揭秘 ISA/IEC 62443 和安全元件

AN3983

简介

作者：Security Pattern 的 Matteo Giaconia 和 Microchip Technology Inc.的 Xavier Bignalet

本应用笔记指导用户如何有效使用 Microchip 安全元件作为构件来创建符合 ISA/IEC 62443 标准的产品。

本文档主要面向负责获取符合 ISA/IEC 62443 标准或认证的产品的工程师和管理人员。

根据 ISA/IEC 62443 标准，Microchip 的 ATECC608 和 TA100 元件可被视为助力工业和自动化控制系统（Industrial and Automation Control System，IACS）产品符合并通过该标准认证的技术支持，特别是在 ISA/IEC 62443 标准的 62443-4-2 部分“IACS 组件的技术安全要求”方面，本文档对此进行了详细说明。

目录

简介.....1

1. 关于 ISA/IEC 62443.....3
   1.1. ISA/IEC 62443 系列的结构和内容.....3
   1.2. ISA/IEC 62443 安全方法.....5

2. ISA/IEC 62443 对产品供应商的要求.....6
   2.1. 如何符合 ISA/IEC 62443-4-2 标准.....6
   2.2. 我们的产品可提供哪些帮助.....7

3. 结论.....11

4. 我们的资源和合作伙伴 Security Pattern 可提供哪些帮助.....12

5. ATECC608 和 Security Pattern 入门.....13

6. 版本历史.....14

Microchip 网站.....15

产品变更通知服务.....15

客户支持.....15

Microchip 器件代码保护功能.....15

法律声明.....15

商标.....16

质量管理体系.....17

全球销售及服务网点.....18

1. 关于 ISA/IEC 62443

ISA/IEC 62443 是一系列标准、技术规范和技术报告，总篇幅约 800 页。该系列标准起源于国际自动化学会（International Society of Automation，ISA）于 2007 年成立的 IACS 安全委员会（ISA99）的一项倡议，随后由国际电工委员会（International Electrotechnical Commission，IEC）发布。

ISA/IEC 62443 旨在应对使用操作技术（Operational Technology，OT）的工业自动化和控制系统的安全需求，这类系统近年来遭受的网络攻击日益增加。这些攻击会带来多种后果，包括危害国家安全的高价值资产（如能源分配、交通网络或医疗行业的瘫痪）、收入损失（如制造业），甚至直接威胁人类生命（如电击、化学品暴露和设备致命故障等）。

OT 系统的安全需求及其面临的威胁与传统信息技术（Information Technology，IT）系统存在较大差异，原因在于两类系统在以下特性方面存在许多不同之处：

- 性能要求（如吞吐率或响应时间）
- 可用性要求（对系统瘫痪的容忍度、对持续运行的需求和工厂认证等）
- 工作环境特性（如使用的操作系统类型、技术更新速度和系统可升级性）
- 风险管理目标（容错能力和预防 HSE 方面的负面后果）

鉴于这些特殊性，最初为 IT 环境而开发的现有安全标准（如属于 ISO 27000 系列的标准）无法高效或有效地满足 IACS 的安全要求。

1.1 ISA/IEC 62443 系列的结构和内容

ISA/IEC 62443 系列标准由 14 个工作成果（标准、技术规范和技术报告）组成，按逻辑分为四个层级：

- 第 1 层：通用
- 第 2 层：政策与程序
- 第 3 层：系统
- 第 4 层：组件

此外，62443 系列还引入了三种角色：

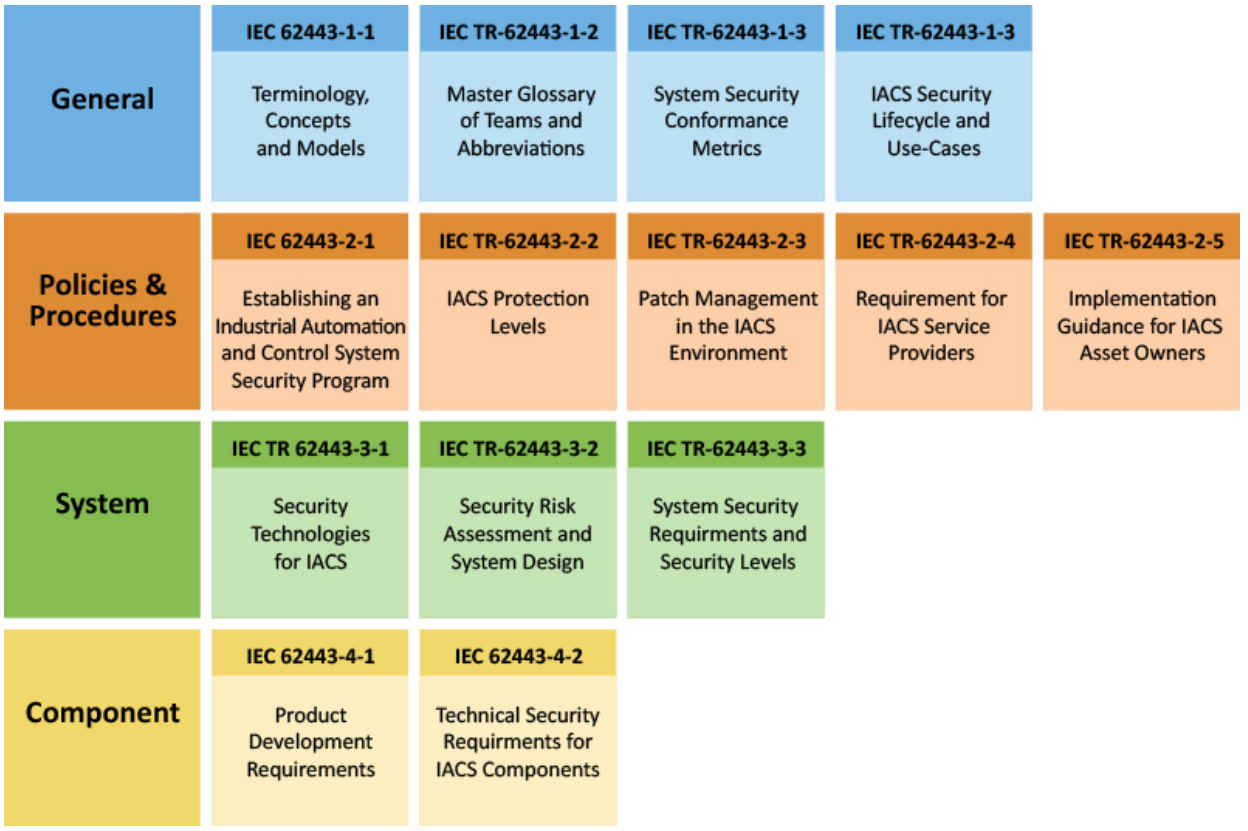
- **资产所有者**（Asset Owner，AO）：工业自动化控制系统的最终用户和操作方。
- **系统集成商**（System Integrator，SI）：负责整合和配置构成 IACS 的子系统和组件，并负责其在目标环境中的部署。
- **产品供应商**（Product Supplier，PS）：工业产品（嵌入式设备（如 PLC 或 RTU）、网络设备（如防火墙）、主机（如 PC）或软件应用程序）的制造商。

该标准的第 1 层（62443-1）名为“通用”，包含一些具有通用性质的工作成果，介绍了贯穿整个系列的基础概念、模型和术语。该层级包括以下 4 个工作成果：

- 62443-1-1：概念和模型
- 62443-1-2：术语和缩写总汇
- 62443-1-3：系统安全一致性指标
- 62443-1-4：IACS 安全生命周期和用例

第 1 层与该标准定义的所有角色同等相关。

图 1-1. ISA/IEC 62443 层级结构



第 2 层（62443-2）名为“政策与程序”，重点关注有效安全计划中的人员与流程方面，其范围涵盖工厂运营。该层级包括以下 5 个工作成果：

- 62443-2-1：IACS 资产所有者的安全计划要求
- 62443-2-2：IACS 安全管理系统的实现指南
- 62443-2-3：IACS 环境中的补丁管理
- 62443-2-4：IACS 解决方案供应商的要求
- 62443-2-5：IACS 资产所有者的实现指南

第 2 层与资产所有者最为相关。

第 3 层（62443-3）名为“系统”，重点关注系统安全的技术相关方面，描述了实现安全性所需的实现和集成的指导原则。该层级包括以下 3 个工作成果：

- 62443-3-1：IACS 的安全技术
- 62443-3-2：安全风险评估与系统设计
- 62443-3-3：系统安全要求与安全级别

第 4 层（62443-4）名为“组件”，重点关注产品和组件的特定安全相关要求，涵盖这些产品的技术内容以及贯穿整个生命周期的管理流程。该层级包括以下 2 个工作成果：

- 62443-4-1：安全产品开发生命周期要求
- 62443-4-2：IACS 组件的技术安全要求

第 4 层与产品供应商最为相关。需要注意的是，第 4 层的内容旨在从最终自动化项目的具体实现中抽象出组件及其功能（重点关注组件的能力）。

1.2 ISA/IEC 62443 安全方法

ISA/IEC 62443 系列阐述了一种面向工业领域的全面安全方法，其中重点强调了以下几个方面的重要性：

- 在定义和处理流程及技术特性时应用风险管理方法。
- 将安全的所有方面纳入一个集成框架中（包括物理安全、人员安全和网络安全）。

这种整体性方法的核心在于满足终端用户的需求（将资产所有者的视角置于中心位置）。

该方法的基石之一是“安全级别”（Security Level，SL）的概念。

ISA/IEC 62443 系列引入了针对安全级别（SL）的定性定义，用以描述系统针对攻击所能提供的保护级别。

图 1-2. ISA/IEC 62443 安全级别

根据 ISA/IEC 62443 系列所阐述的方法，资产所有者（AO）在定义要实现的 IACS 时需要开展风险评估活动。该风险评估活动的结果是为整个 IACS 确定一个“目标安全级别”（Target Security Level，SL-T）。

AO（在系统集成商的协助下）基于该 SL-T 采购子系统和组件，然后在具体的目标环境中实现 IACS。每个组件和子系统的特性以“能力安全级别”（Capability Security Level，SL-C）衡量。

之后，AO 会对系统实现情况进行评估，以验证“实际达到的安全级别”（Achieved Security Level，SL-A）是否满足先前设定的要求（即，检查 SL-A 是否大于或等于 SL-T）。如果未能达到目标安全级别，则需要在系统层面或通过流程和程序采取补偿性对策（包括技术性与程序性的对策）并反复优化，直至完全实现设定的目标安全级别。

使用在开发流程和技术内容方面符合 ISA/IEC 62443 第 4 层标准认证的组件，可以让资产所有者和系统集成商在开展 IACS 的集成、实现和风险管理活动更加高效、更加有效，同时对最终系统的安全性具有更高的信心。

2. ISA/IEC 62443 对产品供应商的要求

若要开发符合 ISA/IEC 62443 标准认证的产品，产品供应商必须关注该标准第 4 层的两个工作成果的内容：

- 产品供应商的流程必须符合标准第 4-1 部分（“安全产品开发生命周期要求”）中规定的要求，该部分定义了一组“实践”并基于“成熟度级别”对产品供应商流程的准备程度进行评级。
- 需要申请认证的具体产品必须符合标准第 4-2 部分（“IACS 组件的技术安全要求”）中规定的技术要求，该部分定义了一组“基础要求”并基于“安全级别”对产品供应商产品的安全能力进行评级。

本文档的内容主要聚焦于如何解决上述第二点问题，旨在通过重点介绍 Microchip 安全元件和 Security Pattern 如何助力您的产品满足合规性要求，简化标准第 4-2 部分的 200 页内容。

2.1 如何符合 ISA/IEC 62443-4-2 标准

在 ISA/IEC 62443 安全方法中，提供了安全级别的定性定义。

若要为产品分配特定的 SL-C（能力安全级别），需进行定量评估。该定量评估基于一系列的组件要求（Component Requirement，CR）及相关的要求增强（Requirement Enhancement，RE），这些要求被归类为基础要求的类别。

该标准定义了 7 类基础要求（FR1 至 FR7）：

FR1	标识和身份验证控制（Identification and Authentication Control，IAC）
FR2	使用控制（Use Control，UC）
FR3	系统完整性（System Integrity，SI）
FR4	数据机密性（Data Confidentiality，DC）
FR5	受限数据流（Restricted Data Flow，RDF）
FR6	及时响应事件（Timely Response to Event，TRE）
FR7	资源可用性（Resource Availability，RA）

每类基础要求都只是单个集合的逻辑分组，每个集合由一个组件要求和若干要求增强组成。

该标准提供了表格来说明达到每个 SL 所需的 CR/RE。

下表提供了一个基于第一类基础要求（标识和身份验证控制）中第 7 项要求（基于密码的身份验证强度）的定量评估示例。

该 CR 有两个相关联的 RE。表中的勾号表示达到给定的 SL 所需的 CR 或 RE。

	SL1	SL2	SL3	SL4
CR1.7——基于密码的身份验证强度	✔	✔	✔	✔
RE1.7.1——人类用户的密码生成和有效期限制			✔	✔
RE1.7.2——所有用户的密码有效期限制				✔

评估示例：

- 如果组件不满足基础 CR，其 SL 为 0。
- 如果组件仅满足基础 CR，其 SL 为 2。
- 如果组件满足基础 CR 和第一个 RE（1），其 SL 为 3。
- 如果组件满足基础 CR、RE（1）和 RE（2），其 SL 为 4。

必须针对每个 FR 类别下的所有 CR/RE 组重复该评估。被评估产品的总 SL 是所有这些评估中获得的最低 SL。总之，若要达到目标安全级别（SL），必须满足所有相关要求。

2.2 我们的产品可提供哪些帮助

ATECC608 是一种助力 IACS 产品供应商满足 ISA/IEC 62443-4-2 规定的组件要求的技术支持。下表列出了 ATECC608 的加密功能和安全保护，稍后将与 ISA/IEC 62443 规范进行对照映射。

表命名	功能
SHA256	SHA-256 和 HMAC 哈希算法，包括片外现场保护/恢复。
安全密钥存储	最多可对 16 个密钥、证书或数据进行 JIL 高评级安全存储。
ECDSA	ECDSA：FIPS186-3 椭圆曲线数字签名（签名/验证）。
ECDH	ECDH：FIPS SP800-56A 椭圆曲线 Diffie-Hellman。
ECCP256	NIST 标准 P256 椭圆曲线支持。
PRF/HDKF	适用于 TLS 1.2 和 1.3 的交钥匙伪随机函数（Pseudo Random Function，PRF）/HKDF 计算。
临时密钥	在 SRAM 中生成临时密钥和执行密钥协议。
报文加密	短小报文加密，密钥完全受保护。
AEC128/GCM	AES-128：加密/解密，GCM 的 Galois 域乘法。
RNG	内部高质量 NIST SP 800-90A/B/C 随机数发生器（Random Number Generator，RNG）。
密钥轮换	可有效进行私钥轮换和公钥认证，并且已在 ATECC608 TrustFLEX 中进行预配置，便于使用。 另外也可有效进行公钥轮换，并且已在 ATECC608 TrustFLEX 中进行预配置，便于使用。这将成为后期密钥配置的重要功能。
防篡改	物理防篡改和边信道攻击保护。
安全密钥配置	Microchip 内部安全密钥配置利用硬件安全模块（Hardware Secure Module，HSM）网络，支持后期阶段配置。
安全引导	ECC-P256 ECDSA 验证，用于签名验证。
密钥禁用	安全元件可根据开发人员定义的逻辑条件禁用密钥。
安全密钥配置	Microchip 内部安全密钥配置服务允许客户利用我们配备硬件安全模块（HSM）的工厂，并确保加密密钥不会暴露给第三方制造商。支持后期阶段配置（联系 Microchip）。

ISA/IEC 62443 要求进行“安全密钥存储”或保护加密密钥。在安全领域，这并不是一个模糊的术语，而是芯片设计中明确的功能。安全密钥存储或密钥保护的实现需要具备一个物理安全边界，然后在这个安全边界内进行加密操作并存储加密密钥。如果密钥和算法不在同一个安全边界内，密钥将可能在交易过程中的某个环节被暴露。这正是 ATECC608 等安全元件在产品认证过程中发挥作用的关键所在。安全元件是经过联合解释库（Joint Interpretation Library，JIL）测试的安全密钥存储器件，具体根据通用标准实践来评估其保护密钥的稳健性。

在强调安全密钥存储的价值之后，紧接着需要解决的下一个问题是如何通过安全的制造流程将密钥加载到这样的设备位置。Microchip 的工厂配备有一套托管的硬件安全模块（HSM）网络，可为客户提供安全密钥配置服务。通过将这项服务加入到安全元件中，客户可以遵循受控的密钥交换流程，将安全存储在设备中的凭证绑定到他们自己的可信链或其客户的可信链，而不会将各种加密密钥暴露给任何第三方（如合同制造商）。此外，Microchip 的安全元件还支持后期阶段配置，允许最终客户在配置流程的后期激活加密密钥。

下表引用了 ISA/IEC 62443-4-2 中定义的组件要求，并指出了 ATECC608 如何作为技术支持助力客户的产品满足每一项要求。下表中列出的每个 CR 和加密功能均指定了安全级别（SL）。

ISA/IEC 62443 标准定义了以下四种类型组件的要求：

- 嵌入式设备（EDR）
- 软件应用程序（SAR）
- 主机设备（HDR）
- 网络设备（NDR）

适用于所有类型组件的组件要求标记为“CR”，而适用于特定组件类型的组件要求根据其适用的组件类型分别标记为 EDR、SAR、HDR 或 NDR。

在阅读下表时，切记 RE 与同属一个基础要求段落的 CR 相关联。例如，“CR 1.1 RE（1）惟一标识和身份验证”是“CR1.1 人类用户标识和身份验证”的一部分。

功能要求		关联要求																	
组件要求（CR）	组件要求增强（RE）	SAR EDR HDR HDR 要求	SAR EDR HDR HDR 增强	标题	NIST SP 800-90A/B/C（RNG）	ECC-P256	ECDSA P256 FIPS186-3（签名/验证）	ECDH FIPS SP800-56A	SRAM 中的临时密钥和密钥协议	适用于 TLS 1.2 和 1.3 的 PRF/HKDF	SHA-256 和 HMAC，包括保存/恢复	AES-128，GCM，加密/解密	报文加密，密钥受保护	JIL 高评级安全密钥存储	防篡改	密钥轮换	密钥禁用	安全引导	安全密钥配置	功能和用途
CR.1.1				人类用户标识和身份验证							1									哈希功能与安全密钥存储功能相结合，可实现对密码文件完整性检查的稳健管理。
	CR 1.1 RE（1）			惟一标识和身份验证							2									哈希功能与安全密钥存储功能相结合，可实现对密码文件完整性检查的稳健管理。
CR 1.2				软件进程和设备标识与身份验证	2	2	2	2						2	2				2	JIL 高评级密钥和证书安全存储以及数字签名验证和生成功能，可实现安全标识与身份验证。
	CR 1.2 RE（1）			惟一标识和身份验证	3	3	3	3						3	3				3	JIL 高评级密钥和证书安全存储以及数字签名验证和生成功能，可实现安全标识与身份验证。
CR 1.5				身份验证器管理					1	1		1	1	1	1	1	1		1	加密密钥生成和安全存储功能，可通过硬件实现对密钥的稳健初始化和生命周期管理。
	CR 1.5 RE（1）			身份验证器的硬件安全					3	3		3	3	3	3	3	3		3	加密密钥生成和安全存储功能，可通过硬件实现对密钥的稳健初始化和生命周期管理。
CR 2.4		SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		移动代码		1	1	1			1	1		1	1	1	1		1	哈希功能和安全存储功能，可实现对代码和数据完整性检查的稳健管理。
			SAR 2.4 RE（1） EDR 2.4 RE（1） HDR 2.4 RE（1） NDR2.4 RE（1）	移动代码真实性检查	2	2	2	2						2	2	2	2		2	密钥和证书安全存储以及数字签名验证和生成功能，可实现对代码和数据的身份验证。
CR2.12				不可否认性	1	1	1	1			1									哈希功能和安全存储功能，可实现对审计信息完整性检查的稳健管理。密钥和证书安全存储以及数字签名验证和生成功能，可实现对审计信息的身份验证。
CR2.12	CR2.12 RE（1）			所有用户的不可否认性	4	4	4	4			4									哈希功能和安全存储功能，可实现对审计信息完整性检查的稳健管理。密钥和证书安全存储以及数字签名验证和生成功能，可实现对审计信息的身份验证。
CR3.1				通信完整性							1									密钥和证书安全存储以及数字签名验证和生成功能，可确保传输信息的完整性和真实性。支持标准对称密钥和非对称密钥算法以及哈希函数的加密引擎，可实现对常用通信密码套件的支持。
CR3.1	CR3.1 RE（1）			通信身份验证	2	2	2	2		2		2	2	2	2	2	2		2	网络密钥管理支持，可实现对 TLS 等标准加密通信协议的支持。
CR3.4				软件和信息完整性							1			1	1	1	1		1	哈希功能和安全存储功能，可实现对代码和数据完整性检查的稳健管理。
CR3.4	CR3.4 RE（1）			软件和信息真实性		2	2	2						2	2	2	2		2	密钥和证书安全存储以及数字签名验证和生成功能，可实现对代码和数据的身份验证。
CR3.8				会话完整性	2				2	2		2	2							网络密钥管理支持和内部 RNG，可生成稳健的惟一会话标识符。
CR3.10			EDRE3.10.1、HD RE3.10.1 和 ND RE3.10.1	更新真实性和完整性		2	2	2			2	2	2	2	2	2	2	2	2	密钥和证书安全存储、数字签名验证和生成功能、对非对称和对称算法以及哈希函数的硬件支持，可实现对软件更新的身份验证和完整性验证。
CR3.12		EDR3.12 HDR3.12 NDR3.12		配置产品供应商可信根										2	2	2	2		2	安全存储功能，可用于保护产品供应商的可信根。
CR3.13		EDR3.13 HDR3.13 NDR3.13		配置资产所有者可信根										2	2	2	2		2	安全存储功能，可用于保护资产所有者的可信根。
CR3.14		EDR3.14 HDR3.14 NDR3.14		引导过程完整性		1	1											1		通过内部签名验证机制和摘要/签名安全存储提供安全引导支持。

索引值： 1 = SL1 2 = SL2 3 = SL3 4 = SL4

我们的产品可提供哪些帮助（续）

功能要求		关联要求																	
组件要求（CR）	组件要求增强（RE）	SAR EDR HDR HDR 要求	SAR EDR HDR HDR 增强	标题	NIST SP 800-90A/B/C（RNG）	ECC-P256	ECDSA P256 FIPS186-3（签名/验证）	ECDH FIPS SP800-56A	SRAM 中的临时密钥和密钥协议	适用于 TLS 1.2 和 1.3 的 PRF/HKDF	SHA-256 和 HMAC，包括保存/恢复	AES-128：GCM，加密/解密	报文加密，密钥受保护	JIL 高评级安全密钥存储	防篡改	密钥轮换	密钥兼用	安全引导	安全密钥配置	功能和用途
CR3.14			EDRE3.14.1、HDRE3.14.1 和 NDRE3.14.1	引导过程真实性		2	2											2		通过内部签名验证机制和摘要/签名安全存储提供安全引导支持。
CR4.1				信息机密性		1	1	1			1	1		1	1	1	1		1	最多可直接对 16 个密钥、证书或数据提供安全加密存储。此外，对对称算法和密钥存储功能的硬件支持可实现对外部存储的数据进行加密。
CR4.3				使用加密		1	1	1			1	1								最多可直接对 16 个密钥、证书或数据提供安全加密存储。此外，对对称算法和密钥存储功能的硬件支持可实现对外部存储的数据进行加密。
CR4.3	CR7.3 RE（1）			备份完整性验证							2			2	2	2	2		2	哈希功能和安全存储功能，可实现对备份信息完整性检查的稳健管理。
CR7.4				控制系统恢复和重构							1			1	1	1	1		1	哈希功能和安全存储功能，可实现对备份信息完整性检查的稳健管理。
索引值： 1 = SL1 2 = SL2 3 = SL3 4 = SL4																			

3. 结论

1. **加密算法的要求：**单纯依赖加密加速器并不能完全解决安全性问题，这正是 ISA/IEC 62443 标准所阐述的核心理念。ATECC608 元件的突出优势在于其超低功耗的休眠模式（仅 30 nA），而设备在其生命周期中有很大一部分时间处于该模式。如果再结合其基于硬件的加密加速器，ATECC608 将能够显著缩短加密操作的执行时间。这一特性使其成为一种出色的解决方案，可通过卸载复杂的加密运算来优化设备的功耗预算。
2. **JIL 高评级安全密钥存储：**Microchip 的安全元件在助力满足 ISA/IEC 62443 合规性方面表现卓越。加密算法只是一种数学运算，若缺乏对相关密钥的妥善保护，安全性将荡然无存。实际上，每次调用加密算法时，安全密钥存储都是不可或缺的。ATECC608 在安全密钥存储方面通过了基于通用标准实践的测试。评级基于 JIL 等级。ATECC608 达到了 JIL 高评级（安全密钥存储方面的最高 JIL 评级），在保证密钥保护的同时，也实现了极高的性价比，为用户提供了强有力的信心保障。
3. **安全密钥配置：**类似地，安全密钥配置与安全密钥存储之间可以进行同样的类比。通过遵循安全的制造流程来处理加密密钥，对于尽可能隔离密钥与任何外部变量至关重要。ISA/IEC62443-4-1 标准同样也强调了这一优势。Microchip 提供了内部安全密钥配置服务，可以代表客户加载加密密钥。Microchip 可信平台将是这一流程的起点。
4. **CryptoAuthLib 库：**确保可以灵活选择单片机或微处理器的基本要素（可考虑使用 PKCS11）。CryptoAuthLib 库提供了一个硬件抽象层（Hardware Abstraction Layer，HAL），其中包含 I^2C 或 SWI 驱动程序，用于使安全元件与单片机或微处理器保持无关。

4. 我们的资源和合作伙伴 Security Pattern 可提供哪些帮助

ISA/IEC 62443 标准强调需要以整体的方式来解决安全问题：安全性不能仅仅依靠技术实现。尽管技术是安全性的重要组成部分，但同样需要结合人员和流程的协同管理。

基于这一整体方法的自然延伸，产品供应商的流程需要符合 ISA/IEC 62443-4-1 标准（“安全产品开发生命周期要求”）。这一标准是实现 CSA [1]和 EDSA [2]产品认证的前提条件（根据该标准的 4-2 部分）。

遵循 ISA/IEC 62443-4-1 标准意味着采用一系列稳健的流程，以确保产品供应商对其产品的管理在安全性方面与技术内容相契合，符合客户的期望，并在整个产品生命周期内保持可持续性。这些要求与常见的安全建议和最佳实践高度一致。

以下是该标准对产品供应商提出的一些关键要求：

- 应用安全设计原则，包括纵深防御
- 正确定义并跟踪安全要求，从产品概念阶段到设计、实现、测试、现场问题管理和产品退役的全流程。
- 将风险管理实践应用于安全组件的设计（威胁建模活动是这种以风险为中心的方法的一个环节）
- 根据每位员工在产品定义、开发和管理中的角色和职责提供相应的安全培训。

作为经认证的 Microchip 安全合作伙伴，Security Pattern 可以提供以下帮助：

- 通过专项咨询或入门培训，帮助工业零部件制造商了解其产品的安全要求，并明确这些要求与 ISA/IEC 62443 标准的关系。
- 协助定义和完善与安全相关的产品要求（包括平台的选择/定义）。
- 指导产品供应商正确应用 Microchip 组件及其丰富的安全功能。
- 在产品开发阶段帮助产品供应商定义系统、简化生产流程（考虑供应链和第三方供应商的安全性），以及开发软件。
- 提供技术支持和专业知识，以搭建公钥基础架构、管理数字证书和实现安全引导等。
- 协助产品供应商根据 ISA/IEC 62443-4-1 标准的要求实施并执行内部流程，同时提供符合 ISA/IEC 62443 标准要求的文档结构。
- 根据 ISA/IEC 62443-4-2 组件要求执行产品差距分析。
- 在与选定的 ISA/IEC 62443 认证机构进行技术讨论时提供支持。
- 提供满足产品供应商员工需求的定制化培训课程，并根据标准的实践 1 要求持续提升和评估安全专业知识。

注：

1. www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab1
2. www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab2

5. ATECC608 和 Security Pattern 入门

如需获取咨询和设计服务，请访问我们认证的安全设计合作伙伴 Security Pattern 的网站。

如需了解以下更多信息，请访问 Microchip 网站：

- CryptoAuthentication™可信平台的概述以及如何开始利用 Microchip 安全密钥配置服务
- CryptoAuthLib 库的 Github 资源库
- 有关适用于 TLS 或 LoRaWan 网络的预配置 Trust&GO ISA/IEC 62443 安全元件的详细信息
- 有关预配置 TrustFLEX ISA/IEC 62443 安全元件的详细信息
- 有关完全可定制的 TrustCUSTOM ISA/IEC 62443 安全元件的详细信息

6. 版本历史

版本	日期	章节	说明
A	2021 年 4 月	文档	初始版本
B	2021 年 12 月	ISA/IEC 62443 系列的结构和内容	更正了图 1-1

Microchip 网站

Microchip 网站（www.microchip.com）为客户提供在线支持。客户可通过该网站方便地获取文件和信息。我们的网站提供以下内容：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题解答（FAQ）、技术支持请求、在线讨论组以及 Microchip 设计伙伴计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

产品变更通知服务

Microchip 的产品变更通知服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请访问 www.microchip.com/pcn，然后按照注册说明进行操作。

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（ESE）
- 技术支持

客户应联系其代理商、代表或 ESE 寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过 www.microchip.com/support 获得网上技术支持。

Microchip 器件代码保护功能

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在正常使用且符合工作规范的情况下，Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。

法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物及其提供的信息仅适用于 Microchip 产品，包括设计、测试以及将 Microchip 产品集成到您的应用中。以其他任何方式使用这些信息都将被视为违反条款。本出版物中的器件应用信息仅为您提供便利，

将来可能会发生更新。如需额外的支持，请联系当地的 Microchip 销售办事处，或访问 www.microchip.com/en-us/support/design-help/client-support-services。

Microchip “按原样”提供这些信息。Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对非侵权性、适销性和特定用途的适用性的暗示担保，或针对其使用情况、质量或性能的担保。

在任何情况下，对于因这些信息或使用这些信息而产生的任何间接的、特殊的、惩罚性的、偶然的或间接的损失、损害或任何类型的开销，Microchip 概不承担任何责任，即使 Microchip 已被告知可能发生损害或损害可以预见。在法律允许的最大范围内，对于因这些信息或使用这些信息而产生的所有索赔，Microchip 在任何情况下所承担的全部责任均不超出您为获得这些信息向 Microchip 直接支付的金额（如有）。如果将 Microchip 器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切损害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任。除非另外声明，在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、Microchip 徽标、Adaptec、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、TimeSource、tinyAVR、UNI/O、Vectron 及 XMEGA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的注册商标。

AgileSwitch、ClockWorks、The Embedded Control Solutions Company、EtherSynch、Flashtec、Hyper Speed Control、HyperLight Load、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、TimeCesium、TimeHub、TimePictra、TimeProvider 和 ZL 均为 Microchip Technology Incorporated 在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、Augmented Switching、BlueSky、BodyCom、Clockstudio、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、EyeOpen、GridTime、IdealBridge、IGaT、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、IntelliMOS、Inter-Chip Connectivity、JitterBlocker、Knob-on-Display、MarginLink、maxCrypto、maxView、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、mSiC、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、Power MOS IV、Power MOS 7、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、RTAX、RTG4、SAM-ICE、Serial Quad I/O、simpleMAP、SimpliPHY、SmartBuffer、SmartHLS、SMART-I.S.、storClad、SQI、SuperSwitcher、SuperSwitcher II、Switchtec、SynchroPHY、Total Endurance、Trusted Time、TSHARC、Turing、USBCheck、VariSense、VectorBlox、VeriPHY、ViewSpan、WiperLock、XpressConnect 和 ZENA 均为 Microchip Technology Incorporated 在美国和其他国家或地区的商标。

SQTP 为 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 均为 Microchip Technology Inc.在除美国外的国家或地区的注册商标。

GestIC 为 Microchip Technology Inc.的子公司 Microchip Technology Germany II GmbH & Co. KG 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

ISBN： 979-8-3371-0628-1

质量管理体系

有关 Microchip 质量管理体系的信息，请访问 www.microchip.com/quality。

全球销售及服务网点

美洲

公司总部
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
电话：480-792-7200
传真：480-792-7277
技术支持：
www.microchip.com/support
网址：
www.microchip.com

亚特兰大
德卢斯，佐治亚州
电话：678-957-9614
传真：678-957-1455

奥斯汀，德克萨斯州
电话：512-257-3370

波士顿
韦斯特伯鲁，马萨诸塞州
电话：774-760-0087
传真：774-760-0088

芝加哥
艾塔斯卡，伊利诺伊州
电话：630-285-0071
传真：630-285-0075

达拉斯
阿迪森，德克萨斯州
电话：972-818-7423
传真：972-818-2924

底特律
诺维，密歇根州
电话：248-848-4000

休斯顿，德克萨斯州
电话：281-894-5983

印第安纳波利斯
诺布尔斯维尔，印第安纳州
电话：317-773-8323
传真：317-773-5453
电话：317-536-2380

洛杉矶
米慎维荷，加利福尼亚州
电话：949-462-9523
传真：949-462-9608
电话：951-273-7800

罗利，北卡罗来纳州
电话：919-844-7510

纽约，纽约州
电话：631-435-6000

圣何塞，加利福尼亚州
电话：408-735-9110
电话：408-436-4270

加拿大 - 多伦多
电话：905-695-1980
传真：905-695-2078

亚太地区

澳大利亚 - 悉尼
电话：61-2-9868-6733

中国 - 北京
电话：86-10-8569-7000

中国 - 成都
电话：86-28-8665-5511

中国 - 重庆
电话：86-23-8980-9588

中国 - 东莞
电话：86-769-8702-9880

中国 - 广州
电话：86-20-8755-8029

中国 - 杭州
电话：86-571-8792-8115

中国 - 香港特别行政区
电话：852-2943-5100

中国 - 南京
电话：86-25-8473-2460

中国 - 青岛
电话：86-532-8502-7355

中国 - 上海
电话：86-21-3326-8000

中国 - 沈阳
电话：86-24-2334-2829

中国 - 深圳
电话：86-755-8864-2200

中国 - 苏州
电话：86-186-6233-1526

中国 - 武汉
电话：86-27-5980-5300

中国 - 西安
电话：86-29-8833-7252

中国 - 厦门
电话：86-592-2388138

中国 - 珠海
电话：86-756-3210040

亚太地区

印度 - 班加罗尔
电话：91-80-3090-4444

印度 - 新德里
电话：91-11-4160-8631

印度 - 浦那
电话：91-20-4121-0141

日本 - 大阪
电话：81-6-6152-7160

日本 - 东京
电话：81-3-6880-3770

韩国 - 大邱
电话：82-53-744-4301

韩国 - 首尔
电话：82-2-554-7200

马来西亚 - 吉隆坡
电话：60-3-7651-7906

马来西亚 - 槟榔屿
电话：60-4-227-8870

菲律宾 - 马尼拉
电话：63-2-634-9065

新加坡
电话：65-6334-8870

台湾地区 - 新竹
电话：886-3-577-8366

台湾地区 - 高雄
电话：886-7-213-7830

台湾地区 - 台北
电话：886-2-2508-8600

泰国 - 曼谷
电话：66-2-694-1351

越南 - 胡志明市
电话：84-28-5448-2100

欧洲

奥地利 - 韦尔斯
电话：43-7242-2244-39
传真：43-7242-2244-393

丹麦 - 哥本哈根
电话：45-4485-5910
传真：45-4485-2829

芬兰 - 埃斯波
电话：358-9-4520-820

法国 - 巴黎
电话：33-1-69-53-63-20
传真：33-1-69-30-90-79

德国 - 加兴
电话：49-8931-9700

德国 - 哈恩
电话：49-2129-3766400

德国 - 海尔布隆
电话：49-7131-72400

德国 - 卡尔斯鲁厄
电话：49-721-625370

德国 - 慕尼黑
电话：49-89-627-144-0
传真：49-89-627-144-44

德国 - 罗森海姆
电话：49-8031-354-560

以色列 - 霍德夏沙隆
电话：972-9-775-5100

意大利 - 米兰
电话：39-0331-742611
传真：39-0331-466781

意大利 - 帕多瓦
电话：39-049-7625286

荷兰 - 德卢内市
电话：31-416-690399
传真：31-416-690340

挪威 - 特隆赫姆
电话：47-72884388

波兰 - 华沙
电话：48-22-3325737

罗马尼亚 - 布加勒斯特
电话：40-21-407-87-50

西班牙 - 马德里
电话：34-91-708-08-90
传真：34-91-708-08-91

瑞典 - 哥德堡
电话：46-31-704-60-40

瑞典 - 斯德哥尔摩
电话：46-8-5090-4654

英国 - 沃金厄姆
电话：44-118-921-5800
传真：44-118-921-5820