关于贸易结算用大型电子衡器设计中防作弊的方法研究

梅特勒-托利多（常州）称重系统有限公司　戴峰

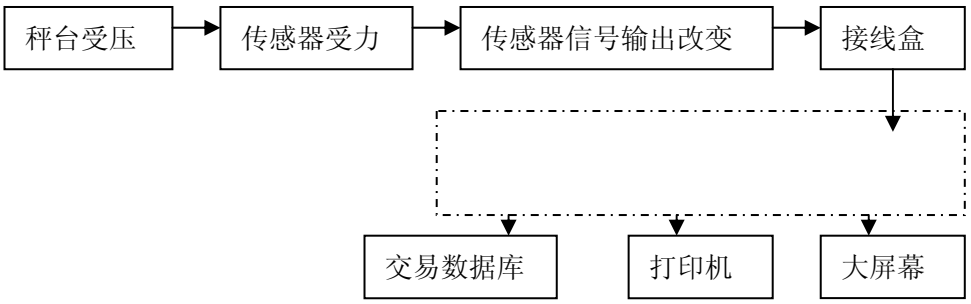
【摘　要】 鉴于目前贸易结算用大型电子衡器使用现场中发现的高科技作弊案例日趋频繁，本文通过对整个衡器系统计量信息链的角度对衡器作弊的可能性作了全面分析，在系统设计角度以及传感器和仪表技术设计细节上给出了解决方案。在给出方案的同时，介绍了国际上关于工业通讯协议以及数据加密技术的最新成果。

【关键词】 电子衡器；防作弊；数字式传感器

按照电子衡器的分类标准，通常可以分成案秤、台秤、地上衡、地中衡、吊秤、皮带秤、料斗秤、检验秤、汽车衡、轨道衡和特种秤等类别，其中，皮带秤、料斗秤、检验秤和特种秤等通常用于企业内部工艺计量而非贸易计量，制造厂商只需要考虑设计和使用的精度保证，不需要考虑防作弊问题。对于案秤和台秤，由于国家法制计量部门有铅封要求，计量法要求各地方计量定期检验并对衡器中的法定相关部分用铅封保护，不法分子较难下手。而地上衡、地中衡、吊秤、汽车衡、轨道衡等，由于体积较大，无法使用铅封保护，又通常放置于室外，不法分子较容易下手通过对这些贸易结算用大型电子衡器进行简单改装以达到通过计量作弊而牟利的目的。

为了避免客户利益受到侵犯，在设计和制造环节考虑贸易结算用大型电子衡器防作弊功能，成为众多电子衡器厂商日益关注的一个重要议题。本文将通过对整个衡器系统计量信息链的角度对衡器作弊的可能性作一分析，并给出了解决方法和应用实例。

以电子汽车衡为例，其计量信息链如下图：



根据上图所示的计量信息链，可以看出，每个阶段都有可能被修改其计量信息而进行作弊，但其作弊难度和易被察觉程度不同，见下表。

作弊环节	作弊方法	作弊难度	易被察觉程度
秤台受压 传感器受力	不完全上衡或者多台车辆同时上衡	低	中
传感器信号输出改变	在传感器组桥处并联电阻，安装遥控装置	高	中
接线盒	在接线盒中并联电阻，安装遥控装置	中	中
仪表	在模拟信号输入端并联电阻，安装遥控装置	中	中
仪表	修改仪表软件中法制相关部分	高	低
称重管理计算机	修改称重管理软件作弊	高	中（PC 软件可以比对仪表原值）

关于不完全上衡或者多台车辆同时上衡等作弊方法，目前的解决方案是汽车衡监控系统，增加红外对射装置，安装于地磅前后两端，当车辆没有完全停好或者与后面车辆距离太近时，系统将自动禁止称量同时报警提示。同时增加摄像抓拍装置，司磅员在磅房内部即可清晰了解到车辆情况。同时称重过程中抓拍的场景照片可供以后随时调用和查看。

关于修改仪表软件或称重管理软件作弊，实施难度较高，通常只有了解软件源代码的专业技术人员才能实施，而且目前国家法制计量监督管理部门正在根据JJF1182-2007《计量器具软件测评指南》制订关于法制计量软件的控制和检测办法，其中会包括目标代码存档和校验和检验等强制性检查，所以这两类作弊不需要重点考虑防范。

余下的三类作弊方式都是通过遥控影响模拟重量信号传播通道而改变称重测量结果的。如何通过技术手段阻止这方面的作弊行为？许多厂商给出了统一的答案，数字式称重传感器……

所谓数字式称重传感器，是指在模拟称重传感器端放置电路板，将模拟重量信号转化为数字信号（或重量值）直接发送给仪表的一种称重传感器形式。发明数字式传感器的本意是为了减少微弱的模拟信号在长距离传输过程中受到的干扰，同时使得模拟称重传感器的一些固有弱点（蠕变、滞后，零点温度系数、灵敏度温度系数）等可以通过数字补偿得以纠正，从而获得更高的计量精度。

防止作弊并非数字式称重传感器的设计本意，除非在其设计过程中对这一因素作特殊考虑。

对于数字式称重传感器，如果试图作弊，有两种方法：1）类似于对模拟称重系统作弊，破坏封装，在传感器模拟端并联电阻并用遥控装置控制。2）通过破解协议，将作弊设备连接到系统数字通讯线上，伪造称重数据。

对于前一种作弊方法，防范的关键在于保护传感器模拟部分不被更改，或更改后能够系统能自动发现。要实现这一需求，必须实现数字传感器的焊接密封，同时需要设计一套检测装置能够侦测传感器外壳被打开后的一系列变化，并给出报警。由于传感器被打开的时候，很有可能系统是处在非工作状态下面的，所以设计的检测装置检测的必须是传感器外壳被一旦打开后就一定会有所改变的状态。梅特勒-托利多在这一方面有多项专利，检测电路可以通过检测密闭传感器壳内惰性气体的浓度以及壳内的相对湿度[专利 ZL200610039728.0,ZL200620068653.4]来判断传感器外壳是否被打开过，即便传感器外壳被打开后重新焊接恢复，高精度的检测电路依然能够检测出异常并报警。

对于后一种作弊方法，防范的关键在于保护其通讯协议。普通的数字式称重传感器通常采用

RS485 通讯，其特点是成本低，与仪表兼容性较好，衡器生产厂可以选择不同厂商生产的数字式称重传感器和仪表组成系统。缺点是：RS485 通讯的速率低（100 米以上只能采用 19200 以下的波特率）、通讯可靠性与拓扑相关，同时传输字符是透明的，用普通设备就可以截取并破解。

为了解决通讯可靠性和通讯协议的加密问题，通讯必须选择多层模式，至少有物理层、数据链路层、数据加密层以及协议层。这与普通的 ISO 通讯分层模式有所不同，解释如下：

1、物理层负责通讯数据的物理传输；

2、数据链路层负责纠错、重发机制，以确保物理层的可靠性；

3、在数据链路层和协议层之间增加数据加密层，将所有的通讯命令和称重数据均以加密数据流方式传输；

4、协议层则解决仪表和传感器之间的通讯命令解析。

物理层考虑到长线高速传输的要求，采用平衡型传输较为合适，再考虑到数据链路层的可靠性及称重数据传输要求短帧的特点，以及称重通讯的实时性要求，CAN 成为一个较有优势的物理、数据链路协议。

控制器局域网络(CAN)是德国 Robert bosch 公司在 20 世纪 80 年代初为汽车业开发的一种串行数据通信总线。CAN 是一种很高保密性，有效支持分布式控制或实时控制的串行通信网络。CAN 的应用范围遍及从高速网络到低成本底多线路网络。在自动化电子领域、发动机控制部件、传感器、抗滑系统等应用中，CAN 的位速率可高达 1Mbps。随着 CAN 在各种领域的应用和推广，对其通信格式的标准化提出了要求。1991 年 9 月 Philips Semiconductors 制定并发布了 CAN 技术规范(Versio 2.0)。该技术包括 A 和 B 两部分。2.0A 给出了 CAN 报文标准格式，而 2.0 给出了标准的和扩展的两种格式。1993 年 11 月 ISO 颁布了道路交通运输工具-数据信息交换-高速通信局域网(CAN)国际标准 ISO11898，为控制局域网的标准化和规范化铺平了道路。

由于物理层和数据链路层一般都是开放式标准协议，所以数据加密层的设计就显得尤为重要。目前世界上关于数据通讯加密方法主要分两大类，一类是称为 DES（Data Encryption Standard），由 IBM 公司设计，在 1977 年 1 月被美国政宣布成为数据加密标准。DES 算法的入口参数有三个：Key、Data、Mode。其中 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种：加密或解密。 DES 算法是这样工作的：如 Mode 为加密，则用 Key 去把数据 Data 进行加密， 生成 Data 的密码形式（64 位）作为 DES 的输出结果；如 Mode 为解密，则用 Key 去把密码形式的数据 Data 解密，还原为 Data 的明码形式（64 位）作为 DES 的输出结果。在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密码形式在公共通信网（如电话网）中传输到通信网络的终点，数据到达目的地后，用同样的 Key 对密码数据进行解密，便再现了明码形式的核心数据。这样，便保证了核心数据（如 PIN、MAC 等）在传输过程中的安全性和可靠性。

而 AES(Advanced Encryption Standard)：高级加密标准，是下一代的加密算法标准，速度快，安全级别高。用 AES 加密 2000 年 10 月，NIST（美国国家标准和技术协会）宣布通过从 15 种候选算法中选出的一项新的密匙加密标准。Rijndael 被选中成为将来的 AES。Rijndael 是在 1999 年下半年，由研究员 Joan Daemen 和 Vincent Rijmen 创建的。AES 正日益成为加密各种形式的电子数

据的实际标准。美国标准与技术研究院（NIST）于 2002 年 5 月 26 日制定了新的高级加密标准（AES）规范。AES 算法基于排列和置换运算。排列是对数据重新进行安排，置换是将一个数据单元替换为另一个。AES 使用几种不同的方法来执行排列和置换运算。AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位（16 字节）分组加密和解密数据。与公共密钥加密使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换和替换输入数据。

回顾整个大型电子衡器的防作弊设计，可以看出：

1、作为整秤（系统）设计方，必须考虑选择有防作弊设计的密封数字式传感器和相匹配的数字式仪表，而且传感器和仪表之间的通讯协议必须是非公开的（增加作弊难度）。

2、作为密封数字式传感器和相匹配的数字式仪表的设计方，要考虑防范两个方面的作弊可能性- 打开传感器外壳在模拟端作弊，或是通过破译传感器和仪表之间的通讯协议作弊。所以在数字式传感器设计时，必须考虑加入侦测传感器外壳是否被打开能力。同时在通讯协议上，必须考虑多层模式，并引入加密算法（DES 或 AES），以确保称重数据传输的可靠性和保密性。

当然，大型电子衡器在用户处实施时，还可以安装视频监视探头以及在称重管理软件中加入车辆历史数据比对等功能以防范非技术性作弊。对这些通用性的防作弊手段，已有成熟的技术模式，本文不再赘述。

参考文献

1.《中国衡器实用技术手册》，中国衡器协会，中国计量出版社，2005.10

2.“基于数字传感器的称重系统通讯方法”，中国发明专利，ZL200710131539.0

3.“密闭容器的泄漏检测反方法”，中国发明专利，ZL200610039728.0

4.“多功能称重传感器”，中国实用新型专利，ZL200620068653.4

5.“智能称重传感器的控制电路”，中国实用新型专利，ZL200620068651.5

6.《现场总线 CAN 原理与应用技术》，饶运涛，北京航空航天大学出版社，2003

7.《计算机网络安全技术》，宋西军，北京大学出版社，2009