燃油加油机防作弊技术分析与对策研究

常　菲
高平市综合检验检测中心　山西　晋城　048000

摘　要：燃油加油机作弊手段多样，涵盖机械结构、电子系统及数据传输等方面。现有防作弊技术分硬件、软件、数据三级，但存在硬件防护被动、软件防护脆弱、数据防护延迟等局限。本文提出多层级动态防护体系构建、基于人工智能的异常检测技术应用、区块链技术用于数据存证、自适应加密算法优化等改进对策，以构建全方位防作弊体系，保障燃油加油机计量准确与交易安全。

关键词：燃油加油机；作弊手段；防作弊技术；动态防护体系；自适应加密

引言：燃油加油机作为燃油交易关键设备，其计量准确性关乎消费者权益与市场秩序。但近年来，部分不法分子为谋取私利，采用多种手段对加油机进行作弊，造成税收流失与市场混乱。随着技术发展，作弊手段不断升级，从简单机械干扰到复杂电子篡改、数据伪造。而现有防作弊技术虽有一定成效，却存在诸多局限，难以应对日益复杂的作弊形势。因此，深入分析作弊手段，研究改进防作弊技术迫在眉睫。

1 燃油加油机常见作弊手段分析

1.1 机械结构作弊

机械结构作弊的核心在于通过物理干预破坏燃油计量流程的完整性，主要针对流量计与计量阀等关键部件。此类作弊手段往往利用硬件设计的固有弱点，通过外力或电磁干扰改变设备运行参数，具有隐蔽性强、难以实时检测的特点[1]。流量计是燃油体积测量的核心装置，其内部齿轮的精密配合直接决定计量精度。部分作弊者通过加速齿轮磨损或利用强磁装置干扰齿轮转动，使流量计在相同燃油通过量下输出更少的脉冲信号，导致实际出油量多于显示数值。此外，计量阀作为控制燃油流出的执行机构，其开关时序对计量准确性至关重要。作弊者可能通过调整阀门弹簧张力或电磁控制参数，使阀门在加油过程中提前终止供油或延迟关闭，从而在未完成完整计量周期时停止计数，造成显示油量与实际出油量存在偏差。

1.2 电子系统作弊

电子系统作弊依托加油机控制程序的漏洞或通信协议的缺陷，通过软件算法或信号层面的干预实现计量欺诈。此类作弊手段利用数字化技术的复杂性，通过篡改程序逻辑或伪造通信信号，使计量系统产生虚假数据，具有实施便捷、影响范围广的特点。脉冲信号是燃油体积与电子计数转换的桥梁，作弊者可能通过修改脉冲当量参数，降低单位体积燃油对应的脉冲数，使加油机在相同燃油通过量下记录更少的脉冲值，进而虚增显示油量。主板程序作为加油机的控制核心，其逻辑严密性直接影响交易真实性。部分作弊者通过逆向分析程序代码，插入跳数指令或虚增交易量的算法模块，使加油机在未实际供油时仍累计油量，或在实际供油量不足时显示正常数值。通信协议干扰则通过阻断或伪造加油机与后台系统的数据交互，使交易记录无法实时上传或被篡改，为后续数据造假提供操作空间。

1.3 数据传输作弊

数据传输作弊聚焦于加油机本地存储与远程通信环节，通过直接修改交易数据或伪造控制指令实现欺诈行为。这种作弊方式巧妙地利用了数据在流转过程中的特性，具有极强的隐蔽性与监管难度。本地存储数据篡改是较为隐蔽的作弊方式，作弊者通过物理接触或远程入侵加油机存储模块，修改交易记录中的油量、金额等关键信息，使历史数据与实际交易情况脱节，掩盖计量异常。远程控制指令伪造则利用无线通信技术的开放性，通过发射特定频率的信号干扰加油机正常工作，或直接伪造后台系统下发的控制指令，强制调整加油机计量参数或触发虚假交易，从而在无物理接触的情况下完成作弊操作，增加监管难度。

2 现有防作弊技术原理与分类

2.1 硬件级防作弊技术

流量计自检依托精密设计实现运行状态实时核验，密封设计强化设备完整性防护，防拆结构可有效规避非法拆解带来的篡改风险，从物理层面阻断通过破坏硬件实现作弊的可能。这种物理防护方式直接、有效，能够从源头上防止作弊行为的发生[2]。计量阀闭环控制依托压力反馈机制精准调节运行参数，确保计量过程始终处于预设范围，避免参数偏移引发的数据失真，提升硬件运

行的稳定性与可靠性。闭环控制机制能够实时监测和调整计量阀的运行状态，保证计量的准确性。主板物理防护通过加密芯片强化核心数据安全，搭配防篡改外壳构建多重防护屏障，既能抵御外部物理冲击，又能防范非法破解与参数篡改，筑牢硬件层面的防作弊防线。加密芯片和防篡改外壳的组合，为主板提供了全方位的保护，确保核心数据的安全。

2.2 软件级防作弊技术

脉冲信号加密传输采用动态密钥校验方式保障数据传输安全，密钥实时更新可规避固定加密模式的破解漏洞，确保信号在传输过程中不被截取、篡改。动态密钥校验方式能够根据时间或操作行为不断更新密钥，提高了数据传输的安全性。程序逻辑校验通过关键数据冗余存储构建校验体系，多节点数据相互印证，及时发现逻辑异常与数据错误，避免恶意程序篡改引发的作弊行为。关键数据冗余存储能够增加数据的冗余度，提高数据的可靠性和完整性。异常操作行为监测聚焦设备运行状态，精准捕捉频繁重启、参数突变等非常规操作，通过预设判定标准识别风险行为，快速触发预警机制，从软件运行层面遏制作弊尝试。异常操作行为监测能够实时监测设备的运行状态，及时发现并处理潜在的作弊行为。

2.3 数据级防作弊技术

交易数据本地加密存储采用区块链存证技术保障数据不可篡改，加密算法对全量交易信息进行处理，确保数据存储的安全性与完整性，为后续溯源核验提供支撑。区块链存证技术利用去中心化和不可篡改的特性，为交易数据提供了可靠的安全保障。远程实时监控依托云端数据比对实现全域监管，本地数据与云端基准数据实时同步校验，及时发现数据偏差与异常波动，打破空间限制实现全天候防作弊管控。远程实时监控能够实现对加油机的远程管理和监控，提高监管效率。通信协议身份认证通过双向数字证书确认交互双方合法性，只有通过身份核验的主体才能实现数据传输与交互，从通信源头阻断非法接入与数据篡改，保障数据传输过程的安全性与合规性。通信协议身份认证能够确保数据传输的安全性和合法性，防止非法接入和数据篡改。三类技术相互配合、层层递进，构建起全方位防作弊体系，兼顾硬件防护、软件运行与数据安全，为各类场景提供可靠的防作弊支撑，适配不同领域的安全管控需求。这种全方位的防作弊体系能够从多个层面保障加油机的安全运行，适应不同场景的需求。

3 现有防作弊技术局限性分析

3.1 硬件防护的被动性

物理防护多依赖预设结构与固定机制实现安全管控，缺乏主动识别与应对未知攻击的能力。各类硬件设备的防护逻辑与核心组件容易成为破解目标，逆向工程技术可通过拆解设备、解析电路原理还原防护机制，进而绕过或篡改硬件防护功能[3]。这种被动防御模式难以应对不断迭代的破解技术，防护效果易受破解手段升级影响而弱化。传感器作为硬件防护的核心感知部件，运行精度直接关联防护有效性。温度、湿度、电磁干扰等环境因素会干扰传感器信号传输与数据采集，导致检测数据出现偏差。部分场景下极端环境还可能造成传感器硬件损耗，进一步降低感知灵敏度，无法精准捕捉作弊行为引发的异常信号，给作弊行为留下可乘之机。

3.2 软件防护的脆弱性

加密算法是软件防护的核心支撑，但其安全性与算法复杂度、密钥长度密切相关。随着计算能力提升，暴力破解技术可通过海量尝试遍历密钥组合，突破传统加密算法的防护屏障。尤其是复杂度较低、密钥长度不足的加密方案，在高强度计算资源支撑下，破解耗时大幅缩短，防护体系易被突破。例如，对于64位密钥的加密算法，在高性能计算设备下可能在1天内被破解。软件程序的逻辑设计难以实现全场景覆盖，开发过程中难免存在逻辑漏洞与设计缺陷。这些未被覆盖的漏洞可能隐藏在程序分支、数据交互等环节，常规测试难以全面排查。作弊者可利用此类漏洞绕过软件校验机制，实施恶意操作却不触发防护预警。漏洞修复往往滞后于漏洞利用，形成持续的安全隐患。例如，一个软件漏洞从被发现到修复可能需要7–14天时间，在这期间作弊者可能利用漏洞进行作弊操作。

3.3 数据防护的延迟性

本地数据存储与处理环节的防护存在明显滞后，篡改行为发生后难以及时察觉。本地数据缺乏实时校验与备份校验机制，作弊者可通过篡改本地存储文件、修改数据记录等方式伪造合规数据。现有防护手段多依赖定期巡检或事后核查发现篡改痕迹，无法在篡改行为发生时立即拦截，导致虚假数据可能被正常使用，引发后续风险。例如，定期巡检周期为1周，在这1周内虚假数据可能已被多次使用。远程监控模式下的数据防护高度依赖网络传输稳定性，网络延迟、中断或波动都会影响数据传输与校验效率。远程端与本地端的数据同步存在时间差，网络异常时同步过程易中断，导致远程端无法及时获取本地数据状态。作弊者可利用网络不稳定窗口期实施数据篡改，远程监控系统难以实时捕捉异常，进一步放大数据防护的延迟问题。例如，网络中断可能持续

10-30分钟，在这期间作弊者可完成数据篡改操作。

4 防作弊技术改进对策研究

4.1 多层级动态防护体系构建

硬件软件数据联动防护机制需打通不同层面技术壁垒，实现设备终端软件系统数据资源的深度协同。硬件层面强化终端设备身份核验与运行状态监控，实时拦截非法接入与篡改行为。软件层面优化防护算法与逻辑架构，提升对恶意程序的识别与阻断能力[4]。数据层面建立全流程流转监控，确保数据采集传输存储各环节的完整性与安全性，形成无死角的防护闭环。动态密钥更新依托时间周期与操作行为触发机制，定期生成全新密钥替代原有密钥，大幅缩短密钥暴露风险窗口。行为指纹识别聚焦用户操作习惯特征提取，涵盖操作频率间隔序列偏好等维度，构建独特行为基线。通过对比实时操作与基线差异，精准甄别异常行为，实现对伪装作弊行为的有效识别。

4.2 基于人工智能的异常检测技术

流量计运行状态智能诊断借助深度学习算法对设备运行参数进行持续分析，捕捉流量波动规律与异常特征。通过对正常运行状态下参数阈值的训练学习，精准定位流量突变异常峰值等违规迹象，及时发出预警信号。该技术突破传统阈值检测局限，提升对隐蔽流量操控行为的识别精度。例如，经过1000次以上正常数据训练后，系统可准确识别流量异常波动，波动范围超过正常值0.5升时发出预警。交易数据模式分析与风险预警围绕数据关联性与规律性展开深度挖掘，梳理正常交易的时序特征金额分布关联关系等核心维度。通过人工智能算法对实时交易数据进行动态分析，识别偏离正常模式的交易行为，提前预判作弊风险。优化算法模型对模糊边界数据的判断能力，减少误判漏判情况。

4.3 区块链技术在数据存证中的应用

交易记录不可篡改存证依托区块链哈希加密技术，对每一笔交易数据进行加密处理后写入区块。区块与前后节点形成链式关联，任何对历史数据的篡改都会导致哈希值发生变化，从技术层面杜绝数据篡改可能。加密后的交易记录永久留存，为后续追溯核查提供可靠依据。分布式节点实时校验通过多节点同步存储交易数据，每个节点均拥有完整数据副本。交易发生时所有节点同时对数据真实性有效性进行验证，只有达成共识后数据才会被确认存储。这种多节点相互监督的机制，有效防范单点篡改与虚假数据录入，保障存证数据的公信力。

4.4 自适应加密算法优化

根据环境参数动态调整加密强度需实时采集网络带宽设备性能攻击强度等环境指标，通过算法模型对指标进行综合评估。针对不同环境场景自动适配对应加密等级，网络环境安全设备负载较低时适当降低加密强度以保障运行效率，面临高危攻击或复杂环境时提升加密等级强化防护能力。例如，在网络带宽为100Mbps、设备负载较低时，采用128位加密强度；当检测到高危攻击时，提升加密强度至256位。抗量子计算攻击的加密方案设计聚焦量子计算技术对传统加密体系的冲击，优化加密算法的数学基础。引入抗量子特性的加密机制，通过复杂数学难题构建加密逻辑，即使面对量子计算的超强算力也能维持加密有效性。兼顾算法安全性与运行效率，实现抗量子攻击与实际应用场景的适配融合，筑牢长期安全防线。

结束语

燃油加油机防作弊工作意义重大，关乎市场公平与消费者利益。现有防作弊技术虽构建起一定防护体系，但局限性明显。多层级动态防护体系、人工智能异常检测、区块链数据存证及自适应加密算法优化等改进对策，从不同层面提升防作弊能力。这些对策相互配合，可形成更严密、高效的防护网，有效应对各类作弊手段，保障燃油加油机正常运行，维护市场秩序稳定，为行业健康发展提供坚实支撑。

参考文献

[1]柴惠,姜琳琳.燃油加油机防作弊技术分析与对策[J].商品与质量,2023(34):37-40.

[2]周建文.燃油加油机防作弊技术分析与实践探究[J].中外交流,2021,28(2):1358.

[3]孙雅杰,姜锐.燃油加油机防作弊技术分析[J].数码精品世界,2023(1):166-168.

[4]盘承平.燃油加油机防作弊技术分析[J].智库时代,2025(10):256-258.