中华人民共和国公共安全行业标准 出入口控制系统技术要求	GA / T 394—2002

1　范围

本标准规定了出入口控制系统的技术要求，是设计、验收出入口控制系统的基本依据。

本标准适用于以安全防范为目的，对规定目标信息进行登录、识别和控制的出入口控制系统或设备。其他出入口控制系统或设备如：［楼宇对讲(可视)系统、防盗安全门等］由相应的技术标准做出规定。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 4208—1993　外壳防护等级(IP代码)(eqv IEC 529：1989)

GB 8702　电磁辐射防护规定

GB 12663　防盗报警控制器通用技术条件

GB / T 15211　报警系统环境试验

GB 16796—1997　安全防范报警设备　安全要求和试验方法

GB / T 17626. 2—1998　电磁兼容　试验和测量技术
静电放电抗扰度试验(idt IEC 61000-4-2；1995)

GB / T 17626. 3—1998　电磁兼容　试验和测量技术
射频电磁场辐射抗扰度试验(idt IEC 61000-4-3：1995)

GB / T 17626. 4—1998　电磁兼容　试验和测量技术
电快速瞬变脉冲群抗扰度试验(idt IEC　61000-4—4：1995)

GB / T 17626. 5—1999　电磁兼容　试验和测量技术
浪涌(冲击)抗扰度试验Gdt IEC 61000-4-5：1995)

GB / T 17626. 11一1999　电磁兼容　试验和测量技术
电压暂降、短时中断和电压变化的抗扰度试验(idt IEC 61000-4-11：1994)

GA / T 73—1994　机械防盗锁

GA / T 74—2000　安全防范系统通用图形符号

3　术语和定义

下列术语和定义适用于本标准。

3.1　出入口　access

控制人员和 / 或物品通过的通道口。

3.2　出入口控制系统　access control system

采用电子与信息技术，识别、处理相关信息并驱动执行机构动作和 / 或指示，从而对目标在出入口的出入行为实施放行、拒绝、记录和报警等操作的设备(装置)或网络。

3.3　目标　object

通过出入口且需要加以控制的人员和／或物品。

3.4　目标信息　object informtion

赋予目标或目标特有的、能够识别的特征信息。数字、字符、图形图像、人体生物特征、物品特征、时间等均可成为目标信息。

3.5　钥匙　key

用于操作出入口控制系统、取得出入权的信息和／或其载体，系统被设计和制造成只能由其特定的钥匙所操作。

钥匙所表征的信息可以具有表示人和／或物的身份、通行的权限、对系统的操作权限等单项或多项功能。

3.6　人员编码识别　human coding identification

通过编码识别(输入)装置获取目标人员的个人编码信息的一种识别。

3.7　物品编码识别　article coding identification

通过编码识别(输入)装置读取目标物品附属的编码载体而对该物品信息的一种识别。

3.8　人体生物特征信息　human body biologic characteristic

目标人员个体与生具有的、不可模仿或极难模仿的那些体态特征信息或行为，且可以被转变为目标独有特征的信息。

3.9　人体生物特征信息识别　human body biologic characteristic identification

采用生物测定(统计)学方法，获取目标人员的生物特征信息并对该信息进行的识别。

3.10　物品特征信息　article characteristic

目标物品特有的物理、化学等特性且可被转变为目标独有特征的信息。

3.11　物品特征信息识别　article characteristic identification

通过辩识装置对预定物品特征信息进行的识别。

3.12　密钥、密钥量与密钥差异　key-code，amount of key-code，differenceof key-code

可以构成单个钥匙的目标信息即为密钥。

系统理论上可具有的所有钥匙所表征的全体密钥数量即为系统密钥量。如果某系统具有不同种类的、权限并重的钥匙，则分别计算各类钥匙的密钥量，取其中密钥量最低的作为系统的密钥量。

构成单个钥匙的目标信息之间的差别即为密钥差异。

3.13　钥匙的授权　key authorization

准许某系统中某种或某个、某些钥匙的操作。

3.14　误识　false identification

系统将某个钥匙识别为该系统其他钥匙。

3.15　拒认　refuse identification

系统未对某个经正常操作的本系统钥匙做出识别响应。

3.16　识读现场　identification local

对钥匙进行识读的场所和/或环境。

3.17　识读现场设备　local identify equipment

在识读现场的、出入目标可以接触到的、有防护面的设备(装置)。

3.18　防护面　protection surface

设备完成安装后，在识读现场可能受到人为被破坏或被实施技术开启，因而需加以防护的设备的结构面。

3.19　防破坏能力　anti destroyed ability

在系统完成安装后，具有防护面的设备(装置)抵御专业技术人员使用规定工具实施破坏性攻击，既出入口不被开启的能力(以抵御出入口被开启所需要的净工作时间表示)。

3.20　防技术开启能力　anti technical opened ability

在系统完成安装后，具有防护面的设备(装置)抵御专业技术人员使用规定工具实施技术开启(如各种试探、扫描、模仿、干扰等方法使系统误识或误动作而开启)，即出入口不被开启的能力(以抵御出入口被开启所需要的净工作时间表示)。

3.21　复合识别　combination identification

系统对某目标的出入行为采用两种或两种以上的信息识别方式并进行逻辑相与判断的一种识别方式。

3.22　防目标重入　anti pass-back

能够限制经正常操作已通过某出入口的目标，未经正常通行轨迹而再次操作又通过该出入口的一种控制方式。

3.23　多重识别控制　multi-identification control

系统采用某一种识别方式，须同时或在约定时间内对两个或两个以上目标信息进行识别后才能完成对某一出入口实施控制的一种控制方式。

3.24　异地核准控制　remote approve control

系统操作人员(管理人员)在非识读现场(通常是控制中心)对虽能通过系统识别、允许出入的目标进行再次确认。并针对此目标遥控关闭或开启某出入口的一种控制方式。

3.25　受控区、同级别受控区、高级别受控区　controlled area，the samelevel controlled area，high level　controlled area

如果某一区域只有一个(或同等作用的多个)出入口，则该区域视为这一个(或这些)出入口的受控区，即：某一个(或同等作用的多个)出入口所限制出入的对应区域，就是它(它们)的受控区。

具有相同出入限制的多个受控区，互为同级别受控区。

具有比某受控区的出入限制更为严格的其他受控区，是相对于该受控区的高级别受控区。

4　系统功能要求

4.1　系统概述

出入口控制系统主要由识读部分、传输部分、管理 / 控制部分和执行部分以及相应的系统软件组成。其原理框图如图1所示。

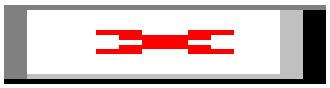


图1　出入口控制系统原理框图

4.2　系统构成模式

出入口控制系统有多种构建模式。按其硬件构成模式划分，可分为一体型和分体型；按其管理 / 控制方式划分，可分为独立控制型、联网控制型和数据载体传输控制型。

4.2.1　一体型与分体型

4.2.1.1　一体型

一体型出入口控制系统的各个组成部分通过内部连接、组合或集成在一起，实现出入口控制的所有功能。一体型结构和组成框图如图2所示。

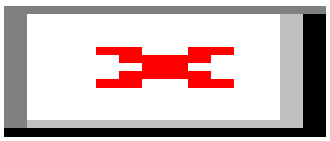
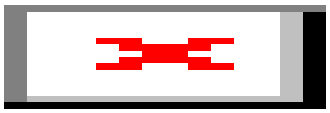


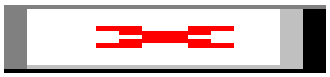
图2　一体型产品组成框图

4.2.1.2　分体型

分体型出入口控制系统的各个组成部分，在结构上有分开的部分，也有通过不同方式组合的部分。分开部分与组合部分之间通过电子、机电等手段连成为一个系统，实现出入口控制的所有功能。分体型结构中常见的模式如图3a)和图3b)所示。



a)分体型结构组成框图之一



b)分体型结构组成框图之二

图3　分体型结构组成框图

4.2.2　独立控制型、联网控制型与数据载体传输控制型

4.2.2.1　独立控制型

独立控制型出入口控制系统，其管理／控制部分的全部显示／编程／管理／控制等功能均在一个设备(出入口控制器)内完成，如图4所示。

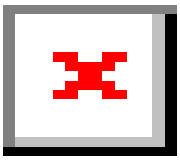


图4　独立控制型组成框图

4.2.2.2　联网控制型

联网控制型出入口控制系统，其管理／控制部分的全部显示／编程／管理／控制功能不在一个设备(出入口控制器)内完成。其中，显示／编程功能由另外的设备完成。设备之间的数据传输通过有线和／或无线数据通道及网络设备实现，如图5所示。

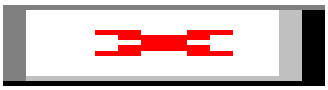


图5　联网控制型组成框图

4.2.2.3　数据载体传输控制型

数据载体传输控制型出入口控制系统与联网型出入口控制系统区别仅在于数据传输的方式不同。其管理／控制部分的全部显示／编程／管理／控制等功能不是在一个设备(出入口控制器)内完成。其中，显示/编程工作由另外的设备完成。设备之间的数据传输通过对可移动的、可读写的数据载体的输入／导出操作完成。如图6所示。

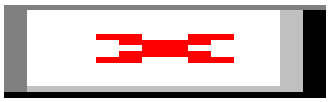


图6　数据载体传输控制型组成框图

4.3　系统防护级别

系统的防护级别由所用设备的防护面外壳的防护能力、防破坏能力、防技术开启能力以及系统的控制能力、保密性等因素决定。系统的防护级别分为A、B、C三个等级。推荐采用的系统各组成部分的防护级别的分级方法见附录A。

4.3.1　系统识读部分的防护级别

系统识读部分的防护能力分级与相应要求见附录A中的表A.1。

4.3.2　系统管理／控制部分的防护级别

系统管理/控制部分的防护能力分级与相应要求见附录A中的表A.2。

4.3.3　系统执行部分的防护级别

系统执行部分的防护能力分级与相应要求见附录A中的表A.3。4.4　系统功能

4.4.1　出入授权

系统将出入目标的识别信息及载体授权为钥匙，并记录于系统中。应能设定目标的出入授权，即：何时、何出入目标、可出入何出入口、可出入的次数和通行的方向等权限。

在网络型系统中，除授权、查询、集中报警、异地核准控制等管理功能外，对本标准所要求的功能而言，均不应依赖于中央管理机是否工作。

4.4.2　系统响应时间

系统的下列主要操作响应时间应小于2s。

a)除工作在异地核准控制模式外，从识读部分获取一个钥匙的完整信息始至执行部分开始启闭出入口动作的时间。

b)从操作(管理)员发出启闭指令始至执行部分开始启闭出入口动作的时间。

c)从执行异地核准控制后到执行部分开始启闭出入口动作的时间。

4.4.3　计时

a)系统校时

系统的与事件记录、显示及识别信息有关的计时部件应有校时功能；在网络型系统中，运行于中央管理主机的系统管理软件每天宜设置向其他的与事件记录、显示及识别信息有关的各计时部件校时功能。

b)计时精度

非网络型系统的计时精度不低于5s / d；网络型系统的中央管理主机的计时精度不低于5s / d，其他的与事件记录、显示及识别信息有关的各计时部件的计时精度不低于10s / d。4.4.4　自检和故障指示

系统及各主要组成部分应有表明其工作正常的自检功能，B、C防护级别的还应有故障指示功能。

4.4.5　报警

系统报警功能分为现场报警、向操作(值班)员报警、异地传输报警等。报警信号的传输方式可以是有线的和/或无线的，报警信号的显示可以是可见的光显示和/或声音指示。　在发生以下情况时，系统应报警：

a)当连续若干次(最多不超过5次，具体次数应在产品说明书中规定)在目标信息识读设备或管理/控制部分上实施错误操作时；

b)当未使用授权的钥匙而强行通过出入口时；

c)当未经正常操作而使出入口开启时；

d)当强行拆除和/或打开B、C防护级别的识读现场装置时；

e)当B、C防护级别的主电源被切断或短路时；

f)当C防护级别的网络型系统的网络连线发生故障时。

在发生以下情况时，系统可报警：

a)当防护面上的部件受到强烈撞击时；b)当出现窃取系统内信息的行为时；c)当遭受工具破坏时。

4.4.6　应急开启

系统应具有应急开启的方法。如：

a)可以使用制造厂特制工具采取特别方法局部破坏系统部件后，使出入口应急开启，且可迅即修复或更换被破坏部分。b)可以采取冗余设计，增加开启出入口通路(但不得降低系统的各项技术要求)以实现应急开启：

4.4.7　指示/显示