量子时代的固件完整性

www.infineon.com/OPTIGA-TPM-SLB9672

目录

随着我们的生活更多走向数字化，安全性作为根本的社会需求，其重要性与日俱增。我们所生活的互联世界正在不断扩展，涵盖了越来越多的“物”，而这进一步推动了对安全的需求。空中下载技术（OTA）给这些“物”的更新带来了明显的好处——但由于可能会被注入恶意代码，致使信息落入第三方的掌控，因此，它也存在相应的风险。

对此，加密技术（包括与 TPM 等硬件设备结合使用的公钥和私钥）提供了强大的安全性，它让用户确信这些攻击的可能性大大的降低了。

然而，随着对量子计算机（利用量子力学现象，解决传统计算机难以应对的数学挑战的机器）研究的深入，情况正在发生转变。量子计算机利用其强大计算能力，将能够破解当今常用的公钥密码，从而严重影响各种形式的数字通信的机密性和完整性。

在本技术白皮书中，英飞凌将着眼于量子计算所带来的威胁，探讨如何发展密码学才能在后量子世界提供安全性和可信度。

量子计算机带来的威胁

量子计算机是一种强大的新型计算设备，它利用量子力学现象，解决传统计算机难以应对的数学挑战。量子计算机使用一组被称为“qbits”的量子位，在一个量子硬件上就能执行计算速度呈指数级增加的并行计算。

目前，量子计算技术的颠覆性已得到证明——至少在小规模上得以证明。在实践中，学术界和工业界的持续研发虽然进展缓慢，但量子计算机的数量仍不断增多。尽管当前规模有限，但专家普遍认为，通用量子计算机将在 2040 年左右问世。目前，量子计算得到了大量资金支持，其中包括来自欧盟的 10 亿欧元和德国的 6.5 亿欧元，而美国已拨款 12 亿美元，用于推动美国的量子技术发展。据研究公司 ResearchAndMarkets 估计，到 2025 年，量子计算的硬件市场规模将超过 60 亿美元。

从积极的角度来看，大规模的量子计算将有助于人工智能、化学模拟、优化和密码学等方面取得突破；然而，这些机器对当前的加密算法又具备潜在破坏性，这给计算机和互联网安全带来了全球性的威胁。

使用一台合适的量子计算机，就可以通过 Shor 整数分解算法，完全破解目前的主流非对称加密系统（特别是 RSA 和 ECC）。早在 2001 年，IBM 和其他公司就演示了这项当时尚处于相对简单层次的技术。RSA 基于大整数分解计算难度大的假设，虽然这对于非量子计算机仍然是有效的，但通过 Shor 算法可以看出，一台理想的量子计算机可以非常有效地进行整数分解。增加这些算法的密钥长度等缓兵之计并不会显著提高其安全性，因此，这意味着需要使用新的非对称算法和/或替代的非对称算法。

另外，量子计算技术对大多数对称加密算法的影响并没有那么大。目前，最知名的攻击要数 Grover 密钥搜索算法，该算法由 Lov Grover 在 1996 年设计。对比其他量子算法（这些算法与经典算法相比实现了指数级的加速），Grover 算法仅提供了二次加速；但它可以在大约 264 次迭代中，暴力破解一个 128 位的对称加密密钥；或者在大约 2128 次迭代中，破解一个 256 位密钥。

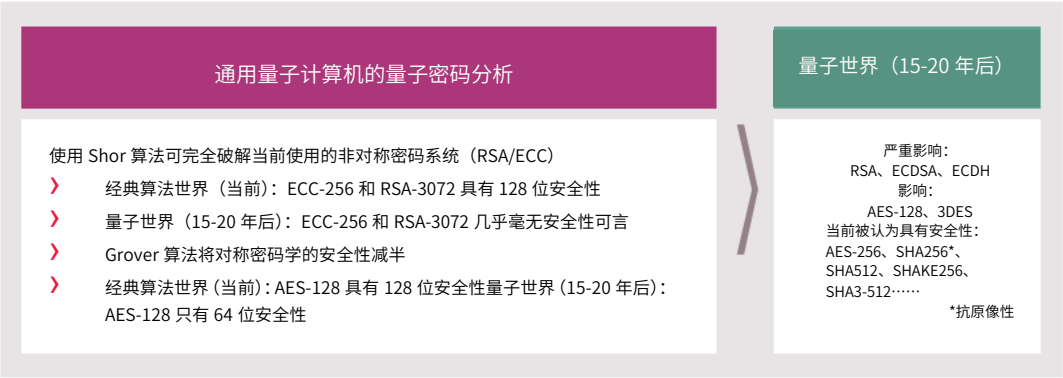

图 1：量子计算技术对当前的加密系统造成重大威胁，特别是非对称加密系统

Grover 算法会导致 AES、SHA-2 或 SHA-3 等常用对称算法的位安全性减半。因此，可以认为 AES-256 和 SHA-256 依然具有适当的安全性。

为何需要现在采取行动?

从时间进程上看，这一威胁看似还很遥远，而且考虑到高成本，量子计算机不太可能普及，所以，从某种程度上说，似乎没有紧迫的必要。当然，对于智能手机、平板电脑和银行卡等许多消费类设备而言，其预期的使用寿命短于我们所讨论的时间范围，因此，乍看上去，并没有什么紧迫性——当前产品在量子计算机问世之前，早已被淘汰。

然而，应该注意的是，所有使用当前加密方案进行加密的数据，都有可能在未来的某个时间点被存储和解密。这意味着，即使是今天的某些数据，在将来也可能面临风险。此外，一些投入巨资的设备，比如某些与国家基础设施（发电站、空中交通管制、大型工厂）相关的设备，预计在量子计算机部署后仍将运行。现代车辆正在越来越多地支持联网以接收 OTA 更新，以及车辆-基础设施互联系统（V2I）和车对车通信（V2V）的更新，这带来了许多潜在的被攻击面，其中一些攻击甚至可以控制车辆。因此，这些车辆正处于风口浪尖之上，而其使用寿命预计为 15 年左右，因此它们也迫切需要解决后量子世界的安全问题。

目前，威胁正在“浮现”，因此，有很多工作要做，特别是在安全标准领域。这些威胁就像计算机病毒一样，将逐渐调整和发展。这意味着，不会有“全面”的解决方案，但企业——特别是所生产的产品预计在 2035 年以后运行的公司——需要立即采取行动，尽可能地降低风险。

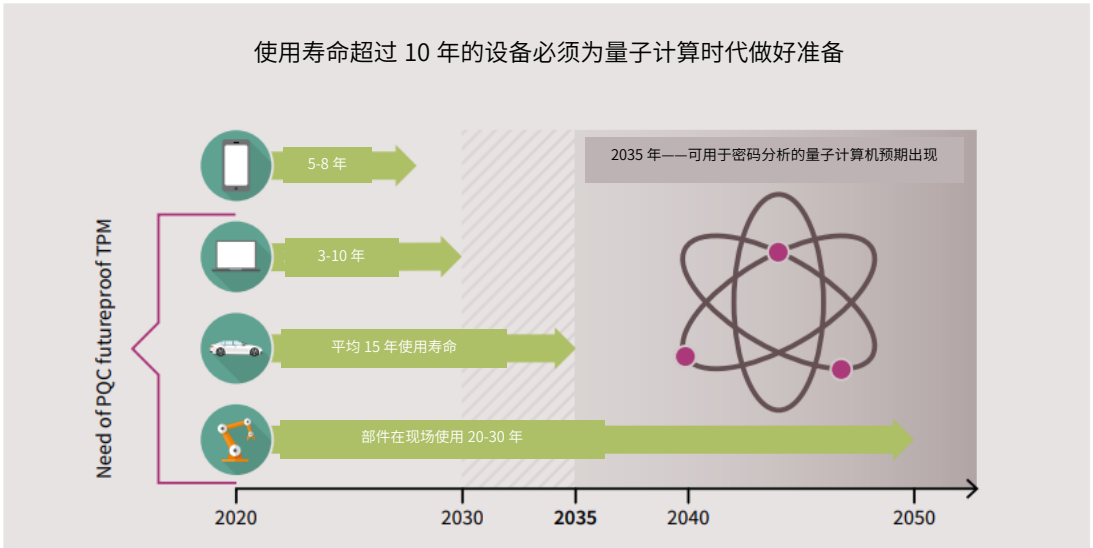

图 2：现在就采取行动，这一点十分重要，特别是那些需要部署数十年的大型基础设施

制定后量子计算标准

2017 年，美国国家标准与技术研究院（NIST）启动了一项长期进程，旨在为后量子计算（PQC）世界制定出统一的安全标准。与 AES 和 SHA-3 采用的方法类似，NIST 征集了有关量子安全的公钥加密、密钥交换和数字签名的方案——不过这一次的范围要更广。

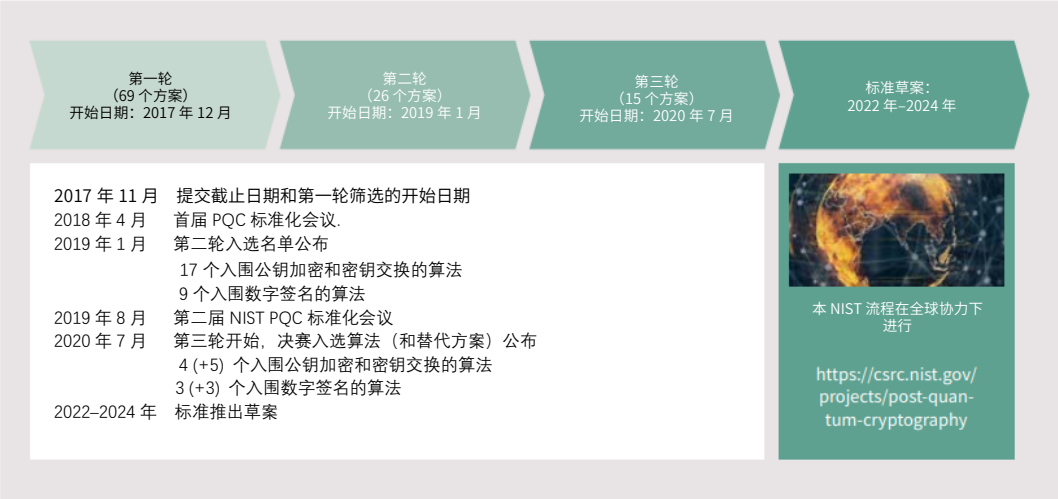

图 3：NIST 正在率领各方为 PQC 世界制定安全标准

NIST 在第一轮中总共收到了 69 份方案——尽管其中很多方案因为在短时间内架构完全遭到破坏或被攻破而被驳回。在 2018 年 4 月的 PQC 标准化会议后，NIST 选出了最有希望的 26 个方案进入第二轮。

这些方案的作者可以在两轮比赛之间合并或修改提交的方案，以便从在此过程中获得的专业知识中受益。

2019 年 8 月，NIST 召开第二次标准化会议，并于 2020 年 7 月宣布了入选第三轮（也是最后一轮）的 15 个方案。由于许多方案速度较慢，而且对处理水平要求高，NIST 也会评估软件和硬件所能实现的性能。

最后一轮的竞争中包含了许多非常有希望的候选算法。但目前，还没有完全决定 NIST 将会选择一个获胜方案，还是会提出将几种替代方法标准化。他们预计将在 2024 年之前交付标准草案——不过为了跟上量子计算的发展步伐，该倡议可能还会继续下去。

由于该过程仍在进行中，而且尚未达成共识，因此，如果今天需要一个 PQC 方案的话，我们还不清楚应该选择哪种算法。但是，有状态的基于哈希的签名可能是一种临时解决方案。

有状态的基于哈希的签名

基于哈希的签名（HBS）是我们目前很容易实现的非对称后量子加密方案。HBS 依赖于众所周知的哈希函数的原像抗性，并且被认为比 RSA 和 ECC 所使用的假设更具健壮性。不同于 RSA 和 ECC 的另一个主要区别是，大多数 HBS 是有状态的，这意味着使用私钥生成的签名数量是有限的，因此，需要跟踪以前使用的密钥。

基于哈希的签名可以追溯到 1979 年，最近的两个有状态的 HBS 方案 LMS 和 XMSS 分别于 1995 年和 2011 年发布。这两个方案由 IETF 在 RFC 8554 和 RFC 8391 中标准化，随后，在 2020 年 10 月，NIST 根据 RFC 中的参数子集，最终确定了其 PQC 标准 SP800-208。

LMS 和 XMSS 使用的主要哈希函数是 SHA-256 或 SHAKE256，它们提供了具有 128 位后量子安全性的 HBS。得益于最小的参数集，这两种方案的签名大小约为 2.5 kB，公钥约为 60 字节。私钥的大小取决于用于签名的性能权衡，这是因为更快的算法会将私钥大小增加到几 kB。

在嵌入式设备上，验证需要几百毫秒，而签名需要几秒钟。生成密钥则可能需要几分钟甚至几小时，具体取决于所需签名的数量。对此，加密哈希加速器可以显著提升性能。

HBS 有很多优点，其中，最值得注意的是它被认为是抗量子的，因此是面向未来的。但主要缺点在于其状态性，这是因为对多个不同的消息重复使用相同的私钥，意味着该方案会被轻易地破坏。因此，谨慎的状态管理必不可少，在相应的签名被释放之前，任何使用过的私钥都需要被可靠地停用。

图 4：基于哈希的签名包含许多有益特点

从性能的角度来看，密钥生成是最关键的步骤，因为在这一步，必须计算一个巨大的哈希树，来确定公共根密钥，而由于参数不同，公共根密钥可能会导致数亿次哈希计算。如果没有实现时间和内存的权衡，则签名生成也是如此。实际上，签名算法会重复使用密钥生成过程中存储的中间结果，尽管这确实会增加私钥的大小。

有状态的 HBS 是嵌入式平台的理想之选，正如 2012 年在 16 位英飞凌 SLE78 智能卡上实现的 XMSS 初步修订版。由于验证速度快且不涉及机密，因此在资源受限的设备上实施是可行的。签名算法也非常适用于嵌入式设备，特别是那些具有安全控制器的设备，其私钥和使用的私钥的状态可以得到安全地控制。

在研究有状态的 HBS 的属性时，显然，这些 PQC 方案非常适用于固件更新——特别是因为它们是目前唯一标准化的非对称 PQC 算法。

TPM 的作用是什么?

由于标准硬件尚未针对安全应用进行优化，因此，典型的嵌入式处理器往往容易受到攻击。复杂的主机软件与安全代码在同一处理器上执行，而且会不可避免地共享内存等资源，从而使系统容易受到威胁和漏洞的影响。考虑到物理攻击时，情况就更加紧急了，因为物理攻击被认为非常容易被实现。这些攻击可能包括“微探测”芯片、观察电源的使用情况，或仅通过注入峰值，来改变操作并揭示代码执行中的弱点。

加入专用安全处理器可防止上述类型的攻击。安全处理器有自己的专用资源，包括允许代码完全在内部执行的受保护内存，这消除了软件方法存在的一些关键漏洞。此外，它旨在安全地存储敏感数据，而且为保护芯片内部的数据不被外部世界访问，其硬件得到了优化。

尽管这种方法增加了一个组件，但却也大幅实现了简化，这是因为安全代码是完全独立的，不必“混入”一般操作代码中，也不必在共享资源上执行。

可信平台模块（TPM）就是一个很好的例子。多年来，这些器件已成功地用于为 PC 提供安全性，而且在嵌入式系统中也愈发普遍。TPM 可以被视为系统内部的“安全性”，这是因为它能够抵抗逻辑和物理攻击——其屏蔽环境可以保护保密数据和加密机密。

TPM 支持多种用例，其中包括基本设备身份验证和通过远程验证保护系统的完整性。这些功能提供了高度的灵活性，从而实现了动态的安全增强方法。“即时”更新可用于添加嵌入式系统所需的、更高级别的未来保护，从而使基于 TPM 的系统能够满足短期安全要求并应对新的用例。

显然，从目前的经典计算世界向 PQC 世界转型将是一段艰苦的旅程，在确定应对方法的同时，为目前设想的威胁制定相关标准的工作也在同步进行中。

应用的安全性无法高于固件更新机制的安全性——换言之，如果固件更新脆弱，则整个系统都将脆弱——因此，目前，HBS 标准将被应用于固件更新机制。

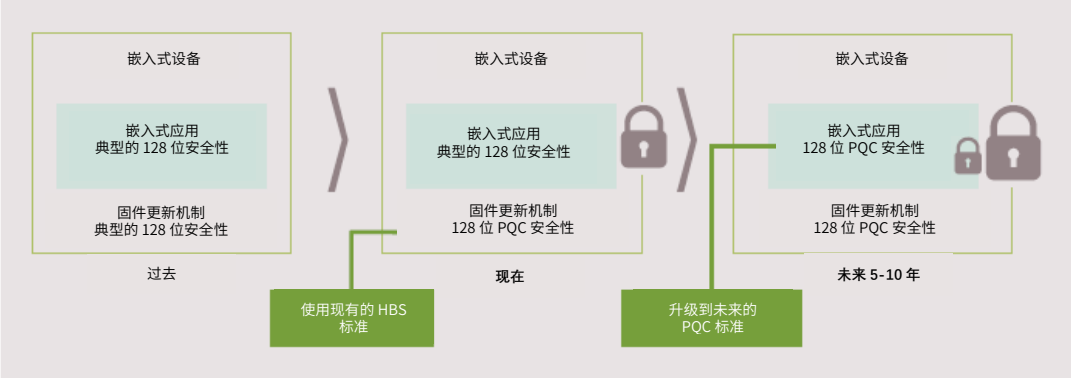

图 5：现在使用 HBS，将能使关键的固件更新免于量子计算的影响

展望未来，随着 PQC 标准的制定和公布（由 NIST 和其他类似机构进行），这些标准将被应用于嵌入式应用，从而为整个嵌入式系统提供 128 位的 PQC 安全。

适用于 PQC 世界的 TPM

英飞凌的 OPTIGA™ TPM SLB 9672 包含一个受 PQC 保护的固件更新机制，这是首款经过独立安全评估和认证、符合 CC 国际标准的器件。事实上，这款新器件是可信计算组织（TCG）列出的官方 TPM 产品，符合其 TCG 2.0 rev. 1.59 规范。

此外，OPTIGA™ SLB 9672 满足即将于 2023 年 4 月生效的 Microsoft Windows 的要求，并符合全新 NIST 标准 SP 800-90B。FIPS 140-2 认证仍在进行中。

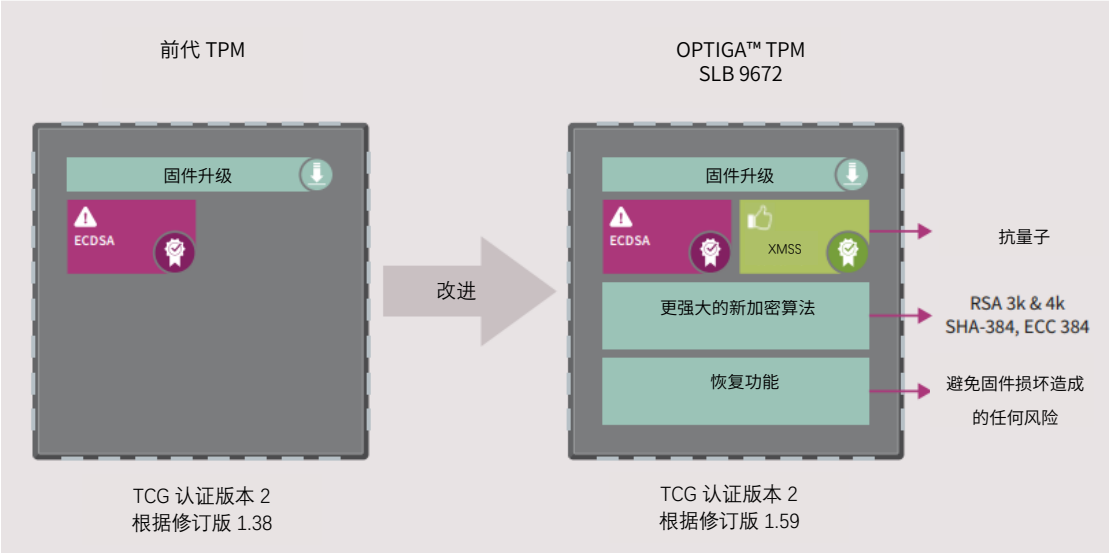

图 6：全新 OPTIGA™ TPM SLB 9672 提供特定的抗 PQC 功能

该全新器件具有许多重要功能，包括更强大的新加密算法，例如 RSA 3k 和 4k、SHA-384 和 ECC 384。OPTIGA™ SLB 9672 的固件更新机制能够处理 XMSS 签名，因此具有量子抗性，而且还具有很多额外的恢复功能，能避免固件损坏的风险。

现在，英飞凌更新授权能够处理 XMSS 密钥的状态性，从而提供安全的固件更新操作，实现了明确的业务连续性。在实际使用过程中，OPTIGA™ SLB 9672 能够透明地检查 XMSS 签名，来验证被传输的数据。

OPTIGA™ SLB 9672 满足严苛应用的要求，其工作温度范围高达-40°C 至+85°C。它目前支持 192 位的密钥长度——不过，即将通过准备中的固件更新扩展到 256 位。

该器件包括三条 GPIO 线和一个 51 kb 非易失性用户存储器，可用于存储密钥或数据。

新 TPM 的应用范围包括服务器和 PC，以及通用计算和数据存储。它还将支持丰富的网络基础设施，包括网关、路由器、无线接入点、网络接口卡和交换机。OPTIGA™ SLB 9672 与 Intel x86、ARM 等其他平台兼容。

英飞凌对 TPM 开发的支持

英飞凌的 OPTIGA™ TPM 2.0 Explorer 是一款基于 GUI 的工具，用户可以使用 Raspberry Pi®轻松、快速地熟悉 TPM 2.0。此外，该软件平台还展示了如何使用 OPTIGA™ TPM 2.0，来提高应用的安全性和可信度。使用该工具，设计人员可以体验 TPM 为智能家居设备和网络设备带来的优势。

设计人员也可以从该工具中受益，因为他们能够探索 OPTIGA™ TPM 2.0 的功能，只需选择按钮，就能调用相关功能或任务，来更快地学习用例。该工具提供即时的视觉反馈，以便审查命令运行和相应的响应。

设计人员可以使用该工具，初始化 TPM 2.0 并显示所有定义的属性，并在需要时全部复位。他们还可以管理非易失性存储器和处理 PCR 索引，以及定义系统如何进入锁定事件并从中恢复。

由于 GUI 工具功能全面、使用简单，因此不论用户的经验或知识如何，他们都可以访问和探索 OPTIGA™ TPM 的功能。

总结

量子计算可能构成重大的安全威胁，特别是对于能够接收远程固件更新的设备和系统。量子计算机凭借其惊人的计算能力，可轻松破解传统的非对称密码，并显著削弱对称加密密钥的安全性。

尽管量子计算机所带来的威胁，还需要十年或更久，但设计人员需要立即采取行动，特别是那些在量子计算时代仍将继续使用（并需要安全运行）的大型基础设施项目。设计人员面临的挑战是，如何应对尚未完全定义且标准仍在制定之中的威胁。

由于现有技术（比如，众所周知的有状态的基于哈希的签名）是基于哈希函数的抗原像性，已被证明可以在 PQC 世界提供保护。这意味着其至少可以使所有固件更新保持适当的安全性。

对此，TPM 提供了必要的硬件支持，英飞凌推出的 OPTIGA™ TPM 非常知名且备受推崇，它已集成到了全球一半的商用 PC 中。英飞凌于 2017 年开始研究 PQC 解决方案，而 OPTIGA™ TPM SLB 9672 就是其首批成果之一。这是世界上第一个具有受 PQC 保护的固件更新机制的 TPM，因此，它对实现 PQC 时代的数据安全大有裨益。

www.infineon.com

英飞凌科技股份公司印制
德国慕尼黑（81726）

文档号：B180-I0823-V2-7600-EU-EC-P
日期：08/2021

请注意！

本文仅用于提供信息之目的，在任何情况下，不得将本文件中提供的任何信息视为就我们的产品的任何功能、条件和/或质量，或产品适合任何特定用途做出的保证、担保或表述。关于我们的产品的技术规格，我们建议您参阅我司提供的相关数据表。我司希望客户及其技术部门评估我司产品是否适合既定的应用。

我司有权随时修改本文件及/或本文件包含的信息。

更多信息

若需获得有关我司技术、产品、产品应用、交付条款和条件，及/或价格的更多信息，请联系距离您最近的英飞凌科技办事处（www.infineon.com）。

警告

由于技术要求，组件可能包含有害物质。若需了解相关物质的类型，请联系距离您最近的英飞凌办事处。

除非得到由英飞凌科技授权代表签署的书面文件的明确同意，否则不得将我们的产品用于任何可威胁生命的应用，包括但不限于医疗设备、核设备、军用设备、对生命至关重要的设备，或任何其他产品失效或产品使用可导致人身伤害的应用。