白皮书

保障患者安全与数据：网络安全在医疗健康领域的关键作用。

silex technology

目录

引言：为什么网络安全至关重要?

无线联网的物联网设备的普及已全面渗透医疗设备行业。随着联网设备数量的激增，远程医疗设备访问带来的特殊风险使得先进网络安全协议的需求愈发凸显。医疗记录的未授权访问可能导致误诊、不当治疗或次优医疗服务，不仅存在患者隐私泄露风险，极端情况下更会直接危及患者生命安全。此外，此类安全隐患还会破坏医疗保险体系的完整性，并威胁医学科研知识产权的保护。

> 根据健康信息共享与分析中心（Health-ISAC）最新研究，
> 2022至2023年间医疗产品的网络安全漏洞激增59%。

健康信息共享与分析中心（Health-ISAC）最新研究显示，2022至2023年间，医疗产品的网络安全漏洞数量激增59%。医疗行业正日益成为勒索软件攻击的重点目标，据IBM估算，2023年医疗数据泄露事件的平均损失已超过1100万美元（约合人民币8000万元）。

在已发现的漏洞中，73%源于应用软件或设备操作系统，剩余27%与设备硬件相关。尽管硬件组件的可追溯性记录已成行业惯例，但设备软件层面的相关文档历来缺失或不完整。当前针对网络安全问题的应对措施，主要集中在全面识别医疗设备内所有软件组件，并主动评估这些组件的潜在漏洞。

应对网络安全问题的监管措施

2021年5月12日，美国总统签署第 14028 号行政令。该政令强调网络安全的重要性，并为向联邦政府销售的软件制定了必须遵循的基础安全实践标准。虽然行政令明确了网络安全标准化的必要性，但相关实施细则直至2024年2月美国国家标准与技术研究院（NIST）完成网络安全框架 (CSF) 2.0版才得以完善。该框架为设备制造商提供了一套可实施的网络安全风险管理流程。

欧盟正在制定新版《网络安全韧性法案》，预计将于2025年颁布。该法案将对申请CE认证（欧盟市场准入必需认证）的产品提出网络安全要求，其中包括须在24小时内上报通用漏洞披露（CVE）等规定。与此同时，日本经济产业省（METI）已发布《软件物料清单 (SBOM) 应用指南》，明确定义了SBOM的创建、维护及使用规范，以应对网络安全风险。

在网络安全监管要求不断变化的背景下，持续保持合规绝非易事。对于医疗器械制造商而言，选择能够持续监控通用漏洞披露（CVE）、联合专家评估漏洞严重性并及时发布安全补丁的合作伙伴至关重要。本白皮书后续章节将重点介绍Silex Technology公司的AMC Protect解决方案——该方案可有效助力医疗器械制造商确保网络安全合规。

对医疗器械制造商的影响

美国食品药品监督管理局（FDA）已向医疗器械制造商发布指南，明确要求在产品全生命周期（TPLC）中实施网络安全风险管理。其中，采用安全产品开发框架（SPDF）是管理全生命周期风险的核心方案。虽然SPDF存在多种实施方式，但其共同目标都是通过标准化流程，最大限度降低医疗器械在整个使用周期内的漏洞数量及危害程度。

符合FDA要求的典型合规框架案例当属ANSI/ISA 62443标准。尽管安全产品开发框架（SPDF）的实施涉及大量技术细节，但从宏观层面来看，遵循FDA网络安全风险管理建议可归纳为三大核心模块：安全风险管理、安全架构设计及网络安全测试。

安全风险管理——评估医疗设备及其运行网络/系统面临的安全风险，揭示通用漏洞披露（CVE）可能导致的患者伤害及其他网络风险。

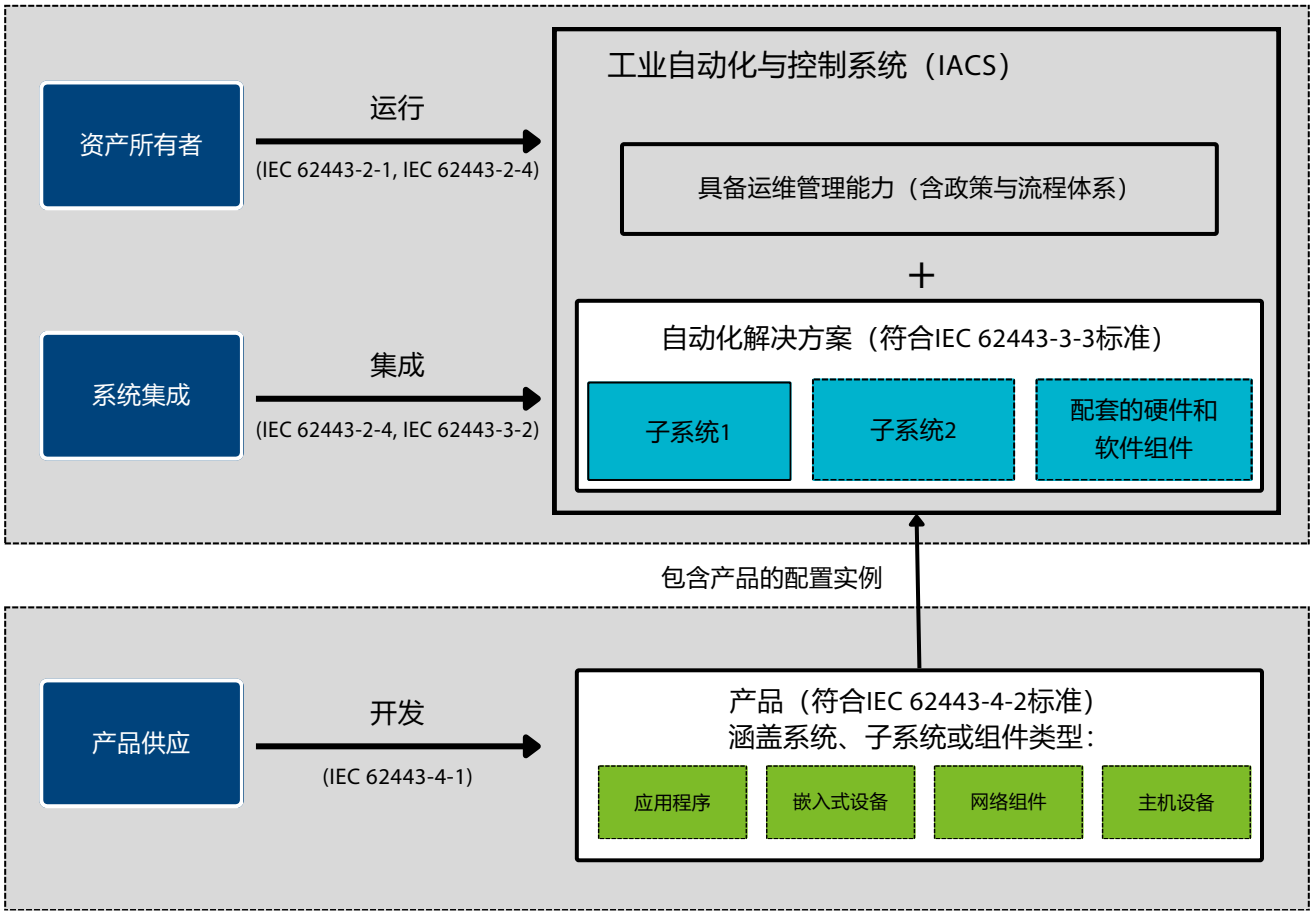
安全架构设计——明确定义医疗设备部署后的端到端连接方案，涵盖医院网络、云基础设施或其他联网设备等应用场景。

网络安全测试——全面检测设备输入输出端口，重点验证网络安全要素，以证明设计控制措施的有效性。

作为产品全生命周期（TPLC）管理的重要组成部分，医疗器械制造商现需编制、分发并维护设备软件物料清单(SBOM)，详细记录设备中的软件构成。除自主开发的应用程序外，SBOM还应包含操作系统、第三方库、第三方SBOM及集成设备固件等详细信息，确保所有软件组件均可溯源至原始出处。

制造商须承担维护产品SBOM准确性的责任，该工作始于软件开发周期之初，并贯穿产品整个生命周期。单个设备的SBOM需与网络系统中其他设备的SBOM进行整合关联，使相关方能基于特定通用漏洞披露（CVE）及时研判网络风险。

在产品完成部署后，制造商应定期开展测试与风险暴露评估。除常规设备测试外，还需运用二进制分析工具持续监控SBOM组件的漏洞情况。一旦发现漏洞，应立即启动既定的应急响应机制进行处理。



什么是数据安全与漏洞?

传统网络安全主要依赖物理安全作为第一道防线。无法通过物理方式接入局域网(LAN)的攻击者很难获取网络资产。然而，由于默认信任已物理接入LAN的网络资产，攻击者一旦绕过物理屏障就能获得无限制访问权限。

这一漏洞促使零信任网络访问(ZTNA)方案应运而生，该方案要求所有用户都必须经过身份验证，无论其物理位置或网络接入方式(有线或无线)。ZTNA在设备通过网络认证后管理资产访问权限，但不管理认证过程本身。与传统的物理线缆可能直接连接未受保护资产的有线网络不同，Wi-Fi连接提供了更多认证选项。

即便实施了零信任网络访问(ZTNA)，Wi-Fi传输信号的覆盖范围仍远大于有线局域网连接。黑客可远程窃听，甚至发现隐藏的SSID。Wi-Fi通过数据加密和密钥保护算法解决了这一安全隐患。

漏洞可能源于硬件、软件、固件或这些因素的组合。对用户的影响包括：设备完全失效、安全信息泄露、设备异常运行或遭受勒索软件攻击等。漏洞可由Silex直接发现，或通过芯片供应商、广泛市场客户及政府机构间接获取。一经确认，这些漏洞将被提交至CVE项目，经审核、分类后按标准编号规则归档。CVE项目作为中央枢纽，负责向相关方归档和分发漏洞信息。

美国国家标准与技术研究院(NIST)进一步开发了与国家漏洞数据库(NVD)同步的CVE清单。NVD采用安全内容自动化协议(SCAP)为CVE编号建立映射关系，从而支持自动化漏洞管理及网络安全政策合规。这一流程允许使用自动化工具监控新发现的漏洞、其影响严重程度及已知解决方案。

Wi-Fi如何保障数据安全?

大多数Wi-Fi用户都熟悉两种网络安全方式。第一种是无需认证的公共热点，允许任何用户接入和使用网络。第二种是家庭或小型企业网络，需要使用WPA2-PSK或WPA3-SAE预共享密钥才能接入。预共享密钥的局限性在于，任何知道密钥的人都可以通过网络认证，并获得相同的、无限制的访问权限。这两种场景都无法满足需要最高安全级别的网络。需要最高安全级别的Wi-Fi网络必须实施WPA3-Enterprise方案。该方法遵循802.1X标准，并要求为每个用户提供唯一的认证凭证。

> 要求最高安全级别的Wi-Fi网络必须实施WPA3-Enterprise方案。

WPA3-Enterprise为企业网络提供了一致的加密认证应用，可成功验证用户身份并保护网络流量。该方案实施验证流程，要求客户端设备在接入网络前必须验证认证、授权和计费(AAA)服务器证书。这一流程能防止中间人攻击，并通过网络管理员定义的传输层安全(TLS)证书策略，避免用户误接受未知网络证书。对于极高敏感度网络，WPA3-Enterprise可选配192位安全模式，该模式通过以下方式提升每个加密原语的工作因子：采用伽罗瓦/计数器模式协议(GCMP)实现认证加密，使用哈希消息认证模式(HMAC)进行密钥派生，通过椭圆曲线迪菲-赫尔曼(ECDH)交换完成密钥建立与认证。

部署WPA3-Enterprise是一项复杂的工作，而这正是Silex Technology区别于其他供应商的优势所在。Silex Technology不仅采用SoC厂商提供的参考驱动，更为企业级应用增添了显著的功能增强，例如在大规模市场BSP中原本不支持的漫游、认证和配置功能。Silex Technology拥有专业能力，可协助在嵌入式医疗设备中实施WPA3-Enterprise，即使目标设备不包含专用用户界面。仅使用"支持"WPA3-Enterprise的参考驱动是远远不够的，医疗设备制造商需要一个值得信赖的合作伙伴来协助实现这些高级安全功能。

> Silex Technology不仅依赖SoC厂商的参考驱动，还为企业级应用提供了重大功能增强。

Silex Technology解决方案：AMC Protect

为帮助医疗器械制造商持续满足不断变化的网络安全合规要求，Silex Technology开发了AMC Protect服务。该服务能够降低SBOM（软件物料清单）创建和维护成本，简化 CVE监控流程，提供专家级漏洞风险评估，并在必要时向客户发布漏洞修补程序。

AMC Protect通过整合来自JPCERT/CC和Silex Technology芯片合作伙伴的CVE信息（通常在漏洞细节公开前就已获取），构建了Silex网络安全数据库。该数据库涵盖基于内核、操作系统、无线设备驱动及开源软件组件的漏洞信息。我们将持续监控数据库对客户的影响，并在发现漏洞时同步评估其严重程度。

Silex Technology采用业界领先的软件成分分析工具来识别和评估SBOM漏洞。该流程通过依赖项分析、二进制访问（当源代码不可用时）、代码指纹分析和代码片段分析，全面识别直接和间接漏洞。

作为持续CVE监控的一部分，客户每周都会收到详细的漏洞报告，说明其SBOM所有组件的状态。当检测到高影响漏洞时，系统会在识别事件后立即发送通知。一旦出现此类高影响漏洞，Silex Technology将直接与受影响客户合作进行评估和修复。

AMC Protect服务层级		Silex AMC Protect服务		
		7天内相关 漏洞（每周）	Silex通知后 30天内关键漏洞	Silex通知后 60天内非关键漏洞
所有	**SBOM和更新** （一个合同和产品的维护）	√	√	√
级别1	**监控/通知** 基于SBOM	√		
级别2	级别1+ **关键补丁软件** （关键漏洞补丁）	√	√	
级别3	级别1&2+ **关键路径软件** （非关键/受影响漏洞补丁）	√	√	√

如需了解更多关于网络安全和AMC Protect的信息，请联系Silex Technology。
（http://www.silex.com.cn）

参考资料

《2023年医疗器械与医疗系统网络安全现状报告》
《FDA医疗器械网络安全指南：行业与FDA工作人员指导文件》
《美国总统行政令14028号》
《美国国家标准与技术研究院网络安全框架2.0版》
《Wi-Fi能否满足联邦政府安全要求？——Aruba白皮书》
《Wi-Fi认证WPA3技术概述》