JJF

吉林省地方计量技术规范

JJF（吉）32—2009

机动车检测系统软件测评指南

Evaluation Guide for Vehicle Test System Software

2009－03－20 发布　　2009－04－20 实施

吉林省质量技术监督局 发布

机动车检测系统软件测评指南

Evaluation Guide

for Vehicle Test System Software

JJF（吉）32—2009

本规范经吉林省质量技术监督局于2009年03月20日批准，并自2009年04月20日起实行。

归口单位：吉林省质量技术监督局

负责起草单位：吉林省计量科学研究院

参加起草单位：深圳市安车科技有限公司

吉林油田公司质量与节能处

本规范条文由吉林省质量技术监督局负责解释

本规范主要起草人：

房法成　（吉林省计量科学研究院）

李德辉　（吉林省计量科学研究院）

闫有余　（吉林省计量科学研究院）

参加起草人：

张疆辉　（深圳市安车科技有限公司）

廉勇凯　（吉林油田公司质量与节能处）

目　　录

机动车检测系统软件测评指南

引　言

本指南是参考计量器具软件测评指南、OIML D-SW(V-025) 及 WELMEC7.1(Issue 2)、WELMEC7.2（Issue 1）并结合我国机动车辆检测设备法定计量工作要求制定的。

1. 范　围

1.1 总则

本指南描述了针对机动车检测系统软件的应用、水平分类以及测评细则编制的基本要求、验证程序和主要验证方法，作为机动车辆检测系统软件测评的指导性文件，也可作为计量管理部门日常监督管理及机动车辆检测系统软件生产企业进行软件测试的参考文件。

机动车检测系统软件的测评应执行机动车检测系统软件测评指南。

1.2 应用

本指南编制目的是为了支持公平一致的机动车辆检测系统软件的测评方法和水平分类，并使其对机动车检测系统的测试结果具有可评估性。

机动车检测系统软件应满足如下技术要求：

1）机动车检测系统软件应有明显的版本号标识，软件版本的变更应有历史记录可查。

2）测量数据和计量参数的存储或传送应有足够的安全保护，防止意外或有意的破坏。

3）检测系统软件应能记录车辆检测过程中的所有检测过程数据和检测结果数据。

4）检测系统软件应能记录所有检测相关人员对软件系统的操作记录。

5）检测系统软件应能保证检测数据在系统的整个过程中保持一致性。

6）检测系统软件应尽可能减少误操作的可能性，应能防止欺骗性使用。

7）检测设备的计量特性不应受到与其连接的设备的特性或远程设备通讯的影响。

8）检测系统软件应保证计量检定校准的结果应用于所对应开展的检测项目中。

2. 引用文献

JJF 1001-1998《通用计量术语及定义》

JJF 1182-2007《计量器具软件评测指南》

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》

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

《通用计量术语及定义》与《计量器具软件评测指南》中有关的术语和定义适用于本指南。下面列出检测系统软件测评工作中适用于本指南的定义和术语。

3.1 机动车检测系统软件

机动车检测站用于机动车检测的计算机联网软件、控制软件、管理软件等模块软件。

3.2 软件标识

软件的名称、版本号、开发单位等标识软件的符号。

3.3 软件保护

软件系统本身的文件存储、软件系统检定参数、检定过程数据、检测标准数据、检测参数、系统设置参数的数据存储，必须有相应的权限才能访问或再次进行检定。

3.4 软件分离

检测系统软件可以被分为法制相关部分和非相关部分，两部分可通过软件接口进行通讯。

3.5 软件一致性

检测系统软件与所获型式批准的软件类似的程度。

3.6 功能测试

检验被测检测系统软件能否完成应有功能的测试。

3.7 软件测试

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。

3.8 黑盒测试

基于需求和功能性的测试。

3.9 白盒测试

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，又叫“结构测试”。

3.10 测试用例

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。

3.11 验证

通过提供客观证据对检测设备软件的规定要求已得到满足的认定。

3.12 认证

第三方依据程序对检测系统软件符合规定的要求给予书面保证。

3.13 评价模块

用于测量软件质量特性或属性的评价技术包，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等。

4. 检测系统软件的应用要求

检测系统软件可从功能性、可靠性、易用性、效率、可维护性五大因素进行测试，并按照软件的技术特性及相应的应用范围制定相应的软件测评细则和程序，满足相应的要求。

4.1 检测系统软件技术特性分类

检测系统软件按技术特性可分为嵌入式系统和通用计算机系统，具备如下特性。

4.1.1 嵌入式软件系统具有的特性

内置的应用软件用于计算，包括法制控制部分和其它部分；

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；

用户接口仅用于检测目的，通常操作模式下受法制控制；

操作系统不含用户界面；

软件及运行环境恒定，没有变成和更改法制相关软件的手段，只能受控升级；

允许存在通过受控的网络交换受控数据的接口；

允许检测数据本地或远程受控存储。

4.1.2 通用计算机系统具有的特性

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）；

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，或通过网络链接，传感器之间应相联；

用户接口可以从不受法制控制的操作模式切换到相对的受控模式；

数据可以本地或远程存储。

4.2 基本要求

适用于各种检测系统软件。

适检车型基本参数录入完备；

适检项目完备；

检测系统软件的测试精度和测试能力不得低于该系统中受控检测设备的测试精度和测试能力。计算机测控系统的检测结果应与受控检测设备二次仪表显示值一致，其误差应在规定的范围内；

检测系统须具备无序调度功能；系统须具备各种查询及统计报表打印功能；系统要具有异常数据分析、报警功能；系统须具有校零功能；

数据输出格式标准应满足相关标准的规定，且数据库具有企业级可靠性；

检测系统所建立的数据库应满足车辆技术管理要求，且将受检车辆的检测原始数据和判定结果全面真实地记录在数据库中。引用检测标准数据应独立地反映在数据库中，当所引用的标准修订时，数据库应能做相应修改；

控制系统软件应具备备份功能，在系统崩溃后，用户能自行恢复软件程序和数据库；

采用软、硬件滤波后，检测结果应不失真；

检测控制系统界面、提示说明及帮助文件应为中文；

系统因故不能正常工作，各工位应具备单机检测功能；检测工位因故死机，系统要具有单工位复位功能，且不影响车辆检测序列和已检测的数据。

4.2.1 软件标识

要求：检测系统软件需要有清晰的、带软件版本号或其它特征性的标识。标识和软件本身是紧密关联的，应能在软件界面上显示出来，如果条件满足可显示在别的显示设备（如点阵屏）上。软件应能提供建立系统信息的功能，应能将检定参数、检定过程数据、检测标准数据、检测参数、系统设置参数、检测过程数据、检测结果数据对应相应的系统信息。

目的与解释：每套检测系统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。

4.2.2 算法和功能的准确性

要求：检测系统软件的计量算法和功能应正确（包括模/数转换结果、数据修正系数、测量不确定度评价等），并能满足法规要求和用户需要。车辆的最终检测结果及其附属信息应能通过检测系统软件正确显示或打印。

检测系统软件的算法和功能应该是可以测定的。

4.2.3 软件保护

4.2.3.1 预防误操作

要求：通过有效的软件保护，能够使检测系统软件的误操作可能性降到最小。

误操作包括由意外物理因素或软件原因（如操作系统崩溃、病毒感染）或用户对软件的无意操作导致检测系统软件程序的配置或系统参数的更改。

目的解释：检测系统软件的系统参数或配置参数被更改会直接造成检测结果的不准确性，影响到检测结果的公正。

举例：用户进入系统参数设置和维护功能模块必须有权限提示操作，系统参数发生更改，系统应该有警告提示该操作可能造成的后果。

4.2.3.2 防止欺骗性使用

检测系统软件通过安装设置后的系统参数，必须能保证是日常使用中系统完成所有检测功能所使用的系统参数，能有效防止人为的通过替换软件或其参数来达到检测作弊的行为。

检测系统软件目前基本都是联网软件，配套的电脑系统跟不同检测设备的电脑系统都有连接，所以软件系统及其参数的存储可能不能固化在一个存储体内，所以必须有有效措施保证软件系统及其配置参数的有效性，不被有意的或无意的损坏。

要求 1：软件系统必须要有完整的版本标识号，且有完整的对应版本号标识软件的功能说明文档，只有文档中说明过的功能才允许用户接口激活使用，接口设计要避免用户用于欺骗性使用

目的解释 1：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功能命令是可接受的。

举例 1：所有来自用户接口的输入命令，只有备档的命令才会被接收，其余命令系统将不会响应。这段程序或软件模块是法制相关的。

要求 2：系统专有参数只有在检测系统的特殊操作模式下可以被调用或选择。他们可以分为两类：一类是固化在系统内不能更改的，一类是通过授权才能使用的，系统的用户或软件开发单位来调节的可输入参数。

要求 3：软件系统应该有用户的操作日志记录，软件的升级记录，车辆的检测记录，设备的使用和维护记录。

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，也可让软件支持硬件检查工具。

要求：如果软件设计故障检测，需要有相应的提示。例如，当设备故障被检测到时，检测设备的检测功能应该失效并能在软件界面或以生成日志的方式产生警告信息。

软件所配备的文档中应该包括故障的列表说明，为方便理解，还应该有侦测算法的描述。

举例：每次启动检测系统软件，软件系统应该能采集所连接的设备的信号量，分析是否存在故障，如果存在故障，则程序应该停止后续功能的使用，不能进行系统的运行，并显示故障信息，写入日志中。

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，也可以让软件支持应检查工具。

要求：如果设计稳定性检测，需要有相应的提示。比如，有危及稳定的因素被检测到时，检测系统软件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：尾气分析仪在器具稳定间隔时间之后，需要进行重新校准。当到达持续的时间间

隔，软件应给出一个警告，如果超过了规定的时间，将停止设备的工作。

4.2.5 特定要求

4.2.5.1 检测过程数据及检测结果数据存储

检测过程数据及检测结果数据存储应具有所有必要的相关信息，能及时保存并且可在不同时间、不同地点使用或数据验证。

检测过程数据及检测结果数据必须要自动存储，且用于存储的存储器应有足够的存储容量。存储容量不够时，可在满足下面要求的情况下删除存储的数据：

1）按照存储的顺序删除，需考虑特殊应用的有关要求。

2）数据通过特定的人工操作才可被删除。

长期存储的技术方案可以采用：

1）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，存储器可以从计算机中移走，或其中的内容可以拷贝到计算机外的任何地方。

2）可移动的或者远程（外接）的存储器：存储器可以从中取出，存储器可以是软盘、闪存或网络中的远程数据库。

检测过程数据及检测结果数据的保存方式必须采用数据库存储，其它的存储方式将不被采用。采用数据库存储，在不采用加密算法以密文存储的情况下，必须保证数据库的数据的安全性，不能人为打开数据库记录进行记录的修改；如果采用加密算法密文的处理必须通过程序内部的算法来解析。

4.2.5.2 系统参数存储

系统参数存储应具有所有必要的相关信息，能及时保存并且可在不同时间、不同地点使用或数据验证。用于系统参数存储的存储器应有足够的存储容量。数据通过特定的人工操作才可被删除。

长期存储的技术方案可以采用：

1）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，存储器可以从计算机中移走，或其中的内容可以拷贝到计算机外的任何地方。

2）可移动的或者远程（外接）的存储器：存储器可以从中取出，存储器可以是软盘、闪存或网络中的远程数据库。

系统参数的保存方式必须采用数据库存储，其它的存储方式将不被采用。采用数据库存储，在不采用加密算法以密文存储的情况下，必须保证数据库的数据的安全性，不能人为打开数据库记录进行记录的修改；如果采用加密算法密文的处理必须通过程序内部的算法来解析。

4.2.5.3 通讯系统传输

软件系统需要在网络上传输或接收相关数据时适用。

数据传输应具有所有必要的相关信息，能在不同时间、不同地点适用或数据验证。

如果数据在不安全的环境中存储或传输，在他们被用作法制目的前，需满足下列要求：

要求 1：传输的数据应含有必要的相关信息。且不受传输延时影响。

数据包括下列信息：

1）传输数据的大小；

2）传输数据的类型；

3）传输数据的结构；

4）传输数据的内容。

数据的传输，需要安全可靠，发送数据端在发送数据完后，未收到接收端的确认信号，不能清空本地的缓冲数据。数据发送缓冲区大小应能容纳多个数据信息。

要求 2：从不安全的存储器读出或从不安全的传输通道接收到数据后，应检查和保护数据，保证他们的大小、类型、结构及内容信息正确性、真实性和完整性。丢弃不规范的数据。

4.2.5.4 相关组件指定与分离和组件接口指定

检测系统软件不能非授权地被其它部分影响。

检测系统软件具有用来与其它外部设备通讯的接口，应对系统组件进行分离和组件接口进行指定。

要求 1：检测系统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，它们组成计算系统的法制相关部分。

目的解释 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它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。

检测系统软件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。命令和他们的作用应该在软件所附的文档中有完整的表述。软件开发者应对软件所附文档做出完整性声明。

要求 3：检测系统软件中，设备标定模块跟检测功能模块一体的，该软件将作为一个整体受到法制保护，但设备标定模块功能的进入需要有独立的进入接口（如按钮、菜单），且该接口是有权限保护的；如果标定模块跟检测功能模块是分离的独立程序，则标定模块程序受到法制保护，应该有独立的登录校验接口（如登录窗口的用户校验），且要保证检测功能模块数据采集处理所采用的参数是经过标定模块标定之后的参数。

4.2.5.5 系统参数设置

检测系统软件在程序界面上应该有相应的系统参数设置界面，显示所有的关于系统参数的设置与维护（系统设置、权限管理、设备资料维护、检测项目维护、检测类别维护、检测标准维护、技术参数维护等）及所连接设备的通信信号通道（模拟量输入通道、数字量输入通道、数字量输出通道，串口号等）。

系统设置：包括系统名称、系统功能、检测站名称等。

权限管理：包括用户设置、用户分组设置、用户日志管理等。

设备资料维护：包括检测设备基本信息、检测设备检定信息、检测设备原始记录、检测设备自检信息、检测设备维护信息等。

检测项目维护：包括检测项目的名称与编号。

检测类别维护：包括检测类别的名称和检测类别的属性。

检测标准维护：包括检测标准的编号、标准名称、标准上下限、标准系列号等。

技术参数维护：包括车辆厂牌信息参数、发动机信息参数等维护。

数字量输入：包括轴重光电、制动光电、电机状态、滚筒信号、车速信号等。

数字量输出：包括电机控制通道、举升器通道、夹紧器通道、以及其它控制通道。

模拟量输入：包括重量信号、制动信号、踏板手刹信号（含汽车和摩托车）。

串口信号：包括主要是采用串口通讯的重量和制动的信号通道，包括类型、端口号等初始化参数。

4.2.5.6 检测系统软件功能模块要求

（一）登录子系统：

要求 1：具有登录，编辑车辆基本数据功能。

要求 2：具有查询和编辑车型基本参数功能。

要求 3：具有对非正常的数据及必需的数据给出明确提示功能。

要求 4：具有系统界面参数配置功能。

要求 5：具有检测项目与检测类别关联功能。

要求 6：具有发送，删除复检车功能。

（二）调度子系统：

要求 1：具有检测无序性调度功能。实现有序报检，无序进检的功能，将进检功能进一步深化，将初检、复检车辆自动分拣，提高车辆检测可操作性。

要求 2：具有在线应急调度功能。具有调度受检车辆，受检车单元内任意项目、任意次数检测的能力，可在线任意改变工位检测顺序及检测项目。

要求 3：具有工位调度任意配置功能。不受线的限制，作为任意调度的延伸，用户可以根据检测车辆检测需要，不受线的限制任意将车辆调度到任一检测工位进行检测，增强用户的灵活性。

要求 4：具有取消车辆检测功能。当车辆受检时出现非正常状况，检测软件系统通过调度可以使相应的检测项目取消或者使剩余的检测项目取消，从而保证车辆已检项目的数据存入数据库，使整个检测流程不受到任何影响。

要求 5：具有检测单元内实现多车同检功能。将检测单元进一步细分为若干检测工序，在检测单元内调度受检车辆到检测工序进行检测，实现检测单元内多车同检。

（三）检测控制子系统：

要求 1：具有对输入输出开关量的判别功能。

要求 2：具有对受控设备传感器信号输出后的信号调理、到数据采集等检测过程的测量控制功能。

要求 3：具有对各个检测项目按照国家相应标准进行检测控制，对检测数据进行评判，检测数据和单项评价结果实时存入数据库，对已保存的检测数据不能更改，曲线数据保存实际采集数据，曲线图像从数据中生成的功能。

要求 4：具有控制检测线各工位显示屏显示检测结果和判定结果，按照检测流程给引车员相应的操作提示的功能。

要求 5：具备对可系统软件标定的各受控设备测量值进行标定的功能，能够将标定过程实时数据发送到系统显示屏，显示受控设备各模拟输入通道的零点输出、AD 值和标定值；通信协议支持时，系统校准界面实时显示数字通信传输量的示值。

要求 6：检测控制子系统应当具备对各工位采样通道进行测试及自诊断的功能，对于故障能及时进行报警指示，对于故障工作可以进行有效屏蔽，确保检测设备正常后恢复该工位的检测能力。

（四）管理子系统：

要求 1：具有协调调度检测车辆、具有车辆检测状态查询、具有数据收集与存储、检测

数据及曲线、图像查询，检测报告打印等相关业务处理的功能。

要求 2：具有自动判定检测数据并能根据检测结果自动生成复检项目，提供技术判断结果录入、内部查询的功能。

要求 3：具有参数配置的功能。配置参数主要包括系统信息设置，检测站基本信息设置，检测项目设置，检测类别设置，各类编码设置（燃油种类、号牌种类、车辆类型、灯制、辖区、车轴形式）等。

要求 4：具有用户管理功能。用户管理主要包括用户权限的分组设置，权限的授权；用户名的更改，用户口令的更改等。

要求 5：具有系统日志管理功能。

要求 6：具有数据管理功能。保存系统所有的车辆基本信息，车辆检测信息，以及与系统相关的所有其它信息，车辆检测数据至少保存两年；并且具有数据管理和维护功能，可以对数据库进行定时备份和手工备份多种备份方式，还可以进行数据库的恢复。

要求 7：具有系统维护功能。系统维护包括检测设备的软件标定、检测判定标准的维护、车辆参数维护、软件维护等功能，为保证数据公正可靠，各项维护工作由具备相关权限人员进行。

4.2.5.7 软件维护升级

经测评通过的检测系统软件，在不涉及计量算法更改的情况下是允许升级的，这些升级包括界面布局调整、入口调整、检测流程及检测功能的更改(特指检定功能与检测功能一体的检测软件系统)及不影响既定检定结果的软件升级和维护。

牵涉更改既定检定结果的维护和升级，需征得计量管理部门的同意并有备案记录可供查询，并经计量检定合格。

要求 1：软件升级应有记录，并有明确的升级标识，经软件测评的软件升级应到原测评部门备案。

4.2.5.8 操作系统和硬件的兼容性

检测系统软件的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）。如果最低配置要求不能满足，则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。

5. 软件测评的基本要求

5.1 软件设计和结构

5.1.1 检测系统软件应按照本指南要求设计，使其法制相关功能的一致性易于评价。

5.1.2 计量检定相关软件应按照不受也不允许其它软件影响的方式来设计。

5.1.3 计量检定相关软件应按照不受也不能够被其它系统接口所更改的方式来设计。

5.1.4 软件的功能性应设计为可测试性

5.2 软件保护

5.2.1 检测系统程序和数据应被保护以避免偶然的或无意的更改。

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。

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。

5.2.4 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。

5.3 检测系统风险分类

对检测系统的测试应考虑安全级别，安全级别的不同不仅取决于客观标准还有专家的主管评价，需要考虑：

1）其骗性风险

社会影响；

被测检测系统的价值；

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

实际中相关专业要求与标准的一致性。

3）可靠性

电、电磁环境的影响程度。

检测过程被重复或中断的可能行。

6. 测评方法

申请单位有提供技术文档资料和检测系统软件源代码的义务。

6.1 文档资料

检测系统生产企业为软件测评提供检测系统软件的程序功能、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。

软件测评的文档包括以下内容：

计量检定相关软件描述：

隶属计量检定相关部分软件的模块功能列表，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；

数据存储或传输的描述；

软件中实现错误侦测功能时，需要故障列表和检测算法描述；

软件开发的软硬件环境说明，网络构架图，计算机类型；

操作手册。

6.2 验证方法

对检测系统软件的验证需要有详细的测试计划、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检测系统的功能和用途紧密相关的。

6.2.1 方法和应用概述

表1 常用验证方法

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	通用	文档	——
VFTM	Validation by functional testing of metrological features 计量特性功能测试验证	算法的正确性、不确定度、数值修约	文档	——
VFTSw	Validation by functional testing of software features 软件特性功能测试验证	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	——
DFA	Data flow analysis 数据流分析	软件分离，命令对检测系统功能影响的评价	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, Walkthrough 代码走查	所有应用	源代码、文本编辑器	程序语言知识、协议、其它IT标准
SMT	Software module testing 软件模块测试	输入输出有清晰定义的使用	源代码、测试环境、专用软件环境	程序语言知识协议、其它IT标准，工具使用说明

6.2.2 所选验证方法描述

6.2.2.1 文档分析和设计验证

目的：文档的符合性。

条件：此步骤是基于检测系统的产品文档。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检测系统，具有概括外部功能描述文档。

2）对于有接口、欺骗性使用风险增加而无法测试的，应有软件功能和接口的描述文档，文档应提供软件可解释的全部命令或信号列表。应详细说明每个命令的作用，且说明软件对非法命令是怎么响应的。

3）如果要求理解和评估软件的功能，应提供软件的算法、加密功能的设计文档。

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。且程序员还需积极配合测评人员来达到验证目的。

6.2.2.2 计量特性功能验证

目的：根据演示数据计算测量值、线性特性、环境影响的补偿等算法的正确性。

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。不限于检

测系统的某个单一技术应用。尽管它不是主要针对软件验证，但测试结果能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软件模块。如果相关规程和规范中覆盖了系统有关计量方面的特性，则可以认为相应的软件模块已经验证过。一般情况下不需要再进行软件分析或测试来验证计量特性。但是需要提防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。

6.2.2.3 软件特性功能验证

目的：参数保护的验证，软件标识的表示，软件自由的缺陷检测，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、检测设备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）软件控制的检测设备常规操作，应使用所有的开关键及定义过的组合，并评价系统的执行结果。图形界面中所有的菜单和其它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测器具的正确响应。

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停止运行。

结果评价：考虑受控软件特性是否正常。

6.2.2.4 数据流分析

目的：法制数据域中检测数据的结构，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检测数据的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它的子程序读取，由此直到完成的检测数据输出到显示设备。通过文本编辑器和使用文本搜寻程序在另外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。

其它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，以及单点对称性。

6.2.2.5 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：测评人员应尽可能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。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。

测评人员也可以重点检查那些已确定比较复杂，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。

测评的首要步骤是通过检测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的的软件生产所用的这些方法，结合和两种方法的检测，所付出的劳动是最少的。

6.2.2.6 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。此方法在验证动态检测数据时是适当的、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与可供参考的期望值进行比较。

结果评价：检测数据和其它被测功能是否正确。

此方法在特殊情况下使用。

6.3 验证程序

验证程序包含分析方法和测试，应按照检测系统的技术特点分析，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 6.2 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，选择下述 A 和 B 验证程序所需考虑的内容有：

欺骗性使用的风险；

可靠性；

与型式批准的一致性。

表 2 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+VFTSw	AD+VFTSw+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+VFTSw	AD+VFTSw	——
4.2.3.2	防止欺骗性使用	AD+VFTSw	AD+VFTSw+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+VFTSw	AD+VFTSw+CIWT+SMT	可靠性要求高时选 B
4.2.4.2	稳定性保护支持	AD+VFTSw	AD+VFTSw+CIWT+SMT	可靠性要求高时选 B
4.2.5	特定要求			——
4.2.5.1	计量数据长期存储（用 L 表示）	AD+VFTSw	AD+VFTSw+CIWT/SMT	高欺骗性使用风险时选 B
4.2.5.2	系统参数存储	AD+VFTSw	AD+VFTSw+CIWT/SMT	高欺骗性使用风险时选 B
4.2.5.3	通用系统传输（用 T 表示）	AD+VFTSw	AD+VFTSw+CIWT/SMT	可预见计量数据在开放式系统中传输时选 B
4.2.5.4	部件执行与分离及接口指定(用 S 表示)		——	——
4.2.5.5	系统参数	AD	AD	——
4.2.5.6	系统软件功能模块	AD	AD+DFA/WT	——
4.2.5.7	维护和升级(用 D 表示)		——	——
4.2.5.8	操作系统和硬件兼容性，可移植性(用 E 表示)	AD+VFTSw	AD+VFTSw+SMT	——

7. 测评结果

7.1 检测系统计量相关软件要求描述

要求：应对数据需求、数据采集方式、数据准确性、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，应要求对隶属计量相关软件的模块列表、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。

7.1.1 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。

7.1.2 测评影响

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。

7.1.3 检测系统的软件技术特性分类

要求：参照前边所述的要求，对检测系统软件技术特性进行分类。

7.1.4 检测系统软件的基本要求和特定要求

要求：根据检测系统测试原理、安全保密性要求对检测系统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。

7.1.5 测评文档资料

要求：参照 GB/T 9385 及 GB/T 8567 的要求编制测试文档。明确软件标识的生成过程及说明，软件标识应包括以下内容：软件号，版本信息，编译生成时间，并可打印输出。

7.2 测评方法

7.2.1 方法选择

要求：应根据检测系统软件的技术特性分类要求、风险等级划分明确测评项目，选择适宜的验证方法。选择可采用审查测试方法，低水平测试采用黑盒测试方法，中高水平测试采用白盒测试方法。

7.2.2 测试用例

要求：测试用例应考虑下列因素：

1）数据的准确性。

2）数据的线性特性。

3）数据的非线性特性。

4）数据是否满足精度要求。

7.3 结果测评

7.3.1 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。

7.3.2 测评结论与建议

要求：应明确检测系统软件经测评后是否符合要求。并提出如何弥补测试中发现的缺陷不足和建议。

吉林省地方计量技术规范

机动车检测系统软件测评指南

JJF（吉）32—2009

吉林省质量技术监督局发布

*

*

297 mm × 210 mm A4纸

2009年4月第1版　　2009年4月第1次印刷