JJF

中华人民共和国国家计量技术规范

JJF 1182—2007

计量器具软件测评指南

Guide for Software Testing of Measuring Instruments

2007－08－21 发布　　2007－11－21 实施

国家质量监督检验检疫总局 发布

计量器具软件测评指南

Guide for Software Testing of Measuring Instruments

JJF 1182—2007

本规范经国家质量监督检验检疫总局于2007年8月21日批准，并自2007年11月21日起施行。

归 口 单 位： 全国法制计量管理技术委员会

主要起草单位： 江苏省计量科学研究院

参加起草单位： 梅特勒-托利多(常州)称重设备系统有限公司

江苏省江阴市富仁高科有限公司

本规范由全国法制计量管理计量技术委员会负责解释

本规范主要起草人：

水利民（江苏省计量科学研究院）

黄松涛（江苏省计量科学研究院）

参加起草人：

戴　峰（梅特勒-托利多(常州)称重设备系统有限公司）

徐东成（江苏省江阴市富仁高科有限公司）

封志明（江苏省计量科学研究院）

胡　强（江苏省计量科学研究院）

宋舒函（江苏省计量科学研究院）

目　　录

引言 …… (1)
1　范围 …… (1)
1.1　总则 …… (1)
1.2　应用 …… (1)
2　引用文献 …… (1)
3　术语和定义 …… (2)
4　计量器具软件的应用要求 …… (6)
4.1　计量器具软件技术特性分类 …… (6)
4.2　基本要求 …… (7)
4.3　特定要求 …… (9)
5　计量器具软件水平分类 …… (16)
5.1　软件设计和结构 …… (16)
5.2　软件保护 …… (18)
5.3　计量器具风险分类 …… (19)
6　型式评价 …… (20)
6.1　文档资料 …… (20)
6.2　基本要求 …… (20)
6.3　验证方法 …… (21)
6.4　验证程序 …… (24)
7　测评细则编制要求 …… (26)
7.1　引言 …… (26)
7.2　测评要求 …… (26)
7.3　测评方法 …… (27)
7.4　结果评价 …… (27)
附录A　计量器具(衡器)软件测评实例 …… (28)

计量器具软件测评指南

引　言

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。计量器具软件，尤其是涉及贸易结算、安全防护、医疗卫生、环境监测、资源保护、法制评价、公正计量等属于国家法制管理的计量器具软件的可靠性和保护能力，日益受到各国的高度重视。因此应对计量器具软件进行控制，以确保计量器具的计量特性符合法制计量要求。

本指南是参考 OIML D－SW（V－025）及 WELMEC 7.1(Issue 2)、WELMEC 7.2(Issue 1）并结合我国法制计量工作要求制定的。

1 范　围

1.1 总　则

本指南描述了针对计量器具软件测试的应用、水平分类、型式评价以及测评细则编制的基本要求、验证程序和主要验证方法，作为计量器具型式评价的指导性文件，也可作为计量管理部门日常监督管理及计最器具生产企业进行软件测试的参照文件。

计量器具计量特性的检定/校准应执行相应的国家计量检定规程或计量校准规范。

1.2 应　用

本指南的编制目的是为了支持公平一致的计量器具软件测试方法和水平分类，并使其对计量器具软件的测试结果具有可评估性。

本指南提出的计量器具软件应用要求，覆盖了不同种类的计量器具软件。各计量专业技术委员会应参照本指南，按计量器具技术特性的分类或应用领域分别制定相应软件测评的细则和程序，提出其特定要求。

以下技术要求能够直接应用于控制计量器具软件：

1）对计量特性有影响并起关键性作用的软件应予以特别标识并得到保护。该标识应易于获得，对软件进行保护的证据记录应保存足够时间。

2）测量数据和重要计量参数的存储或传递应得到足够的保护，以避免意外或有意的破坏。

3）计量器具应具有防止欺骗性使用的特性，同时应将误操作的可能性减至最小。

4）计量器具的计量特性不应受到与其连接设备自身特性或与其通讯的远程设备(包括无线接入设备)的影响。

2 引用文献

GB/T 16260.1—2006《软件工程　产品质量　第 1 部分：质量模型》

GB/T 16260.2—2006《软件工程　产品质量　第 2 部分：外部度量》

GB/T 16260.3—2006《软件工程　产品质量　第3部分：内部度量》
GB/T 16260.4—2006《软件工程　产品质量　第4部分：使用质量的度量》
ISO/IEC DIS 14102：1995《信息技术　CASE工具评价和选择指南》
OIML（TC5/SC2）D－SW(V－025)：2005《计量器具软件通用要求》
WELMEC 7.2（Issue1）：2005《MID软件指南》
WELMEC 7.1（Issue2）：2005《基于MID的软件要求》
GB/T 17544—1998《信息技术　软件包　质量要求和测试》
GB/T 9385—1988《计算机软件测试文件编制规范》
GB/T 8567—2006《计算机软件文档编制规范》
GB/T 11457—2006《信息技术　软件工程术语》
GB/T 15532—1995《计算机软件单元测试》
GB/T 18491.1—2001《信息技术 软件测试 功能规模测量 第1部分 概念定义》
JJF 1001—1998《通用计量术语及定义》
JJF 1015—2002《计量器具型式评价和型式批准通用规范》
使用本指南时，应注意使用上述引用文献的现行有效版本。

3　术语和定义

JJF 1001—1998《通用计量术语及定义》、GB/T 11457—2006《信息技术　软件工程术语》、GB/T 18491.1—2001《信息技术 软件测试 功能规模测量 第1部分 概念定义》中的有关定义适用于本指南。下面引用了一些最相关的定义并列出了计量器具软件测评工作中适用于本指南的其他定义和术语。

3.1　电子计量器具 electronic measuring instrument

利用电子方法或者配备电子设备进行测量的计量器具。对计量特性有影响的辅助装置应作为计量器具的一部分。

3.2　电子设备 electronic device

使用内置电子集成块执行特定功能的设备。它通常作为一个独立单元生产并可以被单独测试。

注：电子设备可以是一个完整的计量器具也可以是计量器具的一部分。

3.3　电子组件 electronic sub－assembly

由电子元器件组成，并有被识别的功能，通常作为电子设备的一部分。

3.4　稳定性误差 stability error

计量器具在使用一段时间之后和其最初固有误差的差别。

3.5　显著稳定性误差 significant stability error

大于相关规程和规范规定值的稳定性误差。

注：下列情况下，稳定性误差即使超过3.5定义的值也不作为显著稳定性误差考虑：

(1) 不能作为测量结果来解释、存储或传输的示值；

(2) 明显的错误示值；

(3) 由于稳定性保护装置的失效而发生的且不能被侦测到的稳定性误差。

3.6 稳定性保护器 stability protection facility

计量器具中能侦测到显著稳定性误差且能产生响应的器件。

3.7 校验器 checking facility

计量器具内能侦测到重大缺陷且能产生响应的器件。

注："有响应"是指计量器具具有任何足够的反馈信息（输出信号），如：光信号，声信号，测量过程的预防等。

3.8 自动校验器 automatic checking facility

运行过程中无需人工干预的校验器。

3.9 间歇自动校验器 intermittent automatic checking facility

在某些时间间隔，或多次测量周期的每一个固定时间间隔下运行的自动校验器。

3.10 永久自动校验器 permanent automatic checking facility

每次测量周期都运行的自动校验器。

3.11 非自动校验器 non－automatic checking facility

运行过程中需人工干预的校验器。

3.12 软件控制的校验器 software controlled checking facility

由软件操作的校验器。

3.13 审计日志 audit trail

连续的数据文件，包含了计量器具校准或配置参数更改记录、软件升级记录，其他可能影响计量特性的法制相关操作或事件记录的各类信息。每条记录都有惟一时间和日期标记。

可包括以下实现方式：

1）事件记录器，是指一系列记录的文件。文件中的每个记录包含事件描述、种类和时间，如：随着参数标识的变化而引起的计量器具特殊参数的变化，参数被更改的时间日期及参数的新值将被写入文件。实现事件记录的程序部分和包含事件数据的文件是法制相关的，应得到保护。

2）事件计数器，是指当计量器具的特殊操作模式发生变化，或计量器具特殊参数或法制相关数据发生变化，就予以计数的不可复位计数器。

3.14 数据域 data domain

程序中用于保存数据的参数、变量、堆栈。它可能属于一个或几个软件模块。

3.15 接口 interface

计量器具的连接部分，它允许几个计量器具、其组件之间，及软件模块之间建立通讯。

3.16 通讯接口 communication interface

利用电子、光学、无线电或者其他技术，在计量器具的组件之间自动传递信息的接口。

3.17 软件接口 software interface

由程序代码和专有数据域组成，在法制相关部分和软件模块之间接收、过滤和传输数据。

注：如果软件中存在除法制相关以外的部分，能够通过软件接口进行通信，并且在某种意义上可以被分离。通信软件部分通过某些可以被完全访问（读或写）的变量（或文件）交换数据。这些接口变量和向接口变量写入数据与从接口变量读取数据的程序代码构成了软件接口(这些接口变量符合硬件接口的线路)。接口变量可以通过诸如全程程序变量、功能参数或数据文件来实现。

3.18 用户接口 user interface

用户和计量器具，计量器具的硬件、软件信息之间传递的接口，比如开关、键盘、鼠标、显示设备、打印机、触摸屏、屏幕上的软件窗口以及生成窗口的软件。

3.19 法制相关参数 legally relevant parameter

受法规控制的计量器具或其组件的参数。法制相关参数可分为两种：类型专有参数和设备专有参数。

1）类型专有参数是指仅仅依赖于计量器具类型法制相关参数。此参数是法制相关软件的一部分。它们在型式评价的时候被固化在计量器具中。

2）设备专有参数是指基于单一的设备或计量器具的参数，包含可调整参数(例如灵敏度或其他修正的参数)和配置参数（如测量范围、分度值、测量单位）的计量参数，通常设备专有参数应受保护，只有在器具的特殊操作模式下是可调节的或者可选的。可分为不可变更的参数和授权用户可进行设置的参数。

3.20 法制相关程序部分 legally relevant program part

实现受法制控制功能的程序代码部分，见图1。

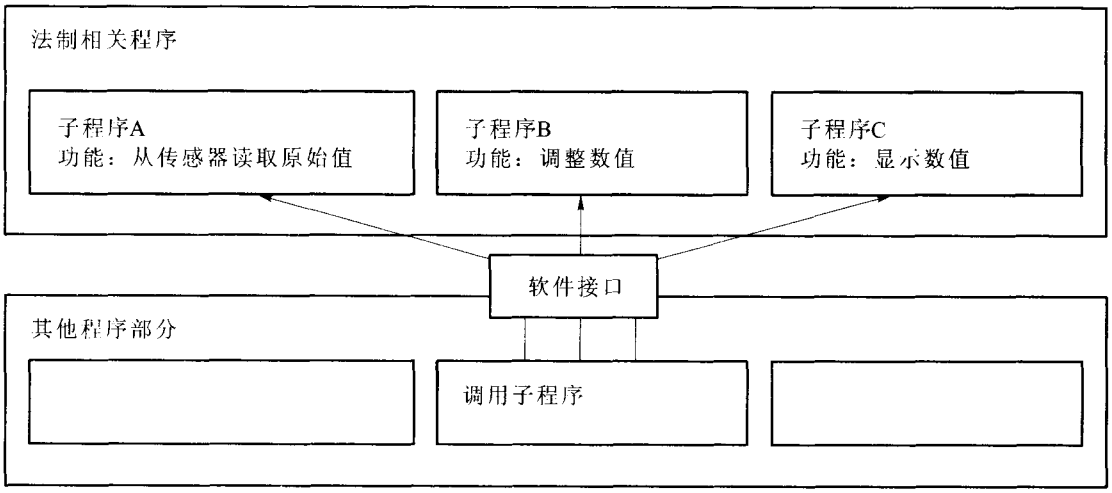

图1 实现法制相关功能的法制相关子程序和其他被分离的程序部分的举例

3.21 法制相关软件部分 legally relevant software part

受法规控制的计量器具、装置、组件中定义或执行功能或表述特性的软件模块部分。

3.22 固定法制相关软件部分 fixed legally relevant software part

法制相关软件中与获型式批准具有相同执行代码的那部分。

3.23 闭环网络 closed network

用户的身份、功能、位置及数量确定的网络。

3.24 开放网络 open network

任意用户(任意功能的计量器具)组成的网络。用户数目、身份和位置可以是动态的，并对其他用户是不可知的。

3.25 计量数据的长期存储 long－term storage of measurement data

计量过程结束后，为法制目的而进行的数据存储。

3.26 软件标识 software identification

和软件或软件模块密切相关的可读字符串。计量器具使用过程中可以进行检查。

3.27 程序、数据、参数完整性 integrity of programs, data, or parameters

程序、数据、参数在使用、传输、存储、维护过程中不被非法或无意修改的特性。

3.28 软件模块 software module

由子程序和数据域组成的逻辑实体。

3.29 软件保护 software protection

通过封缄保证计量器具软件或数据域的安全。只有封缄被移动、损坏、破坏后软件或数据域才会被更改。

3.30 封缄 sealing

以防对计量器具的硬件或软件部分未经授权的访问而对相应组件或部位所做的特别保护。

3.31 软件分离 software separation

计量器具中的软件可以被分成法制相关部分和非相关部分，两部分可以通过软件接口进行通讯。

3.32 可接受方案 acceptable solution

软件模块、硬件单元或特性满足特定要求的设计及原则。方案提供满足特殊要求的举例。

注：一个可接受方案不排斥其他任何满足要求的方案。

3.33 软件一致性 conformity of software

生产中计量器具软件与获型式批准的软件类似的程度。

3.34 功能测试 performance test

检验被测计量器具能否完成应有功能的测试。

3.35 软件测试 software test

根据特定程序测定一个或多个软件特性是否符合要求的技术操作。包括技术文档分析或在受控环境下运行程序，目的在于检验软件是否满足规定的需求或是发现预期结果与实际结果之间的差别。

3.36 黑盒测试 black box test

基于需求和功能性的测试。

3.37 白盒测试 white box test

基于内部设计和代码的内部逻辑知识，覆盖全部代码、分支、路径、条件的测试，

白盒测试又叫“结构测试”。

3.38 测试用例 test case

对一项特定的软件进行测试任务的描述，体现测试方案、方法、技术和策略的文档，内容包括测试目标、测试环境、输入数据、测试步骤、预期结果、测试脚本等。

3.39 验证 validation

通过提供客观证据对计量器具软件的规定要求已得到满足的认定。

3.40 认证 certification

第三方依据程序对计量器具软件符合规定的要求给予书面保证。

3.41 评价模块 assessment module

用于测量软件质量特性或属性的评价技术包。

注：包括评价方法和技术要求，对评价的输入，待测量和待收集的数据，支持的规程、规范和工具。

4 计量器具软件的应用要求

根据 ISO/IEC 9126 规定的质量特性要求，计量器具软件可从功能性、可靠性、易用性、效率、可维护性和可移植性等六大因素进行测试，并按计量器具软件的技术特性分类或应用领域制定相应的软件测评细则和程序，满足相应要求。

4.1 计量器具软件技术特性分类

计量器具软件按其技术特性可分为基于嵌入的计算机系统（用 P 类型表示）及基于通用的计算机系统（用 U 类型表示），并分别具有以下特性。

P 类型计量器具软件具有的特性：

1）内置的应用软件用于计量，包括法制控制部分和其他部分；

2）软件作为一个整体设计，除非可以软件分离，否则视作一个整体；

3）用户接口仅用作计量目的，通常操作模式下受法制控制，也可以切换到不受法制控制的操作模式；

4）操作系统不含用户界面；

5）软件及其运行环境恒定，没有编程和更改法制相关软件的手段，只能受控升级；

6）允许存在通过受控的网络交换数据的接口；

7）允许计量数据本地或远程受控存储。

U 类型计量器具软件具有的特性：

硬件部分：

1）基于通用的计算机系统，可以作为闭合网络的一部分独立存在，如以太网、令牌环网，或开放网络的一部分，如因特网。

2）作为计算机扩展单元的传感器应通过闭合的通信线路链接，或通过网络连接，传感器之间应相联。

3）用户接口可以从不受法制控制的操作模式切换至相对的受控模式；

4）数据可以本地或远程存储。

软件配置部分：

5）可使用任何操作系统，允许有受法制控制或不受控的计量器具应用软件。

6）操作系统和低版本的驱动程序如视频驱动、打印驱动、磁盘驱动仅在执行特殊测试任务时受法制控制。

4.2 基本要求

基本要求适用于各种计量器具软件。

4.2.1 软件标识

要求：法制相关软件需有清晰的、带软件版本号或者其他特征性的标识。标识可以含有多个部分，但须有一部分专用于法制目的。标识和软件本身是紧密关联的，在启动或在操作时应在显示设备上显示出来。如果一个组件没有显示设备，标识将通过通讯端口传送到另外组件上显示出来。

目的或解释：每一在用的计量器具须与获批准型号的计量器具一致。软件标识可以使得软件测试机构检测人员、计量管理人员和用户确定其是否一致。

举例：

1）软件包含一个数值或其他字符的文本字符串用以确定安装的版本。当设备启动时，或在计时器循环控制下，字符串在计量器具的显示器上显示；

2）通过 CRC16 等算法计算执行代码的校验和，替代或附加在 1）中的字符串上作为标识符显示。

4.2.2 算法和功能的正确性

要求：计量器具的计量算法和功能应正确(如模/数转换结果、价格计算、数据修约、测量不确定度评定等)，并满足法规要求和用户需要。计量结果和附属信息应正确地显示或打印。

算法和功能应该是可测的。

4.2.3 软件保护

4.2.3.1 预防误操作

要求：通过软件保护，使得计量器具误操作的可能性降至最小。

误操作是指由意外的物理因素或软件影响(崩溃，病毒感染)或用户对计量器具无意识的操作引起的法制控制下的程序部分或数据的更改。

目的或解释：软件控制的计量器具在功能上常常比较复杂，用户需要较好的操作手册以正确使用并能得到正确的计量结果。结果的表达须明确无误。

举例：用户根据菜单操作，法制相关功能在某一级菜单下。如果测量值可能因某操作而丢失，用户应被警示，且被要求在此项功能执行前进行另一项操作。

4.2.3.2 防止欺骗性使用

要求 1：计量准确的软件能防止未经许可的修改，装载或通过更换存储体来改变。

目的或解释 1：对电脑是计量器具组成部分、有操作系统或是有装载软件选项的计量器具，除采用机器封缄外，应通过软件或硬件本身采取技术措施。

举例 1：

机架中包含封缄的存储体或存储体被封死在印刷电路板上。

如采用的是可写存储体，写保护应封死。电路设计时须防止通过跳线短路使写保护

失效。

重要的计量软件所存放的设备或组件应被机械封缄。严格控制通过简单加密方法，比如：对组件和通用计算机之间的数据传输加密，来更换软件部分。密钥应隐藏于通用计算机的法制相关程序中。仅有这段程序算出相应的值，能解读和使用密钥。其他程序因不能对密钥译码而不能更换软件部分。

要求 2：从用户接口输入的命令，在型式评价时提交的软件文档中应有完整描述。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骗性使用的目的。

目的或解释 2：软件测试机构检测人员、计量管理人员决定是否所有备档的命令是可接受的。

举例 2：所有来自用户接口的输入被输入命令的程序过滤，只有备档的命令才会被允许通过，其余的将被丢弃。这段程序或软件模块是法制相关的。

要求 3：设备专有参数只有在器具的特殊操作模式下可以被调整或是选择。他们被分成两类：一类是固化的（即不会改变的），另一类是由被授权的，如计量器具用户，软件开发者来调节的可输入参数。

型式专有参数对同一型号的样品来说具有同样的值，在型式评价检测时是不变的。

要求 4：通过保护措施，如机械封装或电子加密措施等，防止未授权的访问或者访问时留有证据。

要求 5：通过“电子校验和”验证。

要求 6：采用第三方的信号与采集标准信号比对来验证。

4.2.4 硬件特性支持

4.2.4.1 缺陷侦测支持

产品设计需要故障检测。软件开发者可以在软件或硬件中自由设计检查工具，也可以让软件支持硬件检查工具。

要求：如果软件涉及故障检测，需要有相应的提示。比如，当某故障被检测到时，计量器具就应失效或是产生一个报警报告(日志)。

提交型式评价的文档中应包括故障列表说明。为便于理解，也应有侦测算法的描述。

举例：每次启动法制相关程序会计算程序代码与法制相关参数的“校验和”。这些值已经被事先算好并存在器具中，如果算出的值和预存的值不匹配，程序将停止执行。如果计量没有中断，软件计时器将会循环计算校验和。一旦有错误被检测到，软件会显示错误信息或打开错误指示器，并把发生的时间写入日志。

4.2.4.2 稳定性保护支持

软件开发者可以在软件或硬件中自由设计检查工具，也可以让软件支持硬件检查工具。

要求：如果涉及稳定性检测，需要有相应的提示。比如，当有危及稳定的因素被检测到时，计量器具就应失效或是产生一个报警报告。

稳定性保护工具文档应包含被软件侦测的稳定性错误列表及侦测算法描述。

举例：气体排放分析仪在器具稳定间隔时间之后，需要进行重新校准。当到达持续的间隔时间，软件会给出一个警告，如果是超过了一定的时间，将停止器具工作。

4.3 特定要求

特定要求是针对某些种类的计量器具或应用领域的技术特性。本节中给出的要求基于信息技术的典型技术解决方案，并非在所有法制应用领域中采用。当某技术在计量系统中使用时，应满足除在4.2描述基本要求外，还需考虑下列特定要求。

4.3.1 计量数据自动和长期存储(用L表示)

计量数据存储应具有所有必要的相关信息，能及时保存并且在不同时间、不同计量地点使用或数据验证。

最终测量值用于法制目的时，计量数据必须要自动存储。用于计量数据长期存储的存储器应有足够容量。当存储容量不足时，允许在满足下面要求的情况下删除存储的数据：

1）数据按照存储顺序删除，且考虑特殊应用的有关要求；

2）数据通过特定人工操作才可被删除。

注：通常，涉及存储容量需求的同一数据域（如：程序变量）应充分考虑累计的计量值的存储容量。累计的计量值，须及时更新，如：电量、加油量等。

法制相关计量数据需长期存储时，需要满足以下要求。

法制相关软件部分是指准备存储或发送的数据，或在读、接收数据后校验的软件模块。通过软件方法保护数据，保证它们的标识、计量时间信息正确性、真实性和完整性。

表1中列出了三种不同的长期存储的技术方案。

表1 长期存储的技术方案

集成存储	简单嵌入式计量器具中，用来存储计量数据或参数的集成的存储器如：RAM，闪存，硬盘。无外接有效工具或方法来编辑或改变数据。
通用计算机存储	通用计算机，图形用户界面，多任务操作系统，受法制控制和不受法制控制的任务可并行作业，存储器可以从计量器具中移走，或者其中的内容可以拷贝到计算机里或计算机外的任何地方。
可移动的或者远程（外接）的存储器	任何基本的计量器具(嵌入式的或使用通用计算机的)，它的存储器可以从中取出。这些存储器可以是软盘，闪卡(闪存)，或者网络中的远程数据库。

4.3.2 通讯系统传输(用T表示)

计量器具需要在网络上传输或接收计量法制相关数据时适用。

计量数据传输应具有所有必要的相关信息，能在不同时间、不同地点使用或数据验证。

如果计量数据在不安全的环境中存储或传输，在它们被用作法制目的前，需满足下列需求：

要求1：传输的计量数据应含有必要的相关信息。且不应受到传输延时的影响。

数据包括下面各项信息：

1）带单位的测量值；

2）测量时间戳；

3）测量设备标识或测量地点；

4）明确的测量标识，如：与打印在票据上的值对应的连续数字。

数据传输中，发送方计量器具应具有一直等待到接受方发出数据集正确接受的确认信号。发送设备保留数据在缓存中，一直到接受到确认信号。缓冲区大小可以容纳多个数据集，可按 FIFO 方式调度。

要求 2：从不安全的存储器读出或从不安全的传输通道接受数据之后，应通过软件方法检查并保护数据，保证它们的标识、计量时间信息正确性、真实性和完整性。如果检查到有不规则的数据，必须丢弃。

发送设备的程序计算数据集的检验和(16 位及以上)并把它附加到数据集。它使用秘密的初始值代替所给的标准值。初始值作为一个常量存在程序代码中。接受或读程序也存有这个初始值。使用数据集之前，接受程序计算校验和并与所存的初始值比较。如果两个值匹配，则数据集没有被伪造。否则，程序认为是伪造的并放弃这个数据集。

要求 3：高保护水平应有加密方法。用于加密的密码应隐蔽且安全地存于计量器具或相关组件中。加密强度应符合国家相关标准要求。当封缄被破坏时，需提供一定的方法，这些值才能被输入或读取，且这种方法应受到保护。

举例 3：存储或发送程序的电子签名生成：首先计算一个哈希值，其次把这个哈希值用公钥的密钥加密，得到签名。它被附加在存储的或传输的数据集中。接受方同样计算此数据集的哈希值，并用公钥对附于数据集的签名解密。比较计算和解码得到的哈希值，如相等，数据没有伪造。为证明数据的来源，接受方必须知道公钥是否真正属于发送方即发送设备。另外，公钥会在计量器具上显示出来，在这一领域经过法制验证的公钥是和计量器具的序列号一起注册的。如果接受方确信使用了正确的公钥来解密签名，则不怀疑数据的真实性。

表 2 中列出了三种最常见的网络结构。最简单的是受法制控制的计量器具组成的网络结构，成员(任意功能的计量器具)是基本固定的。闭合网络，部分受法制控制，其成员不受法制控制，但是可知的并且在操作过程中是不改变的。开放网络对使用人员的身份、功能、存在和位置是没有限制的。

表 2　常见的网络结构

序　号	结　构　描　述
1	闭合网络，完全受法制控制 成员的数量是固定的，而且有清楚的身份、功能和连接位置。所有计量器具受法制控制，网络中不存在不受法制控制的计量器具。
2	闭合网络，部分受法制控制 成员的数量是固定的，且有清楚的身份和连接位置。不是所有的计量器具都受法制控制的，因此他们的功能是不可知的。

表 2（续）

序　号	结　构　描　述
3	开放网络 任一成员能连接到网络中。参与其中计量器具的身份和功能及其位置对其他成员来说可能是不可知的。任何包含具有红外或无线通信网络接口的法制受控计量器具的网络都可以认为是开放网络。

注：哈希值(Hash Value)是对原程序进行密码运算(也称单向散列运算)所得到的结果。其特征如下：

1）结果允许数据单元的接收方用以确认数据单元的来源和数据单元的完整性，并保护数据，防止被人进行伪造；

2）有固定的长度，运算是不可逆的；

3）不同的程序其哈希值是不同的，而相同程序其哈希值是相同的并且惟一。

4.3.3　相关组件指定与分离和组件接口指定(用 S 表示)

计量系统的计量部分(不管是软件还是硬件部分)不能非授权地被计量系统其他部分影响。

当计量器具具有用来与其他装置通讯的接口，或计量器具里除计量部分外，还有其他的软件部分，应对组件指定与分离和组件接口指定。

要求 1：计量系统的用来执行法制相关功能的组件或电子设备要有标识，在文档中有清楚定义。它们组成计量系统的法制相关部分。

目的或解释 1：软件测试机构检测人员、计量管理人员决定这部分是否完整，从更深层面来评价计量系统的其他部分是否可以排除在法制相关部分之外。

要求 2：非授权的命令通过接口时，不会对组件和设备的相关功能和数据产生影响。

组件或设备中启用的功能或数据交换的每条命令都应有一个明确的任务。命令和它们的作用应在提交型式评价时所附软件文档中完整表述。没有如命令那样声明和备档的信号或代码对组件或设备的功能和数据将不会起作用。软件开发者需声明命令文档的完整性。

举例：带有的光接口计量系统，其接口用来传输读出的测量值。计量器具存储所有相关的量并保存这些测量值在足够长时间内有效。在这样的计量系统中，计量器具本身是法制相关软件部分。

计量器具的软件能接受所需“量”的测量命令。它把测量的量和附加信息，如时间戳、计量单位结合在一起传回请求的计量器具，软件只接受有效允许“量”的测量命令。对其他无效的命令，软件将丢弃，并返回一个“错误”提示信息。

带封缄的机架里的跳线可以设置计量器具的两种操作模式。一种是软件的校验模式，另一种是非校验模式。在非校验模式中，命令集与校验模式的比较有所不同。比如，有的命令可能调整校准因子，而在校验模式中是不可的。

注：“量”是指需要测量的参数。

4.3.3.1 设备和组件的分离

组件或执行法制相关功能的电子设备应有详细说明。这些“法制相关”组件和设备的接口应有清楚的定义且写入文档，以表明相关功能和数据，不能非授权地受到由接口收到的命令影响。

组件或设备中每个开启的功能或更改数据的命令应有明确任务要求。命令和执行的效果应在软件文档中被完整描述以上报型式评价。

软件开发者应声明命令文档是完整的，没有在文档中声明和记录的信号或代码，对组件或设备的功能和数据不应起作用。

如果法制相关组件或设备与其他法制相关组件或设备互相影响，参见4.2.3。

4.3.3.2 软件部分的分离

要求1：所有执行法制相关功能或包含法制相关数据域的软件模块（程序，子程序，对象）组成计量器具(设备或组件)的法制相关部分，应有如4.2.1所描述的软件标识。如果软件分离是不可能的或不需要，软件整体将被作为法制相关部分。

举例1：一个计量系统有多个载入单元同时连接显示测量值的电脑。电脑上的法制相关软件通过把所有实现法制相关功能的程序编译到一个动态链接库的方法来与非法制相关部分实现分离。一个或多个非法制相关应用程序可调用库中的程序，这些程序从载入单元接受测量数据，计算测量结果，并显示在软件的窗口中。当已完成法制相关功能后，控制权将还给非法制相关应用程序。

要求2：如果法制相关的软件部分与其他的软件部分通讯，软件接口应被定义。所有的通讯只能通过这个接口执行。法制相关的软件部分和接口应在文档中详细说明。软件的所有法制相关功能和数据域的描述应使型式评价机构能够正确做出软件分离。接口由程序代码和专用的数据域组成，命令或数据在软件的各部分之间进行交换，由软件的写代码存储到专用的数据域再通过软件的读代码读出。读和写程序代码是软件接口的一部分。声明的软件接口不会被绕过而直接读写。

在软件法制相关部分，每个开启的功能或数据更改的命令有明确任务要求。

软件开发者应声明命令文档是完整的，没有在文档中声明和存档的命令对软件的法制相关部分应不起作用。

举例2：要求1中软件接口的举例是通过参数和库中程序返回值来实现的。库中数据域没有返回指针。接口的定义固化在编译过的法制相关库中且不能被任何应用程序所改变。绕过参数和库中的数据域地址直接访问是不可能的，这样的编程较复杂。

要求3：软件分离意味着：如果系统资源有限，法制相关软件的优先级高于法制不相关软件。测量任务(由法制相关软件部分实现)不得因为其他任务延时或锁定。

解释3：对软件开发者应采取相应技术手段预防程序员绕过接口，保证没有隐藏的命令。

举例3：要求1、要求2中，法制不相关应用程序控制着库中法制相关程序的启动。省略这些程序的调用将不会发挥系统法制相关功能的作用。下面在系统中运用的规定可满足要求3。

——载入单元发送带加密的测量数据。

——解密的密钥藏在库中，只有库中的程序知道密钥，会读、译、显示测量值。

——一旦应用程序试图读和处理测量值，它将被迫使用库中执行所有法制请求功能的法制相关程序。

要求 1 到要求 3 的举例仅对一个水平分类较高的计量器具软件来说是可接受的技术方案。如果需要更高的防止欺骗性使用保护或有必要更高的一致性时，以上所述的软件分离是不可接受的。此时，软件须作为一个整体被法制控制。

4.3.3.3 共享示值

通过显示设备或打印机给出软件法制相关部分的信息和其他信息时，示值信息的差别应清楚和确定。

要求：提供可以区分不同远程地点的计量器具或计量场所的名称或标号。

举例：在加油系统的打印输出方面，含计量结果的行应打上星号。这样可以对每一票据向用户解释。如果有必要更高的防止欺骗保护，不应使用单独的打印输出，应有更高安全措施的计量器具来显示计量结果。

4.3.3.2 条要求 1 是可以显示在多个显示设备上，要求 3 是满足软件分离和密码的要求时，也允许显示在多个显示设备上，测量值显示在不同的软件窗口。要求 3 中所说的方法保证了只有法制相关程序部分才可以读测量值。在操作系统的每一窗口采用附加的技术方法来满足 4.3.3.3 中的需求。窗口中显示的法制相关数据是由动态链接库中的程序来产生和控制的。在测量过程中，这些程序循环检查相关的窗口是否仍在当前存在其他窗口之上，如果不是的话，就将其当前显示。

如果有更高防止欺骗性使用的保护，非定制的通用计算机不合适作为计量系统的一部分，有必要用其他硬件来保证足够保护水平。

4.3.4 维护和升级(用 D 表示)

只有具有如下特性的计量器具才可以升级。

硬件：

计量器具要受法制控制。可以是 U（通用的计算机系统）或 P（嵌入式系统）型。通讯连接可以是直连方式，如：RS232，USB，或通过部分/全部受法制控制的闭合网络，如以太网、令牌环网，或是开放网络，如因特网。

软件：

计量器具软件可以全部受法制控制，也可以被分离。法制相关软件的升级必须满足下列要求，如果不能软件分离，全部的升级都要符合要求。

只有批准的法制相关软件版本允许使用或升级使用。对同种计量器具，可有不同的升级方法。下列 4.3.4.1 和 4.3.4.2 中选项可同等选择，通过检查确认升级软件是否符合要求。确认的内容应包括在操作过程中的软件同一性、调整的合法性及模式(所在国可能的相应特性)的一致性。

跟踪升级中，升级分成：载入，安装/激活两步。即软件在载入之后暂存，而不是马上激活。因为如果检验失败的话，将丢弃载入的软件而保持老版本。

验证升级中，软件在安装前也有可能载入后暂存，不过它是由技术方案来决定的，也可能一步完成载入和安装。

计量器具软件升级流程图如图 2 所示。

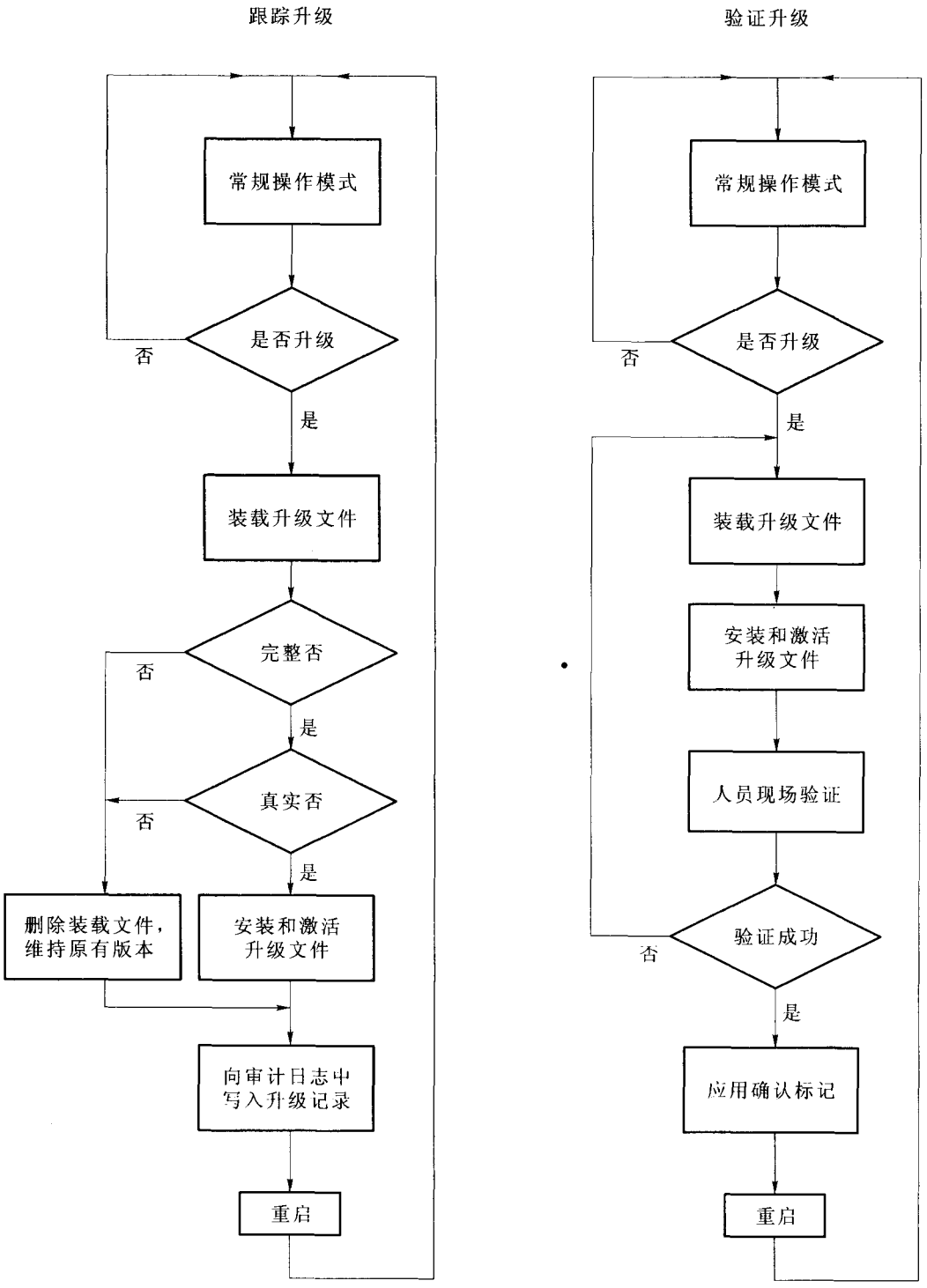

图 2　软件升级流程图

4.3.4.1　验证升级

软件可以从本地直接在计量器具装载，或通过网络远程升级。计量器具法制相关软件升级（更换另外批准的版本或重新安装）在得到证实且更新加密措施后，才能用以法制目的。校验人员必须在工作现场。载入和安装可以是两个步骤，也可以合并成一步，

取决于技术方案的需要。

4.3.4.2 跟踪升级

跟踪升级是对校验过的计量器具或设备更换软件的程序，更换之后可以不要验证。跟踪升级嵌入计量器具软件的要求（4.3.4.2 1）到4.3.4.2 6））应与法规要求一致。可以从本地直接在计量器具装载或通过网络远程升级软件。升级记录保存在记录索引里。它有以下几步：装载、完整性检查、来源检查(鉴定)、安装、登录和激活。

1）软件的跟踪升级应是自动的。软件升级程序完成的环境(硬件、软件、文档资料）应与型式评价要求的一样。

2）计量器具（设备、组件）具有固定的不可升级的法制相关软件，这部分应具备必要的用来满足跟踪升级需求的检验功能。

3）通过一定的技术方法用来保证载入软件的真实性，即保证载入软件来源于计量器具的所有者。如载入软件检验失败，计量器具将放弃载入的软件。可以由如签名的加密方法实现。载入时检验签名。

4）通过一定的技术方法来保证载入软件的完整性，即软件载入前没有被非授权的更改。如载入的软件检测失败，计量器具放弃它并采用前版的软件。可通过加入载入软件的校验和或哈希值来实现，在载入时验证。

5）通过一定的技术方法来保证事后的控制，如器具的记录索引完全可追踪法制相关软件跟踪升级。这一要求使得检查变得可信，通过反向追溯适当一段时间后法制相关软件跟踪升级，使得法制受控器具的计量监督变得可靠。记录索引包含以下信息：升级过程成功/失败、安装版本的软件标识、事件时间戳、下载处标识。不论升级成功与否，每次升级须有对应记录条目。

6）通过一定的技术方法来保证只能经计量器具的用户明确同意才可升级。应依据国家法规具体落实这一需求。

7）若1）到6）的需求不能满足，仍有可能升级法制不相关的软件部分，此时，应满足下列需求：

1）根据4.3.3.2，法制相关和不相关软件有明显区分；

2）整个法制相关软件部分是固定，即不能不破坏密封而升级；

3）在型式评价报告中描述的法制不相关部分升级是可接受的。

4.3.5 操作系统和硬件兼容性，可移植性（用E表示）

计量器具软件的软件开发者应确定硬件和软件环境匹配。软件开发者应声明正确运行软件功能所需的最低配置(处理器、存储器、硬盘、通讯、操作系统版本)。如最低配置需求不满足，法制相关软件应提供技术方法防止运行。

应提供保证软件功能正确运行的恒定环境。

应保持法制相关软件运行环境的恒定(硬件、操作系统、整个系统配置)，下列情况应避免使用没有保护措施的通用计算机：

1）若需求高符合性；

2）若需求固定的软件，常用于跟踪升级；

3）若须使用加密算法或密码。

另外：批量生产的计量器具和获型式批准的计量器具应当一致。可以有不同层次的一致性要求。

1）每台计量器具所带文档中描述的相关法制功能与型式批准的要一致(执行代码可能不一样)。

2）部分法制相关源代码要与型式批准的一致，法制相关软件其他部分遵从上述1)条的要求。

3）所有的法制相关源码要一致。

4）所有的执行代码要一致。

专业委员会对每种器具或应用领域都要规定相应水平。对特种器具可从这些一致性水平中选取，由计量管理部门确定其水平定义。

5 计量器具软件水平分类

参照4.2及4.3的应用要求，计量器具软件技术特性分类及软件开发者、软件测试机构、计量管理部门的不同要求对计量器具软件实施不同的水平分类。

软件开发水平主要针对软件开发者。

软件检验水平主要针对负责型式评价的软件测试机构。

软件符合水平主要针对计量管理部门。

5.1 软件设计和结构

5.1.1 计量器具软件应按照本指南的要求设计，使其法制相关功能的一致性易于评价。

1）软件开发水平

低等：只要其相关功能符合指定要求，软件结构等可不考虑。

中等：软件流程的总体设计、详细设计和测试方案、用户手册等应清晰描述。

高等：软件及其文档全面符合软件工程CMM2的要求。

2）软件检测水平

低等：检查指定要求的功能符合性。

中等：检查软件的总体设计、详细设计框图和测试方案。

高等：检查软件源码及其软件工程涵盖的文档，符合软件工程CMM2的要求。

3）软件符合水平

低等：软件开发者对软件的修改应有记录。

中等：修改需要符合软件工程CMM2的要求，并提交计量管理部门备案。

高等：总体设计和详细设计等不允许修改，编码的修改应提交计量管理部门，获得批准后方可实施。

5.1.2 法制相关软件应按照不受也不允许受其他软件影响的方式来设计。

1）软件开发水平

低等：清晰分离法制相关软件和非法制相关软件，以低耦合的方式来交互以实现法制功能。

中等：法制相关软件与非法制相关软件有严格的交互规范，按照该规范来交互。

高等：法制相关软件的交互规范应受保护。

2）软件检测水平

低等：检查法制软件和非法制软件耦合性。

中等：检查交互规范，使用可能的方式测试交互规范。

高等：通过源码测试，分析交互规范的受保护程度。

3）软件符合水平

低等：不影响法制软件的功能，软件开发者对非法制软件做出修改应有记录；对交互接口做出修改，应到计量管理部门备案。

中等：影响法制软件的功能、接口和调用方法的非法制软件修改，应提交计量管理部门，获得批准后方可实施。

高等：除了修正错误，法制软件应位对应；对不会影响交互接口的非法制软件修改应提交计量管理部门，获得批准后方可实施。

5.1.3 法制相关软件应按照不受也不能够被计量器具接口所更改的方式来设计。

1）软件开发水平

低等：接口有严格的安全使用规范，按规范操作接口不会更改法制相关软件。

中等：接口受保护，有相关的法制软件来检查接口使用是否符合规范。

高等：没有计量器具接口或计量器具接口应被密封。

2）软件检测水平

低等：检查接口的安全使用规范，按照使用规范使用接口来检测。

中等：按照可能的非安全使用情况测试接口。

高等：源码测试，保证接口检测的完整性；或检查接口的密封性。

3）软件符合水平

低等：接口功能基本不变的情况下，接口硬件、接口的调用方法发生更改，对法制相关软件的修改到计量管理部门备案，在软件标识上予以标明。

中等：接口硬件、接口功能、接口的调用方法发生更改，需要提交计量管理部门备案，如对法制软件部分构成影响应获得批准后方可实施。

高等：除了修正错误外，该模块应位对应；必要的错误修改需要提交计量管理部门获得批准后方可实施。

5.1.4 软件的功能性应设计为具有可测试性。

1）软件开发水平

低等：软件的原始输入和输出结果可以获知。

中等：软件的中间重要数据可以获知。

高等：软件能进入授权的调试模式，提供足够的检测点。

2）软件检测水平

低等：检测软件的原始输入和输出结果。

中等：基于软件文档找出中间步骤，获取数据来检测。

高等：分析源码，利用足够多的检测点来检测。

3）软件符合水平

低等：计量器具的原始输入和输出结果方法不可更改，若更改应到计量管理部门备

案。

中等：获取中间数据和功能的接口不可更改，若更改要到计量管理部门备案。

高等：源码的检测点和授权的调试模式不可更改，若更改要到计量管理部门备案。

5.2 软件保护

5.2.1 法制相关程序和数据应被保护以避免偶然的或无意的更改。

1）软件开发水平

低等：程序和数据有定时的或与机器开关机结合的检测方法、恢复方法。

中等：每次对重要程序、重要数据的使用都要有减少错误的检测和恢复方法。

高等：增加硬件的机制来保护重要程序和数据。

2）软件检测水平

低等：按照用户手册正常操作，计量器具的法制程序和数据不会被无意更改。

中等：非正常操作计量器具或在高频环境和其他可能恶劣环境中操作计量器具，计量器具法制程序、数据、功能不会更改。

高等：分析源码，检测硬件的稳定性。

3）软件符合水平

低等：不涉及法制相关程序、数据的修改，应到计量管理部门备案。

中等：涉及对法制相关程序、数据的修改，应提交计量管理部门批准。

高等：保护方法不允许修改，若方法、数据格式等修改，都应提交计量管理部门，获得批准后方可实施。

5.2.2 法制相关程序和数据应被保护以避免遭到破坏或被未授权者有意识地更改。

1）软件开发水平

低等：法制相关程序和数据需要有严格的操作规范，操作模块和操作授权严格定义。

中等：法制相关程序和数据的访问具有加密、授权等机制，重要数据具有恢复机制。

高等：有硬件的方法保护重要程序和数据，避免调试、明码直接访问等。

2）软件检测水平

低等：检查操作规范，分析用户手册，对数据设置等敏感操作做试图破坏和非授权访问，法制相关程序和数据应稳定可靠。

中等：对硬件或保护机制作模拟攻击。

高等：分析源码和拆卸计量器具（必要时），检查硬件保护机制。

3）软件符合水平

低等：保护方法的接口不变，不涉及法制相关程序、数据的修改，应到计量管理部门备案。

中等：更改操作规范，涉及对法制程序、数据的修改，提交计量管理部门，获得批准后方可实施。

高等：保护方法不允许修改，若操作规范、数据格式、硬件保护机制等发生变化，都要提交计量管理部门，获得批准后方可实施。

5.2.3 只有被批准和验证了的软件允许被用于法制目的。它应清晰和明确，并且其结果的表达是由法制相关程序所产生的。

1）软件开发水平

低等：软件标识清晰明确，法制计算和法制数据的显示满足技术规范要求。

中等：软件判断其标识，可被读出或显示，不混淆法制数据结果表达和非法制数据结果表达。

高等：软件标识应有法制相关程序或硬件验证。

2）软件检测水平

低等：检测软件标识，操作可能的显示功能，显示结果不允许出现不满足技术规范要求的结果表达。

中等：读出或显示软件标识，操作可能的显示功能，由法制相关程序产生的计量结果与其他结果应明显区分。

高等：分析源码，检查软件标识、电子标识的产生和验证过程。

3）软件符合水平

低等：软件标识未经批准不允许修改。计量结果显示格式的修改要提交计量管理部门备案。

中等：软件标识和电子标识的产生、判断方法，计量结果显示的格式等做出更改，需要提交计量管理部门，获得批准后方可实施。

高等：任何对软件标识、电子标识、显示格式的更改都要提交计量管理部门，获得批准后方可实施。

5.2.4 在软件控制硬件的过程中，能够产生假测量值的功能缺陷应能被检测到并采取措施。

1）软件开发水平

低等：检查硬件的设置参数、检查硬件的输入数据。禁止计算错误。

中等：提供硬件的校准功能或错误侦测功能，提供可能的计算算法。

高等：提供多硬件冗余控制，进行比较和判断。

2）软件检测水平

低等：正确、多次、充分的构造输入数据，检测计量器具结果的正确性和稳定性。

中等：检测计量器具极限值和硬件边缘操作等功能。

高等：分析硬件物理或化学等特性，分析源码处理的科学性和准确性。

3）软件符合水平

低等：硬件参数的调整，计算方法的改进等只要不影响计量器具功能和正确性，应到计量管理部门备案。

中等：计量传感器的更改、计算方法的更改、校准算法的更改等应提交计量管理部门，获得批准后方可实施。

高等：任何与软件控制相关的硬件、算法、配置参数的更改都应提交计量管理部门获得批准后方可实施。

5.3 计量器具风险分类

对计量器具的测试应考虑其安全级别，安全级别的不同不仅取决于客观标准还有各组专家的主观评价，需要考虑以下几方面：

1）欺骗性使用风险

社会影响；

被测计量器具的价值；

改动计算机程序可能的获利；

可能获利所需的成本；

查明欺骗性使用可能性。

2）必需的一致性

实际中相关专业级别要求与标准的一致性。

3）可靠性

电、电磁环境的影响程度。

4）计量过程被重复或中断的可能性

6 型式评价

申请单位有提供技术文档资料和计量器具软件源代码的义务。

6.1 文档资料

计量器具生产企业为型式评价提供计量器具软件的程序功能、相关数据结构和接口的文档，不允许存在任何未归档隐藏的功能。

型式评价的文档包括以下内容：

法制相关软件描述；

隶属法制相关部分软件的模块列表，包括对所有功能和测量影响的声明；

软件接口描述；

软件标识的生成描述；

基于不同验证方法，软件开发者提供的源码对测试机构应保证可用；

应保护的参数列表和保护方法描述；

最低系统配置的描述；

操作系统安全方法的描述；

算法精度描述；

用户界面＼菜单＼对话框的描述；

明确的软件标识和说明；

每一接口命令列表的完整说明；

数据存储或传输的描述；

软件中实现错误侦测功能时，需有故障列表和检测算法描述；

软件开发的软硬件环境说明，网络结构图，计算机类型；

操作手册。

申请型式批准还应附有其他文档，以证明计量器具软件设计和特性符合有关规程或规范等规定文档的要求。

6.2 基本要求

计量器具的法制管理要求、计量要求、技术要求及型式评价步骤应符合 JJF 1015

的相关规定。

计量器具软件应进行完整的功能测试。

如果计量器具的尺寸或配置不允许其作为一个整体单元来测试，并且计量器具相关的一部分装置(模块）在模拟环境可以完全正常运行，那么相关规程或规范应指出可以对计量器具软件模块进行分离测试。

一般情况下，计量器具软件样品由申请单位自行送样。对于大型或者在线的计量器具软件，在技术机构的实验室安装、验证有困难的，可由技术机构提出，经委托的政府计量行政部门同意后，技术机构可以派技术人员到申请单位的生产现场或者使用现场进行验证。

6.3 验证方法

为获得批准，计量器具软件需遵照有关规程或规范进行验证。验证包括如下适当的方法选择。缩写的解释在表3中，表4给出对在第4章描述的每一软件需求验证程序概述，在有关规程或规范准备的过程中，提及的验证程序可根据计量器具种类和应用领域加以选择。

对计量器具软件的验证需要具有详细的测试计划、完备的测试条件、准确的测量方法及合适的测试工具。根据 GB/T 17544 的要求，可以采用静态测试或动态测试的方法。静态测试方法包括：代码审查、代码走查、静态分析等方法，动态测试方法包括：黑盒测试和白盒测试等方法，软件检测关注的重点是和计量器具的类型和用途紧密相关的。对计量器具软件进行型式评价时，应重点考虑以下验证方法和内容。

6.3.1 方法和应用概述

在验证过程中，针对不同的案例可参考表3的方法。

表3 分析和测试方法

缩写	描　　述	验证方法	验证条件	专业技能
AD	Analysis of the documentation and validation of the design 文档分析和设计验证（6.3.2.1）	通用	文档	——
VFTM	Validation by functional testing of metrological features 计量特性功能测试验证（6.3.2.2）	算法的正确性，不确定度，数值修约，价格计算。	文档	——
$VFTS_W$	Validation by functional testing of software features 软件特性功能测试验证（6.3.2.3）	用户界面，通讯的可靠性，共享示值，避免欺骗性使用。	文档、文本编辑器	——

表 3（续）

缩写	描　　述	验证方法	验证条件	专业技能
DFA	Data flow analysis 数据流分析（6.3.2.4）	软件分离，命令对计量器具功能影响的评价。	源代码，文本编辑器（简单程序），工具（复杂程序）。	程序语言知识，方法说明。
CIWT	Code inspection，Walk-through 代码走查（6.3.2.5）	所有应用	源代码，文本编辑器	程序语言知识，协议，其他 IT 标准。
SMT	Software module testing 软件模块测试（6.3.2.6）	输入输出有清晰定义的应用	源代码，测试环境，专用软件工具	程序语言知识协议，其他 IT 标准。工具使用说明。

6.3.2　所选验证方法的描述

6.3.2.1　文档分析和设计验证

目的：文档的符合性。任何案例中都需要的基础步骤。

条件：此步骤是基于计量器具的产品文档。根据文档要求划分适当的范围：

1）对于没有接口、低欺骗性使用风险、功能测试可以验证所有特性的简单计量器具，应有概括外部功能描述文档。

2）对于有接口、如果欺骗性使用风险增加而无法测试某些功能的计量器具，应有软件功能和接口的描述文档。此文档中对计量特性产生影响的软件功能应有详细说明。对于接口描述，文档应提供软件可解释的全部命令或者信号列表。应该详细说明每个命令的作用，且说明计量器具对非法（文档没有说明的）命令是怎样响应的。

3）如要求理解和评估软件的功能，应提供软件的算法、密码功能、重要的计时限值等附加文档。

4）当不清楚如何验证软件程序的功能，厂家有义务提供测试方法。另外，程序员需回答检验人员的问题来达到验证目的。

一般在文档完成和被测装置计量功能的软件包被明确标识之后进行验证。

描述：测试人员要尽量用口头语言和图表的方式理解计量器具的功能和特性，并且判定是否符合相关规程或规范的要求。应考虑和评估计量要求及软件功能要求，如：防止欺骗性使用、参数的调整保护、不允许的功能、与其他计量器具通讯、软件升级、缺陷检测等(在第 4 章中已详细描述)。文档的格式应按照 GB 8567 和 GB 9385 的要求进行编制。

结果评价：根据软件开发者提供的文档，在测试报告中给出计量器具所有文档符合性的结果。

补充说明：如果对文档的检查不能给出可证实的验证结果，需要附加的步骤。常采用功能测试来验证计量功能。

6.3.2.2 计量特性功能验证

目的：根据原始数据计算测量值、线性特性、环境影响补偿、价格计算中的舍入等算法的正确性。

条件：操作手册、功能模式、计量参考资料、测试装置。

描述：有关规程和规范中的多数测试方法是基于不同条件下的参考测试方法。它不限于计量器具的某个单一技术应用。尽管它不是主要针对软件验证，但是测试结果能够作为某些软件模块验证的说明，一般情况下甚至可以应用到大多数重要的计量软件模块(计量特性非常重要)。如果相关规程和规范中覆盖了器具有关计量方面的特性，那么相应的软件模块可认为已验证过。一般情况下不需再进行软件分析或测试来验证计量器具计量特性。但是需提防计量器具的单点应对性等可能的欺骗性使用。

结果评价：算法是否正确，所有情况下测量的值是否在最大允许误差之内。

6.3.2.3 软件特性功能验证

目的：参数保护的验证，软件标识的表示，软件自有的缺陷检测，系统配置(特别是软件环境的配置)。

条件：操作手册，软件文档，功能模式，测试装置。

描述：根据操作手册、计量器具或者软件文档中描述的功能进行验证，主要验证以下特性：

1）软件控制的计量器具常规操作，应使用所有的开关键及定义过的组合，并评价器具的执行结果。图形界面中所有的菜单和其他的图形元素都应该激活检查。

2）参数保护的有效性，可以通过激活保护手段并尝试更改参数来检查。

3）存储数据保护的有效性，可以通过更改文档中的一些数据，然后检查程序是否检测到更改来检查。

4）软件标识的生成和表示，可以通过实例检查来验证。

5）如果软件支持缺陷检测，那么要验证相关的这部分软件，可通过激活、执行或模拟一个故障来检查器具的正确响应。

6）如果法制相关软件的配置或环境要求是恒定的，可以进行非法的更改来检查其保护措施。软件应该禁止这些更改或者停止运行。

结果评价：考虑受控软件特性是否正常。

补充说明：软件控制的计量器具的一些特性或功能在实际中不能像其所描述的那样被验证。有接口的器具，一般来说通过随机试验是不能够检测到非法命令的。除非得通过一个命令生成器来产生这些命令。对一般验证水平，做到此即可，对扩展验证水平还需做软件分析等。

6.3.2.4 数据流分析

目的：法制数据域中计量值的结构，软件分离检查。

条件：软件文档，源代码，编辑器，文本搜寻程序或特殊工具，程序语言知识。

描述：此方法的目的是找出软件中所有与计量值计算或对其有影响的部分。在硬件端口上传感器测量到的原始数据是可用的，子程序搜寻并读取它们。在可能经过某些计算后子程序把它们存为一个变量，由这个变量产生的中间值被其他的子程序读取，由此

直到完成的计量值输出到显示设备。通过文本编辑器和使用文本搜寻程序在另一个源代码文档中寻找变量或子程序名与当前在文本编辑器中打开的源代码文档进行比较，所有的用于存储这些中间值的变量和传输这些值的子程序都可以在源代码中获得。

其他数据流的查找也可通过从输入接口到查询命令执行结果的方法实现。

此外，通过以上方法也可发现隐藏的软件接口及变量，以及单点应对性。

结果评价：验证根据4.3.3.2的软件分离是否成功。

补充说明：如果软件分离清晰，一致性要求高，需要很强的操作保护，此方法作为6.3.2.1 3）和6.3.2.5的补充。

6.3.2.5 代码走查

目的：如果要提高检查力度，用此方法可以验证软件的任何特性。

条件：源代码，文本编辑器，测试工具，程序语言知识。

描述：检测人员应尽量理解源代码的各个部分，判定需求是否都满足，程序功能和特性是否与文档一致。这种静态测试方法是一种多人一起进行的测试活动，要求每个人尽量多提供测试用例，这些测试用实例是作为检查程序逻辑与计算错误的出发点，在执行测试用例时，会发现程序缺陷。这种方法不如代码审查检查的范围广，覆盖率高(代码审查：检查代码和设计的一致性；检查代码执行标准的情况；检查代码逻辑表达的正确性；检查代码结构的合理性；检查代码的可读性)。

结果评价：是否和软件文档一致，是否和需求一致。

检测人员也可以集中检查那些已确定较复杂、易错、表述不完整的算法和功能上。通过分析和查验来检查源码的各个部分。

检验的首要步骤是通过计量数据流的分析确定法制相关部分。一般来说，这部分不用代码检查或走查方法。相比以无故障或性能优化为目标的软件生产所用的这些方法，结合两种方法的检测，所付出的劳动是最少的。

补充说明：这是6.3.2.1方法的补充。

6.3.2.6 软件模块验证

目的：只有在有高一致性要求和避免欺骗性使用保护要求的情况下，当在已有的资料上无法独立检查程序功能时使用。此方法在验证动态计量算法时是适当的、经济的。

条件：源代码，高级工具（至少是一个编译器），软件模块测试的运行环境，数据输入装置和相应的可供参考的数据输出装置，自动测试工具。

描述：在测试环境中测试软件模块，专用的测试程序模块会产生所需的输入数据(测试用例)。测试程序收到被测模块的输出数据后和可供参考的期望值进行比较。

结果评价：计量算法或其他被测功能是否正确。

补充说明：特殊情况下使用。

6.4 验证程序

验证程序包含分析方法和测试，应按照计量器具技术特点分析、建立测试模型、设计测试用例、采集实际数据(或测试具体源代码）等步骤设计验证程序，有关规程或规范可指定验证程序的细节有：

执行6.3描述的何种验证方法；

生成何种测试用例；

如何完成测试结果的评价；

在测试报告中和测试证书里包含何种结果。

根据不同需求，选择 A 和 B 验证程序所需考虑的内容有：

欺骗性使用的风险；

应用领域；

可靠性；

与型式批准的一致性。

水平分类为低、中等的（或风险等级不高的）可以参照表 4 中验证程序 A（标准测试水平）执行，水平分类为高等或欺骗性使用风险较高时可以按照表 4 中验证程序 B（扩展测试水平）执行。

表 4　不同软件验证程序和方法组合建议

	要　求	验证程序 A（标准测试水平）	验证程序 B（扩展测试水平）	备　注
4.2.1	软件标识	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT	一致性要求高时选 B
4.2.2	算法和功能正确性	AD + VFTM	AD + VFTM + CIWT/SMT	——
4.2.3	软件保护			——
4.2.3.1	意外，误操作	AD + $VFTS_W$	AD + $VFTS_W$	——
4.2.3.2	防止欺骗性使用	AD + $VFTS_W$	AD + $VFTS_W$ + DFA/CIWT/SMT	欺骗性使用风险高时选 B
4.2.4	硬件特性支持			——
4.2.4.1	缺陷侦测支持	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT + SMT	可靠性要求高时选 B
4.2.4.2	稳定性保护支持	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT + SMT	可靠性要求高时选 B
4.3.1	计量数据长期存储（用 L 表示）	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT/SMT	高欺骗性使用风险时选 B
4.3.2	通讯系统传输（用 T 表示）	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT/SMT	可预见计量数据在开放式系统中传输时选 B
4.3.3	相关部件指定与分离和部件接口指定（用 S 表示）		——	——
4.3.3.1	设备和组件的分离	AD	AD	——
4.3.3.2	软件部分的分离	AD	AD + DFA/WT	——
4.3.4	维护和升级（用 D 表示）		——	——
4.3.4.1	验证升级	AD	AD	——

表 4（续）

	要　求	验证程序 A （标准测试水平）	验证程序 B （扩展测试水平）	备　注
4.3.4.2	跟踪升级	AD + $VFTS_W$	AD + $VFTS_W$ + CIWT/SMT	高欺骗性使用风险时选 B
4.3.5	操作系统和硬件兼容性，可移植性（用 E 表示）	AD + $VFTS_W$	AD + $VFTS_W$ + SMT	——

7　测评细则编制要求

各计量专业技术委员会应参照本指南，按计量器具技术特性的分类或应用领域分别制定相应软件测评的细则和程序，提出特定要求，在制定相应测评细则时应按以下内容和格式编制，测评活动可参照 GB/T 15532 的要求实施。

7.1　引言

7.1.1　编制目的

要求：阐明编制测评细则的目的并指明计量器具的应用领域。

7.1.2　术语和定义

要求：列出细则中除本指南以外所引用的术语和定义。

7.1.3　引用文献

7.2　测评要求

7.2.1　计量器具法制相关软件要求描述

要求：应对数据需求、数据采集方式、数据准确性、时间特性（包括响应时间、更新处理时间、数据转换与传输时间、运行时间等）、功能划分、运行需求（包括屏幕格式、报表格式、菜单格式、输入输出时间等）、硬件接口、软件接口、故障处理、安全保密需求、可使用性、可维护性及可移植性的要求进行描述。必要时，应要求对隶属法制相关部分软件的模块列表、必须保护的参数列表和安全保密保护方法描述，包括软件对所有功能和测量的影响声明。

7.2.2　测评环境

要求：应明确软件系统运行时的最低配置要求、条件与限制及实际工作状态的环境影响。

7.2.3　测评工具

要求：应明确是否采用自动化软件测试工具，测试工具主要功能和作用及支持的软硬件平台。可参照 ISO/IEC 14102 的要求选择测试工具。

7.2.4　计量器具软件技术特性分类

要求：应参照第 4 章的要求，对计量器具软件技术特性进行分类。

7.2.5　计量器具软件基本要求和特定要求

要求：应参照第 5 章的要求，根据计量器具测试原理、使用场合、安全保密性要求

对计量器具软件进行风险等级划分及对软件水平进行分类，有关划分和分类应有解释说明。

7.2.6 测评文档资料

要求：应参照 GB/T 9385 及 GB/T 8567 的要求编制测试文档资料。明确软件标识的生成过程及说明（附照片），软件标识应包括以下内容：软件号，版本信息，编译时间（年、月、日、时、分、秒），并可以通过打印输出。

7.3 测评方法

7.3.1 方法选择

要求：应根据计量器具软件的技术特性分类及要求、风险等级划分和对软件水平分类明确测评项目，选择适宜的验证方法。选择对用户文档可仅采用审查测试方法；对低等水平的测试可仅采用黑盒测试方法；对中、高等水平的测试宜采用白盒测试方法。

7.3.2 测试用例

要求：制定测试用例应着重考虑下列因素：

1）数据的准确性；

2）数据典型性；

3）可操作性；

4）边缘性、全面性、可覆盖性、完整性、统一性。

7.4 结果评价

7.4.1 测试结果及适用范围

要求：应说明所完成的各项测试的范围及其局限性，未得到充分测试的情况及原因，测试所发现的缺陷和不足，以及可能给软件运行带来的影响。

7.4.2 建议

要求：应提出如何弥补测试中所发现缺陷和不足的建议。

7.4.3 测评结论

要求：应明确计量器具软件经测评后是否符合要求的判定方法和所达到的软件水平。

附录 A

计量器具（衡器）软件测评实例

A.1 测评要求

A.1.1 计量器具法制相关软件要求描述

软件名称及版本号：××××计价秤软件 V2.0 版本。

××××为高端的条码打印计价秤。其软件功能如下：

1）称重/显示/打印；

2）数据上/下载；

3）多种使用模式；

4）数据库管理；

5）报表统计。

其中，称重/显示/打印部分是法制相关软件。称重和显示是计价秤最基本的功能。对于计重类计量器具，××××条码秤根据称出的商品重量和商品单价，计算出总的金额，输出到显示屏和打印机。

A.1.2 接口定义描述

1）输入接口

××××条码秤的输入接口有两种：

键盘接口：键盘是操作员与秤交互的接口，××××共 104 个键，在不同的操作模式下每个键所代表的含义也不同。而且可实现动态配置。

重量输入接口：为了称出商品的重量，系统必须通过传感器把商品的重量转变为电信号送入系统处理。

2）输出接口

××××的输出接口包括两部分：

显示接口：××××条码秤前后显示屏可任意选择中文屏、英文屏。

打印接口：××××条码计价秤采用热敏打印机，打印介质为标签和收据纸。

3）网络接口

××××条码计价秤带有以太网接口，并可选配无线接口。通过网络接口，可把多台秤连入网络，实现数据的实时更新。

A.1.3 性能需求描述

1）数据准确度

数据库数据保证可靠的存取，网络通讯串口通讯数据可靠准确，称重应符合国家计量检定规程的要求，标签或收据打印清晰无误。

2）时间特性

称重及打印操作响应时间快，重量示值的稳定时间应小于 1s。

A.1.4 故障处理描述

正常使用时不应出错，对于用户的输入错误应给出屏幕提示。若运行时遇到不可恢

复的系统错误，也必须保证数据库完好无损，交易数据不能丢失，对于标签或收据打印时的数据错误应给出适当的提示，同时能够自动修正相关错误，错误提示可以屏幕显示，也可以打印在对应出错数据项处。

A.1.5 数据管理描述

在××××条码计价秤中，存在以下几类需要保存的重要数据：

1）称重校正参数；

2）重要操作历史数据，如：数据库出错、改变秤的校正参数等；

3）配置信息；

4）商品信息；

5）营业数据。

1）项和2)两项数据特别重要，但这类数据量少，写数据的几率也很小，而且仅需开机读入一次，所以对于这类数据管理较简单，数据的检索、更新和读写速度以及存储器的容量是次要的，重点应考虑它的安全性和可靠性。

3）项数据量小，4)项和5)项数据量大，他们共同的特点是数据的种类多，数据的检索、更新频繁，并且能通过PC进行数据的更新。几乎程序的每个运行周期都需检索一次，特别是营业数据，每做一次交易都需记录一次。对这类数据的管理就比较复杂，既要求存储器的容量要大，数据的读写速度也要快，数据的检索、更新要快而简便，因此采用数据库来管理这类数据。

数据的安全措施是通过数据分块进行加密处理，并通过CRC校验保证其数据完整性。

A.2 测评环境

温度：(－10～40)℃；

湿度：(30%～60%)RH；

电压：(80～240)V(AC)；

软件开发环境：Realview Developer Suite V3.2

操作系统：UC/OS2 V2.0

处理器：Samsung 44b0 ARM7TDMI

A.3 测评工具

测评工具名称	版本
Code Test	V3.5
键盘测试仪	V2.0

A.4 软件技术特性分类

该设备为嵌入式计量设备，CPU为ARM7，采用UC/OS2嵌入式实时多任务系统，满足P类计量器具软件要求。

A.5 软件基本要求和特定要求

A.5.1 基本要求

表 A.1 基本要求

序号	评价项目	评价内容（大纲要求）	验证方法	评价过程描述	单项结论（水平分类结果）
1	软件标识	法制相关软件需有清晰的、带软件版本号或者其他特征性的标识	源码审查	更改软件源码，编译后检查软件标识	中
2	算法和功能正确性	计量器具的计量算法和功能应正确	源码审查	代码走查 功能测试	高
3	软件保护				
3.1	意外，误操作	通过软件保护，使得计量器具误操作的可能性降至最小	破坏性测试	对键盘操作的权限进行设置，通过键盘测试仪做随机测试	高
3.2	防止欺诈	a）计量精密的软件能防止未经许可的修改，装载或通过更换存储体来改变； b）从用户接口输入的命令，在型式评价时提交的软件文档中应有完整描述	源码审查破坏性测试	代码走查，设计测试用例进行破坏性测试	高
4	硬件特性支持				
4.1	缺陷侦测支持	产品设计需要故障检测	图纸/文档审查	图纸、实物对照检查	中
5	稳定性保护支持	稳定性检测，需要有相应的提示	破坏性测试	针对样机的破坏性测试	中

A.5.2 特定要求

表 A.2 特定要求

序号	评价项目	评价内容（大纲要求）	验证方法	评价过程描述	单项结论（水平分类结果）
1					
1.1	设备和组件的分离	计量系统的计量部分不能非授权地被计量系统其他部分影响	图纸/文档审查（AD）	图纸、实物对照检查	中

表 A.2（续）

序号	评价项目	评价内容（大纲要求）	验证方法	评价过程描述	单项结论（水平分类结果）
1.2	软件部分的分离	a）所有执行法制相关功能或包含法制相关数据域的软件模块； b）如果法制相关的软件部分与其他的软件部分通讯，软件接口应被定义； c）软件分离意味着如果系统资源有限，法制相关软件的优先级高于法制不相关软件。测量任务（由法制相关软件部分实现）不得被其他任务延时或锁定	软件设计文件审查（AD）	设计文件 代码比对	中
2	共享示值	如果应用程序允许远程的指示器，要提供相应的计量器具或计量场所	功能测试（VFTSw）	——	中
3	数据存储由通讯系统传输	a）传输的计量数据应含有必要的相关信息。且不应受到传输延时的影响； b）从不安全的存储器读出或从不安全的传输通道接受数据之后，应通过软件方法保护数据，保证它们的标识、计量时间信息	代码审查（CIWT）	交易数据传输具备重发机制和可靠性验证机制，对交易重量的记录	中
4	维护和升级				
4.1	验证的升级		图纸/文档审查（AD）恶意侵入测试	设计文件审查，非法修改软件，测试是否可以完成升级	高
4.2	跟踪升级		文件审查（AD）	审查升级后版本是否可追溯，在线升级有可靠性	低

A.6 测评方法

A.6.1 方法选择

1）文件审查；

2）源码审查；

3）功能测试；

4）破坏性测试。

A.6.2 测试用例

1）密码测试

型式评价用例编号：××××

描述：SCALE PASSWORD 使用效果，测试使用中的无效结果。

状态：新产品型式评价试验。

预期结果：开机时有提示输入 SCALE PASSWORD，输入正确则进入待机状态；如不正确，应要求重输。

实际结果：秤重启后，没有输入 SCALE PASSWORD 提示。

测试结论：SCALE PASSWORD 在使用中无效。

测试时间：××××年××月××日

测试人员：×××

2）文本输入测试

描述：进行超限文本的输入。

状态：新产品型式评价试验。

预期结果：系统对文本输入的极限有控制。最多 4 行，总共 200 个字符。

实际结果：进行极限字符输入，每行 50 个字符左右，共输了 4 行，但打印只有 3 行，文本输入时许多功能按键无法正常使用。

测试结论：文本输入状态下，功能按键使用出错，打印出错。

测试时间：××××年××月××日

测试人员：×××

3）设置后负净重标签打印测试

描述：选择 ENABLE 并按 down 键打印。

状态：新产品型式评价试验。

预期结果：设置被保存，对于 6/15kg 量程的秤 20e 为 40g，放小于 40g 的载荷，无法自动打印标签，但可以按打印键打印出标签。对于 15/30kg 量程的秤，20e 为 100g，放小于 100g 的载荷，无法自动打印标签，但可以按打印键打印出标签。

实际结果：负净重状态下也可以打印标签。

测试结论：设置后负净重标签自动打印出错。

测试时间：××××年××月××日

测试人员：×××

A.7 结果评价

A.7.1 测试结果及适用范围

××××计量器具软件满足（或不满足）型式评价大纲的技术要求。

A.7.2 建议

略

A.7.3 测评结论

序号	评 价 项 目	评价内容 （大纲要求）	单 项 结 论
1	软件设计和结构		
	一致性	5.1.1	高
	独立性	5.1.2	高
	接口设计	5.1.3	高
	可测试性	5.1.4	中
2	软件保护		
	程序和数据保护 1	5.2.1	高
	程序和数据保护 2	5.2.2	高
	软件标识	5.2.3	中
	硬件错误检测	5.2.4	中
3	型式批准文件		
	技术资料完备	6.1	中

中华人民共和国
国家计量技术规范

计量器具软件测评指南

JJF 1182—2007

国家质量监督检验检疫总局发布

*

中国计量出版社出版
北京和平里西街甲2号
邮政编码 100013
电话（010）64275360
http://www.zgjl.com.cn
北京市迪鑫印刷厂印刷
新华书店北京发行所发行

*

880 mm×1230 mm 16开本 印张2.5 字数48千字
2007年10月第1版 2007年10月第1次印刷
印数1—1 500
统一书号155026－2282 定价：32.00元

JJF1182-2007