情况纷繁复杂：开发互联产品的五大挑战

互联生态系统研究报告

UL Solutions

Safety. Science. Transformation.™

物联网 (IoT) 以其连接性改变了世界，这已不是什么秘密。从智能手表等简单的物件到在所有区域都配备传感器的智能城市，物联网自动化使我们所有人受益。

然而，研究表明，物联网市场的发展速度比分析师预测的要慢。鉴于其巨大的潜力，这怎么可能？

以下是制造商在开发互联产品时面临的主要挑战。

将

智能

功能添加到对象后，
复杂性列表就会增加。

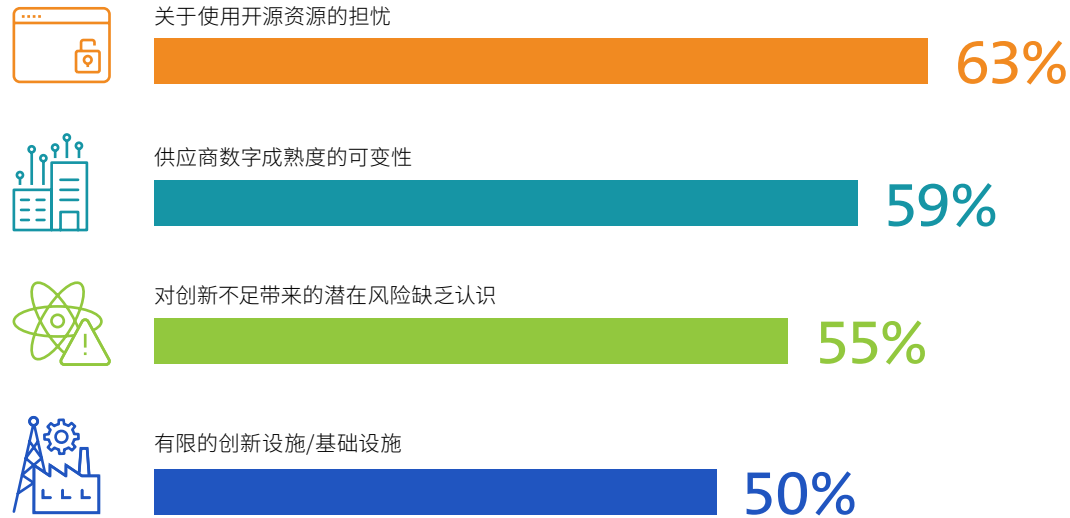
什么是物联网？

物联网是指具有至少一个可以通过交换或无线网络连接的物理组件的功能集合。其中包括物理组件、设备的各种计算元素内的常驻软件，以及驻留在移动应用程序或云实例中的任何软件。

挑战 #1
开发互联产品比看起来更难

物联网创新可能看起来很容易，但将联网产品推向市场可能比您想象的要困难得多。凭借无数的技术、设备、应用程序和管理平台，即使是一个设备的制造也可能很复杂。将物联网功能构建到互联产品中需要时间，并且需要组织重新考虑其当前的运营。

当被问及哪些挑战使组织无法追求更高水平的创新时，高管们表示：[1]



挑战 #2
产品功能在现实环境中会失效

制造商知道，物联网设备的数量、类型和用途每年都在扩大，但许多消费者的体验并不尽如人意。消费者担心，如果物联网设备进入其家庭和生活方式后发生故障，可能会造成致命的后果。请记住，人们购买的是解决方案，而不是产品，它们是互联解决方案生态系统的一部分。每个产品都需要与所有解决方案配合使用。

83%

的消费者担心由于性能问题而失去**对智能家居的控制。**[2]

62%

的消费者担心随着物联网的普及，**连接问题将会增加。**[2]

46%

的公司认为产品可靠性是技术购买决策**最重要的购买标准。**[3]

21%

的消费者由于设备的功能和用途有限放弃了**可穿戴设备。**[4]

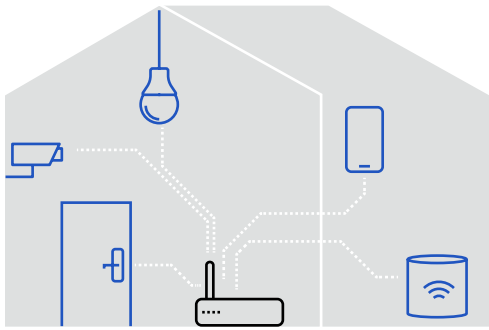
物联网技术可能达不到其所承诺的便利性，

三分之一的人

难以操作

其智能小工具。[5]

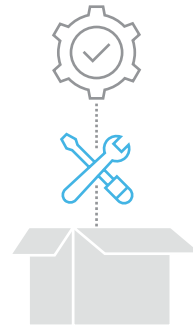
为何功能在现实环境中会失效



连接性
用于收集和路由目的的产品之间缺乏信令或双向通信可能会导致设备故障和用户沮丧。

始终询问:
设备是否无缝连接？是否保持互联？如果发生电涌，会快速重新连接吗？它是否以适当的速度无缝连接以进行数据传输？

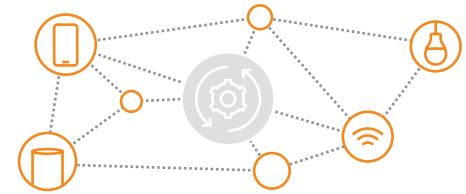
设备配置
许多产品仍然需要手动配置，用户可能会发现这有问题。随着互联生态系统的发展，自动配置成为必须具备的条件。



始终询问:
设备开箱即可轻松设置吗？

设备负载
由于互联产品的数量随着项目活动的增加而增加，服务器场成为处理大量数据的必要条件。

始终询问:
处理是否允许在产品和服务器之间无缝传输数据？



集成问题
互联产品应用程序通常与各种路由器、智能集线器或其他系统集成。

始终询问:
设备是否适应其互联生态系统中的操作系统升级、新应用程序和新设备？

操作环境
互联产品在各种环境和条件下运行。

始终询问:
用户会在什么条件下操作产品？

挑战 #3
网络安全风险在日常生活中根深蒂固

随着对互联系统频繁通信和共享数据的需求，对互联产品的攻击途径显著增加。网络攻击真实存在，任何互联产品（从冰箱到心脏起搏器）都可能面临黑客威胁。一旦网络犯罪分子获得控制权，他们可以在几秒钟内接管对象的功能或转向网络上的其他产品或系统。与其将安全作为事后的想法，不如将其嵌入到您构建产品的方式中。

通过数字了解一下为什么我们需要领先一步：

5 分钟
物联网设备上线后，一般需要多长时间会遭遇攻击[6]

38,182
仅在 2020 年 3 月，基于物联网的恶意软件尝试次数[8]

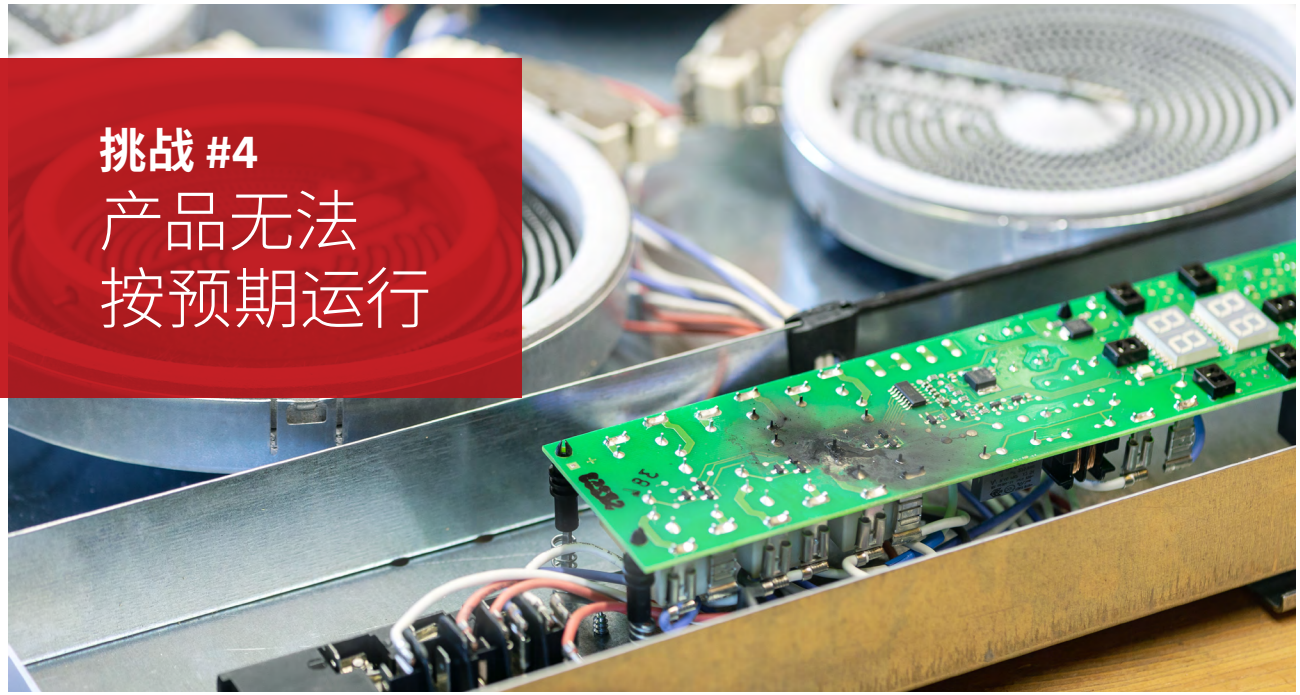
7 天
恶意软件攻击造成的平均时间成本[7]

38.6 亿美元
恶意软件攻击公司的平均成本
（包括客户流失率、客户获取增加、声誉损失和商誉受损）[9]

57% 的物联网设备容易受到中度或高度严重性的攻击，这使它们很容易成为攻击者的目标。[10]

互联系统和设备中的网络安全漏洞最常见的原因是产品设计和实施中缺乏安全最佳实践。最常见的原因通常属于以下五个方面之一：

- 糟糕的产品设计
- 不安全的通信协议
- 不充分的验证程序
- 有限的软件更新
- 不正确的实现或设备/应用程序使用



挑战 #4
产品无法按预期运行

风险管理对安全风险的看法

“随着自动驾驶汽车、工业物联网、智能家居等的兴起，技术故障有可能对人身和财产造成物理伤害。富有远见的公司应该确保他们承担这一日益增长的责任。”

Marsh & McLennan Companies

许多互联产品在金融技术、医疗技术和健康技术等敏感领域发挥着至关重要的作用，这些领域优先考虑人身安全和保护个人数据需求。产品到达客户面前的那一刻，必须完美无缺。功能不佳或管理不善的产品在最好的情况下会对品牌声誉产生负面影响，在最坏的情况下会伤害用户。安全不应仅限于最终产品；还应牢记安全的制造过程。

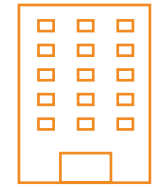
81%
的消费者表示他们需要能够信任一个品牌才能从其那里购买。[13]

50%
的最终用户越来越担心物联网设备对身体造成伤害的风险。[11]

42%
的高管预计，物联网故障的风险会随着复杂性的增加而增加。[12]

挑战 #5
监管合规的不确定性增加

随着全球监管机构对物联网的兴趣增加，不确定性也在增加。公司担心并期望监管优先于创新。当前的立法行动侧重于保护物联网设备和保护消费者隐私和数据。由于安全法规和要求可能因国家/地区而异，因此始终建议了解特定市场的法规。



66%

的公司正在预留资金以遵守法律和法规。[14]

40%

的高管预计，合规风险在未来三到五年内会变得越来越复杂。[15]

无论是网络安全、安全、互操作性还是无线，总有一个全球市场准入组成部分，因为不同国家的地区特定要求各不相同。

结论
对于互联产品，挑战在于复杂性

随着物联网采用的增长，实施解决方案、最佳实践和控制措施的重要性也越来越高，这些解决方案不仅可以保护设备的功能和安全性，还可以保护整个互联生态系统的功能和安全性。公司需要了解他们在制造、购买和使用什么。将连接性和安全性以及处理漏洞和管理生命周期和支持的流程结合到产品开发中至关重要。

要了解有关物联网互操作性和连接测试服务的更多信息，请访问 UL.com/IOP

最初需要考虑的问题

- 该产品将在哪里销售?
- 哪些标准适用于我的产品?
- 如何为消费者提供良好的用户体验?
- 如何减少连接问题?
- 如何检查以确保我的设备已连接、保持连接并提供其预期功能?
- 开发安全可靠的产品的最佳实践是什么?
- 什么级别的安全适合我的产品?

为何选择 UL Solutions?

UL Solutions 是全球应用安全科学专家，可为您的互联产品提供互操作性和网络安全测试和认证支持。我们可以帮助您评估产品与其他设备和主要连接/物联网平台和标准无缝运行。这可以帮助您向消费者提供可靠、安全和稳妥的互联产品，改善客户体验和品牌声誉。

- UL Solutions 帮助制定了 1,600 多项标准，用来界定产品安全、信息安全、质量和可持续性。
- UL Solutions 已经批准了许多物联网和无线标准机构的测试实验室，例如蓝牙® 特别兴趣小组 (SIG)、Thread 小组、连接标准联盟 (CSA) 和开放互联论坛 (OCF)。
- 我们能够为大多数互联产品、移动应用程序、Wi-Fi 重新连接的稳健性、功能、长期连接性能等执行真实世界互操作性测试。
- 我们可以开发定制的测试解决方案以满足您的特定要求。
- UL Solutions 是您的单一来源服务提供商，提供包括最终产品测试、认证和验证在内的一整套服务，可帮助您更快地进入目标市场。

请立即联系我们。

适用的服务包括以下方面的测试和认证：

智能助手
- 谷歌助手
- Amazon Alexa

连接标准和平台
- Samsung SmartThings
- Matter
- MFi
- Thread
- CSA (Zigbee)
- OCF
- 蓝牙®
- USB IF

无线移动设备标准
- 全球认证论坛 (GCF)
- PTCRB

网络安全标准和评级
- UL Solutions 认证的物联网设备安全等级[16,17]
- 《联网产品的软件网络安全标准》(UL2900-2-1)，第2-1部分：《医疗和健康系统的联网组件的特殊要求》
- 《联网产品的软件网络安全标准》(UL 2900-2-3)，第 2-3 部分：《安全和生命安全信号系统的特殊要求》
- IEC 62443

来源

1. UL Solutions。（2020 年 4 月）。新十年的创新和安全。
2. Dynatrace。（2018 年 8 月）。消费者信心报告。
3. Statista。（2020 年 9 月）。技术采购最重要的购买标准（新冠疫情背景下）。https://www.statista.com/statistics/1169718/worldwide-it-purchase-buying-criteria-covid/
4. Ericsson。（2019 年 9 月）。可穿戴技术和物联网。https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/wearabletechnology-and-the-internet-of-things/
5. ADT。（2019 年 8 月）。家是智能所在。
6. NETSCOUT。（2019 年 8 月）。恐怖时代的黎明。
7. Purplesec。（2020 年 2 月）。2020 年网络安全统计。
8. Symantec。（2019 年 4 月）。ISTR 2019：物联网网络攻击日趋多样化。
9. Purplesec。（2020 年 2 月）。2020 年网络安全统计。
10. 帕洛阿尔托。（2020 年 3 月）。第 42 单元物联网威胁情报报告。https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20 NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf
11. Marsh & McLennan Companies。（2018 年 10 月）。物联网：无限的连接和失败的方式。https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2018/dec/IoT--Limitless-Connections-and-Ways-to-Fail/Internet-of-Things_%20Limitless%20Connections.pdf
12. Marsh & McLennan Companies。（2020 年 3 月）。灾难性风险的新定义：技术产业风险研究。
13. Edelman。（2019 年 2 月）。Edelman 2019 信任度调查报告。
14. Marsh & McLennan Companies。（2020 年 3 月）。灾难性风险的新定义：技术产业风险研究。
15. Marsh & McLennan Companies。（2020 年 3 月）。灾难性风险的新定义：技术产业风险研究。
16. https://www.ul.com/resources/lot-security-rating-levels-guide
17. https://www.ul.com/services/ul-verified-iot-device-security-rating

UL Solutions

UL.com/IOP

CMIT22CS248552.4

回到第一页