对 OIML D-SW 国际计量软件指南的理解和浅析

梅特勒-托利多（常州）称重设备系统有限公司　戴　峰

【摘　要】 计量检定/校准、数据处理及测量不确定度分析中广泛应用计算机技术和测量软件，测量软件对测量结果的准确性和可靠性起到至关重要的作用。本文通过对 OIML D-SW 这一技术标准的理解和解读，介绍了国际上对计量器具软件的通用性要求。并为即将颁布的国家技术规范“计量器具软件测评指南”做了技术铺垫。

【关键词】 OIML　计量器具　软件

Key Words：OIML，Measuring Instruments，Software

伴随着信息技术的不断进步，计量器具的自动化、智能化程度日益提高，其测量控制也从简单电路系统到发展到复杂的嵌入式系统乃至工控系统，软件已成为计量器具中的一个核心部件。基于 OIML、NTEP 等现有标准中仅对计量器具的外部性能有所规定，所以国际计量法制组织（OIML）下属的 SC2 技术委员会起草了 D-SW，“General Requirements for Software Controlled Measuring Instruments”这一技术文件，该文件定义了对计量器具控制软件的通用要求，同时考虑了与加拿大计量软件标准和欧洲计量器具指令（MID）中的软件要求。

适用范围：1）指导对于计量器具控制软件功能和性能的符合性确认；2）提供给 OIML 技术委员会作为制定计量器具软件规范国际建议的基础；3）该指南仅适用于受软件控制的计量器具或电子设备。

OIML D-SW 代表了目前 IT 技术的水平，原则上可适用于所有依靠软件控制的计量仪表、电子装置和专用部件，在所有 OIML 的国际建议中需要被考虑。OIML-SW 国际计量软件指南主要包括大部分：1）对计量器具中所应用软件的要求；2）型式审批的具体规则；3）验证方法。以下根据我对这三方面的具体要求的理解逐一解释。

1．对计量器具中所应用软件的要求

OIML D-SW 中对计量器具软件的要求分为两类，一类为通用要求，适用于所有计量软件。第二类为特殊软件要求，仅适用于某些特殊应用领域的计量软件。

1.1　通用软件要求主要包括以下几部分：软件标识、算法和功能正确性、软件防护、硬件功能

支持。

1.1.1　软件标识

指所有计量相关软件（受到计量法规控制的软件）必须有软件版本识别信息，并能通过显示或其它设备接口读取。软件版本识别信息需要与形式审批备案的信息一致。

1.1.2　算法和功能性

指 A/D 转换结果、价格计算方法等算法和功能必须正确并符合有关标准要求，同时必须被正确地显示或打印。

1.1.3　软件防护要求

指计量器具中的法制相关软件需要具备对误操作或恶意更改的防范能力。例如，用户不按照说明书进行操作，应给出警告信息，而且计量结果不应该受到影响。另外，需要采用保护措施防止外界对计量器具中的法制相关软件的恶意更改。除了传统的保护手段如铅封以外，其它保护手段如密码验证等方法都可以被采用以确认软件更新的合法性。如果允许通过用户接口输入命令，那么这些命令必须在提交型式评定的软件文档中列出。所有与计量性能有关的参数设定也必须受到保护，同时可以被显示或被打印输出以便检验。采取这些机械铅封、电子或软件密码等保护手段是为了阻止对法制相关软件或参数的非法修改或使其留下纪录（如铅封破损）。

1.1.4　硬件功能支持

计量器具中的软件需要支持硬件的自检功能，如对 EEPROM、A/D 等关键部件的出错检测。送审文档中需要包括可以被软件检测到的所有错误列表以及检测方法或算法（如 EEPROM 中的 CRC 校验和）。计量器具软件同时需要确保计量性能的可靠性，如对于衡器软件，需要定时地检查传感器的零点和 SPAN 漂移，以及根据法定的检定周期确认是否需要提醒用户进行再次标定。

1.2　特殊软件要求

以下要求可能仅适用于某些特殊的计量（系统）软件。当某些特定技术（如 PC、Windows 等开放式软硬件平台）被用于计量设备时，需要考虑这些特殊的软件需求。

1.2.1　界定并分离法制相关部件并界定部件之间的接口

一个计量设备（系统）中的法制相关部件（包括软件和硬件）应该不受其它部件的影响。如基于工业 PC 的称重仪表中的计量软件和计量硬件（A/D 板）与系统内的其它部件通过接口（如 STD 总线）进行通讯时，其计量性能应不受其它部件的影响。

1.2.1.1　设备之间及子系统之间的隔离

一个计量系统中实现法制相关功能的所有子系统或电子设备需要被界定，并在提交型式批准的有关文档中加以说明。同时需要确保其法制相关功能和参数不可以被非授权的接口命令修改。

例如一台数字式汽车衡，数字式仪表和数字式传感器都是其中实现法制相关功能的子系统，两者之间是互相隔离的，通过特定的接口（如 RS-485 或 CAN 总线）进行通讯，但是通讯命令必须经过加密，以确保第三方无法通过该接口改变计量功能或伪造计量数据。

1.2.1.2　软件部件之间的隔离

所有执行法制相关功能或包含法制相关数据的软件模块必须要被分离出来，否则整个软件都将按法制相关软件受控。例如：在某些应用场合用计算机替代称重仪表，计算机上的称重功能被包装成一个称重处理动态链接库，该动态链接库完成从传感器获取称重信息，然后进行一系列的数据换算，转换成重量数据再在屏幕上显示。其它非法制相关软件可以通过调用该称重动态连接库获得重量数据。这就实现了一个复杂系统中法制相关软件和非法制相关软件的隔离。

如果法制相关软件部件与其它软件部件之间有通讯，那么必须定义软件接口，所有通讯必须通过该软件接口实现。软件接口包括程序代码和相关的数据域。所谓接口代码即接口调用函数，所谓相关数据域即通过接口函数交互的命令和数据，它们都需要遵从有关约定，并确保安全性。通讯法制相关软件部件及其接口必须在送审文档中加以定义并说明。

如果系统资源有限，必须优先保证法制相关软件部件所需要的资源。如处于一个多任务系统中，必须分配给法制相关软件部件更高的任务优先级，以确保它不被其它软件任务推迟或中断。

1.2.2　共享的指示装置

被法制相关软件或其它软件用来输出信息的显示或打印输出称为指示装置。法制相关软件输出的计量信息和其它软件输出的普通信息可能会共享一个指示装置（如显示器、打印机）。在指示装置共享的情况下，必须要求这两类信息有所区分，同时严格禁止非法制相关软件控制或改变法制相关软件输出的计量信息。

1.2.3　数据的存储和传输

如果一些应用要求计量数据的采集和使用不在同一时间或地点，就需要将计量数据在被合法使用在一个安全的环境中存储或传输。存储或传输过程必须符合计量法规要求。同时必须通过软件手段确保数据同步和数据完整性，并检查计量数据的采集时间。如果检查到有关计量数据不符合以上要求，则需要忽略该数据或标志为无效。

对于高保护等级要求的应用场合，还必须在数据存储和传输的两端采用加密、解密手段。所有涉及到法制计量要求的仪器、设备或子系统必须采用密钥系统，并且密钥仅允许在开启铅封的状态下被输入或修改。

1.2.3.1　自动存储

当法制要求的计量结果产生前，计量数据必须被自动存储。为了满足可能情况下长时间的数据存储，系统必须提供足够的存储空间。当存储空间用完时，仅在同时满足以下两大条件时允许删除有关存储数据：

1）按照先入先出的次序根据数据结构来删除数据

2）数据删除需要在特定的手工输入确认后方可执行

以上规则要求始终保留最新的数据，并且需要介入人工确认以确保删除操作可靠性。

1.2.3.2　传输延时

要求计量行为不受传输延时的影响。如果网络连接断开，计量数据不应丢失（在本地暂时存储）。

1.2.4　操作系统与硬件的兼容性，轻便性

生产商需要考虑硬件和软件环境是否合适，同时必须申明正确的计量功能执行所需要的最小资源和合理配置（CPU，RAM，硬盘，通讯方式，操作系统等）。在无法达到计量功能执行所需要的最小资源和合理配置时，必须采用技术手段禁止法制相关软件运行。

如果计量功能的正确执行需要一个固定的环境，那就必须采取措施确保环境的稳定性。特别是在采用通用计算机实现计量功能时，必须固定硬件、操作系统、系统配置甚至禁止打开机箱。

1.2.5　在线产品与型式样机的一致性要求

生产商需要按照批准的型式样机和备案设计文件的要求生产计量设备和法制相关软件。针对不同应用，具体有以下不同级别的一致性要求：

a）备案设计文件中注明的法制相关软件功能应该和产品中的一致（执行代码可以不同）

b）产品中部分法制相关软件的源代码与备案文件一致，其它符合 a)

c）产品中所有法制相关软件的源代码与备案文件一致

d）产品中所有法制相关软件的执行代码与备案文件一致

1.2.6　软件维护和二次配置

只有经过型式审批的法制相关软件版本才被允许使用。根据计量设备和所涉及的 OIML 国际建议的不同，针对其软件存在以下的不同要求。

1.2.6.1　版本升级后的合法性确认

计量设备软件可以通过本地（如透过串口 FLASH，通过软驱或光驱进行软件安装）升级或透过网络进行远程升级。在法制相关软件被升级后，计量设备不得立即被用于法制计量目的。必须请法制计量监督人员在现场验证该版本升级合法，然后才能将升级后的计量设备投入使用。

1.2.6.2　版本升级的跟踪

按照相应国际建议的要求，需要对计量设备中的软件版本升级进行跟踪。所有的版本升级都需要留下纪录。软件版本升级的跟踪步骤如下：加载、完整性检查、原始版本检查、安装、登录并激活。

升级的跟踪必须是自动实施的，升级过程中软件保护环境的要求与型式审批要求的保护等级一致。计量设备中必须应该保留一个不能被升级的法制相关软件，以实施软件版本升级跟踪并检测升级后的软件功能。同时需要采用技术手段保障升级软件的可靠性，例如验证其软件许可认证文件或是软件指纹（隐藏在软件中的一列代码）是否与型式审批的一致。如果验证失败，设备拒绝新版本软件的加载，继续沿用前一个软件版本。另外，需要通过校验和或 Harsh 码来见检查升级软件的完整性，为通过完整性检验的，设备同样拒绝新版本软件的加载。

为了保障对法制相关软件的管理和监督，要求通过一定技术手段在计量设备内建立以下的软件审计信息，其中需要保存：成功/失败的升级纪录；安装软件的版本和识别号；重要事件的时间纪录；

以及下载的软件补丁的识别号。任何对软件的升级操作都会被记录在软件审计信息中。

部分国家的法律要求软件升级前必须得到使用者的许可。

如果在计量设备中非法制相关软件与法制相关软件彼此独立，并且法制相关软件必须在打开铅封的前提下才能被升级，同时型式批准中允许非法制相关软件的升级不受控，那么，计量设备中非法制相关软件的升级就可以不必遵循上述规范。

2．计量设备软件型式审批

2.1　软件型式审批文档要求

计量设备制造商需要申明并记录程序功能、相关数据结构以及接口， 提供给计量主管部门进行计量设备软件型式审批。

标准的软件型式审批文档（所有计量设备均适用）基本包括：

- 对法制相关软件的描述
  - 软件模块、功能、对计量的影响
  - 软件界面描述
  - 软件识别号
  - 受保护的参数及保护手段
- 最小系统配置
- 操作系统加密手段
- 算法精度（A/D 转换输出的滤波，价格计算，归整等）
- 用户界面、菜单、对话
- 软件识别号和从计量设备中读取识别号的方法
- 接口命令集
- 存储或发送的数据流定义
- 如果软件中包含错误检测功能，列出错误种类和检测方法
- 系统硬件的总体介绍，如方框图，计算机型号，联网形式等
- 操作手册

除此以外，型式审批申请还需要附上证明计量软件符合现有计量法规有关条款的说明文件。

2.2　软件型式审批中的确认流程

尽管在 OIML 的一些文件中列出了对型式审批的测试流程，但是这些测试流程都是基于已知的测试设定和测试条件，并且依靠相对精确的计量装置。而对于软件而言。“测试”和“确认”意味着截然不同的两个概念。软件的准确性和正确性不能采用一般的计量测试手段来测量，而需要采用一些软件工程方面的测试和确认手段。对于不同的计量软件要求，需要采用合适的确认方法。OIML D-SW 列出了一些软件确认的方法，并针对计量软件的具体要求，给出了相匹配的软件确认方法。

2.3　常用的软件确认方法

软件工程学中常用的软件确认方法包括：设计文档审查、软件功能审查、代码走查（软件代码审查）、软件模块测试，这些方法在软件工程书中都有详细的说明，在此不再赘述。除了以上方法，OIML D-SW 还提出了法制计量功能确认测试和计量数据流分析方法。

法制计量功能确认测试主要是确认从原始测试数据到最终计量结果之间的计算过程和算法的正确性。举电子计价秤为例，其中的算法如：线性补偿、蠕变补偿、温度补偿、重量分度换算、零点跟踪、价格圆整等等。具体的确认方法主要是根据设备制造商提供的操作手册和有关计量法规，对产品的法制计量功能逐项进行测试，以确认其软件处理的法规符合性。

计量数据流分析，是指通过构造法制相关的计量数据流图，分析其所有处理过程是否受控。以电子计价秤为例，从称重传感器输出信号经 A/D 采样，经滤波模块、数据补偿模块、重量换算模块到价格计算、显示打印模块，每个流经的软件模块都需要被审查确认合乎计量法规。具体的确认方法是根据设备制造商提供的软件文档和源代码，再凭借软件知识来分析其数据流、软件模块结构及实现，并判断其是否满足计量法规要求。

2.4　确认程序

确认过程中包括了各种分析和测试，这一程序中主要考虑以下三方面：

1）常用的软件确认方法

2）测试结果的评估标准

3）测试报告中需要提供的结论

OIML D-SW 在附录中给出了不同重要等级的计量设备软件在确认程序的要求。

2.5　被测设备

OIML D-SW 要求提供制造商完整的计量设备用以做功能测试，如果因为设备体积等愿意无法提供整套设备，可以提交单独的计量模块用以测试。

3．检定

如果相关官价有关于计量设备的控制法规，有关部门需要定期在使用现场检查其软件标志和更改的合法性，以确认与符合型式批准样机的一致性。

4．重要度等级评估

OIML D-SW 要求对所有计量设备考虑具体情况区分对其软件控制的重要度：

1）欺诈行为的严重性：对社会的不良后果、计量商品的价值等

2）制造商实现软件控制的难度

3）可靠性要求：环境条件、出错影响

4）再次测量的可能性：许多场合的计量行为都具备不可重复性（如加油机，出租车里程计）

以上几项判断准则，有关计量设备符合的条件越多，对其软件实施法制计量控制的重要度就越高。

中国国家技术监督局于 2005 年指定江苏省计量技术研究所门组织人员依据 OIML D-SW 和

WELMEC WG7 起草了《计量器具软件测评指南》，将对国内的计量设备按其重要等级逐步实施软件测评，对某些涉及国计民生的计量设备如税控加油机、计价秤等将加强软件控制力度，以预防通过高科技手段进行作弊和欺诈行为。作者受江苏省计量技术研究所邀请参与了该指南的起草工作。个人认为，作为衡器厂商的设计人员，应该主动关注这一领域国际国内的有关标准并做好技术准备，以确保设计产品的标准符合性。在此，仅根据个人的浅薄理解，对 OIML D-SW 作一剖析，许多内容从原文根据个人理解意译，不当之处，请同行专家指正。

参考文献

〔1〕Document OIML D-SW Working Draft 1WD，“General Requirements for Software Controlled Measuring Instruments”. 2006-1-27，OIML TC5/SC2/N7