IoT Security Foundation – 最佳做法用户 – IoT Security Foundation – IoT Security Foundation

IoT Security Foundation

物联网安全合规框架

2018 年 12 月

通告、免责声明、使用条款以及版权、商标和许可

通知

物联网安全基金会（简称“IoTSF”）发布的文件将会定期进行审查，并且可能随时更新或更改。IoTSF 出版物（包括本文件）的最新状态可在以下公共网站上查看：https://iotsecurityfoundation.org。

使用条款

IoTSF 在提供本文件方面所起的作用是推广当代物联网安全最佳做法，以造福社会。提供本文件时，IoTSF 并未基于使用第三方提供的内容，验证、认可或确认任何第三方，也未验证用户做出的任何声明。

提供本文件并不构成或解释为 IoTSF 向本文件的任何收件人或用户或任何第三方提供服务。

免责声明

（与信息安全的任何方面一样，）物联网安全并不是绝对的，并且永远无法得到保证。新的漏洞不断被发现，这意味着需要定期监测、维持和审查与特定用例和操作环境有关的政策和实践。

IoTSF 是一个非盈利组织，不时发布物联网安全最佳做法指引资料。IoTSF 发布的资料包括安全专业人员、研究员、行业经验丰富的人员以及 IoTSF 会员和合作伙伴的其他相关来源提供的资料。IoTSF 制定了一个多阶段流程，旨在发布之前，通过质量保证同行评审开发当代最佳做法。虽然 IoTSF 善意提供信息，并竭尽全力地提供正确、最新和高质量的指引，但 IoTSF 仅按“原样”提供所有资料（包括本文件），不作任何明示或暗示性担保、承诺或保证。

本文件内容仅供参考，并不意味着全面。IoTSF 或其任何成员（或其各自的高级职员、员工或代理人）并未或不会作出与本文件或本文件的任何使用有关的任何陈述、担保、保证或承诺（无论明示或默示），并未或不会接受对本文件收件人或用户或任何第三方负有与本文件或本文件的任何使用有关的任何责任或义务，包括与本文件或其内容的充分性、准确性、完整性或及时性有关。明确拒绝承认任何此类责任或义务。

本文件的任何内容均不得排除以下任何义务：(i) 由疏忽过失造成的死亡或人身伤害；或 (ii) 欺诈或虚假陈述。

接受或使用本文件即表示，收件人或用户同意受本免责声明的约束。本免责声明受英国法律管辖。

版权、商标和许可

致谢

衷心感谢 IoTSF 成员对本版本文件作出的重大贡献：Abhay Soorya, Gemserv Ltd
Alex Margulis, Intel Corp
Arun Sambordaran, Gemserv Ltd
Chris Hills, Phaedrus Systems Ltd
Chris Shire, Infineon Technologies Ltd
Graham Markall, Embecosm Ltd
Ian Phillips, Roke Manor Research Ltd
Isaac Dangana, Red Alert Labs Ltd
Jan Krueger, Intel Corp
Jeremy Bennett, Embecosm Ltd
John Moor, IoT Security Foundation
Lokesh Johri, Tantive 4
Mark Beaumont, Roke Manor Research Ltd
Nick Hayes, Thinkstream Ltd
Pamela Gupta, Outsecure Inc
Peter Burgers, Display Link Ltd
Richard Marshall, Xitex Ltd
Richard Storer, MathEmbedded Ltd
Robert Dobson, Device Authority Ltd
Roger Shepherd, Chipless Ltd
Sean Gulliford, Gemserv Ltd
Trevor Hall, DisplayLink Ltd

同行评审人员
Brian Russell, Cloud Security Alliance
Colin Blanchard, BT Plc
Eric Vetillard, NXP Semiconductors NV
James Willison, Unified Security Ltd
Jeff Day, BT Plc
Marek Hubbell
以及其他相关人员，不再赘述！

目录

1 目的和用途

1.1 简介

物联网安全基金会（IoTSF）的成立旨在解决联系日益紧密的世界中的物联网安全挑战。其特殊使命是***“帮助确保物联网安全，以促进物联网的实际应用，并实现物联网效益最大化。为此，IoTSF 将努力促进规定、制造和使用物联网产品和系统之人了解有关适当安全的知识和最佳做法”。***

简而言之，对于供应商、运营商和最终用户而言：**“建立安全的物联网系统，购买安全的物联网产品，确保物联网安全”。**

本物联网安全合规框架（简称“框架”）将引导用户全面了解结构化提问和证据收集流程。这可确保实施适当的安全机制和实践。

本框架旨在通过指引所有公司全面了解综合要求检查清单和证据收集流程，帮助其做出高质量的明智的安全选择。在此过程中收集的证据可用于向客户和其他利益相关者申明符合最佳做法。

提供良好的安全性能需要预先就设计和用途做出决策 – 通常称为***安全设计***。在大多数情况下，相比于在产品创建之后设法增强产品的安全性，或围绕产品设置安全措施，在设计阶段设法解决产品的安全性问题的成本更低，而且需要付出的努力更少。除了架构、设计特点、实施、测试、配置和维护等技术问题之外，需要做出决策，以设法解决用例、业务模式、责任水平和风险管理等问题。

在本文件和 IoTSF 发布的其他文件中，“最佳做法”或“最佳做法安全工程”出现的频率非常高。这些最佳做法源自于 IoTSF 会员的综合专业知识，以及其他相关组织的出版物和指南，并且 IoTSF 会员在自己的公司内使用和测试这些最佳做法。尽可能参考现有标准和最佳做法资料，以避免不必要的重复。本文件的最后章节载有外部参考资料和相关机构列表。

1.2 目标受众

本框架可供组织内部使用，以进行自我评估或自我验证，或由第三方审计机构进行评估或验证。也可根据采购机制部分采用本框架，以帮助规定供应商合同的安全要求。本框架的目标受众为以下利益相关者：

- 组织内提供物联网产品、技术及/或服务的**经理**。本框架综述了采用最佳做法所需的管理过程，使高级管理人员和项目经理能够提出正确问题，并评估答案，因此对于他们非常有用

- **开发员和工程师、物流和制造员工**，他们可以在日常工作和项目审查中使用本框架所载的详细要求，以验证不同职能部门（如硬件和软件开发、物流等）对最佳做法的使用。在填写合规检查清单[参考文献 19]时，将编制证明文件，以证明在开发周期时限和第三方（如审计机构或客户）方面的合规性

- **供应链经理**，该结构可用于指导安全实践审计。因此，它可以在生产组织（如上所述）内使用；并由生产商的客户进行检查

- 参与审计或认证过程的**受信任的第三方**

1.3 范围

本文件的范围包括但不限于：

- 业务流程
- 物联网中的“物”，即联网产品和/或设备
- 聚合点，如构成网络连接的一部分的网关和集线器
- 网络，包括有限和无线连接、云和服务器元素

1.3.1 物联网安全的关键问题

关键合规要求概述如下：

关键要求	需要采取的行动	框架参考
管理治理	必须指定高级管理人员负责产品安全和客户信息隐私。	2.4.3、2.4.11
专为安全而设计	硬件和软件的设计必须考虑到安全威胁。	2.4.4、2.4.5、2.4.6、2.4.7
适用的加密	这些功能应源自最佳做法行业标准。	2.4.8、2.4.9
安全网络框架和应用	采取预防措施，以确保应用程序、Web 界面和服务器软件安全	2.4.12、2.4.13
安全生产流程和供应链	确保产品的安全性在制造过程或最终客户交付和安装过程中不会受到损害。	2.4.10、2.4.12、2.4.13
为客户提供安全保障	产品“开箱即用”，且在日常使用过程中安全可靠。配置和控件应指导设备管理人员维护设备安全性，并提供软件更新、漏洞披露策略和生命周期管理。	2.4.14

1.3.2 信任供应链

所有最终用途产品均是使用组件集（通常采购自各种供应商）生产的。这些部件可以是电子或机械组件、软件模块或软件包，包括开源软件。其中许多部件将从第三方供应商采购。重要的是，所有部件和供应链物流都必须接受安全审查/审计。

然后，最终物联网产品可以连同其安全评估证据和组件部件文件（共同构成完整的可审计证据包）一起提供。这有助于用户评估产品符合整体***“信任供应链”***的程度[参考文献 36]。

1.4 IoTSF 框架支持资源简介

IoTSF 提供各种资源，以促进最佳安全做法：

- **本框架**文件[参考文献 19]载有结构化安全要求列表和证据收集流程，以指引组织提供保证和进行证据收集。
- **合规检查清单**[参考文献 19]是本框架随附的电子表格，用于帮助收集和记录证据。
- 物联网安全基金会还提供了其他**最佳做法指南**，以帮助了解最重要的主题[参考文献 44]。
- 此外，还可在 IoTSF 网站上找到更多资源，包括指南、文件、文章和博客。

所有 IoTSF 出版物均会定期进行维护和审查，以保持最新状态 – 鉴于网络安全的动态性质，这是一个至关重要的属性。

这是第三次公开发行版本，并且根据出版物维护和改进流程，欢迎用户提供意见反馈，以应对新的安全威胁。您可以通过发送主题为**“合规框架意见反馈”**邮件至 contact@iotsecurityfoundation.org，发送意见反馈和建议，以改进本框架。

未来版本可能包括特定应用程序或产品类别的扩展。

1.4.1 相较于 V1.1 版合规框架的变化

本框架 1.1 版仅述及消费类产品。本框架 2.0 版所述的内容包括应用范围更广泛的产品 - 从消费者到企业，包括 B2B 市场。

本版本的新增内容：

- 变更为基于风险的方法 – 提供更灵活的适用性
- 删除应用特定限制
- 增加业务和技术相关关键字，以便根据不同利益相关者的利益过滤相关要求 – 请参阅“关键字”章节 0
- 类别和适用性级别合并
- 附加说明文字
- 本框架会随附电子表格，以支持证据收集。

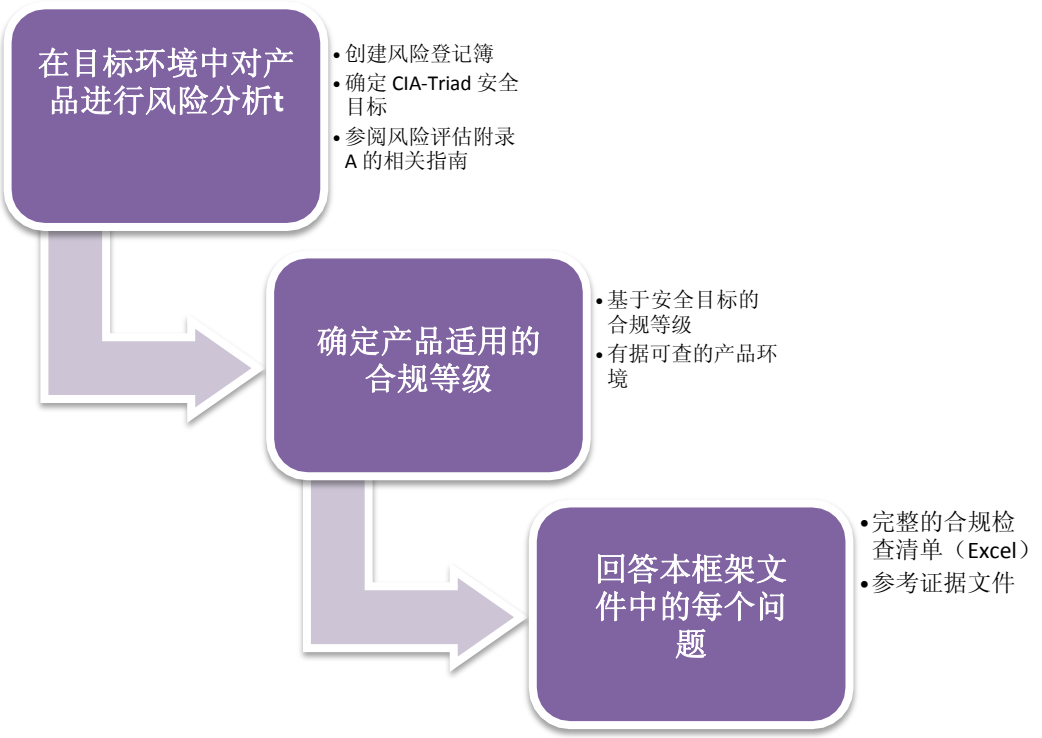
第 2.4 节详述的要求章节和编号已尽可能根据本框架的先前版本进行维护，以保持一致性。

2 物联网安全合规框架

2.1 流程

本框架针对组织和产品的各个方面提出了全面的安全要求。对每项要求的回复都需要输入合规检查清单[参考文献 19]，并附上附表或证据。对于被视为“不适用”的要求，必须说明原因。还应列出任何可降低任何安全风险的替代对策。

合规流程可分解为以下步骤：



2.1.1 风险评估

就安全而言，***背景决定一切***- 每个应用程序的用例和操作环境都有所不同。本框架用户有责任确定其所述使用环境中的风险偏好，从而确定所采用的安全措施的特定合规等级（第 2.2 节）。

为实现上述目标，**全面的风险评估是使用本框架的先决条件**。风险评估过程将有助于确定产品/服务的合规等级。第 2.2 节详细阐述了合规等级，以及其与安全专业人员常用的保密性、完整性和可用性（也称为 CIA Triad [参考文献 1]模型）的关系。作为一般规则，应采用尽可能高的合规等级，不仅考虑产品的直接背景，而且考虑产品/服务最终为其所用的系统的潜在危险。

风险评估过程的基本概要载于附录 A。风险管理技术也可在 NCSC、ENISA 和 NIST 等组织的出版物中找到[参考文献 39、40 和 41]。

2.2 合规等级

确定各种物联网类应用的安全目标是一种主观性非常强的工作。即使在消费者和企业等垂直行业中，安全措施和管制强度也会因实际用例而异。为了使本框架在各种应用中更加实用，本版本采用了一种基于风险的方法，该方法源自常用的 CIA Triad[参考文献 1]。虽然 CIA Triad 模型并不完美，但其优点是简单，并且可以根据核心原则建立良好的安全实践。

根据产品拟用于的市场和应用，风险评估可能需要更高的合规等级，以便降低确定的风险水平。请考虑以下示例：以远程监测站中所用的 Wi-Fi 中继盒的虚构案例为例，如果认为其对企业运营造成的威胁较低，则可以根据合规等级 1 的要求进行评估。但是，当具有更高威胁依赖性的医院部署 Wi-Fi 中继盒时，则可以根据合规等级 4 的要求进行评估。第 2.2.1 节提供了另一个示例。

为了对产品应用适当的安全合规级别，使用以下合规等级对检查清单中的要求进行了分类：

- *等级 0：生成的数据损坏或失去控制可能会对个人或组织产生很小的影响*
- *等级 1：生成的数据损坏或失去控制可能会对个人或组织产生有限的影响*
- *等级 2：除了等级 1 外，部署的设备旨在抵御可能会对个人或组织产生重大影响，或者对许多人产生影响的可用性攻击。例如限制与其连接的基础设施的操作*
- *等级 3：除了等级 2 外，部署的设备旨在包含敏感数据，包括敏感的个人数据*
- *等级 4：除了等级 3 外，如果生成的数据损坏或失去控制可能会影响到关键基础设施，或造成人身伤害*

对于每个合规等级，完整性、可用性和保密性级别如下**表 1** 所示。

合规等级	安全目标		
	保密性	**完整性**	**可用性**
等级 0	基本	基本	基本
等级 1	基本	中	中
等级 2	中	中	高
等级 3	高	中	高
等级 4	高	高	高

表 1：合规等级安全目标

保密性、完整性和可用性级别的定义如下：

- 保密性
    - 基本 – 设备或服务处理公开信息
    - 中 – 设备或服务处理敏感信息，包括个人身份信息，一旦其损坏，就可能对个人或组织产生有限的影响
    - 高 – 设备或服务处理非常敏感的信息，包括个人身份信息，一旦其损坏，就可能对个人或组织产生重大影响
- 完整性
    - 基本 – 一旦设备或服务损坏，就可能对个人或组织产生轻微或可忽略的影响
    - 中 – 一旦设备或服务损坏，就可能对个人或组织产生有限的影响
    - 高 – 一旦设备或服务损坏，就可能对个人或组织产生重大或灾难性的影响
- 可用性
    - 基本 – 一旦设备或服务不可用，就会导致轻微中断
    - 中 – 一旦设备或服务不可用，就会对个人或组织产生有限的影响
    - 高 – 一旦设备或服务不可用，就会对个人或组织产生重大影响，或对许多人产生影响

    [上述定义是以参考文献 11、12、13 和 14 为基础制定的]

请注意：本框架合规等级仅供参考。供应商可能知道一些会改变等级值的应用特定问题。被视为“不适用”的要求必须提供可信的证据，以说明案例。

2.2.1 确定安全目标 – 示例

为了通过实际示例进行说明，请考虑商业温室中使用的联网恒温器所需的安全特性。可以通过以下方式确定该设备的合规等级选择：

- 保密性为基本：基本假设是恒温器不存储敏感、机密或个人身份信息
- 完整性为中：对于商业温室中使用的恒温器来说，数据完整性不佳可能会对业务/财务状况产生影响
- 可用性为中：商业温室环境中使用的恒温器可能是环境控制系统的一部分。因此，单个传感器故障的影响很小，但是跨多个传感器的拒绝服务攻击具有更大的商业风险

在这种情况下，恒温器可以按以下方式进行分类：

合规等级	安全目标		
	保密性	完整性	可用性
等级 1	基本	中	中

表 2：合规等级安全目标示例

2.3 填写合规检查清单

预计遵守本框架将会成为组织安全流程的一个组成部分，并将为业务保证提供支持证据。合规检查清单[参考文献 19]是随附的电子表格，可在产品生命周期的不同阶段使用。首先在概念阶段确定安全需求，然后列出收集的证据，最后签发产品发布的安全要求。

仅在确定第 2.2 节所述的合规等级之后，证据收集过程才能开始实施。这可通过使用风险评估实现（参阅附录 A）。

一旦确定了合规等级，随附的电子表格会自动导出适用的强制性要求（M）或建议性要求（A）。该电子表格还可用于优化产品设计，以及确定某项变更是否会允许选择较低的合规等级。例如，通过不收集或处理敏感的个人数据，或者可能为客户提供自动故障转移至替代服务，以维持服务可用性。

2.3.1 关键字

为提高本文件的易用性，已使用下表中定义的关键字对第 2.4.3 节至第 2.4.16 节中的要求进行了分类。

主要 关键字	说明	次要 关键字	说明
系统	要求 适用于 设备/产品 或服务的技术要素	***软件***	要求直接适用于 设备或服务软件
		硬件	要求直接适用于设备/服务硬件的电子器件（PCB、 处理器、组件等）
		物理	要求直接适用于 设备的机械方面，如 外壳、外形规格等。
业务	业务 要求并不 直接与 设备/产品 或服务的 操作功能 相关	***流程***	间接影响设备或服务的 安全特性的活动流
		策略	间接影响设备或服务 的安全特性的说明 和指南
		责任	间接影响设备或服务 安全特性的角色或 责任

表 3：关键字类别

请注意：术语设备和产品在本文件中被认为是可互换的

2.3.2 合规要求满足责任

合规要求将由组织中的各种角色共同设法满足。由于每个组织都不同，因此无法确切规定这些角色，但如下表 4 所示，每个要求部分都可能需要经理和其他员工予以关注。使用合规检查清单电子表格时，可通过使用相关关键字来确定任何个别要求的责任，这些关键字可通过筛选器进行选择。

章节	主题	主题受众和典型职责
2.4.3	业务安全流程、策略 和责任	管理层负责管理 开发和部署物联网设备的业务。
2.4.4	设备硬件和物理安全	设计和生产员工负责硬件 和机械质量
2.4.5	设备软件	设备应用程序质量管理由软件 架构师、产品所有者和发布经理负责。
2.4.6	设备操作系统	管理层和设计员工负责选择第三方操作系 统，或评估内部开发软件的 质量。
2.4.7	设备有限和无线接口	设计和生产员工负责设备 通信安全。
2.4.8	身份验证和授权	设计和生产员工负责确保物联网系统接口安全和身份验证 基础。
2.4.9	硬件加密和密钥	设计和生产员工负责确保物联网

	硬件	系统硬件安全、密钥管理和 加密。
2.4.10	Web 用户界面	设计和生产员工负责确保物联网 产品或服务的 Web 系统安全。
2.4.11	移动应用程序	设计和生产员工负责确保物联网 产品或服务的移动应用程序安全。
2.4.12	隐私	管理层和员工负责数据 保护和隐私法规遵从。
2.4.13	云云和网络元素	设计和生产员工负责确保物联网产品或服务的云或网络系统 安全。
2.4.14	供应链和生产安全	管理层、设计和生产员工负责确保物联网产品或服务的供应链 安全。
2.4.15	配置	设计和生产员工负责确保物联网 服务配置和设备安全。
2.4.16	设备所有权转让	管理层、设计和生产员工 负责产品和服务的供应链管理。

表 4：合规责任

相关要求应显示为“已满足”，并引用产生设计的适用证据。

随附的合规检查清单允许根据每个相关要求输入收集的证据，以证明合规，或输入该证据的链接。可从许多来源和人那里收集这些证据。证据应由负责完成本框架的人进行核实，并且此类核实应予以记录。

有关高风险等级 3 设备的业务流程的已填写合规检查清单片段示例如下图 1 所示。

要求	合规等级和 适用性	主要关键字	次要关键字	需要的合规方法
由某个人或角色（通常是董事级高级管理人员）全权管理和负责产品、服务和业务层级的安全。	对于等级 3 是强制性的	业务	责任	等级 3 审计： 已任命 CSO： （插入 URL）
由某个人或角色全权管理，以确保遵守本合规检查清单流程。	对于等级 3 是强制性的	业务	责任	等级 3 审计： IT 安全经理 “姓名”
建立了有据可查的业务流程，以确保安全。	对于等级 3 是强制性的	业务	流程	等级 3 审计： 业务流程文件 – 内联网链接

公司遵循行业标准网络安全建议（如英国 Cyber Essentials、NIST 网络安全框架、ISO27000 等）。	建议性，适用于所有等级	业务	策略	等级 3 审计：可用的证书（插入 URL）

图 1：部分填写的合规检查清单示例

2.3.3 证据

本框架是一份汇总检查清单，应辅以产品设计文件（包括风险登记簿）使用。还必须记录为处理每个风险行式项目而采取的风险缓解措施的证据。

此类记录应妥善保管，我们建议进行备份。在产品受到实际威胁的情况下，这些记录可能非常有用，但也可用作组织中使用的任何业务合规制度的证据。记录保管员应允许访问任何参考证据和支持文件，以便进行审计。尤其应该检查 URL，以确保其至少在产品生命周期和任何保修期内，可供随时访问。还应注意对查看证据材料所需的任何工具或应用程序进行妥善维护。

从宣称其已使用本框架的供应商采购产品、系统和服务时，组织可以要求使用内部资源或可信第三方（“T3P”）对收集的证据进行审计。如果记录在案的证据会暴露敏感信息（如知识产权或商业敏感信息），则可以使用 T3P。

2.4 合规术语和适用性

2.4.1 术语

下列术语“必须”、“不得”、“必需”、“应”、“不得”、“应该”、“不应该”、“建议”、“可以”和“可选”均按照 RFC2119 中的定义使用[参考文献 25]。

2.4.2 合规级别

合规级别的定义如下：

强制性	**应满足此要求，因为这对实现产品的安全目标至关重要。**
建议性	除非有合理的产品原因（如经济可行性、硬件复杂性），否则应满足此要求。应记录偏离要求的原因和用于减少任何安全风险的替代对策。

例如，在下表中，显示的合规等级是“强制性，适用于等级 2 及以上等级”，这意味着该要求对于所有其他级别（即 2、3 和 4）是强制性的。

2.4.3 合规适用性 – 业务安全流程、策略和责任

本节的目标受众是负责管理物联网设备开发和部署业务的人员。必须指定高级管理人员负责产品安全和客户信息隐私。

有几个要求等级已通过关键字进行确定。应根据评估的产品，将每个等级分配给指定人员。若需进一步指引，请参阅 IoTSF 最佳做法指南[参考文献 44]。

每项要求的适用性被定义为对任何设备的已评估风险级别是**建议性**或**强制性**的，则默认为强制性的。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.3.1	由某个人或角色（通常是董事级高级管理人员）全权管理和负责产品、服务和业务层级的安全。	强制性，适用于所有等级	业务	责任
2.4.3.2	由某个人或角色全权管理， 以确保遵守本合规检查清单流程。	强制性，适用于所有等级	业务	责任
2.4.3.3				
2.4.3.4	公司遵循行业标准网络安全建议（如英国 Cyber Essentials、NIST 网络安全框架、ISO27000 等）。	强制性，适用于等级 2 及以上等级	业务	策略
2.4.3.5	已制定相关策略，以便与内部和第三方安全 研究人员就产品或服务进行互动。	强制性，适用于所有等级	业务	策略
2.4.3.6	已制定相关政策，以便消除可能影响安全，并影响或涉及所提供的产品或服务采用的技术或组件的风险。	强制性，适用于等级 2 及以上等级	业务	策略
2.4.3.7	根据 IoTSF 漏洞披露指南[参考文献 19]或类似公认流程制定了相关流程和计划，以便在发生安全漏洞 或损害时进行识别。	强制性，适用于所有等级	业务	流程
2.4.3.8	制定了相关流程，以便在发现漏洞或安全漏洞的情况下，为高管人员提供一致性的简报，特别是负责媒体关系或发布公告的高级管理人员。特别是，在发生安全漏洞事件时所作的任何公开声明都应尽可能全面 准确地说明事实。	强制性，适用于所有等级	业务	流程
2.4.3.9	根据 IoTSF 漏洞披露指南 [参考文献 19]或类似公认流程制定了安全通知	强制性，适用于所有等级	业务	流程

	流程，以通知合作伙伴/用户有关任何安全更新的消息。			
2.4.3.10	应使用标准方法，如 OWASP、Octave 或 NIST RMF 风险管理框架[参考文献 35]进行安全威胁和风险评估，以在开始设计之前确定风险和不断演进的威胁。	强制性，适用于所有等级	业务	流程
2.4.3.11	根据安全策略，开发用于漏洞披露报告的特定联系人网页。	强制性，适用于所有等级	业务	策略
2.4.3.12	根据安全策略，为漏洞披露通信提供专用的安全电子邮件地址和/或安全在线页面。	强制性，适用于所有等级	业务	策略
2.4.3.13	根据安全策略，为漏洞披露制定冲突解决流程。	对于等级 3 是强制性的及以上等级	业务	流程
2.4.3.14	根据安全策略，发布组织为漏洞披露制定的冲突解决流程。	建议性，适用于所有等级	业务	流程
2.4.3.15	根据安全策略，制定漏洞披露的响应步骤和绩效目标。	强制性，适用于所有等级	业务	流程
2.4.3.16	根据安全策略，制定安全咨询通知步骤。有关示例，请参阅美国认证计划[参考文献 46]。	强制性，适用于所有等级	业务	流程
2.4.3.17	安全策略应符合 ISO 30111 或类似标准。	建议性，适用于所有等级	业务	策略
2.4.3.18	如果存在实时或正常工作时间预期，则必须定义一个程序，用于通知联网组件即将发生的停机更新时间。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.3.19	为更新过程的每个阶段分配责任。	对于等级 2 是强制性的及以上等级	业务	责任
2.4.3.20	为更新过程的控制、日志记录和审计分配责任。	强制性，适用于等级 2 及以上等级	业务	流程 角色
2.4.3.21	设有联络点，以便第三方供应商就安全问题进行联系。	强制性，适用于等级 1 及以上等级	业务	流程 角色

2.4.3.22	在支持远程更新的情况下，制定了相关流程/计划，以便在持续或补救的基础上验证“更新”和更新设备，例如，可从 IoTSF 最佳做法指南 L 部分 [参考文献 44]获得软件更新指引。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.3.23	应对电源供电受限的设备的安全更新策略进行评估，以平衡维护设备完整性和可用性的需求。	强制性，适用于等级 2 及以上等级	业务	策略
2.4.3.24	指定一名所有者负责评估产品中使用的第三方 提供的组件（硬件和软件），例如操作系统供应商提供了填写妥当的 IoTSF 框架合规检查清单[参考文献 19]、 文件或同等文件。	强制性，适用于等级 2 及以上等级	业务	角色
2.4.3.25	如果设备支持远程软件升级，应制定一项透明且可审计的策略，其中包含用于修复发现的任何漏洞的行动计划表。	强制性，适用于等级 2 及以上等级	业务	策略

2.4.4 合规适用性 – 设备硬件和物理安全

本节的目标受众是负责硬件和机械质量的人员。有关物理安全（B 部分）、安全启动（C 部分）和安全操作系统（D 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.4.1	产品的处理器系统设有 不可撤销的硬件安全启动过程。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.4.2	产品的处理器系统设有 不可撤销的“可信启动硬件安全启动”过程。	强制性，适用于等级 2 及以上等级	系统	硬件
2.4.4.3	产品的处理器系统设有 慎重的不可撤销的硬件安全启动过程。	强制性，适用于等级 3 及以上等级	系统	硬件
2.4.4.4	安全启动过程是默认启用的。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.4.5	任何调试接口（例如 I/O 端口，如 JTAG）仅与 生产设备上经授权和验证的实体 进行通信。	强制性，适用于等级 1 及以上等级	系统	硬件 软件
2.4.4.6	硬件具有防篡改功能，并且已启用该功能。防 篡改级别必须根据 风险评估结果予以确定。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.4.7	硬件设有防篡改的 实体保护措施，以减少 攻击面。防护级别根据风险评估结果予以确定。	强制性，适用于等级 3 及以上等级	系统	硬件 物理
2.4.4.8	硬件设有防篡改的 过程的实体保护措施。防 护级别根据风险评估结果予以确定。	强制性，适用于等级 2 及以上等级	系统	硬件
2.4.4.9	所有未作为产品正常操作一部分使用的通信端口（如 USB、RS232 等）都无法实际访问，或只能与经授权和 验证的实体进行通信。	强制性，适用于所有等级	系统	硬件、物理、软件

2.4.4.10	尽可能安全地禁用或删除生产设备中的所有产品开发测试点。	强制性，适用于等级 2 及以上等级	系统	硬件 物理
2.4.4.11	已使用防篡改措施来识别对最终用户的程序集的任何 干扰。	强制性，适用于等级 2 及以上等级	系统	硬件
2.4.4.12				
2.4.4.13	在生产设备中，微控制器/微处理器不允许从产品非易失性[FLASH]存储器中读取固件。如果使用单独的非易失性存储设备，则内容须加密。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.4.14	如果产品的凭证/密钥存储在其处理器外部，则存储和处理器应以加密方式配对，以防止未经授权的软件使用凭证/ 密钥存储。	强制性，适用于所有等级	系统	硬件
2.4.4.15	如果生产设备配有 CPU 监视器，则会启用该监视器，并在未经授权尝试暂停或暂停 CPU 执行时重置 该设备。	强制性，适用于所有等级	系统	硬件
2.4.4.16	如果产品具有生成真随机数的硬件源，则将其用于所有相关的密码操作， 包括 Nonce、初始化向量和密钥生成算法。有关指引，请参阅：NIST SP 800-90A [参考文献 3]。	强制性，适用于所有等级	系统	硬件、软件
2.4.4.17	产品应具有生成真随机数的硬件源。	强制性，适用于等级 2 及以上等级	系统	硬件

2.4.5 合规适用性 – 设备软件

本节的目标受众是负责设备应用程序质量的人员，例如**软件架构师、产品所有者和发布经理。**有关安全操作系统（D 部分）、凭证管理（F 部分）和软件更新（J 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.5.1	产品设有防护措施，以防止 将未经验证的软件和文件加载到其上。如果产品旨在允许加载未经验证的软件，则此类软件只能以有限 权限和/或在沙箱中运行。	强制性，适用于所有等级	系统	软件
2.4.5.2	如果设备支持远程软件 更新，则软件映像将由经批准的签署机构进行数字签名。	强制性，适用于所有等级	系统	软件
2.4.5.3	如果支持更新，则在更新过程开始前，软件更新包须由设备验证其数字签名、签名证书 和签名证书链。	强制性，适用于所有等级	系统	软件
2.4.5.4	如果设备支持远程软件升级，则软件映像须在传输至设备的过程中 进行加密。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.5.5	如果产品具有正常操作不需要的任何虚拟端口，则仅允许这些端口与经授权和验证的实体进行通信，或在装运时安全地禁用。 如果端口用于现场诊断，则停用端口输入命令，并且输出不会提供任何可能危及设备的信息，例如凭证、 内存地址或函数名称。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.5.6	为防止设备软件操作暂停 或中断，配有监视计时器， 且不能将其禁用。	强制性，适用于所有等级	系统	硬件、软件
2.4.5.7	产品的软件签名信任根 存储在防篡改的内存中。	强制性，适用于所有等级	系统	硬件
2.4.5.8	产品设有防护措施，以防未经授权地将软件还原到可能不太安全的 早期版本。	强制性，适用于所有等级	系统	软件
2.4.5.9	设有防止将非生产软件安装到生产设备上的措施 。	强制性，适用于所有等级	业务	流程

2.4.5.10	生产软件映像应按如下方式进行编译：确保删除所有不必要的调试和符号信息，以防 意外发布多余数据。	强制性，适用于所有等级	业务	流程
2.4.5.11	如果软件在产品供应商的 可信环境之外的产品上运行，开发软件版本须关闭所有调试功能。	对于等级 2 是强制性的及以上等级	业务	流程 策略
2.4.5.12	已采取措施保护产品软件免于敏感信息泄露和旁道攻击。	强制性，适用于等级 3 及以上等级	系统	软件、硬件
2.4.5.13	产品的软件源代码遵循语言子集（如 MISRA-C）编码标准的 基本良好做法。	强制性，适用于等级 2 及以上等级	业务	策略
2.4.5.14	产品的软件源代码遵循 由开发人员进行的静态漏洞分析的基本良好做法[参考文献 37]。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.5.15	软件架构的设计必须能识别和圈出敏感软件组件， 包括加密过程，以协助 检查、审查和测试。必须 控制从其他软件组件进行访问，并且仅限其进行已知且可接受的 操作。例如，安全相关 进程应在应用程序处理器硬件 中以更高的权限级别执行。	强制性，适用于等级 1 及以上等级	业务系统	流程软件
2.4.5.16	遵循定义的可重复流程，开发、测试和维护软件源代码 。	强制性，适用于所有等级	业务	流程
2.4.5.17	用于编译应用程序的生成环境和工具链在访问受控且可审计的生成 系统上运行。	强制性，适用于等级 2 及以上等级	业务	策略 流程
2.4.5.18	用于创建软件的生成环境和工具链可以进行配置管理和版本控制， 并定期验证其完整性。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.5.19	如果有，生产软件签名密钥 可以进行访问控制。	强制性，适用于所有等级	业务	策略
2.4.5.20	生产软件签名密钥妥善存储在符合 FIPS-140-2 2 级[参考文献 5]或同等或更高标准的存储设备中 。	强制性，适用于等级 2 及以上等级	业务	策略
2.4.5.21	如果设备软件通过 TCP/IP 或 UDP/IP 与产品相关的网络服务器或应用程序进行通信，则设备软件可以在适当情况下使用证书固定或公钥/私钥或等效物。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.5.22	对于无法进行软件更新的设备，确更换支持的条件 和期限应清楚明确。	强制性，适用于所有等级	业务	策略

2.4.5.23	检查所有输入和输出的有效性， 例如使用“模糊”测试检查预期（有效）和意外（无效）输入刺激 的可接受响应或输出。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.5.24	软件的设计旨在满足风险评估中确定的安全要求；例如，在 意外无效输入或错误软件操作的情况下，产品不会变得 危险，或危及其他联网系统的安全。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.5.25	对于无法按时安全安装整个更新的设备，提供部分安装更新支持。	建议性，适用于所有等级	系统	软件
2.4.5.26	对于网络接入受限或不定时发生的设备，提供部分 下载更新支持。	建议性，适用于所有等级	系统	软件
2.4.5.27	如果存在实时性能期望，则更新机制不得妨碍这些期望的达成（例如， 以低优先级运行更新进程）。	建议性，适用于所有等级	系统	软件
2.4.5.28	如果设备不支持安全启动，则在进行固件更新时，用户数据和 凭证应重新初始化。	强制性，适用于所有等级	系统	硬件、软件
2.4.5.29	如果设备无法自行验证更新的真实性（例如由于无加密功能），则只允许实际用户进行本地更新，并由其 承担相关责任。	强制性，适用于所有等级	系统	软件
2.4.5.30	当设备无法自行验证更新的真实性时，应可以还原至 上次已知的正确配置，该配置已在尝试 更新之前存储到设备上。	强制性，适用于所有等级	系统	软件
2.4.5.31	更新完整性保护和保密性的加密密钥 根据行业标准安全地进行管理， 例如 FIPS 140-2[参考文献 5]。	强制性，适用于所有等级	业务	流程 策略

2.4.5.32	可以根据行业标准，在制造过程中安全地提供加密密钥，以进行 更新，例如 FIPS 140-2[参考文献 5]。	强制性，适用于所有等级	业务	流程策略
2.4.5.33	一旦不再需要，则用于存储敏感资料（如加密密钥、密码/密码短语等）的内存位置 须尽快进行安全审查。这些包括但不限于堆、堆栈和静态分布存储上的 位置[参考文献 47]。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.5.34	对包含敏感资料的内存位置进行安全审查之后， 任何可能存储敏感资料的缓存都将被清除 。	强制性，适用于等级 3 及以上等级	系统	硬件 软件
2.4.5.35	应发布报废政策，明确规定设备接收软件更新的最短时间和支持期限时长的原因。应向用户清楚说明每次更新需求，并且更新应易于 实现。	强制性，适用于所有等级	业务	策略
2.4.5.36	如果可能，应根据适当的周期向设备推送软件更新。供应设备时，应向用户清楚说明该周期。供应链合作伙伴应告知用户，设备需要 更新。	强制性，适用于所有等级	业务	策略

2.4.6 合规适用性 – 设备操作系统

本节的目标受众是负责选择第三方操作系统，或评估“内部”开发的调度程序和控制序列器质量的人员。为简洁起见，下文所用的操作系统（OS）一词意味着所有此类选项。有关安全操作系统（D 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.6.1	操作系统在发布之前进行了相关安全更新。	建议性，适用于所有等级	业务	流程
2.4.6.2				
2.4.6.3	在软件开发过程结束时，已禁用或从软件中删除了所有不必要的帐户或登录。例如，开发或调试帐户。	建议性，适用于所有等级	系统	软件
2.4.6.4	文件、目录和持久性数据被设置为正确运行所需的最低访问权限功能。	建议性，适用于所有等级	系统	软件
2.4.6.5	如果密码绝对必须存储在本地文件中，则密码文件归设备操作系统的最高权限帐户所有，并且只能由其访问和写入。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.6.6	所有操作系统非必要的服务均已从产品的软件、映像或文件系统中删除。	建议性，适用于所有等级	系统	软件
2.4.6.7	对最有特权帐户的所有操作系统命令行访问都已从操作系统中删除。	建议性，适用于所有等级	系统	软件
2.4.6.8	产品的操作系统内核及其功能不会被外部产品级接口和未经授权的应用程序调用。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.6.9	应用程序以尽可能低的权限级别运行，并且只能通过适当的访问控制机制访问其所需的资源。例如，具有一个或多个网络接口、不受控制和任何意外的数据包转发功能的产品都应被阻止。	强制性，适用于所有等级	系统	软件
2.4.6.10	操作系统支持的所有适用安全功能都已启用。	对于等级 1 是强制性的及以上等级	系统	软件
2.4.6.11	操作系统与应用程序分离，并且只能通过定义的安全接口进行访问。	建议性，适用于所有	系统	软件

		等级		
2.4.6.12	操作系统采用分离架构，将受信任的应用程序与不受信任的应用程序分开。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.6.13	产品的操作系统内核的设计使得每个组件都能以所需的最小限度安全功能运行（例如微内核架构）。	强制性，适用于等级 2 及以上等级	系统	软件

2.4.7 合规适用性 – 设备有线和无线接口

本节的目标受众是负责设备安全的人员。有关凭证管理（F 部分）和网络连接（H 部分）的指引，请参阅 IoTSF 最佳做法指南[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.7.1	产品可以防止未经授权地连接到自身或与产品连接的其他设备。例如，每个接口和互联网层协议都设有防火墙。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.2	已针对所需/定义的安全行为，审查并记录了网络组件和防火墙（如果适用）配置。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.7.3	在设有网络接口的产品中，为了停止安全域的桥接，应阻止不受控制和任何意外的数据包转发功能，以停止不合需要的通信路径。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.4	设备仅支持无众所周知的漏洞的应用程序层协议版本。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.7.5	如果检测到未经授权的变更，则设备应向消费者/管理员发出问题警报，并且不应连接到比执行警报功能所需网络更广阔的网络。	强制性，适用于所有等级	系统	软件
2.4.7.6	所有未使用的产品端口都已关闭，只有所需的端口处于活动状态。	对于等级 1 是强制性的及以上等级	业务	流程
2.4.7.7	如果连接需要密码或密钥进行连接验证，出厂设置或重置的密码对于每台设备都是唯一的。示例包括 Wi-Fi 访问密码和蓝牙 PINS。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.7.8	在使用初始配对过程时，应使用强验证；需要与设备进行物理交互，或持有共享密钥。例如，蓝牙数字比较[参考文献 38]。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.9	如果无线接口具有初始配对过程，则在提供正常服务之前，变更出厂设置的密钥或重置密码。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.7.10	对于任何 Wi-Fi 连接，已使用 WPA2[参考文献 51]、采取 AES 的更高版本或类似强度加密，并且不安全的协议（如 WPA 和 TKIP）已被禁用	强制性，适用于等级 1 及以上等级	系统	软件

2.4.7.11	如果使用 WPA2 WPS，每台设备有一个唯一的随机密钥，并执行以指数方式增加的重试尝试延迟。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.12	所有网络通信密钥均按照行业标准（如 FIPS 140-2[参考文献 5]）或类似标准安全存储。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.13	如果使用 TCP 协议（如 MQTT），则其受到无已知漏洞的 TLS 协议版本。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.14	如果使用 UDP 协议（如 CoAP），则其受到无已知漏洞的 DTLS 协议版本。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.15	如果使用加密套件（如 TLS），则应应列出所有密码套件，并根据最新的安全建议（如 NIST 800-131A[参考文献 2]或 OWASP）进行验证。如果发现了不安全的密码套件，则应将其从产品中删除。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.7.16	产品使用的所有加密技术（如 TLS 密码套件）均应列出，并根据产品销售和/或装运目的地的进出口要求进行验证。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.7.17	如果通信中断或变得不可用，则不得损害设备的本地完整性。	强制性，适用于所有等级	系统	软件
2.4.7.18	产品仅启用产品操作所需的通信接口、网络协议、应用程序协议和网络服务。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.19	通信协议应保持最新版本，且无任何众所周知的漏洞和/或适用于产品。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.7.20	产品发布后的通信协议应在整个产品生命周期内，保持最安全的版本，且无任何众所周知的 漏洞。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.7.21	如果进行了恢复出厂设置操作，设备应发出警告，除非更新，否则安全操作 可能受到损害。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.7.22	如果启用了 RF 通信（如 ZigBee 等），天线功率被配置为限制映射资产的能力，以限制 WAR-Driving 等攻击（参阅 https://techterms.com/definition/wardriving）。	建议性，适用于所有等级	系统	软件
2.4.7.23	启用了协议中的协议匿名功能（如蓝牙），以限制位置跟踪功能。	建议性，适用于所有等级	系统	软件

2.4.7.24	在网络连接丢失的情况下，设备应尽可能合理地 保持运行和本地功能，并在恢复断电的情况下，设备应干净利落地恢复。设备应能以合理的状态和有序的方式恢复网络连接，而不是大规模重新连接。	强制性，适用于所有等级	系统	软件

2.4.8 合规适用性 – 身份验证和授权

本节的目标受众是负责物联网系统接口安全和身份验证基础的人员。有关凭证管理（F 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.8.1	产品含有一个防篡改的唯一设备标识符（例如芯片序列号或其他唯一的硅标识符），例如将代码和数据绑定到特定的设备硬件。这可以克隆的威胁 。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.8.2	如果产品有一个安全的时间源，可通过一种方法来验证其完整性，例如安全 NTP https://www.ntpsec.org。	强制性，适用于所有等级	系统	软件
2.4.8.3	如果使用用户界面密码进行登录身份验证，出厂设置或重置的密码对于产品系列中的每台设备都是唯一的。如果使用无密码身份验证，则相同的唯一性原则适用。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.4	产品不接受使用空密码。	对于等级 1 是强制性的及以上等级	系统	软件
2.4.8.5	产品不允许新密码包含与用户帐户关联的用户帐号名。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.6	密码输入遵循行业标准惯例，例如 3GPP TS33.117 密码策略[参考文献 17]、NIST SP800-63b[参考文献 26] 或 NCSC[参考文献 48]有关密码长度、分组字符和特殊字符的建议。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.7	产品可以抵御暴力重复登录尝试，例如以指数增加的重试尝试延迟。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.8	产品使用符合行业标准的行业标准加密算法，安全地存储任何密码，例如 NIST SP800-63b[参考文献 26]或类似标准。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.9	产品支持对根/最高特权帐户的访问控制措施，以限制访问敏感信息或系统 。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.10	访问控制特权进行了定义、充分论证和记录。	对于等级 1 是强制性的及以上等级	业务	流程

2.4.8.11	产品仅允许受控用户帐户访问；若无正当理由，不支持使用匿名或访客用户帐户进行访问。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.8.12	产品允许在安装或调试时，禁用、清除或重新命名出厂设置的或 OEM 登录帐户。	建议性，适用于所有等级	系统	软件
2.4.8.13	产品支持在安装或调试时，更改任何或所有出厂默认用户登录密码。	强制性，适用于所有等级	业务	流程
2.4.8.14	如果产品设有密码恢复或重置机制，则已进行评估，以确认该机制不会轻易被未经授权方滥用。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.8.15	当在用户界面上输入密码时，实际通行短语会默认隐藏。	对于等级 1 是强制性的及以上等级	系统	软件
2.4.8.16	产品认可经授权的完全恢复出厂设置，和设备的所有授权信息。	建议性，适用于所有等级	系统	软件
2.4.8.17	如果产品能够从攻击中远程恢复，则应恢复到已知良好状态，以实现设备的安全恢复和更新。	强制性，适用于所有等级	系统	软件

2.4.9 合规适用性 – 硬件加密和密钥管理

本节的目标受众是负责物联网系统硬件密钥管理和加密安全的人员。有关加密（G 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级	主要关键字	次要关键字
2.4.9.1				
2.4.9.2	如果存在，已使用 NIST SP800-22[参考文献 4]、FIPS 140-2[参考文献 5] 或类似合规流程对真随机数生成器源进行了真实随机性验证。	建议性，适用于所有等级	系统	硬件
2.4.9.3	制定了安全提供密钥的流程，包括生成、分配、更新、撤销和销毁。例如按照 FIPS140-2[参考文献5] 或类似流程。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.9.4	采用一种安全的密钥插入方法，以防止密钥被复制。	强制性，适用于等级 1 及以上等级	系统	软件

2.4.9.5	所有产品相关的加密功能都没有众所周知的十足弱点，例如未使用 MD5 和 SHA-1，如NIST SP800-131A[参考文献 2]中规定的那些功能。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.9.6	所有产品相关的加密功能在产品的生命周期内都是很安全的，例如NIST SP800-131A[参考文献 2]中规定的那些功能。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.9.7	产品将所有敏感的未加密参数（如密钥）存储在安全的 防篡改位置。	强制性，适用于等级 1 及以上等级	系统	硬件
2.4.9.8	用于生产软件签名的加密密钥链不同于用于任何其他测试、开发或 其他软件映像或支持要求的加密 密钥链。	建议性，适用于所有等级	系统	软件
2.4.9.9	在设备制造过程中，所有非对称加密私钥对于每台 设备都是唯一的，并按照 FIPS 140-2[参考文献 5]的规定确保其安全。这些私钥必须是真正随机 内部生成的，或安全地 编程到每台设备中。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.9.10	所有密钥长度都足以满足所需的保证级别，例如 NIST SP800-57 1 部分所述。	强制性，适用于等级 2 及以上等级	业务	策略

2.4.10 合规适用性 – Web 用户界面

本节的目标受众是负责物联网产品或服务 Web 系统安全的人员。有关应用程序安全（E 部分）和凭证管理（F 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.10.1	如果产品或服务提供基于 Web 的用户界面，则使用 强验证。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.2	如果产品或服务提供基于 Web 的界面，则须将公共区域和限制 区域分开进行验证。	强制性，适用于所有等级	系统	软件
2.4.10.3	如果产品或服务提供 基于 Web 的管理界面，则对 Web 服务器进行强验证。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.4	如果使用 Web 用户界面密码进行登录身份验证，则初始密码或恢复出厂设置密码 对于产品系列中的每台设备都是唯一的。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.5	Web 用户界面受自动会话空闲注销超时功能保护。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.6	用户密码不以纯文本格式存储。需要使用强密码，并且密码中含有一个随机混淆值。若需了解更多信息，请参阅 3GPP TS33.117 密码策略[参考文献 17]、NIST SP800-63b[参考文献 26] 和 NCSC[参考文献 48]。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.7	当在用户界面上输入密码	对于等级 1 是强制性的	系统	软件

	时，实际通行短语会默认隐藏，以防撷取密码。	及以上等级		
2.4.10.8	Web 用户界面应遵循良好做法指南，例如 OWASP[参考文献 30]中所述的指南。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.10.9	已在部署之前，并且会 在部署之后持续进行 漏洞评估。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.10.10	所有通过接口传输的数据都应在适当的情况下进行验证。这可能包括检查数据类型、 长度、格式、范围、真实性、来源 和频率。	强制性，适用于所有等级	系统	软件
2.4.10.11	使用 URL 编码或 HTML 编码对 Web 应用程序中的输入进行安全审查，以包装数据并将其视为文字文本，而不是 可执行脚本。	强制性，适用于所有等级	系统	软件
2.4.10.12	使用白名单等措施验证所有输入和输出，该白名单包含 经授权的数据来源和此类 数据的有效属性。	强制性，适用于所有等级	系统	软件
2.4.10.13	仅限获得授权的操作员访问管理界面。例如 使用证书对管理接口 进行相互身份验证。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.14	缩短会话的生存期，以降低会话劫持和重播攻击的风险。例如为了缩短时间，攻击者必须撷取会话 Cookie，并 使用其访问应用程序。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.10.15	检查所有输入和输出的有效性，例如使用“模糊”测试检查预期（有效）和意外（无效）输入刺激的可接受响应 或输出。	强制性，适用于等级 1 及以上等级	业务	流程

2.4.11 合规适用性 – 移动应用程序

本节的目标受众是负责物联网产品或服务移动应用程序安全的人员。有关应用程序安全（E 部分）和凭证管理（F 部分）的指引，请参阅 IoTSF[参考文献 44]。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.11.1	如果使用应用程序的用户界面密码进行登录身份验证，则初始密码或恢复出厂设置密码对于产品系列中的每台设备都是唯一的。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.2	密码输入遵循行业标准，例如 3GPP TS33.117 密码策略[参考文献 17]或 NIST SP800-63b[参考文献 26]的建议。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.3	移动应用程序确保任何相关数据库或文件都具有防篡改或访问限制功能。一旦检测到数据库或文件被篡改，数据库或文件就会被重新初始化。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.4	当应用程序与产品相关远程服务器或设备进行通信时，会通过安全连接进行通信，例如使用证书固定的 TLS 连接。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.5	产品使用行业标准加密算法安全地存储任何密码，例如参阅 FIPS 140-2[参考文献 5]。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.6	当在用户界面上输入密码时，实际通行短语会默认隐藏，以防撷取密码。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.11.7	所有通过接口传输的数据都应在适当的情况下进行验证。这可能包括检查数据类型、长度、格式、范围、真实性、来源和频率。	强制性，适用于所有等级	系统	软件
2.4.11.8	安全管理界面：重要的是，仅限获得授权的操作员和管理员访问配置管理功能。对管理接口进行强验证，例如通过使用证书进行验证。	强制性，适用于等级 1 及以上等级	系统	软件

2.4.11.9	使用白名单等措施验证所有应用程序输入和输出，该白名单包含经授权的数据来源和此类数据的有效属性，参阅 NIST SP 800-167[参考文献 34]。	强制性，适用于所有等级	系统	软件

2.4.12 合规适用性 – 隐私

本节的目标受众是负责数据保护和隐私法规遵从的人员。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.12.1	产品/服务存储服务提供所需的最少量的用户个人信息。	强制性，适用于所有等级	系统 业务	软件 策略
2.4.12.2	产品/服务确保所有个人信息在存储时，以及进行设备外通信时，都会进行加密，请参阅 IoTSF 指引[参考文献 44]H 部分（网络连接）	强制性，适用于等级 1 及以上等级	系统业务	软件策略
2.4.12.3	产品/服务确保仅限获得授权的人员才能访问用户的个人数据。	强制性，适用于所有等级	系统 业务	软件 策略
2.4.12.4	产品/服务确保个人信息尽可能匿名化，尤其时在任何报告中。	强制性，适用于所有等级	系统 业务	软件 策略
2.4.12.5	产品制造商或服务提供商应确保为用户建立数据保留策略并进行记录。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.12.6	有一种或多种方法告知产品所有者：哪些个人信息会被收集，为何收集个人信息，以及将个人信息存储在何种。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.12.7	产品所有者可以使用一种或多种方法来检查/验证哪些个人信息会被收集和删除。	强制性，适用于所有等级	系统	软件
2.4.12.8	产品/服务符合产品销售所在地的本地和/或地区个人信息保护法律，例如 GDPR[参考文献 14]。	强制性，适用于所有等级	系统业务	软件流程
2.4.12.9	任何设备的供应商或制造商都应提供有关设备在最终用户网络中的功能如何影响其隐私的信息。	建议性，适用于所有等级	业务	流程

2.4.12.10	任何设备的供应商或制造商应提供有关如何设置设备，以维护最终用户隐私和安全的明确信息。	强制性，适用于所有等级	业务	流程
2.4.12.11	任何设备和/或服务的供应商或制造商应提供有关如何移除和/或处置设备，以维护最终用户隐私和安全的明确信息。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.12.12	任何设备或服务的供应商或制造商应提供有关最终用户维护设备和/或服务隐私和安全的责任的明确信息	强制性，适用于等级 1 及以上等级	业务	流程
2.4.12.13	在设计设备和服务的安全性时，应考虑到可用性。减少可能对安全和隐私产生不利影响的用户决策点。	强制性，适用于所有等级	系统	软件
2.4.12.14	产品或服务仅根据用户的授权记录音频/视频数据（例如，未经明确授权，不得进行被动记录）。	强制性，适用于所有等级	系统	软件
2.4.12.15	供应商或制造商进行隐私影响评估（PIA），以识别个人识别信息（PII），和设计保护用户隐私的方法[参考文献 49]。	建议性，适用于所有等级	业务	流程

2.4.13 合规适用性 – 云和网络元素

本节的目标受众是负责物联网产品或服务云或网络系统安全的人员。

请求编号	要求	合规等级	主要关键字	次要关键字
2.4.13.1	所有产品相关云和网络元素都进行了最新的操作系统安全更新，并且制定了相关流程，以确保对其进行更新。	强制性，适用于等级 2 及以上等级	业务系统	流程软件
2.4.13.2	任何产品相关 Web 服务器都已关闭其 Web 服务器标识选项（例如 Apache 或 Linux）。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.3	所有产品相关 Web 服务器都已禁用其 Web 服务器 HTTP 跟踪和跟踪方法。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.4	所有产品相关 Web 服务器的 TLS 证书都由可信证书颁发机构签署，处在有效期内，并制定了续期流程。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.5	产品制造商或服务提供商制定了一个监测相关安全公告的流程，以确保所有产品相关 Web 服务器使用的协议无任何众所周知的弱点。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.13.6	与产品相关的 Web 服务器支持适当安全的 TLS/DTLS 密码，并禁用/删除对已弃用密码的支持。例如，参阅 ENISA[参考文献 27]、SSL Labs[参考文献 29]、IETF RFC7525[参考文献 28] 和 NCSC[参考文献50]，以获取指引。	建议性，适用于所有等级	系统	软件
2.4.13.7	产品相关 Web 服务器已禁用 TLS 连接的重复重新协商。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.8	相关服务器已禁用未使用的 IP 端口。	对于等级 1 是强制性的及以上等级	系统	软件
2.4.13.9	如果与 Web 服务器相关的产品使用 TLS 加密通信并请求客户端证书，则服务器仅在客户端证书及其信任链有效时建立连接。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.10	如果与 Web 服务器相关的产品使用 TLS 加密通信，则会实施证书固定。例如，使用 OWASP[参考文献 31]或	建议性，适用于所有等级	系统	软件

	类似组织的证书和 公钥固定指引。			
2.4.13.11	所有相关服务器和网络元素都禁止使用空密码。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.12				
2.4.13.13				
2.4.13.14	所有相关服务器和网络 元素都执行符合行业标准惯例的密码，例如 3GPP TS33.117 密码策略[参考文献 17]、NIST SP800-63b [参考文献 26]和 NCSC 指引[参考文献 48]的建议。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.15	用户帐户登录尝试连续失败的最大允许次数遵循 3GPP TS33.117 密码策略[参考文献17]的建议。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.16	所有相关服务器和网络元素都使用采用行业标准加密算法的加密实现来存储任何密码，例如参阅 FIPS 140-2[参考文献 5]。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.17	所有相关服务器和网络元素都支持访问控制措施，以仅限特权帐户访问敏感信息或 系统进程。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.18	所有相关服务器和网络元素都禁止匿名/访客访问，但对公共信息的只读访问除外。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.19	如果作为云服务运行，则该服务符合行业标准云安全原则，如云安全联盟[参考文献 18]、NIST 网络安全框架[参考文献 21] 或英国政府云安全原则[参考文献 24]。	建议性，适用于所有等级	系统	软件
2.4.13.20	如果产品或服务具有任何安全关键或影响寿命的功能，则服务基础结构应设有防 DDoS 攻击的保护措施，例如流量下降或缩孔。参阅 NIST SP 800-53 SC-5[参考文献 32]。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.13.21	如果产品或服务具有任何安全关键或影响寿命的功能，则服务基础结构应具有冗余功能，以确保服务连续性和可用性。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.22	输入数据验证应	对于等级 1 是强制性的	系统	软件

	按照 NIST 800-53 SI-10[参考文献 33]所述的行业实践方法进行。	及以上等级		
2.4.13.23	如果作为云服务运行，则该云服务基于 TCP 的通信（如 MQTT 连接）使用最新的 TLS 标准进行加密和验证。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.24	如果作为云服务运行，则基于 UDP 的通信使用最新的数据报传输层安全性（DTLS）协议进行加密。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.13.25	如果设备标识和/或配置注册表（例如事物阴影）是在云服务中实现的，则对该注册表进行配置，以仅限获得授权的管理员进行访问。	强制性，适用于所有等级	系统	软件
2.4.13.26	产品相关云服务将 API 密钥绑定到特定的物联网应用程序，而不是安装到未获授权的设备中。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.13.27	产品相关云服务 API 密钥没有硬编码到设备或应用程序中。	强制性，适用于所有等级	系统	软件
2.4.13.28	如果作为云服务运行，则为任何可以配置设备的网关/服务定义和实现特权。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.13.29	产品相关云服务数据库在存储期间进行加密。	强制性，适用于所有等级	系统	软件
2.4.13.30	产品相关云服务数据库仅限获得授权的个人、设备和服务进行读取/写入访问。	强制性，适用于所有等级	系统	软件
2.4.13.31	产品相关云服务使用纵深防御架构进行设计，该架构由虚拟私有云（VPC）、防火墙访问和基于云的监控组成。	强制性，适用于所有等级	系统	软件
2.4.13.32	当作为云服务实现时，对云服务的所有远程访问都是通过安全手段（例如 SSH）实现的。	强制性，适用于所有等级	系统	软件
2.4.13.33	产品相关云服务监控是否符合连接策略，并报告不合规连接尝试。	强制性，适用于等级 2 及以上等级	系统	软件
2.4.13.34	物联网设备应使用终端至云端安全硬件（如零接触预配）连接到云服务。	建议性，适用于所有等级	系统	硬件

2.4.14 合规适用性 – 供应链和生产安全

本节的目标受众是负责物联网产品或服务供应链安全的人员。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.14.1	本产品在出厂前已将生产过程中使用的全部生产测试和校准软件擦除、删除或提供保护。这旨在防止在使用获得授权的生产软件时，更改制造后产品，例如为获得功能更强大的 RF ERP 而对 RF 特性进行黑客攻击。如果服务中心需要此类功能，则应在完成任何维修活动后将其删除或移除。	建议性，适用于所有等级	系统	软件
2.4.14.2	任何硬件设计文件、软件源代码和带有完整描述性注释的最终生产软件映像都会加密存储在非现场位置，或由第三方托管服务加密存储。	建议性，适用于所有等级	业务	流程
2.4.14.3	在制造过程中，所有设备都由产品供应商使用唯一的防篡改标识符（如序列号）进行记录，以便可以识别克隆或复制的设备，并禁用或防止其与系统一起使用。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.14.4	设备的生产系统设置了一套相关流程，以确保任何具有重复序列号的设备都不会被装运，也不会被重新编程或销毁。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.14.5	如果产品拥有一套可信安全启动流程，则使用以其安全启动、经身份验证的软件模式运行的处理器系统进行整个生产测试和任何相关校准。	建议性，适用于所有等级	系统	软件
2.4.14.6	如果生产设施不受信任，则应使用安全控制的区域和流程进行设备预配。例如，实现通用标准 EAL5+/6 认证[参考文献 6、7、8 和 9]中要求的控制。	建议性，适用于所有等级	业务	流程
2.4.14.7	如果供应链中添加了新的所有者，则应沿着供应链传输受密码保护的所有权证明，并对其进行扩展。此过程应以开放标准为基础，如增强型隐私 ID、ISO 20008/20009[参考文献 42] 中定义的证书。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.14..8	维护产品中使用的所有程序库（开源等）的可审核清单，以支持在部署期间进行知情漏洞管理。	建议性，适用于所有等级	业务	流程

2.4.15 合规适用性 – 配置

本节的目标受众是负责设备和物联网服务配置安全的人员。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.15.1	设备和任何相关 Web 服务的配置都具有防篡改功能，即敏感配置参数只能由获授权人员进行更改（证据应列出参数和获得授权进行更改的人员）。	强制性，适用于等级 1 及以上等级	业务	策略
2.4.15.2	应通过授权服务及时预配设备的配置，以替换任何现有的预配置，以确保安全操作。	强制性，适用于等级 1 及以上等级	业务	流程

2.4.16 合规适用性 – 设备所有权转让

本节的目标受众是负责数据保护和设备所有权管理的人员。

请求编号	要求	合规等级和适用性	主要关键字	次要关键字
2.4.16.1	如果一台或多台设备能够将其所有权转让给其他所有者，则应将先前所有者的所有个人信息从设备和注册服务中删除。当所有权转让或最终用户希望从服务或设备中删除其个人信息时，此选项必须可用。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.16.2	如果一台或多台设备用户希望终止服务，则应从设备和相关服务中删除所有个人信息。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.16.3	服务提供商应无法通过设备标识反向查找设备所有权。	强制性，适用于等级 2 及以上等级	业务	流程
2.4.16.4	如果所有权发生变化，则设备配有一种不可撤销的停止使用和重新调试方法。	强制性，适用于等级 1 及以上等级	系统	软件
2.4.16.5	向服务提供商进行设备注册[参考文献 16]应是安全的（证据中所需的方法和论证）。	强制性，适用于等级 1 及以上等级	业务	流程
2.4.16.6	设备制造商确保 设备的标识独立于最终用户，以确保匿名性并遵守 相关的本地数据隐私法律，如欧盟的 GDPR[参考文献 14]。	强制性，适用于等级 1 及以上等级	业务	策略

3 参考文献和缩略语

3.1 参考文献和标准

本文件提述的参考文献来源于以下组织、出版物和/或标准：

- 3GPP（第三代合作伙伴项目）
- CSA（云安全联盟）
- DoD（美国国防部）
- ENISA（欧盟网络与信息安全局）
- ETSI（欧洲电信标准协会）
- EU（欧盟）
- FIPS（美国联邦信息处理标准）
- GSMA（GSM 协会）
- IETF（互联网工程任务组）
- IoTSF（物联网安全基金会）
- ISO（国际标准组织）
- JTAG（联合测试行动组）
- NCSC（英国国家网络安全中心）
- NIST（美国国家标准与技术研究所）
- OWASP（开放式 Web 应用程序安全项目）

本文件使用的参考文献如下所示。

1. NIST Special Publication SP800-57 Part 3 Revision 1” NIST Special Publication 800 – 57 Part 3 Revision 1 Recommendation for Key Management Part 3: Application – Specific Key Management Guidance” January 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdfhttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
2. NIST Special Publication 800-131A Revision 1 ”Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” November 2015
3. NIST Special Publication 800-90A Revision 1 “Recommendation for Random Number Generation Using Deterministic Random Bit Generators” June 2015
4. Special Publication 800-22 Revision 1a “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” April 2010
5. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
6. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 CCMB-2012-09-001 CCMB-2012-09-003
7. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002
8. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4
9. Draft Framework for Cyber-Physical Systems; NIST; October 2016

10. UK Government advice on Password Guidance, Simplifying your approach, CESG and CPNI Sept 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf
11. DoDI-8500.2 IA Controls: http://www.dote.osd.mil/tempguide/index.html
12. NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, NIST, April 2010: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
13. Key definitions of the Data Protection Act, ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions
14. Overview of the General Data Protection Regulations (GDPR), ICO: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr
15. Annex J (normative): List of Privacy Attributes and Clause 11 Privacy Protection Architecture using Privacy Policy Manager（PPM)

    http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
16. Example of IoT application id registry and possible privacy profile

    registry https://appid.iconectiv.com/appid/#
17. 3GPP TS33.117.Catalogue of general security assurance requirements produced by ESTI https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928
18. Cloud Security Alliance, Cloud Security Alliance is a not-for-profit organization promoting best practices for security assurance within Cloud Computing https://cloudsecurityalliance.org
19. IoTSF Compliance Framework, Compliance Checklist and Vulnerability Disclosure Guidelines can be found https://iotsecurityfoundation.org/best-practice-guidelines
20. NIST National Institute of Standards and Technology www.nist.gov
21. NIST Cyber Security Framework https://www.nist.gov/cyberframework
22. Octave, programming language https://www.gnu.org/software/octave/
23. UK Cyber Essentials: UK government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks https://www.cyberaware.gov.uk/cyberessentials
24. UK Government Cloud Security Principles is for consumers and providers using cloud services https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
25. IETF – RFC2119 “Key words for use in RFCs to Indicate Requirement Levels” https://www.ietf.org/rfc/rfc2119.txt
26. NIST SP800-63b Revision 1” NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management” June 2017 https://pages.nist.gov/800-63-3/sp800-63b.html
27. ENISA “Algorithms, Key Sizes and Parameters Report – 2013” https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report
28. IETF RFC7525 “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)” https://tools.ietf.org/html/rfc7525
29. SSL Labs “SSL-and-TLS-Deployment-Best-Practices” 31 March 2017 https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
30. OWASP “Transport Layer Protection Cheat Sheet” https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
31. OWASP Certificate and Public Key Pinning https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

32. NIST Special Publication 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations” – SC-5 Denial of Service Protection

    https://nvd.nist.gov/800-53/Rev4/control/SC-5

33. NIST 800-53, Revision 4, “Security Controls and Assessment Procedures for Federal Information Systems and Organizations” - SI10 Information Input Validation

    https://nvd.nist.gov/800-53/Rev4/control/SI-10

34. NIST Special Publication 800 – 167 “Guide to Application Whitelisting”

    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

35. NIST SP 800-37 Rev. 1 “Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach Risk Management Framework” https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final or Otave from ENISA https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

36. Supply Chain of Trust by Hayden Povey of Secure Thingz and the IoTSF http://www.newelectronics.co.uk/article-images/152099/P18-19.pdf

37. Static Code Analysis Tools https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

38. Bluetooth Numeric Comparison https://csrc.nist.gov/publications/detail/sp/800-121/rev-1/archive/2012-06-11 page 14

39. UK Government Cyber security risk assessment guidance https://www.ncsc.gov.uk/guidance/risk-management-collection

40. NIST Special Publication 800-30 guidance for conducting risk assessments https://www.nist.gov/publications/guide-conducting-risk-assessments

41. EU ENISA guidance of Cyber Security Risk Management https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

42. Security Policy ISO/IEC Standards for Vulnerability Disclosures ISO/IEC 29147 and ISO/IEC 30111 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip and https://www.iso.org/standard/53231.html

43. Enhanced Privacy standard for Anonymous Signatures ISO/IEC20008 https://www.iso.org/standard/57018.html

44. IoTSF Best Practice Guidelines for Connected Consumer Products V1.1 https://www.iotsecurityfoundation.org/best-practice-guidelines/#ConnectedConsumerProducts includes at time of publication individual guidelines for the following topics:

    A. Classification of data

    B. Physical security

    C. Device secure boot

    D. Secure operating system

    E. Application security

    F. Credential management

    G. Encryption

    H. Network connections

    J. Securing software updates

    L. Logging

L. Software update policy

45. CIA Triad has no original source , but for more info visit: https://www.techrepublic.com/blog/it-security/the-cia-triad
46. Examples of security vulnerability advisory programs: https://www.us-cert.gov/report and https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy
47. Example of memory sensitization:

    SEI CERT C Coding Standard Recommendation MEM03-C: “Clear sensitive information stored in reusable resources” https://wiki.sei.cmu.edu/confluence/display/c/MEM03-C.+Clear+sensitive+information+stored+in+reusable+resources

    ISO/IEC TR 24772:2013 “Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use”

    “Sensitive Information Uncleared Before Use”

    https://www.iso.org/standard/61457.html Other references:

    MITRE CWE-226 “Sensitive Information Uncleared Before Release” https://cwe.mitre.org/data/definitions/226.html

    CWE-244 “Improper Clearing of Heap Memory Before Release ('Heap Inspection')” https://cwe.mitre.org/data/definitions/244.html
48. NCSC password guidance https://www.ncsc.gov.uk/guidance/password-collection
49. Privacy Impact Assessment advice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ and https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
50. NCSC guidance on TLS management https://www.ncsc.gov.uk/guidance/tls-external-facing-services
51. WPA - Wi-Fi Protected Access is the name given to wireless security standard IEEE 802.11i-2004 https://standards.ieee.org/standard/802_11i-2004.html

3.2 定义和缩略语

就本文件而言，以下缩略语适用。

3.2.1 定义

匿名	**在符合市场需求的情况下，所有权转让时需要匿名身份。欧盟数据隐私或德国隐私条例适用。**
应用程序	应用程序（也称为最终用户程序）是指用于执行一组协调功能或任务的软件程序，这些功能或任务可能因安装或型号而异。物联网应用的示例包括网络浏览器、传感器管理或执行器控制器。这与系统软件不同，系统软件执行设备中主处理器的操作软件。
身份验证	身份验证是指识别身份的过程。它是一种将传入请求与一组标识凭证相关联的机制。提供的凭证将与设备或身份验证服务中的凭证一起检查。

启动	设备开机时使用的初始进程，旨在使系统做好运行准备（通常包含低级安全启动步骤）。
消费者	是指将物联网设备和/或服务用于个人用途的最终用户，但不一定是购买者（商品或服务分销链中的最终用户）。
部署	将产品投入客户试用或服务中。
加密	使用公认的算法和受保护的密钥确保数据安全，以致其仅在解码后才有意义，并且只能由有权访问相关算法和密钥的人解码。
企业	以商业或非营利为目的，共享信息技术资源的商业组织。
固件	存储在硬件中的计算机程序和数据 – 通常存储在只读存储器（ROM）或可编程只读存储器（PROM）中 – 因此在程序执行期间不能动态地写入或修改程序和数据。
物联网产品类别	一类网络产品，所有这些产品都会为该特定物联网产品实现一组公共的 IoTSF 定义功能。
交互式帐户	交互式帐户包括允许基础结构变更的非个人帐户，如根帐户、管理员帐户、服务帐户、批帐户、超级用户帐户或特权帐户。
相互身份验证	相互身份验证是指在通过连接发送任何敏感数据之前，通信链路中的两个实体相互验证对方的来源和完整性的安全进程或技术。 在网络中，客户端会对服务器进行身份验证，反之亦然。它是某些协议中的默认身份验证模式。 SSH，请访问 https://tools.ietf.org/html/rfc4250），在其他协议中是可选的身份验证模式：TLS，请访问 https://tools.ietf.org/html/rfc8446。
Nonce	Nonce 是术语“使用一次的数字”的缩略词。它通常是身份验证协议中发出的随机或伪随机数，以确保旧通信消息在重播攻击中不能再次使用。
操作系统	操作系统（OS）是指管理设备硬件和软件资源，并为软件程序提供公共服务的系统软件
加入	将设备注册到其服务或解决方案中，以启用设备注册[参考文献 16]、配置和数据传输的方法。
所有权转让	如果设备通过供应链转移，并更改所有者，此方法可确保可靠和安全的所有权转让。
个人信息	个人信息由欧盟一般数据保护条例（GDPR）定义： https://ec.europa.eu/info/law/law-topic/data-protection_en。 “个人数据”是指与已识别或可识别的自然人（“数据主体”）有关的任何信息；可识别的自然人是指可以 直接或间接识别的自然人，特别是通过参考标识符识别，如

	姓名、识别号码、位置数据、在线标识符或一个或多个该自然人特定的实际、生理、遗传、心理、经济、文化或社会身份的因素。
安全启动	确保设备仅启动受 OEM 信任的软件的进程。
安全协议	在注册和所有权转让过程中安全可靠地交换信息的方法。
软件	除非另有明确说明，否则在本文件中，术语软件还包括产品中的任何固件元素。
强验证	基于使用以下两个或多个要素的程序 - 归类为知识、所有权和内在性： i) 仅用户或设备知道的东西，例如静态密码、代码、个人识别号； ii) 仅用户或设备拥有的东西，如令牌、智能卡、移动电话； iii) 用户或设备特有的东西，例如生物特征，例如指纹。 此外，选定的要素必须相互独立，即违反其中一个要素不会损害另一个要素。其中至少有一个元素应该是不可再次使用且不可复制的（固有的除外），并且无法通过互联网秘密窃取。强验证程序的设计应保护所定义的身份验证数据的机密性，其他示例包括 NIST 特别出版物 800-63B[参考文献 26]和欧洲中央银行：关于互联网支付安全的建议 http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf?95e6bba1ef875877ad3c35cf3b12399c
信任供应链	如果物联网系统使用具有多个来源的设备或服务组件，则所有来源均可证明其符合本框架的相关要求。这将导致物联网系统中的设备和服务具有以下属性： • 产生可靠的信任根和安全身份 • 从源头保护应用程序代码 抑制灰色制造并保护 IP • 确保仅对有效的应用程序进行编程 • 集成可靠的密钥结构，以便进行所有权委托 • 启用生命周期更新和修补
防篡改证据固定	产品外壳设有保护措施，以确保任何未经授权的打开尝试都会留下尝试证据，例如，在产品外壳接缝处贴上标签，以确保接缝在受到扰动后碎裂。
防篡改	产品外壳设有防护措施，以防未经授权打开。通过使用专用紧固件或其他需要使用产品独有的专用工具的功能实现。

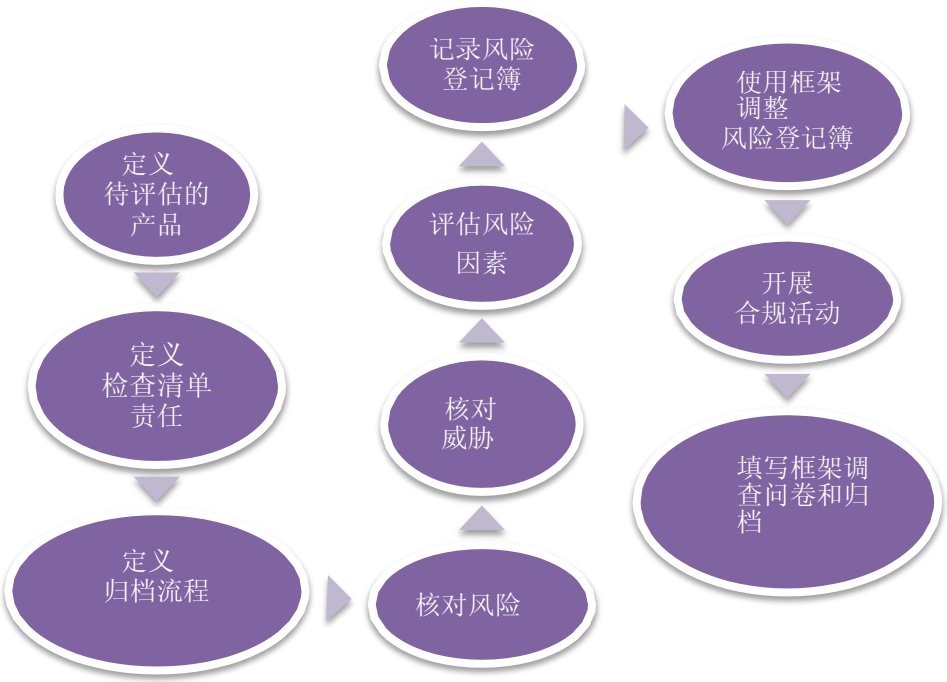
3.2.2 缩略语

CoAP	受限应用协议
DDoS	分布式拒绝服务
DTLS	数据报传输层安全
EAL	评估保证级别
ERP	有效辐射功率
HTML	超文本标记语言
HTTP	超文本传输协议
IP	互联网协议
MD	消息摘要
MQTT	消息队列遥测传输 - ISO 标准 ISO/IEC PRF 20922 OEM 原始设备制造商
PRNG	伪随机数生成器
SHA	安全哈希算法
SSH	安全套接外壳
TRNG	真随机数生成器
TBC	待确认
TBD	待定
TCP	传输控制协议
TLS	传输层安全性
T3P	可信第三方
UDP	用户数据报协议
URL	统一资源定位器
WPS	Wi-Fi 保护设置

附录 A 风险评估

1. 风险评估步骤

安全流程的核心是了解受保护的内容及其来源。识别不受保护的内容也很重要。完成该程序的方法有很多，但建议使用众所周知的最佳做法、风险管理标准[参考文献 39、40 和 41]。风险管理技术也可以在若干常见的商业培训出版物中找到。风险评估过程的概要如以下流程图和项目符号列表所示：



- 创建产品的安全风险列表
    - 使用头脑风暴技巧、思维导图或其他团队创造力技巧。
    - 生成涵盖业务和技术威胁的列表：
        - 例如，“负面宣传导致品牌形象受损”、“产品召回成本”、“产品暴露用户 Wi-Fi 凭证”
        - 如果安全性受到损害，则会影响到用户的产品的安全特性
        - 本框架可用于通过考虑合规等级标准来支持创建风险列表
- 评估风险列表中每个项目发生的“概率”
- 评估风险列表中每个项目的“成本”（在可检测性和恢复方面的影响）- 如果发生

- 把成本乘以概率，即可得到“危险系数”
- 按“危险系数”整理列表。这可能是一个百分比，也可能只是概率x影响

此列表将成为“风险登记簿”文件，然后可用于指导和充分论证解决产品安全性问题所需的工作。该工作旨在将风险“概率”因素降低到可接受的水平。

简化风险登记簿示例

威胁 高=H，低 =L	概率	影响/成本	危险系数
加密和密钥管理威胁	L	H	LH
Web 用户界面威胁	H	H	HH
移动应用程序威胁	L	L	LL
隐私威胁	L	H	LH

2. 安全目标和要求

下一步是确定产品的安全目标和非安全目标。危险系数高且需要通过设计降低风险的项目通常被视为安全目标，危险系数低且没有理由证明需要设法降低风险的项目被认为是非安全目标。每个目标都必须清楚说明需要保护的资产和相关威胁。任何被排除在外的目标也应予以说明和解释，以表明其已得到考虑。

然后根据安全目标制定安全要求。两者之间的主要区别在于，安全目标规定了需要保护的内容，而安全要求是实现所需保护的手段。安全要求文件是产品开发生命周期中的一个重要里程碑，应在设计开始前准备就绪。

3. 安全要求设计和实现

安全要求文件可以为设计和验证团队提供信息。安全特性的设计方法与常规功能要求的一般设计方法没有区别。但是，验证方法并非如此。功能要求验证的目的是验证系统是否能够正确地完成其设计目标。安全验证还应尝试模拟非法或意外情况（例如写入寄存器中的保留位或应用不正确的通电顺序），并验证系统行为是否可预测，以及安全资产是否不会受到损害。

www.iotsecurityfoundation.org