GB/T23111《非自动衡器》中提出的软件防作弊措施

深圳市芯海科技有限公司　贾颐康

【摘　要】 本文主要简介了 OIML 国际建议，R76《非自动衡器》（2006 年版）和国家标准《非自动衡器》中有关防止作弊措施的基本内容和要求，并阐述了在实际实施中应当注意的问题和建议。

【关键词】 防作弊措施法制相关软件；法制相关参数；法制相关数据；型式特性参数；装置特性参数；循环冗余检验（CRC）

一、引言

30 多年前，当电子计价秤开始在民间贸易市场中应用时，衡器管理人员终于松了一口气：违规者再也不能通过改变游砣和增砣的重量进行作弊了。然而，在电子计价秤广泛应用的今天，30 年前的现象在当今的民间贸易市场中重现了：相当数量的计价秤经过改造，就具备了作弊功能，尤其是通过修改软件而实现的作弊功能，更不容易被广大消费者所识破。与机械衡器相比，对电子衡器进行以作弊为目的的改造，技术含量高，手法隐蔽，改造后的器具具有逃避监督的效果，即使专职人员也不容易获取作弊的证据。对这种现象如不加以制止，不但会严重侵害消费者的利益，对社会的和谐、稳定、健康发展也会产生消极因素。

其实，利用科技手段对电子衡器等计量器具进行作弊并不是中国的特有现象，世界各国无论先进与落后，或多或少都有作弊现象发生。为了遏制作弊现象，国际法制计量组织 OJML 提出了一些适合在计量器具中采用的重点防止利用软件技术进行作弊的技术措施，例如，在 R-76 号国际建议《非自动衡器》最新的版本 2006 版中，就增加了若干软件防作弊的要求。由于在世界范围内目前尚缺乏足够的实践支持，为了更清晰地表达防作弊要求，R-76 还对防作弊要求做了教科书式的注解，并列举了“可接受（采纳）的方案”，这就为我们研发具体的软件防作弊技术提供了具体的技术指导。国家标准 GB/T23111《非自动衡器》不但在内容上是等同采用 R-76，在版面格式上也完全按照 R-76 编排，这样，业内人士能够阅读到中文版的“R-76 国际建议”的相关内容了。

对于 GB/T23111《非自动衡器》中提出的软件防作弊措施，我们可以从两个层面学习和理解，一是在概念层面，是对法制相关软件的定义、特征和分类的描述；二是在操作层面，是针对不同类型的软件可采用的不同的防作弊方法。另外，国家标准 GB/T7724-2009《电子称重仪表》也引用了这部分内容，称重仪表的设计、制造、检定、计量管理者同样也要掌握这些内容。下面分四个专题进行探讨，由于笔者水平有限，欢迎大家对其中的误謬与遗漏加以指正。

二、法制相关软件

法制相关软件（Legally relevant software）是 R-76：2006 版新增的最重要的概念，是指衡器及其电子模块（以下统称为衡器）中产生、改变计量结果和主要指示、影响计量性能的程序、参数及数据。这些软件必须纳入法制计量管理和监督的范围。在较大的应用系统中（例如将 PC 机用

作指示器的衡器），往往包含与法制相关软件关联的非法制相关软件，例如支持法制相关软件运行的操作平台、设备驱动程序等，以及利用衡器计量数据控制其他设备的控制程序与控制指令。如果法制相关软件与非法制相关软件能够被分离并能加以识别，非法制相关软件运行不会干预计量结果和主要指示，或两者之间的数据交换符合法制计量管理的要求，则无需对非法制相关软件进行法制计量管理和监督。对于许多无法分离法制相关软件与非法制相关软件的衡器（如计价秤、安装了称重指示器的衡器等），整个软件均视为法制相关软件。

法制相关软件包括程序、法制相关参数和法制相关数据三部分。

程序是指固化或下载安装到衡器中的控制、产生、改变和影响法制相关参数和法制相关数据的编码序列（或称计算机软件），一种衡器通过型式批准，其程序版本即被认可，之后无论生产者、销售者、管理者、操作者等等所有的人，对其程序进行任何改动都是违法的。

法制相关参数是指软件中表示衡器计量特征和计量性能的数据，又分为型式特性参数（Type specific parameter）和装置特性参数（Device specific parameter）。

型式特性参数是产品设计时确定的数据，比如滤波器结构参数、稳定判断参数、零点跟踪参数等等，软件版本识别码也是一个型式特性参数。同一族、同一型号、同一规格的所有产品的型式特性参数是相同的，型式批准时这些参数被认可，在以后的制造、检定、贮运、销售、使用中均不得改变这些参数，否则就是违法行为。

装置特性参数是决定每一个单件产品计量特性的数据，如衡器校准时产生的某些数据（如空秤调整值、量程系数等），即使相同型号、规格的同一批产品的每一件个体产品，其装置特性参数也各不相同。首次检定以及周期检定时，授权人员可激活专门的操作程序修改装置特性参数，非检定时间以及非授权人对此类参数的修改则是违法的。

法制相关数据是指衡器产生的称重结果，包括主要指示中的所有诸如毛重、皮重、与重量有关的金额等等数值，以及计量单位、标识代码与指示符号等等，衡器应能保证称量结果的产生、显示、存储、打印、传输等都是正确的，使衡器产生不正确称量结果的任何改动都是违法的。

三、对通过衡器程序作弊的防范措施

程序是法制相关软件的主体，对衡器中的法制相关参数和法制相关数据的改动必须通过程序的运行来实现，当前最流行的作弊手段就是更换程序：将原衡器上经型式批准、检定过的正版程序卸下，更换一个非法程序即可。

GB/T23111 公布的防止通过更改程序作弊的防范措施经过“有效申请”、“型式评价”、“周期检定与日常监督”三个环节才可实现：

1、有效申请中的防范措施

首先，在申请型式批准时，申请人应在随试验样机提交的文件中注明：

（1）软件版本标识，包括：

a）版本号；

b）循环冗余校验（CRC）生成多项式（CRC-16 或 CRC-32）；

c）实际安装在试验样机上的程序机器码的 CRC 校验和。

（2）所采用的各个保护措施，包括：

a）对访问装置特性参数的授权人的个人识别码的识别方法；

b）所能提供的被保护的调整部件或预置部件受到干预的证据；

c）带有存储装置的电子器件的序列号及其保存、读取方法与保护措施；

d）软件版本标识的保存、读取方法与保护措施；

e）联接法制相关软件与非法制相关软件的接口的保护措施；

f）通过接口的指令、数据的保护措施；

g）存储数据的数据量与存储器容量；

h）对存储数据的保护措施；

i）当能够安装由互连网下载的已获批准的法制相关软件时，软件下载过程和阻止意外或恶意修改的安全保护措施；

j）阻止下载未获批准的计量软件的措施；

k）存储由网络传输的数据的保护措施。

（3）法制相关功能的详细描述，包括：

a）硬件系统说明，如结构框图，计算机型号，网络类型等等；

b）法制相关软件的软件环境说明，如操作系统，驱动要求等；

c）法制相关功能的说明，如开关、键、操作过程、显示、指示等；

d）有关测量运算规则的说明，如稳定平衡，价格计算，化整规则等；

e）菜单和对话框的说明（如果存在）；

f）全部命令和参数的说明，包括通过受保护的软件接口在法定相关软件和关联软件间交换的命令和参数，以及该清单的完整性承诺。

（4）承诺所采取的保护措施在型式批准、检定后保证软件版本不被修改。

评价部门首先应对申请提交的文件进行审核，文件中包含上述内容描述才是有效申请。如果随试验样机提交的文件的内容不完整，其申请就得不到批准。

2、型式评价中的防范措施

其次，在型式评价中对试验样机进行所有保护措施的实际保护效果以及法制相关功能的正确性进行验证，验证内容有：

a）检查是否产生覆盖法定相关软件所有机器码的校验和或等效信号；

b）检查如果代码是由文本编辑程序伪造时，是否不能启动法定相关软件；

c）检查法制相关参数是否只能由授权人员经特殊的个人识别代码进行修改；

d）检查是否所有装置特性参数受到充分保护（例如通过校验和）；

e）检查是否是通过规定的受保护软件接口将规定的法定相关程序模块与关联软件模块分开；

f）检查受保护的软件接口本身是否是法定相关软件的组成部分；

g）检查衡器是否产生合适的软件标识，它覆盖所有法定相关软件和型式特定参数的程序模块；

h）检查是否在给出一手动命令后能显示规定的软件标识；

i）检查是否按照文件描述的方式产生校验和（或者其它信号）；

j）当存储的数据包含再现初始称重值必要的所有相关信息（如毛重、净重、皮重、小数点符

号、单位、数据组的标识，衡器或承载器的标识号码、数据组的校验和等等，下同）时，检查存储容量和防止无法接受的数据丢失的措施；

k）检查已存储数据和传递是否正确；

l）检查存储的数据是否受到合适的保护（数据在向存储装置传送期间是否至少使用奇偶检验保护），以免意外的或恶意修改；

m）检查可下载软件存储装置的数据是否采用校验和的方法进行适当的保护；

n）检查存储的数据是否能够被识别及显示，识别编码的储存是为以后使用和在正式交易介质上记录（打印）；

o）检查用于交易的数据是否是自动存储，而不取决于操作人员的意愿；

p）检查是否是通过在符合法定受控的装置上显示或打印标识的方法验证存储的数据组；

q）在衡器主板是否留有适当位置供粘贴防作弊标识以及是否方便粘贴防作弊标识；

r）其他必要的检查。

所有检查项目与文件描述一致并获得通过，方可认为该软件是符合法制要求的。

3、周期检定与日常监督中的防范措施

有效申请与型式评价中的防范措施的目的是防止可能被作弊行为利用的软件获得型式批准，也就是说，获得型式批准的软件不会被用于作弊。但是，前面两个环节并不能防止取得产品生产许可以及产品销售以后合格的软件被替换，周期检定与日常监督中的防范措施的目的在于防止合格的软件被替换。具体监督措施有：

a）检查带存储装置的电子器件或组件是否被替换；

b）检查粘贴在主板上的防作弊标识是否与型式批准证书中记载的一致；

c）检查粘贴在主板上的防作弊标识是否与检定证书中记载的一致；

d）检查由电子存储装置读出的防作弊标识是否与粘贴在主板上的防作弊标识一致。

注：防作弊标识包括：带存储装置的电子器件或组件的识别码及其校验和、软件版本号、程序机器码的CRC校验和、法制相关参数修改标记、法制相关参数的CRC校验和等。

四、对通过修改法制相关参数作弊的防范措施

由于每一台衡器的计量特性（如Max、d、称量误差等）的正确与否决定于法制相关参数，即使使用正确版本的衡器软件，仍可通过修改法制相关参数达到作弊目的，其中修改装置特性参数中的量程系数是作弊的主要途径。通常，法制相关参数中的量程系数的确定方法是：先由授权人员输入一个识别码，激活衡器校准程序，然后按照程序进行衡器校准操作，例如在承载器上放置规定质量的砝码，按指定的按键，校准程序就会按照预定的算法生成量程系数并予以存储。如果激活衡器校准程序后没有按照规定的质量放置砝码，例如所放置的重物的质量只有规定质量的80%，生成的量程系数就会比正确的数值大25%，相当于读到的数值比真正的重量值大25%。如果故意不按规定的质量值进行衡器校准，就是作弊行为。

GB/T23111公布的防止通过修改装置特性参数进行作弊的防范措施是：

a）为授权人员开设一个密码输入程序，由授权人员设置密码来阻止他人激活衡器校准程序；

b）提供对法制相关参数进行修改的证据。

GB/T23111列举了一个可以接受（采纳）的方案：

在衡器电子部件中安装一个专门用于记录装置特性参数更改次数的不可复位的事件计数器，每当对装置特性参数进行一次修改，该计数器就会自动产生一次增量，当进行一次周期检定之后，授权人读出该计数器的值并备案于本次的检定合格证书中，在下一次周期检定之前，先读取该计数器的值，如果此时的计数器值与前一次记下的备案值相等，则认为装置特性参数未被更改，如果此时计数器值与备案值不相等，则认为有人曾经修改过装置特性参数。

在法制相关参数中，除了装置特性参数外，还有型式特性参数，由于确定型式特性参数的方法只有两种，一是将其写在程序中，这时修改型式特性参数如同修改程序。二是修改型式特性参数的办法与修改装置特性参数的方法相同。所以以上两种措施已经能够防止对型式特性参数的修改，从而无需单独采取防止修改型式特性参数的防范措施。

五、对通过修改法制相关数据作弊的防范措施

除了更换程序，更改法制相关参数能够取得作弊效果外，直接更改称重结果是更简便的作弊手段。尤其是将主要指示等法制相关数据存储、传输到另外的非法制计量设备中的进行显示、打印或存储的情况下，这时衡器的程序与法制相关参数都是正确的，接收数据的设备中则装有作弊程序，该程序将接收到的称重结果进行篡改即可获得作弊效果。

GB/T23111公布的防止通过更改法制相关数据进行作弊的防范措施是：

a）所有定义的功能、命令、数据等，从法定相关软件到所有其他连接的软件或硬件部分间的交换都经过受保护的接口。保护方法如加密、CRC校验等；

b）对法制相关数据的存储是自动进行的，不取决于操作人员的意愿；

c）存储的法定相关数据必须包含全部必要的相关信息以便重现初始称量信息，其中主要指示包括毛重值、净重值和皮重值，小数点符号，计量单位等。其他信息包括存储数据的CRC校验和、数据识别信息（如序号）、日期、时间以及多台衡器或承载器与数据存储装置连接时的衡器识别号或承载器识别号等；

d）打印输出时，应同时打印数据识别信息；

e）检定时，所有关联的设备，无论其是否是法制计量设备，都要同时交检。

在GB/T23111提出的以上各防止作弊措施中，都离不开一个基本的技术手段----CRC校验和，其专业称谓叫做“循环冗余校验码”，CRC原本是数据传输的差错控制手段之一，大致原理是：将待发数据作为被除数，用一个“生成多项式（实际运用中相当于一个多字节二进制数码，例如CRC-16实际就是一个双字节数，CRC-32则是四字节数）”做除数进行除法运算，除得的结果是“商”和“余数”，将“商”放弃不用而将得到余数（校验码）随数据一同发出，在接收数据的一端，再用相同的“生成多项式”再次与收到的数据进行除法运算，如果计算所得余数与之前收到的余数相等，则收到的数据就是原发出的数据，如果不等，就表明数据被改变，从而确认数据是否是有效的。

六、结束语

尽管GB/T23111提出了对法制相关软件的管理要求，但由于在世界范围内缺乏足够的实践支持，与对衡器的计量要求和技术要求相比，其方法落实到实际的操作中的可操作性要复杂的多。目前来看还要先解决许多技术课题和管理课题：

1、需由设计制造方面承担的工作

与正常的衡器功能不同，衡器的防作弊功能是一种“后台”功能，衡器正常使用时，防作弊功能不运行，这并不影响正常的计量与操作功能的运行，只有进行防作弊功能检查时，这部分功能才发挥作用。这就要求衡器的设计制造者在实现衡器正常的计量与操作功能外，还要增加专门便于型式评价部门和计量管理部门查验的功能。

（1）CRC 校验和的产生：GB/T23111 提出的所有的措施都建立在 CRC 校验和的基础上，所以要有产生 CRC 校验和的技术方法。从原理看 CRC 校验和产生于除法，似乎应该在计算机程序中解决，但实际上用软件（计算机程序）解决就意味着占用宝贵的软件资源和工程人员无休止的重复从事大量低水平工作完成平时并不使用的程序，这是制造商不愿做的事，较廉价的解决方式是利用能够自动产生程序机器码、法制相关参数、法制相关数据等 CRC 校验和的专用存储器件，同时，该存储器件还能够读出所有校验码以及能够提供受保护的软件版本识别码和集成电路识别码。

（2）不可复位的事件计数器：该计数器只用于对更改法制相关参数的操作进行计数，既可用软件实现，也可用硬件实现，但用硬件实现比用软件实现成本要低的多，这个事件计数器必须安装在存储器件的内部，以防被更换。

（3）供授权人员设置密码的输入程序：激活衡器校准程序的密码应该是可反复设置的，以便检定人员确定和变更自己的密码。衡器出厂时使用一个通用密码，当检定后，检定人员将该密码更改为只有自己知道的密码以避免他人激活校准程序。

（4）供查验专用防作弊标识码的数据输出通道：必须为电子部件安装一个统一要求的、用于输出各种防作弊标识码的专用或兼用的数据输出通道，以供型式评价或周期检定时查验防作弊标识。与一般称重数据的输出通道不同之处在于，后者是按照用户要求设置的，而前者必须按照计量管理部门的要求设置。

（5）在主板上留有供粘贴防作弊标识的位置，其位置与空间还要便于使用工具读取。

2、需由计量管理部门承担和完成的工作

对于计量管理部门，增加防作弊功能检查后，管理手段与技术装备都要进行相应的增加。而且所增加的内容尚需多个部门分别准备。

（1）制定统一的接收专用防作弊标识码的数据接口标准，只有统一了该接口，型式评价部门以及各地衡器管理站、所才有读取各种衡器的防作弊标识的条件。

（2）研究和监制用于读取带有存储器件的电子装置中专用防作弊标识码的读出器具，并统一配置到各个基层衡器管理站、所。

（3）在型式评价报告书中增加有关防作弊功能检查的记录表。

（4）在型式批准证书中增加记载软件版本号、程序机器码校验和、主板及存储器件识别码等防作弊标识的栏目。

（5）在周期检定证书中增加记载软件版本号、程序机器码校验和、主板及存储器件识别码、事件计数器备案数等防作弊标识的栏目。

（6）研究和确定准备粘贴在主板上的防作弊标识的形式（如条码标签）与内容。

（7）研究和监制用于制作可粘贴的防作弊标识的制作器具，并统一配置到相关各个基层衡器

管理站、所以及授权的制造商。

（8）研究和监制用于读出粘贴在主板上的防作弊标识内容的读出装置，并统一配置到相关各个基层衡器管理站、所。

总之，从技术角度实现衡器的防作弊功能并不困难，但全面达到GB/T23111提出的防作弊要求还要社会各方面共同协作。再有，作弊行为是一种社会现象，仅靠技术手段不可能杜绝这种社会现象，杜绝社会上的衡器作弊现象，更需要衡器的设计制造者承担更多的社会责任。