

执行 GA/T394 需要注意的几个问题

北京艾克塞斯科技发展有限公司 朱峰

1、关于本标准讨论的“出入口控制系统”的范围及定义

GA/T394-1 中对本标准的范围规定如下：

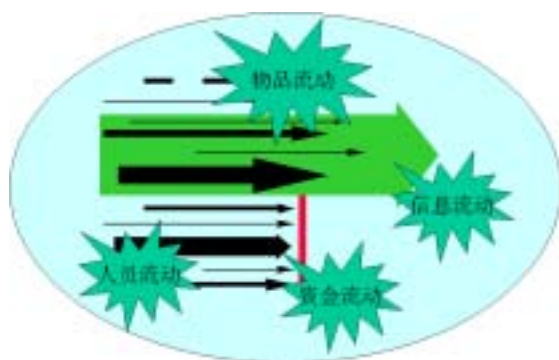
本标准规定了出入口控制系统的通用技术要求，是设计、验收出入口控制系统的基本依据。

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。其它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。

GA/T394-3.2 中对“出入口控制系统”的定义如下：

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。

对于广义的出入口控制系统，其范围可以是对人员流动、物品流动、信息流动、资金流动等的管理与控制。



广义的出入口控制系统



本标准所讨论的出入口控制系统

对于本标准讨论的出入口控制系统而言，仅是以安全防范为目的，对人员流动、物品流动的管理与控制。它不仅须采用电子与信息技术为系统平台，而且具有放行、拒绝、记录、报警这四个基本特征或称要素。

把出入口控制系统看成仅是对目标人员通过受控门的管理与控制，是很不全面的。同样，仅对出入目标在出入口实施放行与拒绝操作而无事件记录及报警功能的系统，亦非本标准所讨论的范围。

2、关于“受控区、同级别受控区、高级别受控区”及设备安装位置和连接要求对安全防范的影响

GA/T394-3.21 中对“受控区、同级别受控区、高级别受控区”的定义如下：

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。

GA/T394-4.6.4.2~4.6.4.2 中对设备安装位置的要求如下：

如果管理与控制设备是采用电位和/或电脉冲信号控制和/或驱动执行部分的，则某出入口的与信号相关的接线与连接装置必须置于该出入口的对应受控区、同级别受控区或高级别受控区内。

GA/T394-4.6.3.3 中对连接的要求如下：

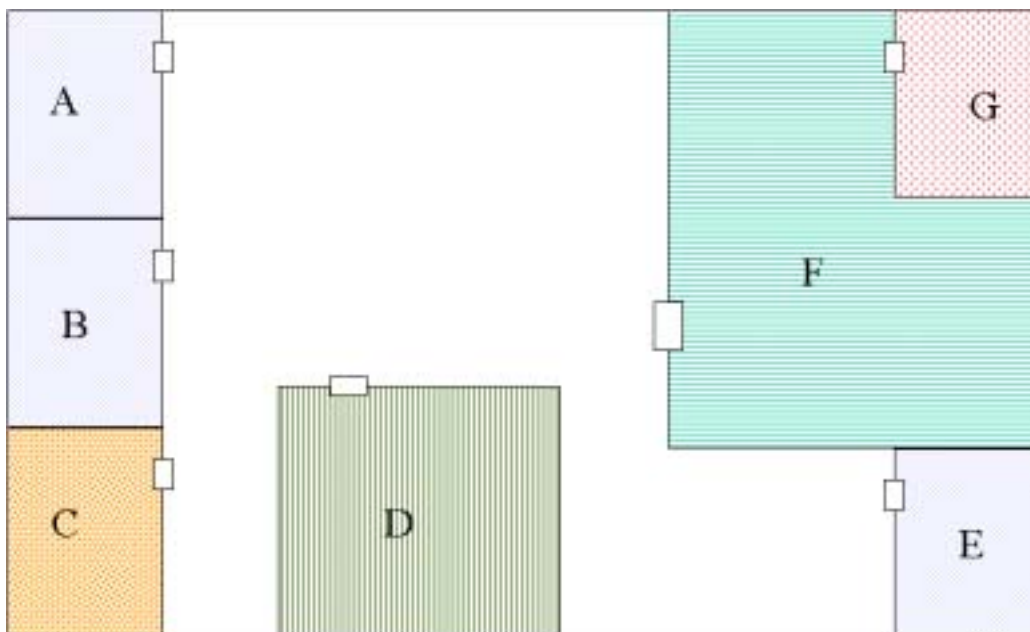
执行部分的输入电缆在该出入口的对应受控区、同级别受控区或高级别受控区外的部分，应具有相应的抗拉伸、抗弯折性能，须用强度不低于镀锌钢管的保护材料加以保护。

在出入口控制系统中，应特别注意受控区域及其级别，以及现场设备安装位置和连接线缆的防护措施等因素对安全的影响。

出入口控制等技防系统在某种意义上来说，好比设置了一个技术迷宫，它增加了非法入侵者的作案难度，延迟作案时间，并能提早报警以便及时处警。但在实际应用中，非法入侵者在初步了解技防系统后，并不去直接去解开迷宫通路而是寻找系统的薄弱点进行攻击从而到达犯罪目的。在出入口控制系统中，执行部分的输入线缆及其连接端，就是一个易于被攻击的薄弱点。

为此在 GA/T394 中对出入口控制系统特别提出了“受控区”等概念和对执行部分输入线缆的端接与防护要求，以便指导我们的系统设计、施工安装、检测验收工作。

举例来说，一个管理了从 A-G 共 7 个受控区域的出入口控制系统（比如某个公司的多个办公室），如下图：



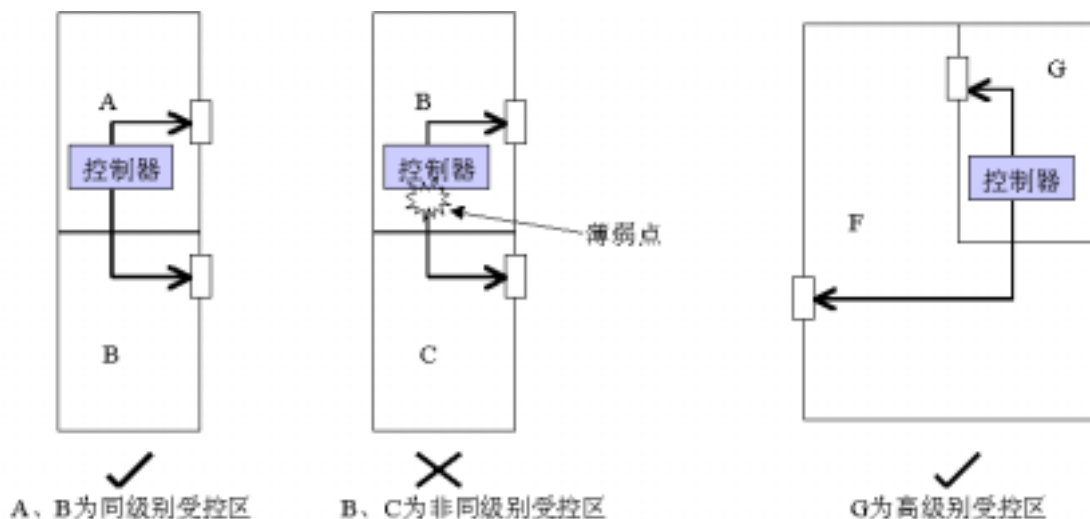
其中：A、B、E 三个区域为同级别受控区，即它们对目标的授权是一致的，能进入 A 区的目标也可进入 B、E 区，能进入 B、E 区的目标也同样能进入 A 区。G 区是相对于 F 区的高级别受控区，即能进入 G 区的目标一定能进入 F 区，而能进入 F 区的目标不一定能进入 G 区。C 区和 D 区分别是相对于其它受控区的非同级别受控区，即能进入该区的目标不一定能进入其它区，而能进入其它区的目标也不一定进入该区。若能进入 G 区的目标也能进入其它任何区的话，那么 G 区就是该出入口控制系统的最高级别受控区。

该例子若是某公司的多门联网门禁系统的话，有许多问题值得探讨：

问题一：采用多门门禁控制器应特别注意其安装位置。

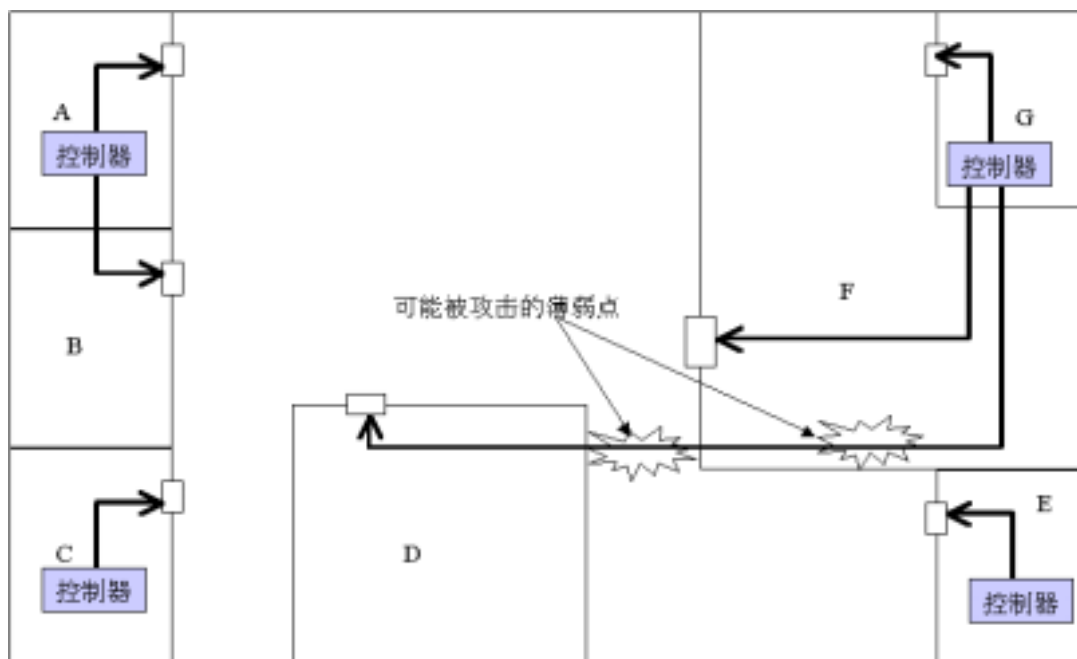
目前采用直流或脉冲信号等非编码信号直接驱动电控锁具的门禁控制器占很大比例，在本例中采用双门控制器控制 A 和 B 两个门是合理的，若控制 B 和 C 门就存在问题，控制器安装在 B 区内 C 区就不安全，控制器安装在 C 区内 B 区就不安全。

安装在 G 区的双门控制器控制 G 和 F 两个门是否合理呢？答案是肯定的。



问题二：采用多门门禁控制器应特别注意对电控锁连接线的防护。

当电控锁的连接线必须离开本受控区、同级别受控区、高级别受控区敷设时，有可能成为被实施攻击的薄弱点，必须严格防护。



在多出入口系统中要想提高安全性和可靠性，减少工程施工带来的安全隐患，建议尽量采用联网控制的单出入口控制器。若必须采用多出入口控制器，则应安装在高级别防区内并做好对执行部分输入线缆的防护。

3、关于“识读现场设备、防护面”及其应用的意义

GA/T394-3.13 中对“识读现场设备”的定义如下：

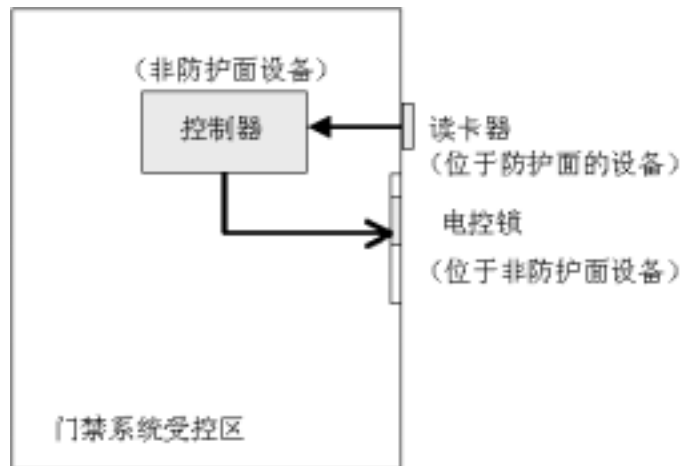
在识读现场的、出入目标可以接触到的、有防护面的设备（装置）。

GA/T394-3.14 中对“防护面”的定义如下：

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。

出入口控制系统的主要作用就是使有出入授权的目标快速通行，阻止未授权目标通过。受控区是出入口控制系统提出的基本概念，在犯罪分子欲实施技术开启和破坏时，安装在受控区内的系统设备（如控制器、管理计算机）相对于安装在受控区外的设备（如读卡器）要安全的多。

由于出入口控制系统的特点决定了在大多数情况下其部分设备须暴露在受控区外，因此在本标准中许多地方都提到了“防护面”，在条文中强化了对位于“防护面”设备的防破坏、防技术开启等方面的要求，弱化了“非防护面”设备在这方面的要求。



4、关于系统的绝对“计时”与相对“计时”问题

GA/T394-4.5.1.3 中对计时的要求如下：

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它的与事件记录、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，其它的与事件记录、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。

绝对计时的准确性，代表了系统时间与标准时间（如北京时间）误差的大小，相对计时的一致性，体现了一个系统中多个带有独立计时的设备之间计时差异。因为各个带有独立计时的设备在采集某一个目标的出入事件信息时，会将其时间信息附加该信息上，这样会形

成该目标在系统内的行动轨迹，一旦相对计时的一致性存在差异，系统会给出错误的结果，这在实际的案件侦破过程中会误导我们的工作。因此在本标准中特别强调相对“计时”问题，



相对计时不一致造成的后果，使破案老手遇到新问题

5、关于“应急开启”需注意的问题

GA/T394--4.5.1.6 中对“应急开启”的要求如下：

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。

出入口控制作为一种电子系统，必须考虑在遇到电源不正常、线路损伤、电子元器件失效等特殊情况下的应急开启问题。但应注意：无论采用上述 a)、b) 哪种方案，都不能以牺牲系统的防破坏、防技术开启指标为代价，因为这会使应急开启成为系统易被攻击的薄弱点。

下面是两种常用的采取冗余设计的应急开启方案：

方案一：在有多出入口的一个受控区，采用两套以上的独立控制单元分别控制，互为冗余备份。



方案二：采用传统机械钥匙作为电子钥匙的冗余备份，当电子系统发生故障不能正常开启时，用传统机械钥匙应急开启。该机械钥匙由系统最高授权者妥善保管。



在双开门设计中，一扇用电控锁，另一扇用机械锁是常用的方案

6、关于“通过目标的安全性”及“紧急险情下的安全性”问题

GA/T394-5.2 中对“通过目标的安全性”的要求如下：

系统的任何部分、任何动作以及对系统的任何操作都不应对出入目标及现场管理、操作人员的安全造成危害。

GA/T394-5.3 中对“紧急险情下的安全性”的要求如下：

如果系统应用于人员出入控制，且通向出口或安全通道方向为防护面，则系统须与消防监控系统及其它紧急疏散系统联动，当发出火警或需紧急疏散时，不使用钥匙人员应能迅速安全地通过。

英文“Security”和“Safety”翻译成中文都是“安全”，但它们的含义有所不同，“Security”是“安全”的社会属性，“Safety”是“安全”的自然属性。以防入侵、防盗窃、防抢劫、防破坏、防爆炸等为目的的安全技术防范系统主要针对的是“Security”；而防火、防目标被非人为因素伤害等是“Safety”涉及的问题。当同时出现这两种“安全”问题时，在大多数情况下应优先解决“Safety”问题。这是设计系统与产品的基本原则。



在出入口控制系统中，识读部分与执行部分是出入目标最易接触的部分，也是最有可能对出入目标的造成伤害的部分。但不同的产品类型，其对安全的影响也是不同的。

在生物特征识别中，指纹、掌形识别等需人体直接接触的识读装置就不如面部、眼虹膜识别这类不需人体直接接触的识读装置安全，因为直接接触的识读装置的接触面若不能及时清洁，就有可能成为某些传染性疾病的媒介。

另外，直接担负阻挡作用的执行机构，其启闭动作本身必须考虑出入目标的安全，如电动门的关闭动作必须等待出入目标安全离开时方可进行，档车器必须等待车辆离开方可落

下档车臂等。

在安防系统中与紧急疏散及消防系统联系最为紧密的就是出入口控制系统。出入口控制系统强调的是对空间的隔离，以保证“Security”；而紧急疏散及消防系统强调的是能快速逃离，以保证“Safety”。



在“Safety”优先的原则指导下，出入口控制系统的设计必须满足紧急疏散及消防的需要，这并不是说出入口控制系统所管理与控制的每个出入口必须与消防联动。但在 GA/T394-5.3 的条件下必须联动，保证在火灾等紧急情况发生时，用于闭锁或起到阻挡作用的出入口控制执行部件能自动释放疏散出口，不使用钥匙人员应能迅速安全地疏散。

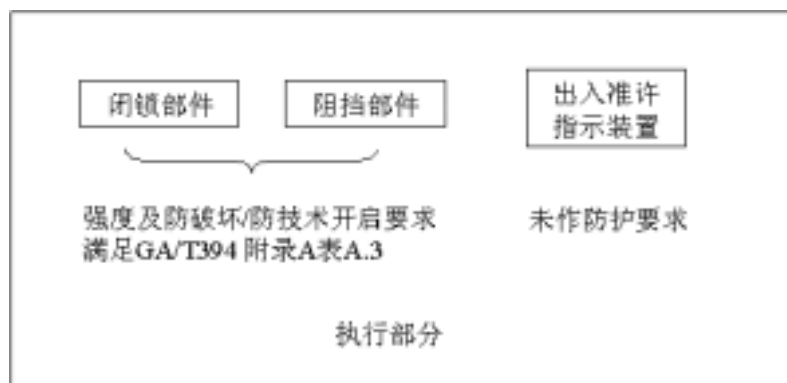
7、关于“执行部分”的类型及防护要求问题

GA/T394-4.5.2.3 b)中对“执行部分”的类型要求如下：

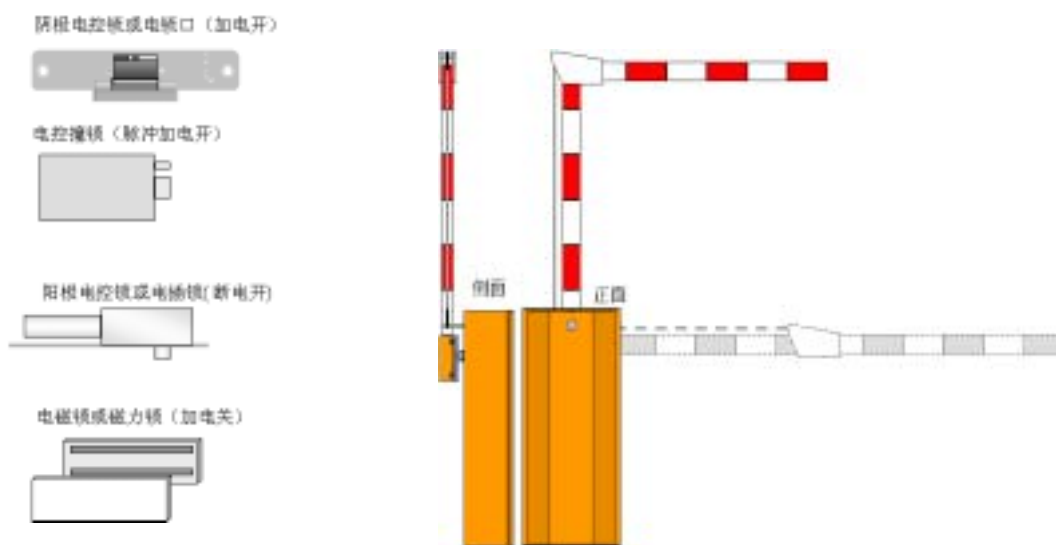
执行部分由闭锁部件或阻挡部件以及出入准许指示装置组成。

本标准所讨论的“执行部分”的类型主要由 a)闭锁部件；b)阻挡部件 c)出入准许指示装置 d)前三种的组合部件或装置。

不同的管理要求、安全要求、现场环境以及需控制的出入目标种类、通过率指标等要求的不同，使得“执行部分”的产品型式、结构也有很大的差异。应用 GA/T394 要注意“执行部件”多样性的特点，不要认为“执行部件”就一定是“电控锁具”，这是很片面的理解。同时还应注意 GA/T394 附录 A 表 A.3 对“执行部分”的防护要求主要针对闭锁及阻挡部件，对指示装置（部件）未作要求。



在停车库（场）出入口使用的电动栏杆机，是常见的阻挡指示部件，它仅能起到阻挡指示作用，不能起到对其控制的出入目标 机动车的阻挡作用，要想达到阻止普通车辆非法闯入的高安全要求场合，必须使用有足够抗撞击能力的挡车设备。如：某驻华使馆的地下停车库的出入口采用了地面升降式阻挡设备、它能有效的阻止一般的“汽车炸弹”袭击，而普通的电动栏杆机根本做不到这点。



8、关于“防破坏、防技术开启”问题

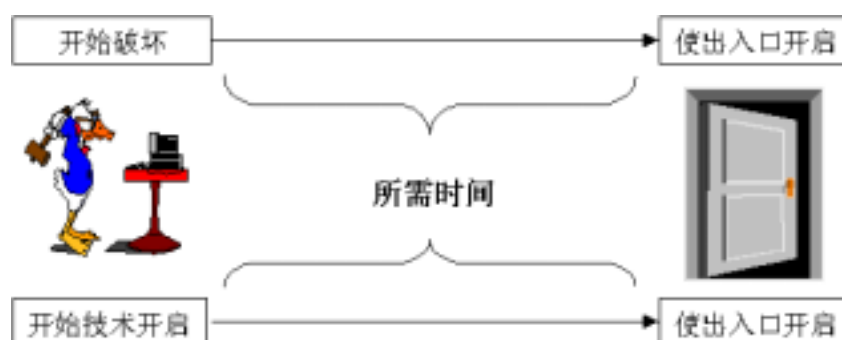
GA/T394-1.15 中对“防破坏能力”的定义如下：

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）。

GA/T394-1.16 中对“防技术开启能力”的定义如下：

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），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）。

这里应特别注意：不要把“防破坏”看成“防设备被破坏”，而要看，位于防护面的设备遭到破坏性攻击时，出入口不被开启的能力。



举例来说：（例1）位于某出入口防护面的读卡器在遭到破坏性攻击1分钟后，该读卡器已完全损坏，但犯罪分子在随后的40分钟内一直未能将出入口打开。（例2）而位于另一个出入口防护面的一体化门禁机的设计的非常坚固，犯罪分子用了8分钟才把它破坏，但在随后的1分钟内就把出入口打开了。在这两个例子中，例1的防破坏能力要强于例2的防破坏能力。

GA/T394 中对“防破坏能力”及“防技术开启能力”的技术指标见 GA/T394 附录 A“系

统防护级别推荐表”，它用 3 个子表对系统识别部分、系统管理/控制部分、系统执行部分的“防破坏能力”及“防技术开启能力”分别给出了规定。对无防护面的设备、出入准许指示部件，不作要求。

在实际应用中，要根据不同的安全与管理要求选择系统与产品，满足“防破坏”及“防技术开启”要求。