【探讨】破解了消防主机的协议，就可以突破“智慧消防”的市场吗

原创 南渠 金小鼎 2025年08月01日 08:15 浙江

想在“智慧消防”的市场竞争中占据一定的份额，通过“破解主机协议”的方式是否可行？是否存在法律的风险？未来的市场方向在哪里？



巧思善辩的厂商们，往往愿意将“智慧消防”与“传统消防”进行区分对立，向客户宣传介绍时，只要添加了一些ICT（信息、通讯）技术，就愿意把自己包装成从“存量市场”向“增量市场”的跃迁的新玩家。然而，从行业技术来区分，消防的市场还是分布在建筑、电气、机电设备、安装施工、技术服务等领域内。如果一定要证明有新人入场，无非是与信息通讯领域玩家的“联姻”。

踌躇满志的厂商们，在冲进“智慧消防”市场时，绕不开的一道门是火灾自动报警系统及控制主机，不仅门上有一把锁，还是密码锁——协议。以信息化技术与服务为看家本领的“智慧”新贵们，就用上了外挂——远程联网设备。早些年，联网就连了吧，通过授权或是解析，最多就是获取了一些报警及动作信号数据。但随着争夺市场的发展，已经有厂商动起了破解控制与通讯协议的主意。

如果仅仅从破解协议的技术手段来讲，如今已不是多大的难题，消防主机厂商们所使用的专用协议并非“坚不可破”。何况在商业竞争中，利用经济利益与人性弱点的盘外招也是层出不穷。这样的非法破解，存在哪些风险呢？

法律风险：破解消防主机专用协议的行为，在法律层面存在明确的违法风险，且可能涉及多重法律责任。

以下从法律依据、风险维度、技术场景等角度综合分析：

一、法律定性：破解行为构成侵权

1. 知识产权侵权消防主机的专用协议，通常属于软件著作权或技术秘密的保护范畴：

著作权侵权：协议代码作为软件组成部分，受《著作权法》保护，未经许可的反编译、逆向工程可能构成侵权。

技术秘密侵权：若协议包含未公开的加密逻辑或通信规则，破解行为可能侵犯企业的商业秘密权。

2. 违反《反不正当竞争法》破解行为若用于开发兼容性产品，可能构成**“擅自使用他人技术成果”**的不正当竞争行为。

二、风险维度：民事、行政与刑事责任

1. 民事责任

赔偿损失：权利方可主张实际损失或侵权获利索赔（如协议研发成本、市场利润损失）。

合同违约责任：若破解方曾签署保密协议或技术服务合同，可能触发高额违约金。

2. 行政责任

根据《计算机软件保护条例》，知识产权的行政管理部门可责令停止侵权、没收工具并处以罚款（最高非法经营额5倍）。

3. 刑事责任（情节严重时）

侵犯著作权罪 ：若以营利为目的，复制协议代码并传播，可能面临3-7年有期徒刑。

侵犯商业秘密罪：造成权利人损失超50万元，可处3年以下有期徒刑。

三、技术场景中的特殊风险

1. 消防系统的特殊性

破解协议若导致消防主机误报、漏报或联动失效，可能因危害公共安全被追究重大责任事故罪 。

例如：篡改火灾报警信号传输规则，延误灭火救援。

2. 协议转换模块的灰色地带

部分企业通过“协议转换器”实现新旧设备兼容，但若未经授权解析专用协议，仍可能被认定为侵权。

总之，破解消防主机专用协议存在违法的高风险，可能触发民事赔偿、行政处罚乃至刑事责任。在消防系统等涉及公共安全的领域，法律的容忍度更低。已有多家主机厂商发表声明，反对侵权。

建议通过技术替代方案（如采用新国标协议）或合法授权途径实现兼容需求，避免法律纠纷。若确需技术研究，需提前评估行为边界并咨询法律意见。

市场方向：消防主机专用协议逐步收敛，国标协议将逐步成为主流

在2024年，消防技术领域的一项标志性事件——GB4717-2024《火灾报警控制器》发布。作为我国火灾自动报警系统的核心标准，已于4月29日正式发布，并于2025年5月1日起实施，替代已沿用19年的2005版标准。

编制组在调研中发现两大突出问题：

一是，现有产品操作面板与操作方式缺乏统一标准，影响操作效率；例如消控员的考试、上岗、就业存在障碍；

二是，现有产品与消防电气控制装置之间缺乏统一的通信协议，在控制功能与数据分析功能方面存在不足，不利于智慧消防技术发展。

GB4717-2024《火灾报警控制器》三大显著变化：

变化一：操作界面标准化

操作面板标准化：新标准彻底改变了以往不同厂家控制器操作面板各异的混乱局面，通过强制性统一按键与指示灯的布局，实现了全国统一的"操作面板"。

专用功能按键：新标准要求控制器必须设置独立的确认按钮（键）和联动启动控制按钮（键）。

变化二：通信与数据管理的智能化升级

独立通信线路：新标准明确规定控制器的消防系统设备控制总线必须采用独立的通信线路，不得与消防系统报警总线、消防系统联动总线共用，以提高系统可靠性和抗干扰能力。

消防联动通信模块：具有联动控制功能的控制器通过消防联动通信模块与消防电气控制装置通信时，连接的设备总数不得超过62个。

运行数据存储单元：引入运行数据存储单元（俗称"黑匣子"）的概念，新标准要求控制器必须配备独立可拆卸的运行数据存储单元，采用金属外壳，防护等级不低于IP54。

变化三：安全防护性能的全面提升

外壳防护等级：控制器外壳防护等级（IP代码 ）不应低于GB/T 4208中IP30的要求，这意味着控制器必须能够防止直径不小于2.5mm的固体异物侵入。这一防护等级虽然不算很高，但已经能够满足大多数室内安装环境的需求，有效防止灰尘和意外接触导致的短路或损坏。

随着2025年新标强制实施后，新生产消防主机需支持FECbus协议，推动市场向标准化迁移。应用需要也将驱动开放架构，物联网（如消防物联平台）要求数据互通，加速淘汰私有协议，转向IP化通信（如BACnet /IP）。

如何在竞争中占据优势?

在“智慧消防”市场竞争格局遭遇瓶颈、撞墙疗愈、期待重构的背景下，企业需同时具备**技术创新力与商业布局能力**方能占据优势。结合**政策导向、技术演进与市场需求**，具备以下特征的企业，将展现出相对明显的潜力：

一、技术层面：以芯片级创新与智能化构建壁垒。我国工业正在先进制造业与高端智能化的征途上大步流星，芯片自主化与性能突破已有先例，场景化技术适配是符合我国工业门类大而全特征的最优解题方法。

二、商业策略：全链条布局与市场精准卡位。产品矩阵拓展与成本控制是已形成商业优势厂家常选择的方法，实现产品体系与方案落地的全周期覆盖，构建“预警-报警-疏散-灭火”闭环产品线，同时不断优化供应链。市场分层渗透，面向高端市场，以技术优势切

入超高层建筑、工业场景，树立标杆案例；面向下沉市场，推出高性价比方案，覆盖县域市场；敢于海外拓展，通过本地化认证（UL/FM/EN标准）和合作研发，抢占欧美及“一带一路”市场。

三、生态协同：政策红利与跨界融合。当前，政策红利早已掠过了大数据与信息化技术的海面，AI模型和具身智能为代表的新兴技术才是翻涌的浪涛。前期，已投入大量真金白银的厂商们，虽然搭建了智慧运维SaaS平台 ，提供设备监测、预测性维保，越来越多地被客户所采纳与接受，但同质化严重。由于应用成效也不够明显，也在被质疑与抛弃；融资租赁模式，虽然可以降低客户采购门槛，但绑定长期需求的特点，对运营服务的资金压力、变现能力、服务韧性都是较高的挑战。

“智慧消防”市场的竞争本质是 **“技术自主化+场景精细化+生态协同化”** 的综合较量。**短期靠芯片与AI技术破局，中期以全链条产品矩阵覆盖增量场景，长期则需构建开放生态。**企业需以政策为帆、技术为桨，方能在未来消防安全需求的市场中占据制高点。



南渠

喜欢作者

阅读 143