关于 OIML R76 的防作弊规定的解析

——目前衡器行业最为关注的热点问题讨论之二

上海大和衡器有限公司　陈日兴

【概　要】 电子衡器的防作弊问题一直是我国衡器行业与衡器质量技术检测机构最为关心的热点话题之一。本文主要针对最新版国际法制计量组织 OIML R76-2006《非自动衡器》国际建议中关于防作弊规定与检测要求，结合目前国内贸易用电子衡器普遍存在的问题进行了论述。

【关键词】 OIML R76　贸易用电子衡器　防作弊　软件保护

前　言

被国内衡器行业普遍喻之为“衡器界圣经”的国际法制计量组织（OIML）R76《非自动衡器》国际建议，经过十多年的全国范围的宣贯，已广泛被国内同行所接受，为我国非自动衡器的标准、规程与 OIML 的全面接轨奠定了基础。国际法制计量组织 OIML R76《非自动衡器》国际建议从 1992 年版开始就对电子衡器的防作弊问题进行了专门的规定，在随后历年的修订讨论中，又不断地完善了相关的规定与检测要求。由于历史的原因，在目前现行的非自动衡器国家检定规程中，对于贸易用电子衡器（包括电子计价秤、电子台案秤、电子汽车衡等产品），有些防作弊内容至今还没有被采纳。现在随着最新版的 OIML R76-2006 的正式发布，不折不扣地采纳电子衡器的防作弊规定已势在必行。

1. OIML R76-1992 版中防作弊内容

1.1　JJG555-96《非自动衡器》中已采纳的内容

我国现行的 JJG555-96 非自动衡器国家检定规程（详见[1]）中，采纳了 OIML R76-1992 版（详见[2]）中部分防作弊内容，例如在 OIML R76-1992 版中 4.1.2 安全性描述如下：

“衡器应不具有可能方便于作欺骗性使用的特征”；

“衡器的结构应保障：意外受损或控制元件被错误调整，一旦干扰衡器的正常功能时，应有明显警告”；

“衡器控制的设计，应保障控制的动作能进入预定的设计位置，除非动作中全部显示失灵，各键的标记应不含混”；

“对禁止接触或调整的元件和预置控制器，应提供保护的方法。对要求的保护可用国家法规做出规定”；

“衡器可配备一个自动或半自动的量程调整装置。该装置应装配在衡器的内部。加密保护后，外部的影响实际上不会对其产生作用”；

“对重力敏感的衡器，可装备一个补偿重力变化影响的装置。加密保护后，外部的影响或接触实际上不会对其产生作用”。

1.2 JJG555-96《非自动衡器》中没有采纳的内容

OIML R76-1992版中下述内容没有被我国现行的JJG555-1996非自动衡器国家检定规程所采纳：

“4.8.1 防止在‘称量’位置以外称量：如果衡器具有一个以上的锁定装置，那么这些锁定装置只允许有‘锁定’与‘称量’两个稳定的位置，而且只有在‘称量’位置才能进行称量。”

“4.11.3 称量的不可能性：当选择装置（不同承载装置与不同载荷测量装置之间的选择装置）在使用时，称量应是不可能的。”

“4.11.4 组合使用的识别：承载器与载荷测量装置的组合使用应容易识别。”

“4.15.4 计价衡器的特殊应用：所有的累计付款价均应打印，而总价应等于所有这些打印价格的代数和。”

上述条款之所以没有被JJG555-96所采纳，原因是当时对于这些内容没有吃透或者说还认识不足，虽然在笔者起草的最新的国家标准GB/T7722-2005《电子台案秤》（详见[3]）中将上述所有内容已作出了规定，但是在各地的执行过程中，包括一些质量技术检测机构也认为，国家标准仅仅是推荐标准，各企业可执行也可不执行。特别是“所有的累计付款价均应打印”这一条款，早在上世纪九十年代中期，澳大利亚国家标准局就已向我国的相关企业指出这一措施执行的必要性，但遗憾的是，直至目前我国在执行的力度上还是大打折扣，造成了带有累计键而不带打印功能的电子计价秤在各地市场上比比皆是。大家可以设想一下，在市场上使用此类电子秤如果不经意而误操作、重复操作或卖方作弊的话，很可能造成累计的付款价改变，从而损害了买方的利益。笔者为此也多次在不同的场合呼吁：要么取消累计键、要么增加打印功能，两者应取其一。并在《中国计量》（详见[4]）、《上海计量测试》（详见[5]）上有专文阐述，但还是收效甚微。好在最新版的OIML R76-2006对于此条款的规定的再一次的发布，对于该问题的提出是否可以起到推波助澜的作用，将拭目以待。

2. OIML R76-2006版中新增的防作弊内容

2.1 最新版的OIML R76-2006（详见[6]）对于防作弊内容的规定如下：

“4.1.2.4 元件和预置控制器的保护：对禁止接触或调整的元件和预置控制器，应提供保护的方法。对要求的保护可用国家法规做出规定。在Ⓘ级器衡上，灵敏度（或量程）调整装置可以不加保护。可采取的解决办法是：应用管理标记时，密封区域的直径至少为5mm。

可以用软件的方法对元件或预置控制器进行保护。”此规定与OIML R76-1992版的内容基本相同。

2.2 最新版的 OIML R76-2006 对于软件保护方法新增规定如下:

“a. 按照常规的保护办法，衡器的用户和衡器负责人员，必须认识到衡器的法定地位。保护措施应包括保护任何所采用的证据直至下一次检定或法定机构作比较检查。可取的技术方法如下：

信号计数器，即不可复位计数器（指计数到最大数值时，在没有授权人员的干预下，不会回零继续计数）。每当输入一个受保护的衡器操作方式并按装置的特定参数产生一个或多个变量时，该计数器就增加。计数器的基准计数是在（首次和后续）检定时，用适当的软、硬件工具在改进过的衡器上固定下来并加以保护。实际的计数可以采用操作手册和 OIML 证书和评价报告中的程序，使其显示并与基准计数进行比较。

b. 应保护装置特定参数和基准数，以防止无意和意外的改变。对这些数据，应尽可能满足 5.5.2.2 中所适用的软件要求。可取的技术方法如下：

装置特定参数只有授权人员通过专门的（PIN）代码才能变动。例如固定在衡器主板（或其它合适部件）上的衡器系列号（或其他识别），如果带储存装置的电子元件没有防修改的措施，应另外储存。这些数据应用一种至少两位带隐蔽多项式的 CRC-16 校验进行加密。这是一种比较充分的保护方法。基准数和系列号（相应的其他识别）应根据人工指令显示，与衡器主板（或衡器其它合适部件）上固定并保护的相同数据进行比较。

c. 衡器采用软件保护的办法，应为授权人员或机构在主板或主板附近固定基准数提供足够的方便。

注：根据 a.项要求显示的基准数与衡器上固定且受保护的基准数如有差别，表明使用中已有干预，其结果是不符合国家法规的要求（即该衡器不能再用于法制管理的场合）。

可取的技术方法如下：

采用固定安装在衡器上的可调（硬件）计数器，在（首次或后续）检定时调到实际的计数器数字后能够加密保护。”

按照通用的说法，上述专用 PIN 代码实际上是一个 4 位到 8 位的专用输入密码，只有授权人员输入此码，才能对装置特定参数进行数据存取。一般连续 3 次错误输入 PIN 码，软件将会被阻塞。

2.3 循环冗余校验 CRC-16（Cyclic Redundancy Check）简介（详见[7]）

在数字通信传输过程中为保证正确性，需要进行差错控制。

目前最常用的差错控制方法为自动请求重发方式（AQR），向前纠错方式（FEC），混合纠错方式（HEC）等三种。而其中最常用的纠错方式为 AQR 方式，此时的差错控制只需检错功能。传统的检错控制方法有奇偶校验、校验和检测、重复码校验、恒比码校验、行列冗余码校验等。这些方法都是增加数据的冗余量，将校验码与数据一起发送到接收端，将得到的校验码与接受到的校验码比较，两者一致则为传输正确。上述方法缺点是误判率高。

循环冗余校验码（CRC校验）：采用多项式编码方法，被处理的数据块可看作是一个n阶多项式，$t(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$。如一个 8 位二进制数 10110101 可表示为：$1x^7+0x^6+1x^5+1x^4$

$+0x^3+1x^2+0x+1$。当采用CRC校验时，发送方和接收方用同一个生成多项式$g(x)$，首位与末位系数都为 1。发送方用$t(x)$除以$g(x)$，得到余数作为CRC校验码，校验时以计算的校正结果是否为 0 为依据，判断数据帧是否出错。

采用 16 位CRC校验可以保证在10^{14}bit码元中只有一位未被检测出的错误。因此具有编码简单，误判率很低的优点。广泛应用在各种数据传送的差错校验中。

现用一个最简单的 CRC-4 编码举例说明编码过程：

设待发送的数据$t(x)$为 12 位的二进制数据 100100011100。CRC-4 的生成多项式为$g(x)=x^4+x+1$,阶数r为 4,即 10011,首先在$t(x)$末尾添加 4 个 0 构成$x^4t(x)$,数据块就成了 1001000111000000，然后用$g(x)$去除$x^4t(x)$，不用管商是多少，只需要求得余数$y(x)$，下表为给出了除法过程。

除法次数	被除数/ $g(x)$/ 结果		余数 $y(x)$
0	被除数	1001000111000000	100111000000
	除数	10011	
	商	0000100111000000	
1	被除数	100111000000	1000000
	除数	10011	
	商	000001000000	
2	被除数	1000000	1100
	除数	10011	
	商	0001100	

从上表中可看出,CRC-4 编码实际上是一个循环移位的模 2 运算。解码时用接收到的数据去除$g(x)$，如果余数为零，则表示传输过程没有错误。如果余数不为零，则表示传输过程肯定有错误。上述 CRC-4 编码例子与 CRC-16，CRC-32 编码过程一致，仅生成多项式和位数不一致而已。

3．其他软件保护方法介绍

综观目前在我国衡器软件作弊的主要表现手段有：

（1）软件程序接口留后门，使法制检定部门无法识别；

（2）用软件加硬件的综合方法障人耳目、混淆视线，进行作弊；

（3）根据检定规程的要求，使预定的测试点上做手脚，使显示误差为零。

因此为了衡器软件或计量相关数据域的安全，必须采取加载物理铅封、硬件或软件封条的方法

来保护软件。只有铅封、封条被移动、损坏、破坏后，软件或计量相关数据域才会被更改。

3.1 WELMEC 7.1（Issue 1-1999）《基于计量器具指令的软件要求》中软件保护的分级方法

欧洲法制计量联合体 WELMEC 7.1（Issue 1）《基于计量器具指令的软件要求》（详见[8]）中第四章中关于软件的分级定义特别是关于法制分级的定义其中规定了①软件的保护分级、②软件的检查分级、③软件的符合性分级。第①项软件的保护分级可分为三个等级如下：

低级：不需要保护软件，来防止故意要求的更改；

中级：用简单的通用软件工具（文本编辑器）防止软件的故意更改，以便保护法制相关软件；

高级：用特殊的软件工具（调试装置、硬盘编辑器、软件开发工具）防止软件的故意更改，根据数据安全技术所确认的保护等级（例如用于贸易结算）来保护法制相关软件。

该指令指出：采用传统的加密或明显的不允许干预等安全保护措施，显然等效于中级或高级的软件保护。也就是说用于贸易结算的电子衡器的软件保护肯定是中级或高级的。

在 WELMEC 7.1 的“软件检查分级”同样要按低、中、高三个等级的分类中，对于高级检查措施，则要求对程序的源代码进行分析和检查。

从以上的规定可以看出欧盟 WELMEC 对于贸易结算用电子衡器的软件保护与检查的严肃程度。

3.2 中国计量技术规范《计量器具软件测评指南技术规范》中软件保护方法介绍

我国在参考欧盟 WELMEC 7.1《基于计量器具指令的软件要求》与国际法制计量组织 OIML D-SW《软件控制计量器具的技术要求》的基础上，结合我国计量工作的实际情况，由江苏省计量院牵头制定了国家计量技术规范《计量器具软件测评指南技术规范》（详见[9]）并于 2007 年 11 月 21 日正式实施。此规范的出台，结束了我国计量器具检定只能进行硬件检测的历史。计量器具的软件测评包括了软件保护的测评内容，具体描述如下：

（1）预防意外误操作

■ 通过软件保护，使得计量器具意外误操作的可能性降至最小。

■ 法定控制下的程序部分或数据的改变由意外的物理因素或软件影响(崩溃，病毒感染)或用户对仪器无意识的误操作。

（2）防止欺诈

1）对于有操作系统或可以嵌入软件的计算机作为其一部分的计量器具来说，除对计量器具铅封外，还应禁止通过非授权的途径修改计量器具中软件，保证安全的要求。

2）从用户接口输入的命令,应在提交做型式试验的软件文档中有完整描述。只有文档中说明的功能允许被用户接口激活。接口设计要避免用户用于欺诈目的。

3）计量器具确定法制相关参数须防止非授权的更改以保证安全，当前的参数设定应能被显示或打印。

4）通过硬件保护措施（机械封装和加密措施），防止未授权的干涉或者留有证据。

另外还可以通过“电子校验和”验证，即一个程序代码或者一数据集的所有字节相加，模数相

加的方法常用于得到一个具有定量数字的结果。或者采用第三方的多路信号与采集标准信号比对来验证。

4. 结　尾

从以上对我国现行的 JJG555-96《非自动衡器》国家检定规程中防作弊规定与检测要求的分析出发，到最新版国际法制计量组织 OIML R76 及欧盟 WELMEC 7.1 与我国最新版计量器具软件测评的技术规范中对软件保护相关内容的描述，结合目前国内贸易用电子衡器普遍存在的问题进行了论述。笔者认为在中国要真正做到防作弊规定与软件保护检测要求，需要极大提高我国衡器制造行业与衡器质量技术检测机构的整体技术素质。与国外先进工业国家的技术交流与学习沟通技术信息，是加快掌握软件保护检测技术的捷径。

另外需要再一次强调的是：不折不扣地执行国际上最新的有关电子衡器的防作弊规定已势在必行。

以上观点如有不妥，请指正。

参考文献

〔1〕标准：中国计量检定规程《非自动秤通用检定规程》JJG 555-96〔S〕1996

〔2〕标准：国际法制计量组织 OIML TC9/SC1 International Recommendation“Non-automatic Weighing Instruments”《OIML R76: Non-automatic weighing instruments》〔S〕1992（E）

〔3〕标准：中国国家标准《电子台案秤》GB/T7722-2005〔S〕2005

〔4〕专著：陈日兴《关于贸易用电子秤累计付款价必须打印的论述》〔M〕《中国计量》2006 第 10 期

〔5〕专著：陈日兴《电子秤防作弊的又一新举措——关于电子秤累计付款价必须打印的宣贯》〔M〕《上海计量测试》2006 第 6 期

〔6〕标准：国际法制计量组织 OIML TC9/SC1 International Recommendation “Non-automatic Weighing Instruments”《OIML R76: Non-automatic weighing instruments》〔S〕2006（E）

〔7〕专著：刘东《循环冗余校验 CRC 的算法分析和程序实现》〔M〕西南交通大学 2006 年

〔8〕标准：欧洲法制计量联合体 WELMEC WG7.1（Issue 1）《Software Requirements On the Basis of the Measuring Instruments Directive》〔S〕1999（E）

〔9〕标准：中国计量技术规范《计量器具软件测评指南技术规范》〔S〕2007.11

作者简介

作　　者：陈日兴，男，享受国务院政府特殊津贴专家

研究领域：电子衡器产品开发与计量技术

工作单位：上海大和衡器有限公司

职　　称：总工程师
通讯地址：上海市浦东新区庆达路 368 路
邮　　编：201201
电　　话：021-58975205
E-mail：crx8030@sina.com