Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS6

功能规格书 V1.03

info@acs.com.hk
www.acs.com.hk

目录

图目录

表目录

1.0. 简介

本手册阐述了龙杰智能卡有限公司（Advanced Card Systems Ltd., ACS）自主研发的 ACS 智能卡操作系统——版本 6（ACOS6）的特性和功能。

1.1. 特性

ACOS6 具有以下特性：

- 完整的 64 KB EEPROM 应用数据存储容量
- 符合 ISO 7816 第 1、2、3 和 4 部分
- 可转换的高速通讯波特率（9,600 bps 至 223,200 bps）
- 支持 ISO 7816 第 4 部分的文件结构：透明、线性定长、线性变长、循环
- 支持 DES/3DES 加密运算
- 符合 FIPS 140-2 的随机数发生器（基于硬件）
- 具有相互认证功能，能够生成过程密钥
- 具有安全报文发送功能，确保数据传输的真实性和机密性
- 提供多个安全电子钱包，可用于支付应用
- 多级安全访问层次
- 具有防拔插机制，确保文件头和 PIN 命令受到保护

1.2. 技术参数

以下是 ACOS6 卡片的技术参数:

1.2.1. 电气参数

- 工作电压：5 V DC+/-10% (A 类)与 3 V DC +/-10% (B 类)
- 最大电源电流：<10 mA
- ESD 保护：≤ 4 KV

1.2.2. EEPROM

- 容量：64K 字节（65,536 个字节）
- EEPROM 使用寿命：10 万次擦写
- 数据保留时间：10 年

1.2.3. 环境温度

- 工作温度：-25 °C - 85 °C
- 存储温度：-40 °C - 100 °C

1.3. 符号和缩写

缩略语	描述
3DES	3 倍数据加密标准算法 Triple DES
AID	应用标识符 Application/Account Identifier
AMB	访问模式字节 Access Mode Byte
AMDO	访问模式数据对象 Access Mode Data Object
APDU	应用协议数据单元 Application Protocol Data Unit
ATC	帐户交易计数器 Account Transaction Counter
ATR	复位应答 Answer to Reset
ATREF	帐户交易参考 Account Transaction reference
CLA	APDU 命令的类别字节 Class byte of APDU commands
COMPL	逐位补 Bit-wise Complement
COS	卡片操作系统 Card Operating System
DEC(C, K)	用密钥 K 对数据 C 进行 DES 或 3DES 解密 Decryption of data C with key K using DES or 3DES
DES	数据加密标准 Data Encryption Standard
DF	专用/目录文件 Dedicated File
ENC(C, K)	用密钥 K 对数据 P 进行 DES 或 3DES 加密 Encryption of data P with key K using DES or 3DES
EF	基本文件 Elementary File
EF1	个人密码文件 PIN File
EF2	密钥文件 Key File
FCP	文件控制参数 File Control Parameters
FDB	文件类型字节 File Descriptor Byte
INS	APDU 命令的指令字节 Instruction byte of APDU commands
IV_Seq	用于 SM-MAC 的带序号初始向量 Initialization vector with sequence number used in SM-MAC
LCSI	应用周期状态字 Life Cycle Status Integer
LSb	最低有效位 Least Significant Bit
LSB	最低有效字节 Least Significant Byte
MAC	报文认证码 Message Authentication Code
MF	主控文件/目录 Master File
MFP	Mifare Plus 卡 Mifare Plus
MOC	中国建设部标准 Ministry of Construction – China specifications
MSb	最高有效位 Most Significant Bit

缩略语	描述
MSB	最高有效字节 Most Significant Byte
Nibble	半字节；一个字节包含两个半字节 four- bit aggregation; a byte consists of two nibbles
PBOC	中国人民银行标准 People's Bank of China specifications
RFU	保留为将来使用 Reserved for Future Use
RMAC	零售报文认证码 Retail MAC
SL0	Mifare Plus 安全级别 0 Mifare Plus Security Level 0
SL1	Mifare Plus 安全级别 1 Mifare Plus Security Level 1
SL2	Mifare Plus 安全级别 2 Mifare Plus Security Level 2
SL3	Mifare Plus 安全级别 3 Mifare Plus Security Level 3
SAC	标准安全属性 Security Attribute – Compact
SAE	扩展安全属性 Security Attribute – Expanded
SAM	安全存取模块 Secure Access Module
SCB	安全条件字节 Security Condition Byte
SCDO	安全条件数据对象 Security Condition Data Object
SE	安全环境 Security Environment
Seq#	用于 SM-ENC 的序号 Sequence number used in SM-ENC
SFI	短文件标识符 Short File Identifier
SM-ENC	带加密的安全报文 Secure Messaging with Encryption
SM-MAC	带 MAC 的安全报文 Secure Messaging with MAC
TLV	标签-长度-值 Tag-Length-Value
$TTREF_C$	终端交易编号-存款 Terminal Transaction Reference for Credit
$TTREF_D$	终端交易编号-扣款 Terminal Transaction Reference for Debit
UQB	使用限定字节 Usage Qualifier Byte
II	连接 Concatenation

表1：符号和缩写

2.0. 卡片管理

本节概述了卡层级的特性和管理功能。

2.1. 防拔插功能

ACOS6 使用防拔插机制保护卡片数据，避免由于卡片拔插导致的损坏（如在数据更新时突然从读写器中拔出卡片，或者读卡器在卡片数据更新过程中发生机械故障等）。卡片复位后，ACOS6 会检查防拔插数据域，并进行必要的数据恢复。之后 COS 会将事前保存的数据返回至 EEPROM 原来的地址。

2.2. 卡片头模块

ACOS6 是一个具有 64K EEPROM 的卡片操作系统。在初始状态下（没有文件存在），用户可以通过指定地址的读/写二进制命令方式访问该卡片头模块。

2.3. 卡片应用周期状态

ACOS6 具有以下的状态：

1. **预个人化状态** – 卡的初始状态。在此状态中，用户可以自由访问卡片头模块（卡片头模块的定义见上一节）。可以使用读二进制（READ BINARY）命令或修改二进制（UPDATE BINARY）命令通过地址对卡片头模块进行引用。

   用户还可以随意个性化卡片头模块。

2. **个人化状态** – 一旦成功创建 MF 而且**卡片应用周期标识位**未改变，卡片即会进入本阶段。用户不再能够直接访问卡片头块。但可以像在**操作模式**下一样，在卡片中创建和测试文件。

   用户可以在此阶段进行测试，并可以通过清卡（CLEAR CARD）命令返回到预个人化状态。

3. **用户状态** – 一旦成功创建 MF 而且**卡片应用周期标识位**改变，卡片即会进入此阶段。另外用户也可以通过激活卡片（ACTIVATE CARD）命令从个人化状态进入到用户状态。

   一旦设置了卡片应用周期标识位，但没有设置取消激活卡片使能标志，卡片将不能再恢复到之前的状态。清卡（CLEAR CARD）和取消激活卡片（DEACTIVATE CARD）命令将不再有效。

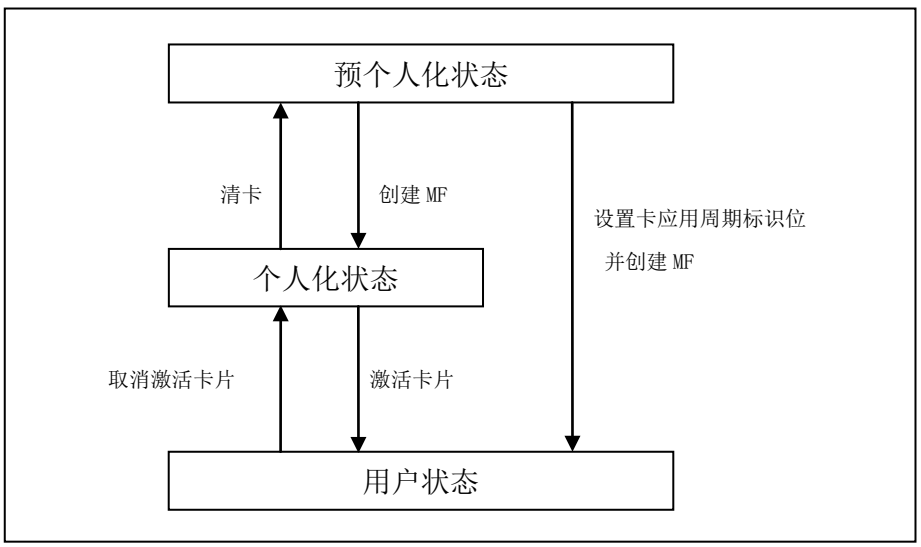


图1：卡片应用周期状态

2.3.1. 典型的卡片开发步骤

1. 用户使用 UPDATE BINARY 命令个人化卡片的头模块。
2. 用户建立自己的卡片文件结构。先建立 MF，接着建立 DF 和 EF。卡片的安全设计也将在该阶段被测试。如果发现任何设计缺陷，用户可以随时通过 CLEAR CARD 命令返回到状态 1。
3. 一旦卡片的文件与安全设计确定下来并完成测试，执行 CLEAR CARD 命令，并改变**卡片应用周期标识位**。
4. 重新创建 MF 后，卡片进入到实际操作模式。用户可以在此阶段重构文件系统，但卡片不能再回到之前的状态。

在 ACOS6 3.01 以及更高的版本中，用户可以选择在卡片头模块进行设置，使 DEACTIVE CARD 命令能够使用。这样就可以通过 Active Card 命令来代替步骤 3 和步骤 4。如果应用程序开发人员希望清除卡片内容，可以使用 Deactive Card 命令。若需要控制对 Deactive Card 命令的使用，可以设置安全属性来进行限制。

2.4. 复位应答

硬件复位（如上电）后，卡片按照 ISO 7816 第 3 部分的规定传送复位应答（ATR），格式与 ACOS2 的 ATR 相同。ACOS6 支持正向约定的 T=0 协议。但未实现协议功能。

关于 ATR 选项的详细描述请参看 ISO 7816 第 3 部分。

2.4.1. 自定义 ATR

ACOS6 的 ATR 可以自定义，包括修改卡片传输速度或向卡片写入具体的身份信息。新的 ATR 必须符合 ISO 7816 第 3 部分的规定，否则卡片可能在下次上电或者复位时变得没有反应或者不可恢复之前的状态。因此，只建议改变 T0（低半字节）、TA1 和历史字节。

3.0. 文件系统

本节探讨 ACOS6 智能卡的文件系统。

3.1. 多层次的文件系统

ACOS6 的文件系统和结构完全符合 ISO 7816 第 4 部分的规定。该文件系统非常类似于现代的计算机操作系统。文件的根是主文件（MF）。卡中的每个应用或数据文件组均可包含在称为专用文件（DF）的目录中。每个 DF 或 MF 都可以在目录下的基本文件（EF）中存储数据。

ACOS6 允许任意深度的 DF 树结构。也就是说，DF 可以嵌套，如下方的 **图 2** 所示。

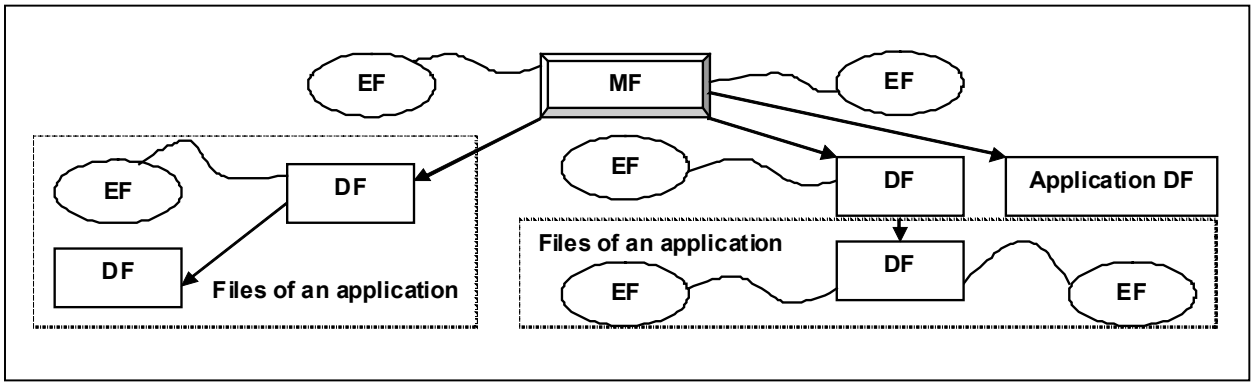


图2： 多层次的 DF 文件系统示例

3.2. 文件头数据结构

ACOS6 通过文件组织用户的 EEPROM 区。每个文件都有一个文件头，即一个描述文件属性的数据块。了解文件头模块的知识有助于应用程序开发人员准确的规划 EEPROM 空间的使用。

3.2.1. 文件类型字节（FDB）

该数据域标识文件的类型，文件头模块的大小取决于文件的类型。

3.2.2. 数据编码字节（DCB）

ACOS6 不使用此数据域，它只是设置为文件头的一部分以符合 ISO 7816 第 4 部分的规定。

3.2.3. 文件标识（FID）

这是一个 16 位的数据域，它是 MF 或 DF 内文件的唯一标识，DF（或 MF）下的文件必须是唯一的。

3.2.4. 文件大小（File Size）

这是一个 16 位的数字域，用于定义文件的大小，但不包括文件头的大小。对于记录类型的 EF 来说，第一个字节表示记录的最大长度（MRL），第二个字节表示记录的数量（NOR）。对于非记录类型的 EF（透明 EF）来说，第一个字节表示文件大小的高字节，第二个字节表示文件大小的低字节。对于 DF 来说，该数据域无用途。

3.2.5. 短文件标识符（SFI）

短文件标识符是一个五位长的数值，表示文件的短 ID。ACOS6 允许通过 SFI 指定文件。FID 的最后 5 位不一定要匹配这个 SFI。同一个 DF 下可能有 2 个文件具有相同的 SFI。在这种情况下，ACOS6 会选

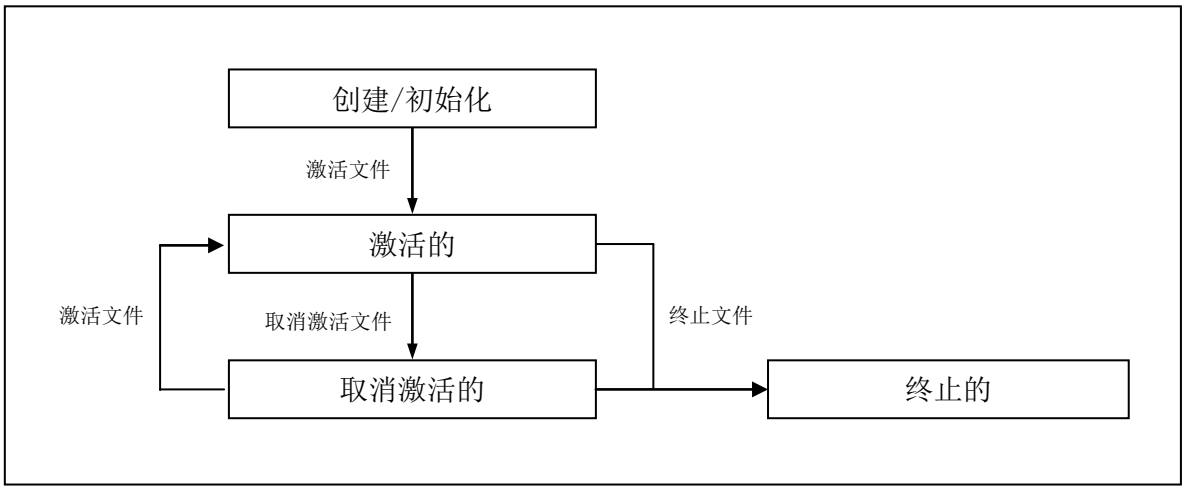
择先创建的文件。

3.2.6. 应用周期状态字（LCSI）

按照 ISO 7816 标准第 4 部分的定义，此字节用于标识文件的应用状态，可以为以下值:

b8	b7	b6	b5	b4	b3	b2	b1	Hex	含义
0	0	0	0	0	0	0	1	01	创建状态
0	0	0	0	0	0	1	1	03	**初始化状**态
0	0	0	0	0	1	-	1	05 或 07	**操作状**态（激活的）
0	0	0	0	0	1	-	0	04 或 06	**操作状**态（取消激活的）
0	0	0	0	1	1	-	-	0C - 0F	终**止状**态

表2： 应用周期状态字节



□3 :应用周期状态**字**

- **在**创建**/初始化状**态，COS **允**许执行对该文件的全部命令。
- **在激活状**态，只有满足该文件的安全条件，COS **才允**许执行对该文件的命令。
- **在取消激活状**态，COS **不允**许执行大部分对该文件的命令。
- **在**终止状态，COS **不允**许执行**任何**对该文件的命令。

3.2.7. 标准安全属性的长度（SAC Len）

该字节表示包含在文件头下的 SAC 结构的长度。

3.2.8. 扩展安全属性的长度（SAE Len）

该字节表示包含在文件头下的 SAE 结构的长度。

3.2.9. DF 名称长度/第一条循环记录

如果文件是 DF，则本数据域表示 DF **名称的**长度。

如果文件是循环 EF，则本数据域表示最后修改的记录的索引。

在其他情况下本数据域无用途。

3.2.10. 父目录地址

这两个字节表示文件父 DF 的物理 EEPROM 地址。

3.2.11. 校验和

为了保证文件头数据的完整性，COS **使用了校**验和。计算方式是异或文件头中**前面的全部字**节。如果发现文件头的校验和错误，则禁止执行对该文件的命令。

3.2.12. 标准安全属性（SAC）

这是一个数据结构，描述对文件进行某些操作所需要满足的安全条件。如 ISO 7816 定义，该数据编码成"AM-SC"模板形式，该数据域的最大长度是 8 字节。更多信息请参看 **4.1.1 节**。

3.2.13. 扩展安全属性（SAE）

这是一个数据结构，描述对卡片进行某些操作所需要满足的安全条件。该数据编码与 SAC 不同，但是同样符合 ISO 7816 的定义。该数据域的最大长度是 32 字节。更多信息请参看 **4.1.2 节**。

对于 DF 文件，文件头模块中还包含附加数据域。

3.2.14. SE 文件标识（仅适用于 DF）

对于 DF 来说，该数据域由 2 个字节的文件标识（FID）组成，对应的文件为该 DF 下的一个子文件。这个子文件叫做安全环境（SE）文件，由 COS 在内部进行处理。

3.2.15. FCI 文件标识（仅适用于 DF）

对于 DF 来说，该数据域由 2 个字节的文件标识（FID）组成，对应的文件为该 DF 下的一个子文件。本 COS 版本不使用此文件。

3.2.16. DF 名称（仅适用于 DF）

对于 DF 来说，该数据域是文件的长名。我们可以通过最长 16 字节的长名来选择文件。

3.3. 内部安全文件

COS 的运作取决于与安全内容相关的内部文件。内部文件被激活时，它的 READ（读）条件应设置为 NEVER（永不）。一般来说，一个 DF 应该具有：(1)一个密钥文件，储存用于校验的 PIN（称为 EF1），(2)一个密钥文件，储存用于认证的 KEY（称为 EF2）；及 (3)一个储存安全条件的 SE 文件。

密钥文件是一种内部线性变长文件。它可能包含(1)PIN 数据结构或者(2)KEY 数据结构。

4.0. 安全机制

文件命令受制于目标文件（或当前的 DF）的安全访问条件。这些条件是基于由系统当前维护的 PIN 和 KEY。如果对应的 PIN 或 KEY 通过校验或认证，卡的命令将被允许。

全局 PIN 直接存储在 MF 的 PIN 文件（EF1）。同样，局部 KEY 直接存储在当前选定的 DF 的 KEY 文件（EF2）。最多允许同时存在 31 个全局 PIN、31 个局部 PIN、31 个全局 KEY 和 31 个局部 KEY。

4.1. 文件安全属性

每个文件（MF、DF 或 EF）的文件头模块中都设置有一套安全属性。安全属性设置模式分为两种：标准安全属性（SAC）和扩展安全属性（SAE）。

4.1.1. 标准安全属性（SAC）

SAC 是一个存储在每个文件内的数据结构。它标识对于该文件什么样的文件操作是被允许的，以及要符合哪些条件对应的文件操作才被允许。

- SE记录存储在SE文件中，SE文件的ID在当前DF的文件头中指定。

4.1.2. 扩展安全属性（SAE）

SAE 是一个数据结构，存储于每个文件当中。它告诉 COS 是否允许文件命令继续进行。SAE 较 SAC 更为通用。它的格式是访问模式数据对象（AMDO）后面紧随一个或多个安全条件数据对象（SCDO）。

4.2. 安全环境

安全条件被编码于一个安全环境（SE）文件中。每个 DF 都有一个专用的 SE 文件，该文件的标识符在 DF 的头模块中指定。每个 SE 记录的结构如下：

<SE ID Template> <SE Authentication Template>

SE 标识模板（SE ID Template）：SE 标识模板是一个强制性数据对象，它的值代表了 SAC 和 SAE 的 SC 字节所指定的标识符。

SE 认证模板（SE Authentication Template）：认证模板（AT）定义了满足 SE 所须具备的安全条件。该安全条件为 PIN 或者 KEY 认证。

4.3. 相互认证

相互认证是卡片与读卡设备之间相互认证对方真实性的过程。相互认证成功执行以后会产生一个**过程密钥**，该过程密钥只在**过程**中有效。这个过程我们这样定义：在相互认证成功执行以后，直到卡片的重新复位或者另外一次成功的相互认证。

4.4. 短密钥外部认证

短密钥外部认证使用卡片随机数结合终端响应的方法获得对卡的授权。它缩短了外部认证的时间或者允许采用更适用于人工输入的一次性密码。

4.5. 确保真实性的安全报文（SM-MAC）

ACOS6 支持两种安全报文 - **确保真实性的安全报文**（SM-MAC）和**确保机密性的安全报文**（SM-ENC）。本节将讨论用于确保真实性的安全报文。用于确保机密性的安全报文将在 **4.6 节**中讨论。

确保真实性的安全报文允许对传入或传出卡片的数据和命令进行验证，从而确保命令没有被修改或重

放。由发送方传送给接收方的数据块附带有四个字节的 MAC。接收方在继续操作之前会先查验 MAC。在执行安全报文发送之前，发送方与接收方必须先通过 **4.3 节**中所述的相互认证获得过程密钥。

4.6. 确保机密性的安全报文（SM-ENC）

ACOS6 3.02 及更高的版本均支持 ISO 安全报文（SM）。安全报文可以确保在卡片和终端/服务器之间传输的数据处于安全状态，不易受到窃听、重放攻击或者未经授权的更改。几乎所有的命令都可以采用由终端发起的安全报文。

4.7. 密钥注入

密钥注入可以用于将密钥或分散密钥从 ACOS6-SAM 或终端安全地载入到目标 ACOS6-SAM 或客户的 ACOS6 卡中。为了描述方便，我们定义含有待注入密钥的 ACOS6-SAM 为*"source SAM"*，而接受导入密钥的 ACOS6/ACOS6-SAM 为**"target ACOS6"**。

"Target ACOS6"使用 Set Key 命令而"source SAM"使用 Get Key 命令来执行密钥注入。.

注：*密钥注入的功能只在 ACOS6-SAM 版本 4.02、ACOS6 版本 3.02 和它们之后的版本中可用。详情见 ACOS6-SAM 参考手册。*

5.0. 钱包应用

ACOS6 带有一个安全的电子钱包应用，可以增加储值卡的功能。与此钱包应用相关的命令包括——查询账户（INQUIRE ACCOUNT）、充值（CREDIT）、消费（DEBIT）和取钱包交易日志（GET PURSE TRANSACTION LOG）。

5.1. 查询账户（Inquire Account）

执行 INQUIRE ACCOUNT 交易时，卡片会返回账户的当前余额和相关信息，有关数据会带有一个 MAC 密码校验和。此签名可以被视为由卡片颁发的用于确认当前余额和前一次交易的证书。用于生成 MAC 密码校验和的密钥可以被指定。

为了防止窃听者利用前一个 INQUIRE ACCOUNT 命令的响应进行重放攻击，读卡设备可以向卡片发送一个参考值来用于 MAC 运算。

5.2. 消费（Debit）

执行 DEBIT 交易会从账户余额中扣除指定的金额。可以消费的最大金额为当前账户的余额。账户余额不允许为负数。

用户能够为 DEBIT 交易指定不同的安全条件来允许多种安全要求。

5.3. 充值（Credit）

执行 CREDIT 交易会向账户的余额中充入指定金额。最大余额（MAX BAL） – 钱包文件的第一条记录 – 使新的余额不得超过指定金额

CREDIT 交易的执行始终应当在高度安全的情况下进行。

6.0. 生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。

7.0. 联系信息

如需了解其他信息请访问 ACS 网站 http://www.acs.com.hk。

如需销售咨询请发送邮件至 info@acs.com.hk。