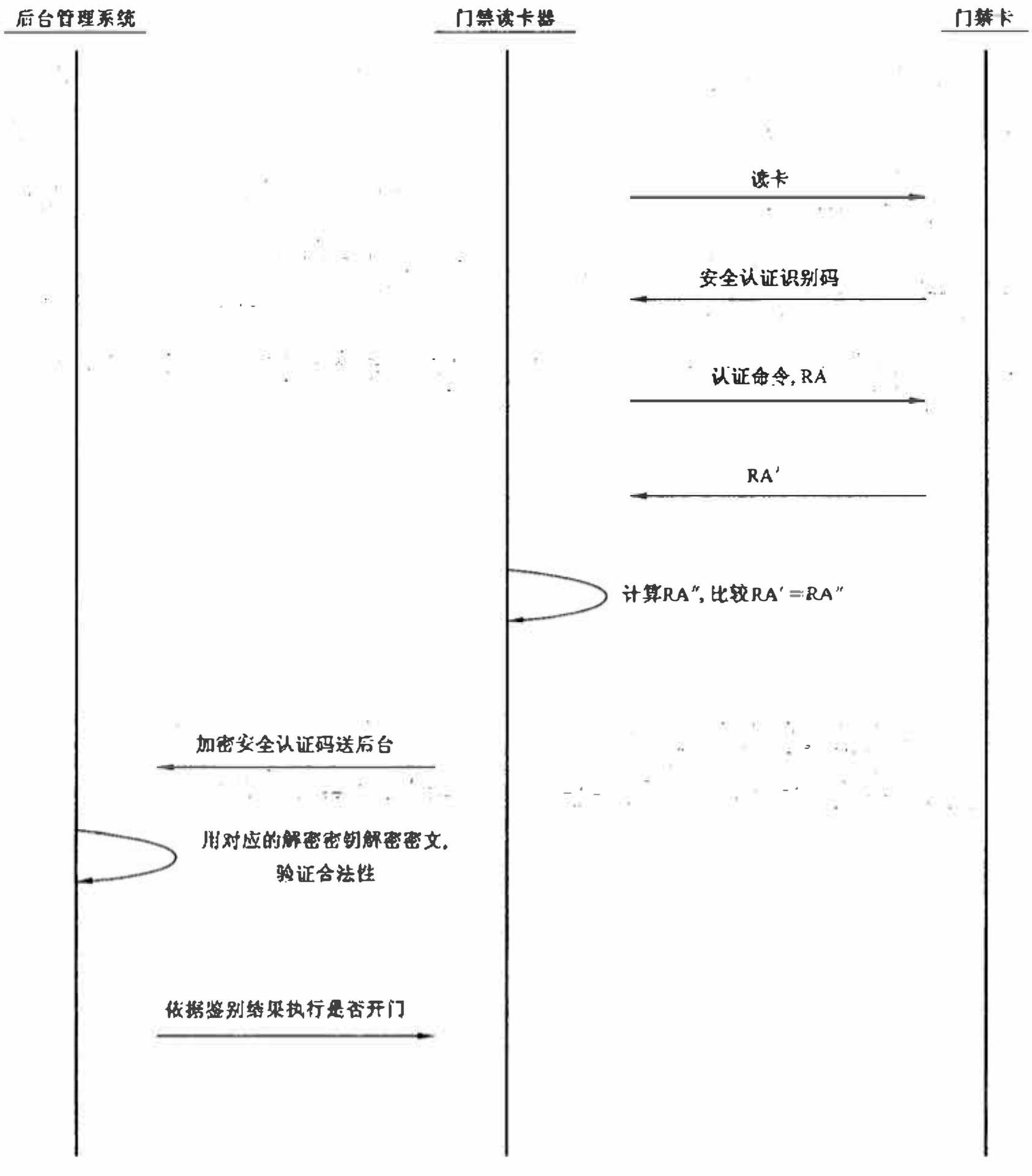


图 C.4　身份鉴别过程