ICS 35.080
L 77

DB37

山　东　省　地　方　标　准

DB37/T 3048—2017

自主可控软件测试与认证规范

2017-11-30 发布　　2017-12-30 实施

山东省质量技术监督局　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由山东省经济和信息化委员会提出并归口。

本标准起草单位：山东省计算中心（国家超级计算济南中心）、山东省软件评测中心、山东道普测评技术有限公司、山东中创软件商用中间件股份有限公司、山东瀚高基础软件股份有限公司、国家网络软件产品质量监督检验中心（济南）、山东亿云信息技术有限公司、山大电力有限责任公司、山东山大华天软件有限公司、山东正中计算机网络技术咨询有限公司、山东华迪智能技术有限公司。

本标准主要起草人：杨美红、韩庆良、韩明军、张海燕、刘娜、郑玉华、周长伦、李继才、张峻、吴梅磊、张建成、李钊、王平、张伟、张文治。

自主可控软件测试与认证规范

1 范围

本标准规定了自主可控软件要求、测试内容、测试流程、测试实施要求和认证。

本标准适用于自主可控软件的标准符合性测试与认证，也可供软件生产商在设计、验证、日常检测和维护时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

3 术语和定义

GB/T 25000.51—2016界定的以及下列术语和定义适用于本文件。

3.1

国产软件

在中华人民共和国境内最终形成，其著作权归属中华人民共和国境内的自然人、法人或其他组织，并且在国内的开发成本不低于总开发成本的百分之五十的软件产品。

3.2

自主可控软件

由软件生产商自身研发设计，全面掌握产品核心技术，拥有自主知识产权，可由软件生产商自主维护来应对安全威胁的国产软件。

3.3

符合性评价报告

说明对自主可控软件实施评价的行为和结果的文档。

注：改写IEEE std610.12-1998。

3.4

测试机构

获得中国实验室国家认可委员会认可的具有软件检测能力的机构，认可的检测能力范围应至少包括对软件功能性、可靠性、易用性，及性能效率的测试。

3.5

认证机构

依据该标准对自主可控软件实施认证的组织机构。

4 自主可控软件要求

4.1 自主性要求

软件应自主研发，且拥有自主知识产权。

4.2 用户文档要求

4.2.1 可用性要求

用户文档对于该软件的用户应是可用的。

4.2.2 完备性要求

用户文档应具有唯一标识，应包含使用该软件所必需的信息，应说明最终用户能调用的所有功能。

4.2.3 正确性要求

用户文档中所有信息都应是正确的，且不应有歧义的信息。

4.2.4 一致性要求

用户文档不应自相矛盾、互相矛盾，以及与产品说明矛盾。

4.2.5 易理解性要求

用户文档应采用软件特定读者可理解的术语和文体。

4.3 软件质量要求

4.3.1 功能性要求

软件的功能是否能执行是可识别的；在给定的限制范围内，用户文档中所陈述的所有功能应是可执行的和准确的。

4.3.2 安全性要求

软件应能够保护信息和数据，使未授权的人员或系统不能阅读或修改这些信息和数据，而不拒绝授权人员或系统对它们的访问。

4.3.3 可靠性要求

软件应按照用户文档中定义的可靠性特征来执行，应识别违反句法条件的输入，并且不应作为许可的输入加以处理；在用户文档陈述的限制范围内使用时，不应丢失数据。

4.3.4 易用性要求

有关软件执行的各种问题、消息和结果都应是易理解的；对具有严重后果的功能执行应是可撤销的，或者软件应给出这种后果的明显警告，并且在这种命令执行前要求确认。

4.3.5 性能效率要求

软件应符合产品说明中有关性能效率的陈述。

4.3.6 维护性要求

软件应按照用户文档中定义的维护性特征来执行。

4.3.7 兼容性要求

软件应按照用户文档和产品说明中所定义的兼容性特征来执行。

5 测试内容

5.1 总则

针对自主可控软件，从自主性、功能性、安全性、可靠性、易用性、性能效率、维护性、兼容性和用户文档等九个方面进行测试。其中，性能效率、维护性和兼容性部分作为考察项，其测试结果能够更全面地展现软件相应能力，但不用于软件整体测试结果的评价。

针对自主可控软件要求，给出以下主要的测试项目。在实际执行过程中，可根据自主可控软件自身特点及软件生产商要求增加测试项目。对于自主性测试、功能性测试、安全性测试、可靠性测试、易用性测试和用户文档测试等六个类别，在符合性评价报告中应至少列出以下所有测试项目，对其中不适用的测试项目，应说明其不适用原因。

5.2 自主性测试

测试内容如表1所示：

表1 自主性测试内容

测试项目		项目说明
自主管理	可行性与计划研究	应有相应的文档或记录能够证明对软件进行了可行性分析，并制定了开发计划。
	需求分析	应有相应的文档或记录能够证明对软件进行了需求分析。
	软件设计	应有相应的文档或记录能够证明对软件进行了设计。
	质量控制	应有相应的文档或记录能够证明对软件进行了质量控制。
	版本控制	应有相应的文档、记录能够证明对软件进行了版本控制。
自主研发	源代码可执行验证	软件源代码编译后生成的软件的功能完整，且与用户文档描述的软件功能一致。
	源代码自主研发验证	软件所有功能都应有对应的源代码，且软件核心功能应由自主研发的源代码独立实现。

5.3 功能性测试

测试内容如表2所示：

表2 功能性测试内容

测试项目		项目说明
完备性	功能实现的完整性	软件中应包括产品说明中所描述的所有功能。
正确性	功能的正确性	产品说明中所有的功能应都能正确执行。
	精度	软件中所有精度应与产品说明中的精度要求一致。

5.4 安全性测试

测试内容如表3所示：

表3 安全性测试内容

测试项目		项目说明
身份鉴别	鉴别机制	软件应提供专用的登录控制模块对登录用户进行身份标识和鉴别。
	登录失败处理	软件连续多次登录失败时，可采取限制非法登录次数、结束会话等措施。
	强口令策略	软件应启用强口令策略，口令长度、类型等具有复杂度限制。
	会话超时机制	软件提供会话超时机制；会话超时后，应使会话进入休眠状态或中断连接。
	错误提示信息	软件认证错误提示信息中不存在确切错误分类信息。
用户权限控制	权限控制功能	软件具有权限控制策略，对于每个角色用户权限控制合理。
	越权控制机制	软件不存在横向越权漏洞。
		软件不存在纵向越权漏洞。
	权限控制范围	软件权限控制范围覆盖系统的主要功能操作。
	限制默认账户权限	软件严格限制默认帐户的访问权限，默认用户权限应合理。
	用户最小权限原则	软件各角色用户应根据业务特性及权限互斥原则，分配最小权限。
访问审计	审计的广泛性	软件审计范围覆盖所有角色用户。
	审计的完整性	软件限制删除、修改或覆盖审计记录，维护审计活动的完整性。
	审计内容全面性	软件审计记录的内容至少包括事件的日期、时间、发起者信息、类型、描述和结果等。
	审计关键事件	软件重要安全事件记录日志。
数据安全	数据保密性	软件重要信息或敏感信息加密传输或存储。
	数据完整性	应能够检测到重要用户数据在传输过程中完整性受到破坏。
	数据有效性	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

5.5 可靠性测试

测试内容如表4所示：

表4 可靠性测试内容

测试项目		项目说明
成熟性	可控制性	在测试过程中，软件不应陷入用户无法控制的状态，如进入死循环，执行其他操作无响应。
	数据完整性	在测试过程中，不应由于软件故障而导致软件丢失数据，破坏数据的完整性。
	避免失效	在测试过程中，不应出现由于软件的故障而导致系统失效的现象。
容错性	抵御误操作	软件应对非法输入、非法操作等进行屏蔽处理。
易恢复性		在发生中断或失效时，软件能够恢复直接受影响的数据，并重建期望的系统状态。

5.6 易用性测试

测试内容如表5所示：

表5　易用性测试内容

测试项目		项目说明
易理解性	描述的完整性	用户在阅读产品说明后应能理解软件的能力。
	明显的功能	软件界面中所有的功能应易于识别。
	功能的易理解性	软件中所有界面对应的功能应易于理解。
	易理解的输入输出	软件界面中所有的输入输出项应易于理解。
易学性	用户文档和/或帮助机制的有效性	软件提供的联机帮助系统和/或文档应能有效地指导用户完成相关操作。
	帮助的获得性	软件应提供帮助的快速定位查找功能，以便用户能正确定位所需的帮助内容。
易操作性	在使用中功能操作的一致性	软件中功能操作界面的组成应保持一致。
	在使用中消息的一致性	软件中提示的信息应易于指导用户操作。
	使用中错误的纠正	在使用软件过程中，用户应能成功撤销其错误操作。
	使用中默认值的可用性	软件应提供参数值的默认值以方便用户使用。
	使用中消息的可理解性	软件中的提示信息不应导致用户操作停顿与失败。
	在使用中操作错误的易恢复性	软件应对关键数据的操作给出警告或在执行前要求确认。
	（用户错误纠正的）可还原性	软件应提供关键操作的可逆处理，以便用户纠正错误。

5.7　性能效率测试

测试内容如表6所示：

表6　性能效率测试内容

测试项目		项目说明
时间特性	响应时间	从发出请求到请求完成为止，用户经历的平均等待时间间隔。
	吞吐率	软件在给定的时间周期内有多少个任务成功的执行。
资源特性	CPU 利用率	在测试过程中服务器端 CPU 的平均使用率。
资源特性	内存利用率	在测试过程中服务器端内存的平均使用率。
容量	并发用户数	软件能够支撑的最大并发用户数量。
	存储数据项数量	软件能够支撑的最大存储数据项数量。

5.8　维护性测试

测试内容如表7所示：

表7　维护性测试内容

测试项目		项目说明
易分析性	状态监视能力	在运行中要记录足以监视软件状态的数据。
易修改性	参数表示的修改性	软件应提供方便的参数修改手段，以便变更软件适应新的应用。

5.9　兼容性测试

测试内容如表8所示：

表8　兼容性测试内容

测试项目		项目说明
适应性	硬件环境适应性	软件兼容产品说明中要求的国产硬件环境。
	软件环境适应性	软件兼容产品说明中要求的国产软件运行环境。
共存性	有效的共存性	软件能够与产品说明中列举的国产软件共存运行。

5.10　用户文档测试

测试内容如表9所示：

表9　用户文档测试内容

测试项目		项目说明
完备性	标识指示	用户文档应具有唯一的文档标识。
	使用信息	用户文档应包含使用该软件所必需的信息。
	陈述所有功能	用户文档应说明在产品说明中陈述的所有功能以及最终用户能调用的所有功能。
	差错和失效、数据丢失条件	用户文档应列出所处置的和引起应用系统失效或终止的差错和失效，特别是那些导致数据丢失的应用系统终止的结束条件。
	备份和恢复指南	用户文档应给出必要数据的备份和恢复指南。
	关键功能细则	对于所有关键的软件功能（即失效后会对安全产生影响或会造成重大财产损失或社会损失的软件），用户文档应提供完备的细则信息和参考信息。
	磁盘空间要求	用户文档应陈述安装所要求的最小和最大磁盘空间。
	应用管理	对用户要完成的应用管理职能，用户文档应包括所有必要的信息。
	集分标识	如果用户文档分若干部分提供，在该集合中至少有一处应标识出所有的部分。
正确性		用户文档中所有信息都应是正确的，且不应有歧义的信息。
一致性		用户文档不应自相矛盾、互相矛盾，以及与产品说明矛盾。
易理解性		用户文档应采用软件特定读者可理解的术语和文体。

6　测试流程

6.1　测试样品提交

送测样品由各参测企业自主提交给测试机构。自测试开始后，参测企业提交的测试样品不允许中途更换，否则视为作废。

各参测企业必须提供纸质或电子形式的可行性分析报告、开发计划、需求分析说明书、软件设计文档、质量控制文档、版本控制文档、用户文档和产品说明，提供含有软件源代码的光盘介质，必要时有责任配合测试机构进行软件安装。

6.2　测试需求分析

根据自主可控的软件要求，以及用户文档和软件产品说明，确定测试内容。

6.3　测试计划

根据测试内容，结合软件类型、应用领域和运行环境等信息，确定测试活动的范围、测试方法、测试进度和测试风险等内容，编制测试计划。

6.4 测试设计

根据测试内容及测试计划中预定的测试方法，进行测试用例的设计。

6.5 测试环境准备

按照测试设计要求，准备相应的测试环境，包括相关软件、硬件设备，以及网络环境等。

6.6 测试执行

按照设计的测试用例，实施测试，形成测试记录。

6.7 测试结果汇总与分析

对测试记录进行整理和综合分析。

6.8 测试结果评价

6.8.1 自主性评价

实施评价以确定软件自主性与4.1要求的符合程度。

6.8.2 用户文档评价

实施评价以确定用户文档与4.2要求的符合程度。

6.8.3 软件质量评价

实施评价以确定软件质量与4.3要求的符合程度。

6.9 报告编制

符合性评价报告应确立自主可控软件与第4章要求的符合性。

符合性评价报告应包含以下各项：

a) 自主可控软件标识；
b) 执行评价的人员姓名；
c) 评价完成日期以及测试完成日期；
d) 用于进行测试的计算机系统（硬件、软件及其配置）；
e) 使用的文档及其标识；
f) 符合性评价活动汇总和测试活动汇总；
g) 符合性评价结果汇总和测试结果汇总；
h) 符合性评价的详细结果和测试的详细结果(应该覆盖所测试的每项测试内容及其对应的测试项目，且每个测试项目包括对应的测试要点及详细测试结果）；
i) 若有时，不符合要求项的清单。

对于纸质的符合性评价报告而言，符合性评价报告的标识（测试实验室、自主可控软件标识、符合性评价报告日期）及其总页数均应出现在符合性评价报告的每一页上。符合性评价报告还应包含：

a) 效果声明：测试结果和评价只与被测试和被评价的项有关；
b) 复制声明：除非以完整报告的形式复制，否则未经测试实验室书面批准不得复制符合性报告。

7 测试实施要求

自主可控软件测试按照测试计划、测试设计、测试执行、测试结果评价四步骤进行实施，每个步骤的产出物依次为测试计划文档、测试用例文档、测试执行记录文档和符合性评价报告：

7.1 测试计划要求

测试计划要求包括：

a) 通过—失败准则，测试计划应指明用于判定测试结果是否证实软件与产品说明和用户文档的符合性准则；
b) 测试环境，测试计划应规定将要进行的测试所处的软件测试环境；
c) 进度，测试计划应规定每个测试活动和测试里程碑的进度；
d) 风险，测试计划应识别、更新并记录测试活动中存在的风险，并提供应对措施；
e) 人力资源，测试计划中应明确每个测试活动所需的人力资源情况；
f) 工具和环境资源，测试计划中应明确执行测试活动所需的工具；
g) 沟通，测试计划中应规定沟通机制和方式，以便在利益相关方之间共享测试文档和测试项。

7.2 测试用例要求

测试用例要求包括：

a) 测试用例说明，每个测试用例的说明都应包括：测试目标、唯一性标识符、测试的输入数据和测试边界、详细实施步骤、系统的预期行为、测试用例的预期输出、用于判断测试用例肯定或否定结果的准则等；
b) 测试用例应对测试准备、开始和执行所必须的动作、停止和最终重新启动测试的条件和动作进行说明；
c) 为提供测试的可重复性和可再现性，测试用例应足够详细。

7.3 测试执行记录要求

测试执行记录要求包括：

a) 测试记录应包括测试用例结果的全部汇总；
b) 测试执行记录应证实已按测试计划执行了所有测试用例；
c) 对于每个测试用例，测试执行记录应包括测试用例标识符、测试执行日期、实施测试人员姓名和职责、测试用例执行的结果和发现的异常清单等。

7.4 符合性评价报告要求

符合性评价报告要求可依据6.9中相关内容要求。

8 认证

8.1 认证要求

认证要求包括：

a) 软件自主性要求，要求软件生产商拥有软件的自主知识产权，能够提供相关证明材料，包括软件著作权登记证书或专利证书；
b) 软件符合性要求，要求经过测试机构测试，并出具符合本标准所要求的符合性评价报告。

8.2 认证申请

8.2.1 认证申请需要提供的资料

软件生产商应根据软件认证机构的要求，提供包括但不限于以下资料：

a) 营业执照复印件；
b) 开发或拥有知识产权的软件的证明材料，包括软件著作权登记证书或专利证书等；
c) 具有测试机构出具的按照本标准进行检测的符合 7.4 中要求的符合性评价报告。

8.2.2 认证受理

认证受理步骤包括：

a) 认证机构对软件生产商提交的认证申请及其资料的完整性、规范性和真实性进行审查；
b) 审查通过后，认证机构与软件生产商确定认证工作安排和认证计划。

8.3 认证实施

认证机构根据软件生产商提交的资料，采用文件审查的方式进行认证：

a) 文件审查：对软件生产商提供的资料所体现的软件的标准符合性、可持续性和合法性进行审查；
b) 现场审查：认证机构在文件审查的基础上，必要时可到软件生产商生产现场进行现场审查。现场审查包括核实自主研发能力、质量控制情况和知识产权情况等；
c) 认证：认证机构根据文件审查和现场审查结果，做出是否符合认证要求的决定。

8.4 认证证书

认证机构在认证通过后，应当向软件生产商颁发认证证书。认证证书的内容应当包括：

a) 认证证书名称；
b) 认证证书编号；
c) 被认证软件名称、版本（系列）；
d) 软件生产商名称、注册地址和邮政编码、联系方式、电子邮箱等；
e) 颁证日期或换证日期，以及认证证书有效期的起止年月日；
f) 认证机构的名称及其标志。