ICS 13.310
A 91

中华人民共和国国家标准

GB/T 37078—2018

出入口控制系统技术要求

Technical specifications for access control system

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中华人民共和国公安部提出。

本标准由全国安全防范报警系统标准化技术委员会(SAC/TC 100)归口。

本标准起草单位:北京艾克塞斯科技发展有限责任公司、公安部第一研究所、国家安全防范报警系统产品质量监督检验中心(北京)、国家安全防范报警系统产品质量监督检验中心(上海)、浩云科技股份有限公司、深圳市捷顺科技实业股份有限公司。

本标准主要起草人:朱峰、卢玉华、金巍、陶磊、史源、龙中胜、何军、龙罡、朱红亮、孙丽萍、李井山、解桂秋。

出入口控制系统技术要求

1 范围

本标准规定了出入口控制系统的构成与应用模式、安全等级、功能与性能要求、安全性要求、电磁兼容性要求、可靠性要求、环境适应性要求、标志以及文件提供。

本标准适用于以安全防范为目的，对指定目标进行授权、识别和控制的，单独的出入口控制系统；也适用于其他电子系统中所包含的出入口控制系统。

注：本标准可作为设计、检测和验收出入口控制系统的基本依据。

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/T 4208—2017 外壳防护等级(IP 代码)

GB/T 15211 安全防范报警设备 环境适应性要求和测试方法

GB/T 15408 安全防范系统供电技术要求

GB 16796 安全防范报警设备 安全要求和试验方法

GB/T 20138 电器设备外壳对外界机械碰撞的防护等级(IK 代码)

GB/T 30148 安全防范报警设备 电磁兼容抗扰度要求和试验方法

GB 50343 建筑物电子信息系统防雷技术规范

GB 50348 安全防范工程技术规范

GA/T 670 安全防范系统雷电浪涌防护技术要求

3 术语、定义、缩略语和符号

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

出入口 portal

出入口控制点 access point

用于放行被授权、拒绝未被授权的人员和/或物品出入的受控物理通道口。

3.1.2

出入口控制系统 access control system

利用自定义编码信息识别和/或模式特征信息识别技术，通过控制出入口控制点执行装置的启闭，达到对目标在出入口的出入行为实施放行、拒绝、记录和警示等操作的电子系统。

注：俗称门禁系统。

3.1.3

受控区 controlled area；protected area

由物理边界定义的具有一个或多个出入口控制点的空间区域。

3.1.4

同权限受控区　controlled area with same permission

具有相同出入权限的多个受控区，互为同权限受控区。

3.1.5

高权限受控区　controlled area with high permission

具有比某受控区的出入权限更为严格的其他受控区，是相对于该受控区的高权限受控区。

3.1.6

目标　object

需要通过出入口且需要加以控制的人员和/或物品。

3.1.7

人员编码识别　human coding identification

获取目标人员的个人编码信息(包括记忆信息和载体信息)的一种识别。

3.1.8

物品编码识别　article coding identification

获取目标物品附属的编码载体而对该物品信息的一种识别。

3.1.9

自定义编码信息识别　custom coding identification

采用人员编码识别及物品编码识别的总称。

3.1.10

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并对该信息进行的识别。

3.1.11

物品特征信息识别　article characteristic identification

通过辩识装置对预定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进行的识别。

3.1.12

模式特征信息识别　pattern characteristic identification

采用人体生物特征信息识别及物品特征信息识别的总称。

3.1.13

凭证　credential

赋予目标或目标特有的，能够识别的，用于操作出入口控制系统、取得出入权限的自定义编码信息或模式特征信息和/或其载体。

注：凭证所表征的信息可以具有表示目标身份、通行的权限、对系统的操作权限等单项或多项功能。通常包括PIN、载体凭证(如：IC卡、信息钮、RFID标签)、模式特征信息等。

3.1.14

识读装置　reader

能够读取、识别并输出凭证信息的电子设备。

注：识读装置的类型包括：编码识读设备、生物特征识读设备、物品特征识读设备等。

3.1.15

请求离开装置　request-to-exit device

用以自由离开受控区的装置。

注：出门按钮是典型的请求离开装置。

3.1.16

防护面　protection surface

安装在识读现场，可能受到人为破坏或被实施技术开启而需要保护的设备结构面。

3.1.17

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)。

3.1.18

出入口控制点执行装置　access point actuator

与出入口控制器相连接，执行开放或保护出入口的操作，完成允许或拒绝目标通过出入口功能的设备。

注：出入口控制点执行装置的类型包括：阻挡设备、闭锁设备、出入准许指示装置等。

3.1.19

出入口控制点传感器　access point sensor

与出入口控制器相连接，用以探测出入口开放状态和/或出入口控制点执行装置启/闭状态的设备(装置、部件)。

3.1.20

出入口控制器　access control unit；

access controller

能够按照预设规则处理从识读装置、请求离开装置和出入口控制点传感器等发来的信息，并通过出入口控制点执行装置对出入口控制点实施控制，同时记录相关信息的单个电子设备，或多个电子设备的组合。

3.1.21

密钥　key code

单个凭证包含的，能够被系统识别的目标信息。

3.1.22

胁迫凭证　duress credential

目标在进行识读操作时，除能发出正常出入请求外，还能引发被胁迫警示信号的一种特殊凭证。

3.1.23

群组出入管理　group access programming

将具有相同权限的目标或其凭证编为一个组，并能对其出入权限统一设置的一种系统功能。

3.1.24

防重入　anti-passback

能够限制经正常操作已通过某出入口(或进入/离开某受控区)的目标，未经正常通行轨迹而再次操作又通过该出入口(或进入/离开某受控区)的一种系统功能。

3.1.25

强防重入　hard anti-passback

违反防重入规则后，禁止该凭证后续通行并发出警示的一种防重入功能。

3.1.26

弱防重入　soft anti-passback

违反防重入规则后，不禁止目标后续通行但发出警示的一种防重入功能。

3.1.27

全局/系统防重入　global/system-wide anti-passback

将受控区的所有授权出入口控制点均设置为防重入的一种系统功能。

3.1.28

区域控制防重入　area controlled anti-passback

约束目标按照设定的通行轨迹依次进/出不同受控区的一种系统功能。

3.1.29

监控台　monitoring console

供系统管理员/系统操作员与出入口控制系统做人机交互的功能装置或软件，可包括多个组件。

3.1.30

识读装置追踪　reader trace

在指定识读装置上对凭证识读时，会在监控台触发警示和/或记录和/或显示的一种系统功能。

3.1.31

凭证追踪　credential trace

对指定的凭证(直接指定或通过目标指定其凭证组合)在所有出入口控制点上识读时都会在监控台触发警示和/或记录和/或显示的一种系统功能。

3.1.32

防尾随　anti-tailgating

防止和/或检测企图在单次操作下使用单目标凭证，同向通过两个或多个目标的一种系统功能。

3.1.33

复合识别　combination identification

系统对某一目标的出入行为采用两种或两种以上的凭证识别，并进行逻辑与判断的一种组合识别方式。

3.1.34

多重识别　multi-identification

同时或在预设时间内对两个或两个以上目标进行识别后才能完成对某一出入口实施控制的一种组合识别方式。

3.1.35

多占用　multi-occupancy

当有目标需要停留在某受控区时，系统保证在任何时候，停留的目标数不小于在该受控区设置的最少停留目标数(两个或两个以上)的一种系统功能。

3.1.36

监管模式　supervisor mode

某目标与另一个指定权限级别的目标(如监管人员)多重识别组合后，才能通过某出入口的一种系统功能。

3.1.37

现场监控　on-site monitoring

由设在识读现场、与系统相连的监控台对系统进行的监控。

3.1.38

非现场监控　off-site monitoring

由设在识读现场外(通常是监控中心)、与系统相连的监控台对系统进行的监控。

3.1.39

验证模式　validation mode

目标在识读现场识读凭证时，由监管人员通过观察现场监控和/或非现场监控的终端屏幕实时显示的目标信息(包括：目标原始图像、身份文字信息等)，对目标进行复核的一种系统功能。

3.1.40

系统管理员　system administrator

有权决定和/或实施出入口控制系统处理规则的人员。

注：系统管理员具有系统管理、授权、设置、操作等的最高权限。

3.1.41

系统操作员　system operator

获得授权操控出入口控制系统监控台的人员。

注：系统操作员具有监控职责，可按照级别被设定为允许或不允许录入、编辑系统数据等的权限。

3.1.42

异地核准　off-site approval

系统操作员或系统管理员采用非现场监控的方式，经对在某出入口的识读现场已通过系统识别的授权目标进行再次确认，才能对此出入口控制点实施远程开启或关闭的一种系统功能。

3.1.43

电梯控制　elevator control

限制人员目标乘用电梯的一种系统功能。

3.1.44

自由出入授权　free access granting

不必对凭证进行识别而开放出入口的一种系统功能。

3.1.45

点名　roll call

列出停留在受控区内的凭证和/或目标信息的一种系统功能。

3.1.46

访客陪同　visitor-escorted access

已预授权的访客目标凭证，需先使用特定权限的其他目标凭证识读通过后，才能授权通过的一种系统功能。

3.1.47

通讯失败运行模式　degraded mode of operation

出入口控制器在与控制中心通讯失败时，出入口控制器默认的受限工作模式。

3.1.48

出入口封锁　blocked access

使用任何凭证(包括预设的有效凭证)都不能开启出入口的一种系统功能。

3.1.49

出入口开放时间　portal open time

从出入口授权开启后到发出开放超时警示前的最长持续开门时间。

3.1.50

释放时间　release timing

根据预设规则设置的出入口控制点执行装置单次开启的时长。

3.1.51

警示　alert

通过发出视觉和/或听觉信号，提示相关人员介入的一种系统功能。

3.1.52

开放超时警示　held-open alert

出入口授权开启后，持续开放时间超过设置的出入口开放时间后发出的警示。

3.1.53

开放超时本地警示 held-open alert at the portal

在出入口控制点用以提示人员尽快关闭已被开启的出入口的一种警示。

注：开放超时本地警示发生在监控台发出开放超时警示之前。开放超时本地警示用以提示现场人员尽快关闭出入口，避免在监控台发出开放超时警示。

3.1.54

胁迫警示 duress alert

通过输入胁迫凭证，向监控台发出被胁迫出入的警示。

3.1.55

配置超时保护 configuration time-out

在配置模式下，系统管理员/系统操作员未在规定时间内进行新的配置操作时，系统自动退出配置模式的一种系统功能。

3.1.56

强制开启 portal forced open

出入口未经授权而被开启的情况。

3.1.57

系统自我保护 system self-protection

用于防止、探测和/或报告，有意和无意破坏和/或干扰系统正常运行的一种系统功能。

3.2 缩略语

下列缩略语适用于本文件。

ACS：出入口控制系统(Access Control System)

ACU：出入口控制器(Access Control Unit)

ID：身份识别信息(Identification Information)

PIN：个人记忆信息凭证(Personal Identification Number)

REX：请求离开装置(Request-to-Exit Device)

3.3 符号

下列符号适用于本文件。

NP：不允许

OP：可选项

M：强制的

NA：不适用

4 系统构成与应用模式

4.1 概念模型

ACS 的概念模型参见附录 A 中的 A.1。

4.2 系统构成

4.2.1 ACS 主要由识读部分、传输部分、管理/控制部分和执行部分组成见图 1。系统有多种构建模式，可根据系统规模、现场情况、安全管理要求等，合理选择。

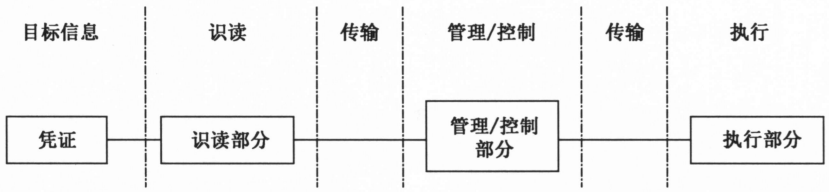
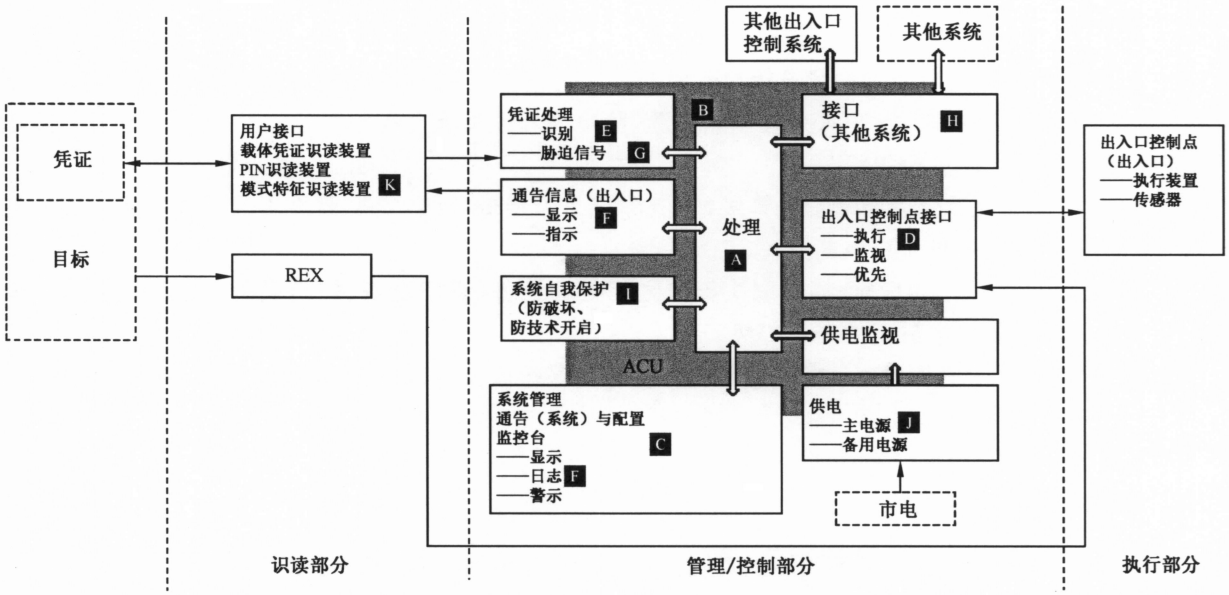


图 1　ACS 逻辑构成示意图

4.2.2　ACS 典型结构见图 2。



注：虚线框内的组件不包括在本标准范围；功能可能位于多于一个的说明框或集中在一个说明框；系统管理通告信息和配置可能只有软件应用来执行；硬件平台的最小要求应指明。

图 2　ACS 典型结构图

ACS 应包括识读部分、管理/控制部分、执行部分。主要配置功能如下：

a）　处理(A)：系统预设规则与产生的预先定义的行为之间的变化比较；

b）　通信(B)：在出入口控制系统组件和确保预设规则应用之间的信号传递；

c）　配置(C)：设置处理规则；

d）　出入口控制点接口(D)：出入口控制点执行功能、监测、优先控制功能；

出入口控制点执行功能：根据预设规则对出入口开放和保护；

出入口控制点监测：出入口的开/闭状态，和/或出入口锁闭装置的释放/锁定状态的不间断报告；

出入口控制点优先控制功能：旁路预设规则，手动对出入口实施的释放/锁定。

e）　识别(E)：对被授权目标出入请求的认可；

f）　通告信息(F)：报警、显示和/或记录日志的功能；

警示：与激活一个指示器以提示人们评估有关的通告信息的子功能；

显示：与系统内发生的可视的和/或可听的变化，展现有关的通告信息的子功能；

日志：与系统日志和归档变化有关的通告信息子功能。

g）　胁迫信号(G)：被授权目标强制性出入请求条件下的无声警示；

h）　与其他系统的接口(H)：系统内功能和/或变化的共享；

i) 系统自我保护(I):用于防止、探测和/或报告有意和无意破坏和/或干扰系统工作行为的系统功能;

j) 电源供给(J):当一个出入口控制系统的一部分(如出入口控制点接口)形成入侵报警系统的一部分时,该部分的电源供给应与入侵报警系统相关标准中电源供给的相关要求相符;

k) 用户接口(K):用户要求出入的方法(如键盘或凭证识读装置)以及出入状态的接受指示。

4.2.3 ACS典型应用模式参见附录A的A.2。

5 安全等级

5.1 一般要求

5.1.1 ACS按照保护对象面临的风险程度和对防护能力差异化的需求,通过对系统中各出入口的识别功能、出入口控制点执行功能、出入口控制点监测、胁迫信号和系统自我保护等功能的配置,构建对应出入口控制点系统功能的安全等级。

5.1.2 ACS按其安全性分为四个安全等级,安全等级1为最低等级,安全等级4为最高等级。安全等级应限定到每个独立的出入口控制点。

5.1.3 单个出入口控制点的安全等级取决于与之相关的设备(识读设备、控制设备、监控台、执行设备等)、凭证及传输等部件中最低的安全等级。

5.1.4 如果系统设备/组件所声明的功能符合本标准的某个安全等级,应在文件中明确表明。

5.2 安全等级的划分

5.2.1 等级1:低安全等级

防范的对手基本不具备ACS的知识,且仅使用常见、有限的工具,当对手在面对最低程度的阻力时很有可能放弃攻击的念头。

注1:该等级通常可用于风险低、资产价值有限的防护对象。

注2:防护的主要目的是阻止和拖延对手行动。

5.2.2 等级2:中低安全等级

防范的对手仅具备少量ACS知识,懂得使用常规工具和便携式工具,当对手意识到可能已被探测之后很可能放弃继续攻击的念头。

注1:该等级通常用于风险较高、资产价值较高的防护对象。

注2:防护的主要目的是阻止、拖延和探测对手的行动。

5.2.3 等级3:中高安全等级

防范的对手熟悉ACS,可以使用复杂工具和便携式电子设备。当对手意识到可能会被认出及抓获,有可能放弃继续攻击的念头。

注1:该等级通常用于风险高、资产价值高的防护对象。

注2:防护的主要目的是阻止、拖延和探测对手的行动,同时可以提供方法,帮助认出对手。

5.2.4 等级4:高安全等级

防范的对手具备攻击系统的详细计划和所需的能力或资源,具有所有可获得的设备,且懂得替换出入口控制系统部件的方法。当对手意识到可能会被认出及抓获,有可能放弃继续攻击的念头。

注1:该等级通常用于风险很高、资产价值很高的防护对象。

注2:防护的主要目的是阻止、拖延和探测对手的行动,同时可以提供方法,帮助认出对手。

6 功能及性能要求

6.1 控制要求

6.1.1 释放时间

出入口控制点执行装置的释放时间应符合表1中A的要求。

6.1.2 出入控制

ACS的出入控制功能应符合表1中B的要求，识读与控制时序应符合附录B所示的时序图要求。

6.1.3 出入口状态监测

出入口的状态监测应符合表1中C的要求。

6.1.4 输入信号

输入信号应符合表1中D的要求。

表1 出入口控制点要求

项目	序号	要求	安全等级			
			1	2	3	4
A 释放时间	1	只能使用制造商预设的释放时间，不可更改	OP[1]	OP[2]	NP	NP
	2	各出入口控制点可配置统一的释放时间	OP[1]	OP[2]	NP	NP
	3	各出入口控制点可配置不同的释放时间	OP[1]	OP[2]	M	M
	4	制造商预设不可更改时的释放时间值应不小于3 s	M	M	NA	NA
	5	当释放时间是可配置的，出入口控制点可根据目标的访问权限设置不同的释放时间	OP	OP	OP	M
B 出入控制	6	对进入受控区提供访问控制	M	M	M	M
	7	对离开受控区提供访问控制	OP	M	M	M
	8	强防重入	OP	OP	M	M
	9	弱防重入	OP	OP	OP	OP
	10	全局/系统防重入	OP	OP	OP	M
	11	对防重入功能的旁路	OP	OP	OP	NP
	12	区域控制防重入	OP	OP	OP	OP
	13	进入/离开超时警示	OP	OP	OP	M
	14	配置有效/无效的时间段	OP	OP	M	M
	15	对凭证的添加、删除、启用、禁用操作	M	M	M	M
	16	访客陪同出入	OP	OP	OP	OP
	17	监管模式	OP	OP	OP	OP
	18	配置复合识别	OP	OP	M	M

表 1（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 出入控制	19	多占用受控区	OP	OP	OP	OP
	20	配置多重识别	OP	OP	OP	M
	21	配置验证模式	OP	OP	OP	M
	22	防尾随	OP	OP	OP	OP
	23	配置异地核准	OP	OP	OP	M
	24	电梯控制	OP	OP	OP	OP
C 出入口 状态监测	25	监测出入口的启/闭状态	OP	M	M	M
	26	监测出入口控制点执行装置的启/闭状态	OP	OP	M	M
	27	只能使用制造商预设的开放时间。开放时间应不少于 10 s	OP	OP[3]	NP	NP
	28	各出入口控制点可配置统一的开放时间	OP	OP[3]	OP	OP
	29	各出入口控制点可配置不同的开放时间	OP	OP[3]	M	M
	30	当开放时间是可配置的，出入口控制点可根据访问权限设置不同的开放时间	OP	OP	OP	OP
D 输入信号	31	输入信号为开关量时，应能处理持续时间大于 400 ms 的信号（如：开关量门状态信号、REX 操作信号等）	OP	M	M	M
注：OP[1]、OP[2]、OP[3] 表示有相同编号的可选项，至少被选择一项。						

6.2 指示/通告要求

6.2.1 ACS 的指示/通告应符合表 2 的要求。

6.2.2 指示包括识读现场指示和监控台指示，在监控台指示的内容应包含事件的类型，发生的位置、日期和时间。

表 2 指示/通告要求

项目	序号	要求	指示	警示	日志	安全等级			
						1	2	3	4
A 识读 现场	1	允许出入	●			M	M	M	M
	2	不允许出入	●			M	M	M	M
	3	在准许出入前（出入口锁定状态）	●			OP	OP	OP	OP
	4	开放超时本地警示。开放超时本地警示时间可统一配置或各出入口单独配置（建议默认值：10 s）		●		OP	OP	M	M
B 监控台	5	允许出入	●			OP	OP	OP	OP
	6	不允许出入			●	M	M	M	M
	7	胁迫	●	●	●	OP	OP	M	M

表 2（续）

项目	序号	要求	指示	警示	日志	安全等级			
						1	2	3	4
B 监控台	8	载体凭证的使用次数	●		●	OP	OP	OP	OP
	9	使用过期凭证而遭到拒绝访问	●	●	●	OP	OP	M	M
	10	复合识别使用了 PIN，且无效 PIN 输入次数超过设置值。 如果无效 PIN 输入次数只能使用制造商预设值时，应不大于 5 次	●	●	●	OP	OP	OP	M
	11	只识读 PIN 信息，且使用无效 PIN 的识读次数超过设置值。如果无效 PIN 输入次数只能使用制造商预设值时，30 s 内的可输入次数应不大于 5 次	●	●	●	OP	OP	NP	NP
	12	在监控台的电子地图（建筑平面图）上显示出入口控制点警示信息	●			OP	OP	OP	M
	13	根据警示内容给出处置指导	●			OP	OP	OP	M
	14	事件记录			●	OP	M	M	M
	15	允许出入后，出入口开启	●		●	OP	OP	M	M
	16	允许出入后，出入口未开启	●	●	●	OP	OP	OP	M
	17	拒绝访问时	●	●	●	OP	OP	M	M
	18	拒绝访问的原因	●	●	●	OP	OP	OP	M
	19	按时间表或手动改变出入口闭锁/释放的状态时			●	OP	OP	M	M
	20	主电源故障	●	●	●	OP	OP	M	M
	21	主电源恢复	●		●	OP	OP	M	M
	22	备用电源故障时（电池欠压和无电池）	●	●	●	OP	OP	M	M
	23	进入和离开配置模式	●		●	OP	OP	M	M
	24	在 ACU 和监控台之间失去通信联系时	●	●	●	OP	M	M	M
	25	使用点名功能时	●		●	OP	OP	M	M
	26	出入口被强制开启	●	●	●	OP	M	M	M
	27	出入口被强制开启后关闭，或强制开启时间超长	●	●	●	OP	OP	M	M
	28	通过类型、地点、时间和日期识别发生的所有事件	●		●	OP	OP	M	M
	29	如果指定了警示信息的优先等级，其显示和日志应包含等级信息	●		●	OP	OP	M	M
	30	如果系统允许指定优先等级，同时接受的警示应按优先等级顺序显示	●			OP	OP	M	M
	31	探测到防拆信号	●	●	●	OP	M	M	M
	32	开放超时	●	●	●	OP	M	M	M
	33	凭证追踪	●		●	OP	OP	OP	M

表 2（续）

项目	序号	要求	指示	警示	日志	安全等级			
						1	2	3	4
B 监控台	34	识读装置追踪	●		●	OP	OP	OP	M
	35	识读装置离线	●	●	●	OP	OP	OP	M
	36	执行装置异常	●	●	●	OP	OP	OP	M
	37	达到最大记录能力 90%时	●	●	●	OP	OP	M	M
	38	跟随警示到达监控台的文字说明显示的最大延迟时间	●	●		OP	OP	OP	2 s
	39	跟随警示到达监控台的图像和图片显示的最大延迟时间	●	●		OP	OP	OP	3 s
	40	具体的警示事件指定的优先等级	●			OP	OP	M	M
	41	监控台接受的警示信息应保持到系统操作员确认	●	●	●	OP	OP	M	M
	42	当达不到多占用受控条件时（未达到最小数量的目标数）	●	●	●	OP	OP	OP	M
	43	所有操作的类型、操作者 ID、时间和日期			●	OP	OP	OP	M
	44	系统操作员对警示的处置意见（包含操作者 ID、时间和日期、被处置的警示事件等）	●		●	OP	OP	OP	M
	45	对访问记录的信息检索、打印、导出等，记录操作者 ID、时间和日期			●	OP	OP	M	M
	46	平均每个识读装置的事件记录能力的最小数量			●	32	500	1 000	1 000
注：●表示有该项要求。									

6.3 识别要求

6.3.1 ACS 的识别应符合表 3 的要求。

6.3.2 ACS 应对比每个凭证来接受或拒绝用户的出入请求。

表 3 识别要求

项目	序号	要求	安全等级			
			1	2	3	4
A 时钟要求	1	系统中含有计时部件的设备，其内置的实时时钟精度应不低于每周±10 s	OP	M	M	M
	2	系统中含有计时部件的设备，其内置的实时时钟应能处理闰年	OP	M	M	M
	3	具有多个含有计时部件设备的互联系统，每个设备时钟应与主时钟或其他可信的时钟源至少每 24 h 同步一次	OP	OP	M	M
	4	系统主时钟可配置与北京时间同步，至少每 24 h 一次	OP	OP	OP	OP
	5	断电后，实时时钟应能保持运行的最小时间周期	OP	24 h	120 h	120 h

表 3（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 出入授权	6	可配置用户访问级别的最少数量	1	8	16	64
	7	可配置访问时间周期的最少数量	0	4	8	16
	8	访问时间段，包括星期、小时、分钟	OP	M	M	M
	9	访问时间段，包括年、月、日	OP	OP	M	M
	10	可配置特定日期（如法定节假日、特殊的工作日和非工作日）的最小数量	0	2	16	24
	11	按群组出入管理方式分配访问权限	OP	OP	OP	M
	12	紧急情况下，系统应能改变一组凭证的访问权限	OP	OP	OP	M
C 识别的设备和方法	13	每个目标对应唯一的 ID	OP	M	M	M
	14	只识读 PIN 信息	OP^1	OP^2	NP	NP
	15	只识读模式特征信息或与其他识别方法（载体凭证、PIN）复合使用	OP^1	OP^2	OP^3	OP^4
	16	只识读载体凭证信息	OP^1	OP^2	OP^3	OP^4
	17	复合识读载体凭证和 PIN 信息	OP^1	OP^2	OP^3	OP^4
	18	当用有效载体凭证但无效 PIN 的访问次数超过设置值时，该载体凭证的访问权限应在设置的时间段内被停用。如果无效 PIN 输入次数只能使用制造商预设值时，可输入次数应不大于 5 次。如果凭证停用的时间段只能使用制造商预设值时，应不小于 45 s	OP	M	M	M
	19	只识读 PIN 信息，且使用无效 PIN 的访问次数超过设置值时，PIN 输入设备应在设置的停用时间段内无效。如果无效 PIN 输入次数只能使用制造商预设值时，30 s 内的可输入次数应不大于 5 次。如果 PIN 输入设备的停用时间段只能使用制造商预设值时，应不小于 45 s	OP	OP	NA	NA
	20	模式特征信息凭证识别的 FAR_{eff} 应满足相应等级的要求	<1%	<0.3%	<0.3%	<0.1%
	21	当系统只识读 PIN 信息时，可分配的 PIN 总数和用户的最大数量之间的最小比率应至少为 1 000∶1 如，当 PIN 使用十进制代码时： 10 个以下用户为 4 位数 100 个以下用户为 5 位数	M	M	NA	NA
	22	载体凭证的密钥量	$>10^4\times n_{max}$	$>10^6\times n_{max}$	$>10^6\times n_{max}$	$>10^6\times n_{max}$
	23	复合识读载体凭证和 PIN 信息，或复合识读模式特征信息和 PIN 信息，PIN 至少有 10 000 种组合（十进制代码 4 位数）	OP	OP	M	M
	24	应使用完整的凭证信息（如：唯一的卡号）进行识别	M	M	M	M
	25	不可使用肉眼能直接辨识编码系统结构的凭证	M	M	M	M
	26	读取的凭证识别码在整个系统中不应被直接显示	M	M	M	M

注 1：OP^1、OP^2、OP^3、OP^4 表示有相同编号的可选项，至少被选择一项。

注 2：FAR_{eff} 表示误识率的有效值，当采用 1∶1 比对时 $FAR_{eff}=FAR$，当采用 1∶n 比对时 $FAR_{eff}=FAR\times n$。

注 3：n_{max} 表示每种凭证在 ACS 中可使用的最大数量。

6.4 胁迫

目标输入胁迫凭证的操作以及传输到监控台的警示应符合表4要求。

表4 胁迫功能要求

序号	要求	安全等级			
		1	2	3	4
1	配置胁迫功能	OP	OP	OP	M
2	在监控台的胁迫警示应区别于其他警示	M*	M*	M*	M
3	输入胁迫凭证的操作不能在胁迫触发的地方产生可视或可听见的信号	M*	M*	M*	M
4	监控台接收的胁迫信号包含位置、日期、时间和目标信息	M*	M*	M*	M
5	不可强制对不同的人员采用相同的胁迫凭证操作	OP	OP	OP	M
注：M* 表示只对本等级支持配置胁迫功能选项的有强制要求。					

6.5 优先控制功能要求

6.5.1 ACS允许暂时旁路预设规则，通过发出手动命令等实现出入口开放/出入口封锁的优先控制功能，应符合表5的要求。

6.5.2 应记录所有被执行的优先控制功能的类型、操作者ID、时间和日期。

表5 优先控制功能要求

序号	优先控制功能要求	安全等级			
		1	2	3	4
1	对单出入口的单个目标的自由出入授权(如：手动单次开启)	OP	OP	M	M
2	对系统范围的自由出入授权	OP	OP	OP	OP
3	通过操作，使单出入口或一组出入口，保持自由出入(如：手动长开)	OP	OP	OP	OP
4	按时间表，使单出入口或一组出入口保持自由出入(如：定时长开)	OP	OP	OP	OP
5	系统不应禁止由其他紧急系统(如火灾、环境)自由出入的自由出入授权	M	M	M	M
6	使单出入口或一组出入口保持锁定(如：手动出入口封锁)	OP	OP	OP	OP
7	按时间表使单出入口或一组出入口保持锁定(如：定时出入口封锁)	NA	OP	OP	OP

6.6 通信要求

6.6.1 等级2、等级3和等级4设备在通讯失败运行模式下，应能执行那些除了受通信失败响以外的所有功能。

6.6.2 等级2、等级3和等级4设备应能确保有关出入口授权的数据信息在所有组件之间(包括：凭证和识读装置之间，识读装置和出入口控制器之间，出入口控制器与监控台之间)的通信完整性。

6.6.3 通信完整性应通过监视/监管通信通道(表6第10项)和保证信息的安全传输的方式来达到。

6.6.4 系统应有防止信息在传输过程中未经授权的阅读和修改的信息安全措施。

6.6.5 在设备测试阶段应提供如何实现信息安全措施的说明。

6.7 系统自我保护要求

6.7.1 系统自我保护应符合表 6 的要求。

6.7.2 位于对应受控区、同权限受控区或高权限受控区域以外的设备，应具有适当的防篡改/防撬/防拆保护措施，满足表 6 第 5 项、第 6 项、第 7 项的要求。

6.7.3 所有接线端子以及机械和电气调整/设置组件，应置于部件外壳内部。

6.7.4 部件外壳应有足够强度以防止对内部元件通过未被监测方式造成可见损坏。具有防护面的用户接口设备(如凭证识读装置，键盘等)，其外壳防护等级应符合 GB/T 4208—2017 中 IP4X 的要求。

6.7.5 具有防护面的用户接口设备，其外壳的机械碰撞强度等级应符合 GB/T 20138 中 IK04 的要求。如果在试验之后，不能通过操纵该设备的内部元件达到允许出入条件，则允许防护罩有损坏。防拆探测应在可能接触内部元件之前产生。

6.7.6 应确保设备的外壳具有一定的机械强度，且在安装后，需要使用工具才能触及设备内部元件。

6.7.7 系统组件之间的互联应提供可信的通信方法。它应能够减少信号延迟、修改、替代或丢失发生的可能性。

6.7.8 凭证与用识读装置之间的通信要求除应满足表 3 和表 6 的相关要求外，还满足下列要求：

a) 等级 3：当单一凭证被用作识别授权方法(未采用复合识别)时，基于接触式芯片或非接触(RFID)的凭证，必需至少具有写入或修改 ID 信息的访问条件；识读器与 RFID 凭证之间应采用加密数据通信；

b) 等级 4：基于接触式芯片或 RFID 凭证的读、写或修改信息都应具有认证和访问条件；识读装置除应与 RFID 凭证之间采用加密数据通信外，其与 ACU 之间的通信也应支持加密。

表 6 系统自我保护要求

项目	序号	要求	安全等级			
			1	2	3	4
A 保护	1	电源断电后，系统各组件的记忆存储信息应保持的最小时间 注：不包括数据保留电池断电	10 min	14 d	14 d	14 d
	2	除监控台外，系统各组件在断电后电源恢复时应自动恢复工作	M	M	M	M
	3	ACU 应有自检功能，对自检结果给出通告	M	M	M	M
	4	系统各部件的设计应确保在安装后，需要使用工具才能触及部件的内部元件	M	M	M	M
	5	如果通过操作内部元件能达到允许出入条件，那么打开拟安装在对应控制区、同权限受控区或高权限受控区域以外的、或者可以从控制区以外访问的设备的外壳应引起防拆探测警示。防拆探测警示应在防拆装置被破坏之前进行	OP	M	M	M
	6	安装在对应控制区、同权限受控区或高权限受控区域外或能从对应控制区、同权限受控区或高权限受控区域外连接出入口控制系统组件的有线线缆，在其开路和短路条件下都不应导致出入口控制点执行设备动作	M	M	M	M
	7	如果通过操作内部元件能达到允许出入条件，对应控制区、同权限受控区或高权限受控区域以外的、或者可以从控制区以外访问的设备，应能探测安装后设备被移除的功能	OP	OP	M	M

表 6（续）

项目	序号	要求	安全等级			
			1	2	3	4
A 保护	8	识读现场设备以及在受控区之外的可接触的其他设备（装置）的外壳应满足相应 IK 等级要求	IK04	IK04	IK06	IK06
	9	当 ACU 与监控台之间的通信中断时，ACU 应能够存储并在通信恢复后上传的每个出入口最小事件数	32	500	1 000	1 000
	10	应能监测 ACU 和 ACS 部件之间的通信。通信丢失时间达到其等级所对应的时间段后，监控台发出警示	NA	OP	10 min	2 min
	11	应使用有效凭证（如密码，信息卡、指纹）才能进行系统管理功能（包括配置）	NA	M	M	M
	12	系统操作员访问权限等级的最少数量	1	1	2	4
	13	当系统操作员只用 PIN 登录时，其信息位数的最小值和信息特征要求 注：N 表示仅需含数字，A 表示应包含字母	4N	5N	6A	8A
	14	当系统操作员只用 PIN 登录时，PIN 信息不允许顺序升序或降序，也不允许相同字符连续使用大于两次	OP	OP	M	M
	15	当系统操作员使用复合识读载体凭证和 PIN 信息，或复合识读模式特征信息和 PIN 信息登录时，PIN 至少有 10 000 种组合（4 位数）	OP	OP	M	M
	16	系统操作员的登录凭证只能由系统管理员设定	OP	OP	M	M
	17	制造商预设的登录凭证应能被重新设置	OP	OP	M	M
	18	电源中断后，存储在 ACU 的记录事件的最小数据保留时间	24 h	48 h	120 h	120 h
	19	当使用公共网络（如互联网）时，ACS 组件之间通信加密	OP	OP	M	M
	20	储存在载体凭证中的信息应加以保护，防止未经授权的修改或复制	OP	OP	M	M
	21	通信通道无论是发生故障还是恢复，都不应导致出入口控制点的开启	M	M	M	M
	22	ACU 与监控台的通信故障不得中断或影响访问决策过程	M	M	M	M
	23	存储在出入口控制点识读装置的处理规则对出入目标应是不可见的	M	M	M	M
	24	光或声按键键盘激活指示器的反馈提示不应直接反映真实的键码	M	M	M	M
	25	ACU 与识读设备应采用加密通信，并对识读设备进行身份认证	OP	OP	OP[1]	M
	26	对于靠机械保护的识读设备和 ACU 之间的通信线路，在指导手册中应包括详细的安装要求	OP	OP	OP[1]	OP

表 6（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 探测和报告	27	监控台在配置模式下，当输入无效配置信息时，系统能发出通告信息	M	M	M	M
	28	配置超时保护	M	M	M	M
注：OP[1] 表示该编号的可选项，至少被选择一项。						

6.8 电源要求

ACS 的供电除应满足 GB/T 15408 的要求外，还应符合下列规定：

a) ACS 各部件可集中或独立供电；

b) 电源应能在表 7 所述的所有条件下支持 ACS 工作，包括对备用电源充电时的特定时期条件。

表 7 电源要求

序号	电源要求	安全等级			
		1	2	3	4
1	供电装置应安置在一个或多个设备中或使用独立的外壳	M	M	M	M
2	提供备用电源，并给出备用电源的额定容量和类型	OP	OP	M	M
3	在满负荷状态下（负荷不包括出入口控制点执行装置），备用电源应确保 ACU 及其附件正常运行的时间	OP	OP	2 h	4 h
4	出入口控制点执行装置为断电开启的设备时，应为该出入口控制点执行装置提供备用电源，并能确保在其满负荷状态下如所列的时间内，该出入口控制点执行装置运行正常	48 h	48 h	48 h	72 h
5	备用电源的充电电池应能在 24 h 内充电到 80%的额定容量，72 h 内达到 100%的额定容量	M*	M*	M	M
6	主电源断电或恢复都不应影响系统的正常运行	M*	M*	M	M
7	对备用电源的欠压和未接入进行通告和/或发出警示	OP	OP	M	M
8	主电源在额定电压的 85%～110%范围内变化时，应正常工作	M	M	M	M
注：M* 表示为适用于有备用电源的设备。					

6.9 防雷接地要求

6.9.1 ACS 应满足 GB 50343、GB 50348 和 GA/T 670 等的相关要求。

6.9.2 ACS 应有雷电防护措施。应设置电源浪涌保护器，宜设置信号浪涌保护器。

6.9.3 ACS 应等电位接地；单独接地电阻不大于 4 Ω，接地导线截面应大于 25 mm^2。

7 安全性要求

7.1 应满足 GB 50348 等国家标准的相关要求。

7.2 ACS 所使用的设备应满足 GB 16796 和相关产品标准规定的安全性要求。

7.3 在具有易燃易爆物质的特殊区域，ACS 应有防爆措施并符合相关规定。

7.4 ACS的室外有线线路宜具有抗干扰措施。

7.5 ACS的任何部分的机械结构应有足够的强度，能满足使用环境的要求，并能防止由于机械不稳定、移动、突出物和锐边造成对人员的伤害。

8 电磁兼容性要求

ACS的所有设备都应适用于相应环境和应用条件的电磁兼容性要求，并满足GB/T 30148的相关要求。

9 可靠性要求

9.1 操作可靠性

9.1.1 通用要求

应提供ACS的正确操作方法，以避免操作人员的误操作。

9.1.2 部件要求

ACS功能操作部件的标记应明确、清晰无误，排列应整齐，以减少误操作。不同权限类别的用户具有不同的操作功能。

9.2 功能可靠性

ACS的设计和配置应确保ACS功能满足本标准的要求，要达到系统功能要求应通过以下实现：

a) 明确的设计和安装说明书；
b) 明确的调试和维护说明书；
c) 合适的产品；
d) 定期维护；
e) 高抗干扰的设计；
f) 设计优良的软件；
g) 部件工作在设计范围内(如电压，温度)；
h) 功能可测(由用户，安装人员操作)；
i) 功能监测(如看门狗电路)。

9.3 系统可靠性

9.3.1 ACS应满足GB 50348等国家标准的相关要求。

9.3.2 ACS所使用的设备，在正常工作条件下其平均无故障间隔时间(MTBF)不应小于10 000 h。

9.3.3 ACS验收后的首次故障时间应大于3个月。

10 环境适应性要求

10.1 环境类别

ACS各部件暴露在GB/T 15211规定的环境类别时，应能够正常运行。

10.2 适应性要求

10.2.1 ACS的所有部件都应适用于相应环境和应用条件。

10.2.2 在有腐蚀性气体和易燃易爆环境中工作的ACS设备，应有相应的保护措施。室外设备的外壳

防护等级应不低于GB/T 4208—2017规定的IP54。

11 标志

11.1 应在ACS设备上清晰而耐久地标出下列信息：

a) 制造商和/或供应商的名称；
b) 类型；
c) 生产日期或批次号或序列号；
d) 供电额定值，例如标称电压、电流和频率；
e) 申明部件应满足的标准号；
f) 安全等级；
g) 环境类别；
h) 安装类别(类别0和类别1)。

注1：安装类别0。设备设计为可安装在该控制器所管理的对应受控区、同级别受控区、高级别受控区以外的区域，能抵御的对手能力较强。

注2：安装类别1。设备设计为仅能安装在该控制器所管理的对应受控区、同级别受控区、高级别受控区以内的区域，能抵御的对手能力弱。

11.2 设备的类型、安全等级、环境类别、安装类别的标识方式应符合附录C的要求。

11.3 端子和引线应该加以编号、加上颜色或者用别的办法来识别。

11.4 标记应耐久和易读，标牌不应被容易取下且不卷曲。

12 文件提供

12.1 同设备一起提供的资料

如果不能从设备上看清楚，应随设备给出正确安装的详细说明书。任何设备在输入极性接反时可能受损的情况，应在使用说明书中陈述清楚。

12.2 系统文件

12.2.1 与ACS有关的文件应简洁、完整、明确。应提供足够的信息，用于ACS的安装、运行、操作和维护。

12.2.2 ACS操作指南(说明书)应将错误操作的可能性降到最低，且其结构设计编排应反映用户的权限级别权限类别。

12.3 设备文件

12.3.1 与ACS部件有关的文件应简洁、完整、明确。文件应确保对ACS部件进行正确安装、操作和维护。应提供足够的信息以确保每个部件和其他ACS部件的集成。

12.3.2 部件文件应包括以下内容：

a) 制造商或供应商的名称；
b) 设备描述；
c) 申明部件应满足的标准号；
d) 认证机构的名称(如被认证)或标记；
e) 安全等级；
f) 环境类别；
g) 安装类别。

附 录 A
（资料性附录）
系统概念模型与典型应用模式

A.1 系统概念模型

ACS 的概念模型见图 A.1。

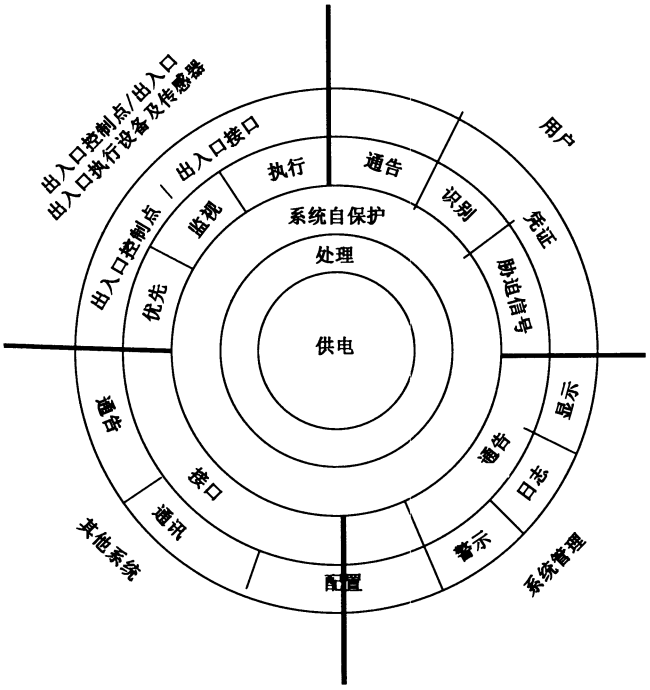


图 A.1 ACS 概念模型

A.2 典型应用模式

A.2.1 ACS 按其硬件构成模式可分为以下型式：

a) 一体型：ACS 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，见图 A.2；

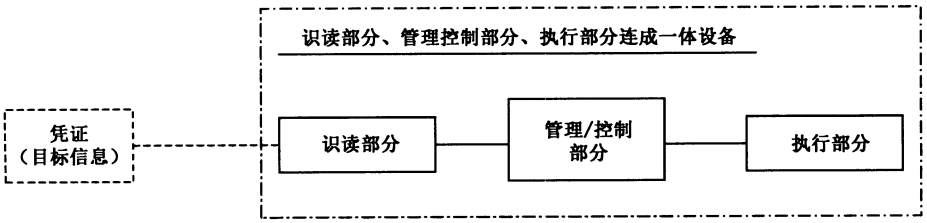


图 A.2 一体型产品组成

b) 分体型：ACS 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，见图 A.3 和图 A.4。

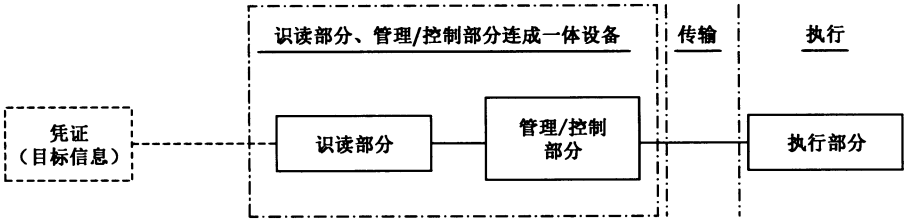


图 A.3　分体型结构组成之一

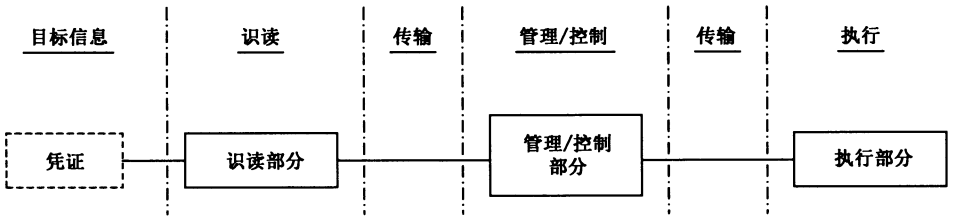


图 A.4　分体型结构组成之二

A.2.2　ACS 按其管理/控制方式可分为以下型式：

a）　独立控制型：出入口控制系统，其管理与控制部分的全部显示/编程/管理/控制等功能均在出入口控制器内完成，见图 A.5；

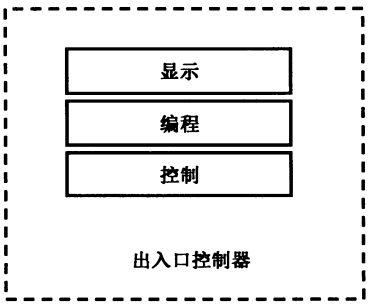


图 A.5　独立控制型组成

b）　联网控制型：ACS 的管理与控制部分的全部显示/编程/管理/控制功能不在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，见图 A.6；

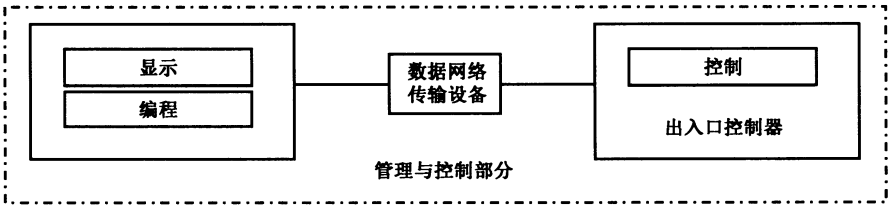


图 A.6　联网控制型组成

c）　数据载体传输控制型：与联网型 ACS 区别仅在于数据传输的方式不同，其管理与控制部分的全部显示/编程/管理/控制等功能不是在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，见图 A.7。

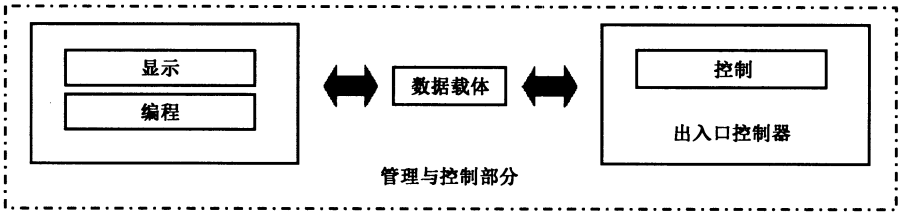


图 A.7 数据载体传输控制型组成

A.2.3 ACS 按现场设备连接方式可分为以下型式：

a) 单出入口控制设备：仅能对单个出入口实施控制的单个出入口控制器所构成的控制设备，见图 A.8；

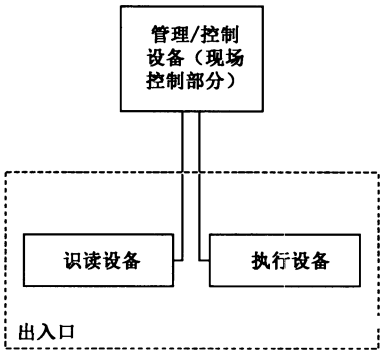


图 A.8 单出入口控制设备型组成

b) 多出入口控制设备：能同时对两个以上出入口实施控制的单个出入口控制器所构成的控制设备，见图 A.9。

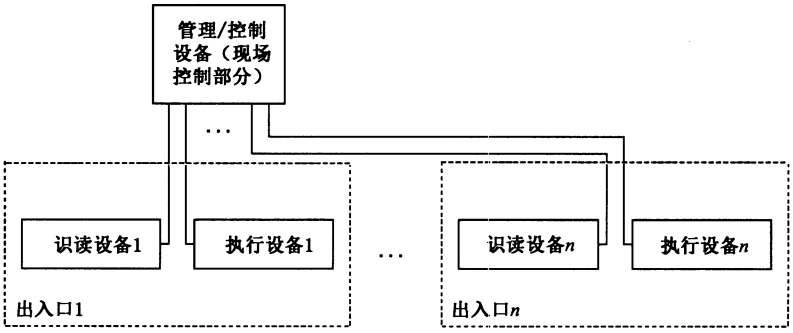


图 A.9 多出入口控制设备型组成

A.2.4 ACS 按联网模式可分为以下型式：

a) 现场总线网络型式：分为普通总线制和环形总线制两种，如：RS485/RS422 现场总线或 CAN 总线等；

1) 普通总线制：ACS 的现场控制设备通过联网数据总线与出入口管理中心的显示、编程设备相联，每条总线在出入口管理中心只有一个网络接口，见图 A.10；

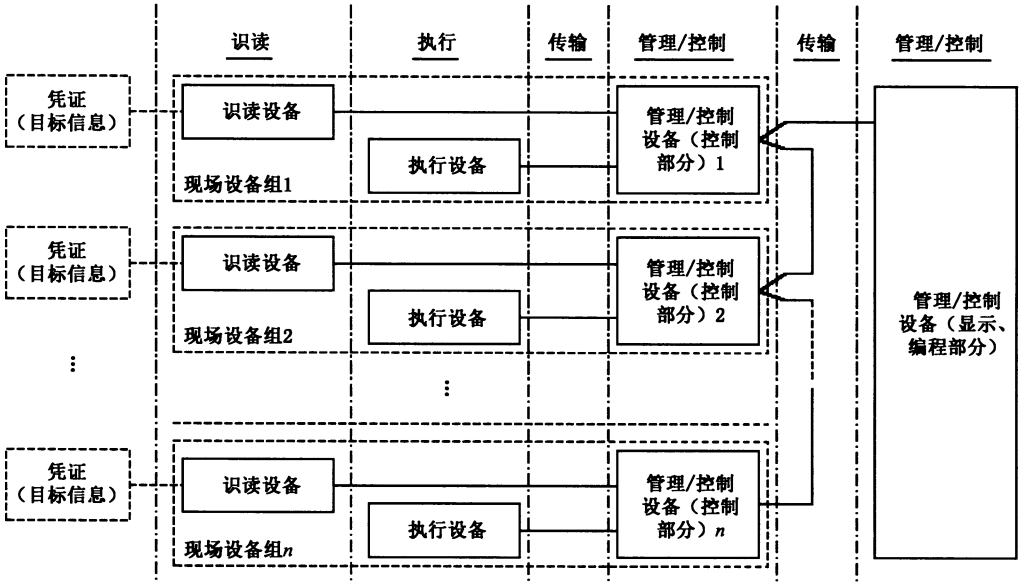


图 A.10　普通总线制系统组成

2）　环形总线制：ACS 的现场控制设备通过联网数据总线与出入口管理中心的显示、编程设备相联，每条总线在出入口管理中心有两个网络接口，当总线有一处发生断线故障时，系统仍能正常工作，并可探测到故障的地点，见图 A.11。

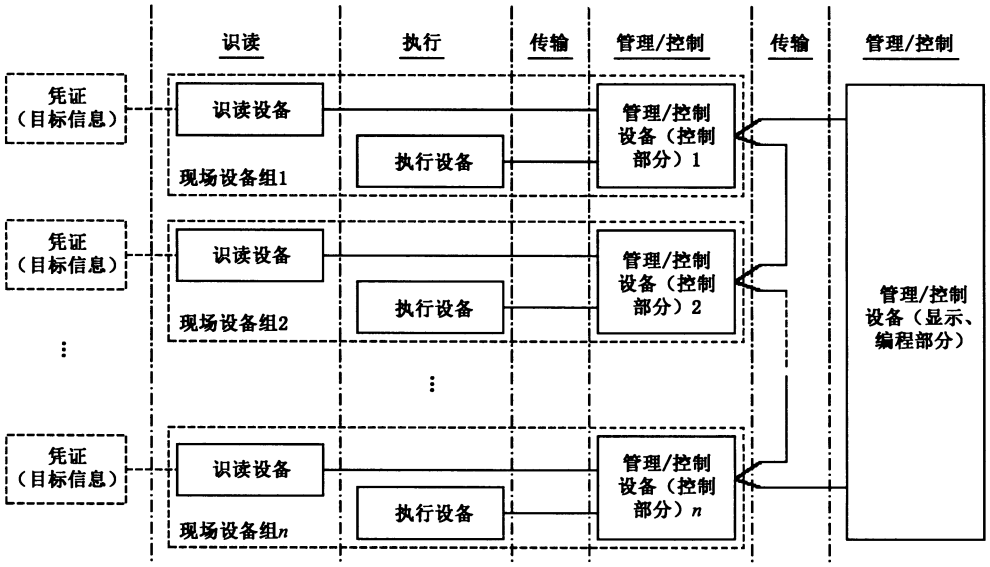


图 A.11　环形总线制系统组成

b）　以太网网络型式：ACS 的现场控制设备与出入口管理中心的显示、编程设备的连接采用以太网的联网结构，见图 A.12；

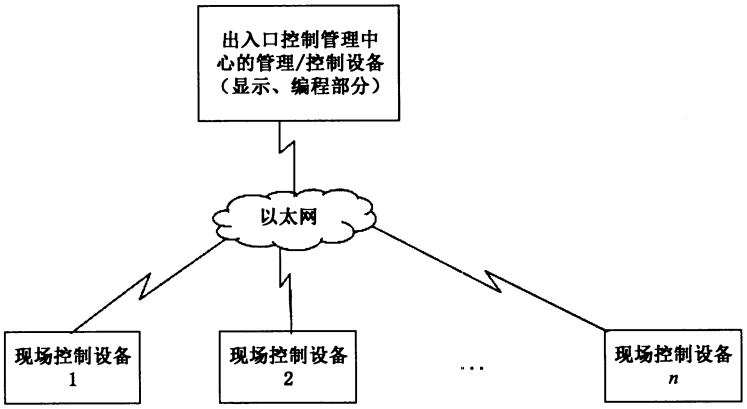


图 A.12 以太网网络型式系统组成示意图

c) 单级网：ACS 的现场控制设备与出入口管理中心的显示、编程设备的连接采用单一联网结构，见图 A.13；

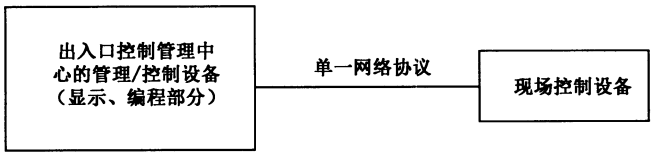


图 A.13 单级网系统组成示意图

d) 多级网：ACS 的现场控制设备与出入口管理中心的显示、编程设备的连接采用两级以上串联的联网结构，且相邻两级网络采用不同的网络协议，见图 A.14。

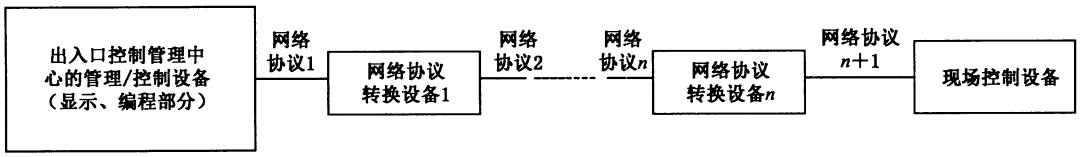
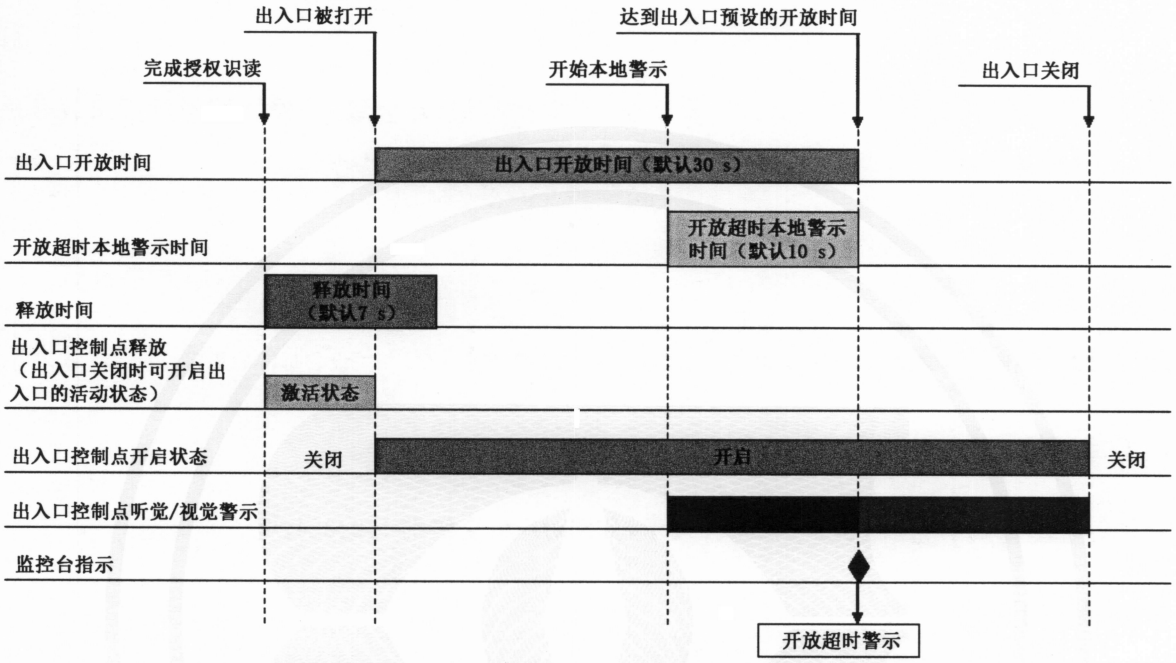


图 A.14 多级网系统组成

附 录 B
（规范性附录）
时 序 图

ACS 的识读与控制时序应符合图 B.1 的要求。



注：开放超时本地警示时间，可以被认为是部分或全部伴随出入口开放时间。这可能影响根据表 2 要求的时间设置。出入口控制点本地可听的和/或可视的开放超时本地警示，可以在开放超时警示信息发送给监控台或在出入口关闭时结束。

图 B.1 ACS 识读与控制时序图

附 录 C
（规范性附录）
设 备 标 识

C.1 标识方式

ACS的设备应采用图C.1的方式对设备类别、安全等级、环境级别、安装级别及厂家编号进行标识。

C.2 设备类型

设备类型应采用设备的缩略语表示。

注：出入口控制器的缩略语为ACU，其他类型设备的缩略语应符合ACS相关设备标准的规定。

C.3 安全等级

安全等级应采用阿拉伯数字1、2、3、4表示，分别对应安全级别1、2、3、4。

C.4 环境类别

环境类别应采用阿拉伯数字1、2、3、4表示，分别对应于GB/T 15211标准中的Ⅰ、Ⅱ、Ⅲ、Ⅳ环境级别。

C.5 安装类别

安装类别应采用阿拉伯数字0、1表示，0对应于可安装在受控区外的设备，1对应于只能安装在对应受控区、同权限受控区、高权限受控区内的设备。

C.6 厂家编号

厂家编号为可选项，可由制造商自行规定。

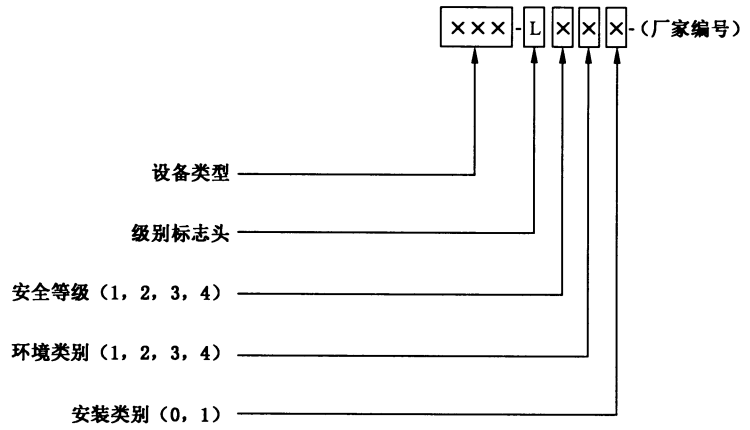


图 C.1　ACS 设备标识方式

示例：ACU-L430-D8022SN8918910，表示本设备为出入口控制器，安全级别 4 级、环境类别Ⅲ级、设备可安装在受控区外、厂家编号为 D8022SN8918910。