|  |  |  |
| --- | --- | --- |
| ICS | 32.020 | |
| T40 | |  |
|  | | | | | | |
|  | | | | | | |
| 团 体 标 准 | | | | | | |
|  | | | |  |  |  |
|  | | | |  | T/CSAEXX－2019 |  |
|  | | | |  |  |  |
|  | | | | | | |
|  | | | | | | |
| 新能源汽车车载控制器软件功能测试标准 | | | | | | |
| **Test Standard for Software function of vehicle Controller for New Energy vehicles**  **Drafting guidelines for commercial grades standard of Chinese medicinal materials** | | | | | | |

（征求意见稿）

在提交反馈意见时，请将您知道的该标准所涉必要专利信息连同支持性文件一并附上。

|  |  |  |
| --- | --- | --- |
|  | | |
|  | | |
| 2019-XX-XX发布 |  | 2019-XX-XX实施 |
|  | | |
| 中国汽车工程学会发布 | | |

目 次

[1 范围 7](#_Toc25676244)

[2 规范性引用文件 7](#_Toc25676245)

[3 术语和定义 7](#_Toc25676246)

[4 测试过程 8](#_Toc25676253)

[4.1 概述 8](#_Toc25676254)

[4.2  测试准备阶段要求 8](#_Toc25676255)

[4.3 测试实施阶段要求 18](#_Toc25676263)

[4.4测试结束阶段要求 30](#_Toc25676269)

[5. 测试问题管理 32](#_Toc25676272)

[5.1问题状态 32](#_Toc25676273)

[5.2问题确认 32](#_Toc25676274)

[5.3测试问题修改 33](#_Toc25676278)

[5.4测试问题关闭验证 33](#_Toc25676279)

[5.5测试问题评审 34](#_Toc25676281)

[5.6测试问题跟踪 34](#_Toc25676285)

[5.7测试问题总结 35](#_Toc25676287)

[6.测试人员能力要求 35](#_Toc25676290)

[6.1汽车业软件测试知识基础框架体系概述 35](#_Toc25676291)

[6.2体系所依据的标准和规范 36](#_Toc25676292)

[6.3体系的基础 36](#_Toc25676293)

[6.4体系的内容 36](#_Toc25676294)

[7.供应商控制器管控要求 38](#_Toc25676297)

[7.1控制器供应商测试实施方法 38](#_Toc25676298)

[7.2第三方测试机构资质要求 38](#_Toc25676301)

[7.3控制器供应商第三方委托测试的要求 39](#_Toc25676306)

[7.4委托第三方测试机构测试流程 41](#_Toc25676313)

[7.5委托第三方测试机构审查流程 43](#_Toc25676323)

[8. 自动化测试框架推荐 44](#_Toc25676331)

[8.1自动化测试框架概述 46](#_Toc25676332)

[8.2任务准备 46](#_Toc25676333)

[8.3任务初始化 47](#_Toc25676340)

[8.4任务执行 48](#_Toc25676345)

[8.5任务结束 51](#_Toc25676349)

前 言

T/CSAE XX-XXXX《新能源汽车车载控制器软件功能测试标准》包括测试开展的要求、测试管理要求、测试人员能力要求、供应商控制器管控要求、自动化测试框架推荐等内容。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文按照GB/T 1.1-2009给出的规则起草。

本文由北京新能源汽车股份有限公司提出。

本文由XXXXX归口。

本文起草单位： 北京新能源汽车股份有限公司、中汽研(天津)汽车工程研究院有限公司、上海滔瑞信息技术有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、合肥工业大学、南京越博动力系统股份有限公司、上汽海外出行、威马汽车技术有限公司等。

本文主要参审单位：重庆长安汽车股份有限公司、广州汽车集团股份有限公司、奇瑞汽车股份有限公司、德斯拜思机电控制技术（上海）有限公司等。

本文主要起草人：黄颍华、刘全周、周震漪、闫书磊、李丹、陈一帆、李麟、郭盈、朱科屹、叶璐、贺林、王劲伟、王星、曹海燕、李惠惠等。

引 言

本标准根据国内现有新能源汽车控制器软件功能测试的需求而编写。

测试是控制器软件开发的关键环节，目前国内控制器测试工作不仅在原有的验收检验领域不断深化发展，而且也越来越多的渗透入上游控制器开发的工作进程中。这些功能的验证和检测工作将为控制器软件开发需求的实现提供有效证明，并且为产品的质量、潜在风险包括产品后期优化升级的方向提供专业的信息。

随着控制器产品需求的高速迭代扩展，测试工作的体量和复杂度也在不断增加，本标准通过提供适当的要求和流程为测试工作推荐指导实践方法。

车载控制器软件测试是通过一系列活动实现的，这些活动可以通过有效组织匹配应用于不同类型的控制器软件开发体系中，尽管本标准针对的是新能源汽车车载控制器测试，但它也为其他工业领域的控制器开发的验收检验工作提供指导。

本标准主要内容如下：

1. 提供了一个新能源汽车车载控制器软件测试生命周期活动要求（测试准备阶段、测试实施阶段、测试结束阶段），并对这些阶段内的必要活动进行了裁剪说明；
2. 提供了一种控制器软件测试问题的管理要求；
3. 应用新能源汽车车载控制器全生命周期活动要求及全生命周期要素管理要求，可规范现有测试流程，避免产品开发的风险；
4. 提供一种控制器软件测试人员能力的评估和培训要求；
5. 提供了一种供应商控制器管控的要求；
6. 提供了一种自动化测试的框架。

新能源汽车车载控制器软件测试活动受控制器开发体系（自主、外包）、开发类型（V型、迭代、敏捷、瀑布等）、开发成熟程度（单一架构、多平台化）的影响并与开发活动和工作成果直接关联，本标准即与控制器软件开发工作强相关。

表1为本标准的整体架构。

表1 《新能源汽车车载控制器软件功能测试标准》概览

|  |  |  |
| --- | --- | --- |
| 《新能源汽车车载控制器软件功能测试标准》概览 | | |
| 1、测试开展要求 | | |
| 测试准备阶段要求 | 测试实施阶段要求 | 测试结束阶段要求 |
| 2、测试问题管理要求 | | |
| 3、测试人员能力要求 | | |
| 4、供应商控制器管控要求 | | |
| 5、自动化测试框架推荐 | | |

新能源汽车车载控制软件功能测试标准

1 范围

本标准规定了新能源汽车车载控制器功能测试开展全过程的要求，包括：

——对测试测试准备阶段、测试实施阶段和测试结束阶段要求；

——对测试问题管理的要求；

——对测试人员能力的要求；

——对供应商控制器管控的要求；

——自动化测试框架推荐。

本标准适用于新能源汽车车载控制器软件功能测试，其他类型控制器的测试可参照使用。

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 20263—2006 导航电子地图安全处理技术基本要求

GB/T 30290.3—2013 卫星定位车辆信息服务系统第3部分：信息安全规范

ISO26262 道路车辆系统设计功能安全

ISO/IEC 27001—2005 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC/IEEE 29119-3—2013 Software and systems engineering — Software testing — Part 3: Test documentation-

3 术语和定义

ISO/IEC/IEEE 29119-1-2013界定的以及下列术语和定义适用于本文件。为了方便使用，以下重复列出了GB/T 20000.1-2014中的某些术语和定义。

3.1

**测试成功 test success**

达成事先设定的测试目标，该测试目标可以是发现既定数量的问题、对需求文档的覆盖情况等，而不是指被测控制器或软件通过测试。

3.2

**静态测试 static testing**

对组件/系统进行的不执行程序代码（软件）的一种测试。例如，对代码评审或静态代码的分析。

3.3

**动态测试 dynamic testing**

通过运行软件的组件或系统测试软件。

3.4

**冒烟测试 smoke testing**

所有定义的或计划的测试用例的一个子集。它覆盖组件/系统的主要功能，以查明程序的绝大部分关键功能是否正常工作，但忽略其细节部分。

3.5

**再测试 verify testing**

首次测试发现问题后，针对已修改程序进行的问题关闭验证测试，通常在回归测试之前完成。

3.6

**回归测试 regression testing**

对已测试已修改程序进行的测试，确保软件的更改没有对未改变的部分带来新的失效。

4 测试过程

4.1 概述

测试开展过程从便于行业理解上划分成测试准备阶段、测试实施阶段、测试结束阶段。以保障测试开展时内容的完整性和测试的有效性。

4.2 测试准备阶段要求

4.2.1 概述

在该阶段会涉及多种文件信息导入，在开始前应建立流程或采用正式文件约定的方式与测试提出方确定上述文件的具体提供方式和格式类型。

4.2.2 主要活动

测试准备阶段的主要活动如下：

1. 制定测试计划；
2. 收集测试依据；
3. 设置准入条件；
4. 入口质量要求；
5. 设置出口准则；
6. 测试环境准备。

4.2.3 测试计划

测试计划中应包含测试范围、测试时间周期、测试依赖资源的确认信息。

4.2.3.1 测试范围确定

根据测试目标确认测试范围。

测试目标按照项目不同阶段的质量要求划分为：研发阶段新功能验证、研发阶段功能变更验证、研发阶段功能调试、量产功能验证、量产后功能变更验证。

针对上述不同的测试目标，其测试范围不应少于以下要求:

1. 研发阶段新功能验证，应对新功能本身开展完整功能需求覆盖测试和代码覆盖度测试，对上层驱动功能、下层受影响功能开展功能集成测试，针对控制器涉及整车上下电、快充、慢充、行车功能开展测试，并确保在测试期间无故障报出；
2. 研发阶段功能变更验证，应对变更部分代码开展功能需求覆盖测试，对上层驱动功能、下层受影响功能开展功能集成测试，针对控制器涉及整车上下电、快充、慢充、行车功能开展测试，并确保在测试期间无故障报出；
3. 研发阶段功能调试，对功能本身开展功能正向测试，对上层驱动功能、下层受影响功能开展集成功能的正向测试；
4. 量产功能验证，应开展完整功能测试；
5. 量产后功能变更验证，开展完整功能测试。

除了以上测试目标外，若有其他测试目标时，可根据被测对象期望的目标质量要求来设置测试范围。

4.2.3.2 测试时间周期确定

测试时间周期需要考虑的内容有:已经确定的测试范围、被测对象质量现状、人员能力现状。已确定的测试范围可参照4.2.3.1，被测对象质量现状要求可参照4.2.6。

人员能力现状是指在已确定被测对象质量的现状前提下，在测试资源无异常的情况下完成既定测试范围内容所需的时间。

宜采用的方法有经验评估和专家评估等。

由于测试准备阶段与测试结束阶段通常都与项目开发的其他活动并行开展，对项目整体影响较小，本标准重点对测试实施阶段的时间周期进行要求。另外测试时间周期是基于风险拟定的。

测试实施阶段时间严格按照以下规则进行划分，其中的再测试与回归测试可以单独进行时间计划排布，按以下方式拟定计划时，应将计划与工作内容细化到1天。

测试实施阶段时间宜参考一下公式进行计算：

…………………………………（1）

式中:

Tp为测试环境搭建时间

Ts为冒烟测试时间

Tf为功能测试时间

Tv为再测试时间

Tr为回归测试时间

测试环境搭建：为被测对象搭建一个保障测试目标有效的测试环境，可以是闭环的，也可以是开环的。测试环境搭建时间主要需要考虑测试工具或软件使用的难易程度、模拟测试环境的难易程度以及此间所涉及的重复性工作量。

冒烟测试：为了保障后续测试的有效性和测试的可实施性，在正式的功能测试开始之前应对被测控制器的基本功能以及对整体功能有影响的部分首先开展测试。冒烟测试时间主要需要考虑冒烟测试的范围大小、自动化程度以及被测对象的质量现状。

功能测试：即既定的测试需求，由具体测试范围大小所决定。

再测试：为了关闭功能测试中所报出的问题而开展的测试，在再测试中应对受影响的功能以及被修改驱动的功能开展集成测试，对该时间影响较大的有问题的数量、问题本身的复杂程度以及软件的集成过程。

回归测试：为了确定问题修改完之后没有引入新的问题而开展的测试，时间上受回归测试范围所决定，而回归测试范围受软件的集成过程、开发的自动化程度以及受影响的代码范围所决定。

针对开发过程中的不同情况预设测试周期的构成方式，可在测试开始前对开发人员做出测试周期的开放式承诺，使测试时间的制定对开发方面更加透明和可预测，有助于开发与测试的合作意愿和测试团队的能力提升。使用者可根据需要按照本标准附录A给出的测试周期构成方式进行测试。

4.2.3.3 确定测试依赖资源

测试依赖资源包括测试活动所需要的外在输入与内在资源。其中外在输入主要指测试提出方以及与本次测试成功与否相关的利益干系人，提供的用以支撑测试实施以及确定测试范围的输入信息、被测对象。测试输入信息包含功能描述文档、接口描述文档、测试目标信息。

被测对象除代码外也泛指被测对象功能整体表现所依存的对象，如在硬件在环测试环境中为了实现风扇开启功能所需的控制器硬件与控制器硬件接插件及附带线束。

内在资源指与测试相关的人员、测试工具、测试软件

本标准在测试准备阶段对功能描述文档、接口描述文档、测试目标信息、被测对象、内在资源进行要求。

1. 功能描述文档；
2. 功能描述文档应具备以下性质，并且提供方须通过含检查项表单在内的评审记录或可追溯的其他信息对测试内容进行承诺：

——一致性：该文档的直接干系人之间就内容已达成一致意见，在使用上不存在理解偏差，直接干系人至少包括文档的编写人、文档依据信息提供人、文档使用人；

——统一性：文档内容之间以及与其成套的文档间无相互矛盾；

——可验证性：有明确的访问或检查接口指引，同时有明确的判定指标；

——可追溯性:与其他文档有追溯关系，或有明确的文件信息表明其来源；

——可理解性：术语用词基于公司或测试开发团队共同约定，若文档依据信息提供方为非软件开发团队时，应由文档编写方创建术语表。

1. 功能描述文档在内容描述时需要遵循以下原则：

——不可使用超过7条语句来描述同一功能情景；

——每条语句仅使用主动语态级用1个过程动词来明确表达需求，应避免错综复杂的语句描述；

——名词的指向应为某项具体的内容，而非指向某个类别的内容，比如不应用“控制器”来替代“电机控制器”；

——在使用全称量词时应确认是否适用，全称量词如，“从不”、“总是”、“没有”、“每个”、“所有的”；

——不可使用不确定的词汇对功能进行描述，比如“可能”、“有时”、“一些”、“部分”；

——不可存在非完整的规格说明条件，在对一个需求进行说明时，应确保涵盖对所有数据范围的描述。例如，当描述“电压大于380V时所有电磁阀打开”时，还应说明电压小于等于380V时电磁阀开启或关闭情况及其引发现象。此外，只有一种情况可以不对全范围数据进行描述，即当接口输出值为布尔类型非A即B时，默认描述完合适输出A后，其他情况均为B，即“当描述温度大于20度时风扇开启（A）”，则默认为当温度小于等于20度时风扇关闭（B），不完全说明时本标准默认为输出取值为相反状态；

——推荐该文档提供者使用自然语言模板进行描述，或者为了使该文档的使用程度更高，使用自然语言模板对编写者进行相应培训，以下推荐一种的自然语言模板：



图1被测模板文件功能描述文件自然语言模板

**注1：**过程动词是指描绘功能性、操作动作的词汇，如发送、断开、闭合。

**注2：**目标文件是指“过程动词”作用的目标。

——该文件在使用自然语言构成的同时，推荐在不同场合增加以下表达方式来清晰对功能的描述：

1. 用例图
2. UML类图
3. UML活动图
4. UML状态图

以上4类图例表达方式为公开技术，本标准不再进行复述。

1. 接口描述文档；

接口描述文档需要描述被测对象存在的物理状态以其接口形式。

该文件用以描述被测目标文件的测试接口，考虑到接口形式、类型并不相同，可通过多类文件进行描述，比控制器硬线接口定义、CAN通讯协议、诊断协议、标定协议文件、以太网协议等。

本标准要求接口名称应与该接口实际功能有匹配关系，接口描述的内容应包含其接口特性所应承载的内容，同时应描述该接口的传输方向。

物理状态为真实控制器的被测对象接口涉及内容广泛，为免疏漏以真实控制器情况下的接口描述为例，如在对数字和模拟通道接口描述时，应包含以下信息：

1. 与数字和模拟通道相连的外围电气负载，可以原理图的形式呈现；
2. 信号类型（模拟量、开关量、PWM等）、收发频率、门限值、准确度设计要求；
3. 若该通道需要开展硬线信号故障注入，应确定接口外接属于执行器还是传感器；
4. 若有外接传感器应给出关联传感器电气特性；
5. 若有执行器应给出关联执行器电气特性。

通信协议用于仿真和接收被测目标文件总线通信信息，模拟与被测目标文件交互的虚拟节点。

所有协议相关文件（如.dbc、.ldf）和通讯矩阵(至少包含：ID、消息长度、信号、发送频率/周期、数据范围、数据分辨率)提供通讯矩阵每个信号的意义解释；对于状态信号，应在后续的功能描述文件中提供详细的状态转换逻辑说明；

如果协议文件中存在CRC校验（或CheckSum），应在后续的功能描述文件中提供详细的校验算法说明。

1. 测试目标信息补充；

测试任务描述应包括测试任务目标来源信息，任务相关的主要利益干系人，任务的直接下发团体及人员，描述任务发起人及主要利益干系人要求开展本次测试的目的、软件用途。在后续设计测试出口准则以及用例设计时应参考本部分内容。

推荐包括下述其中一个或多个测试目标信息在任务表述时被提出：

1. 测试完成后期望达到的质量/性能目标（这个目标如果被提出则应是量化的）
2. 测试未关闭问题的严重程度
3. 测试功能覆盖范围与测试应完成的时间节点
4. 被测对象；

被测对象为代码时，应提供完整的程序，包括其所依赖的库文件。

被测对象的载体若为控制器硬件，此时除了被测对象所搭载的控制器外，同时也应包含带有插针的接插件以及连接线束。

1. 内在资源；

需要确定在实施计划以内完成测试所需的人员及其能力是否匹配，包括其出勤情况等。

需要确定所需工具是否可用，数量是否充足，所需工具如万用表、示波器、HIL测试台架、充电桩、充电卡、手机APP等。

需要确定所需要的测试软件是否完成在测试电脑上的部署，并确认测试电脑对外信息接口状态是否符合公司或团队的要求。

4.2.4 准入条件

准入条件在设置时应考虑在一般外在压力情况下是否可执行，以及是否为测试实施的必要条件。准入条件的设置可告知干系人测试实施的启动条件并对测试进行有效管理。

在以下情况时应考虑将其设置为准入条件：

1. 测试所依存的信息、文件缺失导致测试无法实施，严重影响测试启动；
2. 文件数量庞大，来源复杂，需要额外关注，实时审核测试提出方提供所需的文件和信息；
3. 若同一测试提出方开展的测试，统计数据显示每次发生的问题数量随机性较大，导致测试计划时常无法按时完成，此时应按照4.2.5的要求设置准入条件。

4.2.5 入口质量要求

入口质量作为准入条件的一部分考虑到其重要程度在本部分单独进行要求。

1. 应被描述和证明，证明文件由被测对象提供方提供，若没有相关文档或交付信息时，也应描述为无，此时代表开发前端未开展过任何调试或测试；
2. 不单包含计划内测试内容应该达到的质量，还应包含在测试期间测试需求发生变化的部分应该达到的质量；
3. 文档应描述被测对象在开展本次测试前所经历过的测试，内容应包括测试覆盖范围、测试级别、发现问题列表以及其整改情况。若未开展过任何测试，则应描述其开展过的调试情况，包括调试时长、调试环境模拟情况以及调试发现的问题。

4.2.6 出口准则

出口准则为表明测试何时结束的条件。设置出口准则时应按照如下实施：

1. 测试在不可抗拒力的情况下无法实施应默认为出口准则，无需单独列出；
2. 当4.2.3.1中的测试范围全部完成并通过时应默认为出口准则，无需单独列出；
3. 可作为计划的时间节点应满足时的最低质量要求给出；
4. 可作为因软件问题导致测试无法实施的最长时间要求。

4.2.7 测试环境准备

所搭建的测试环境同时包含开环的部分与闭环的部分，测试环境中的被测对象输入的某个或多个信号与被测对象输出的某个或多个信号，在以下情况下应搭建闭环测试环境：

1. 与被控对象存在关联关系；
2. 输出信号至某个控制器（该控制器为被测对象以外的虚拟节点）的输入信号为同一控制器发送，且两信号间存在逻辑关系。

一般性要求：

1. 测试环境的存在形式与被测对象相关，如被测对象为simulink模型文件，则测试环境也应为模型文件或其他可以与simulink模型文件进行交互的测试环境；
2. 测试环境的运行步长应小于被测对象的程序运行最小步长；
3. 测试环境与被测对象交互部分的仿真程度应符合测试目标的要求；

同时本标准对硬件在环测试设备、测试工具软件进行如下要求。

4.2.7.1 硬件在环测试设备的要求

硬件在环测试设备应包含以下要素：

1. PC上位机：用于承载HIL测试系统中上位机软件的部署；
2. 实时仿真处理器：用于承载实时环境模型，处理实时模型数据，该处理器的选取应考虑需要被承载的环境模型在该处理器上运行时，被测控制器的程序运行时钟步长应为仿真环境模型实时运行最小步长时间的整数倍数，且该整数应大于2；
3. I/O板卡：用于数字量/模拟量/频率量/电阻/电流信号的采集与输出，能够涵盖汽车动力系统、底盘系统等系统所需的所有I/O通道。通道类型和数量可在实施前根据所需测试的控制器接口情况进行匹配，在对被测控制器进行调研时应关注其通道类型、信号范围、准确度要求，对于一些反复变化的信号还应考虑其采集/发送的频率情况；
4. 通讯板卡：用于仿真器与各种总线系统的连接通讯，支持CAN、LIN、车载以太网和FlexRay总线系统，具体选用何种通讯可根据实施方的情况进行选择；
5. 程控电源：用于模拟车载蓄电池电压曲线，为系统供电，并提供安全保护等功能，由于该电源在模拟蓄电池电压的同时，还可能会给I/O板卡供电，为了获得车载蓄电池电压与控制器输入信号电压独立控制的测试效果，宜配备2块以上的程控电源；
6. 故障注入板卡：可以与模拟和数字通道信号链接实现故障注入，通过电磁阀切换或者其他方式实现小电流与故障通道连接。用于故障注入测试，应包含悬空、对地短接、对电源短接、通道与通道间短接。

对于具备不同属性的设备仪器选型宜参考以下要求：

1. 对具有采样率指标的设备仪器，一般宜设备采样频率大于被测量信号的周期频率。例如，电机控制器设备模拟信号采样率大于被测量信号周期频率的50倍；设备数字信号采样率大于被测量信号周期频率的10倍。例如，整车控制器设备模拟信号采样率大于被测量信号周期频率的8倍，设备数字信号采样率大于被测量信号周期频率的8倍；
2. 对具有量程指标的设备仪器宜被测信号正向最大值不超过仪器量程正向最大值的80%，且精度控制在±0.5%以内；被测信号负向最小值不超过仪器量程负向最小值的80%，且精度控制在±0.5%以内；
3. 对具有功率等级的设备仪器宜所提供电压、电流及功率均能满足被测设备要求，且具有不低于20%的功率余量，电流电压精度控制在±0.5%以内，10%负载时功率因素大于98%，阻性负载时纹波小于0.1%，10%～90%电流上升时间小于2MS，当设备发生短路或故障时能够安全及时动作保护。

设备选型时应参考对应的设备说明书，结合被测软件的特点，还应考虑以下宜进行选型：

1. 从自动化扩展方面考虑，PC上位机搭载上设备所需软件工具后，其发送指令开始计时到该信号被实时处理器处理完成并回传截止的时间间隔为T1，应至少为被测控制器中涉及时间控制描述中最小时间T2的0.5倍。T1时间通常与操作系统、工作站性能、软件工具相关，测量条件推荐为当前版本Matlab软件正在打开的同时开始测量；
2. I/O板卡的通道类型及总数根据被测软件的实际情况决定，模拟量大电压采样精度在±0.5%，模拟量小电压采样精度在±0.1%。性能方面宜达到以下要求：

表2设备性能要求

|  |  |  |  |
| --- | --- | --- | --- |
| 通道类型 | 采样率 | 输入/输出范围 | 精度 |
| AI | 10kS/s | 大于等于系统设计最大电压 | 优于控制器的输出精度 |
| AO | 10kS/s | 大于等于系统设计最大电压 | 优于控制器的采样精度 |
| DI | 10kS/s | 大于等于系统设计最大电压 | / |
| DO | 10kS/s | 大于等于系统设计最大电压 | / |

1. 对于CAN通讯通常宜要求如下：独立高速CAN通道，波特率可配置，最高传输速率1Mbps，可导入配置的dbc文件，通道数量满足被测控制器的网络数量；
2. 程控电源配置宜：电压范围大于被测控制器的最大额定电压，电流范围满足被测控制器的最大工作电流，具有程控功能。

由于车载控制器分类比较多，例如电机控制器、整车控制器、电池管理系统、DC-DC控制器等，不同控制器台架的在环测试设备有所不同，可根据其具体情况及测试目的配备其他必要的测试设备。

4.2.7.2 测试工具软件的要求

测试工具软件分为两类，一是用于运行测试环境，二是用于测试执行。

1. 运行测试环境的工具；

模型环境测试和软件集成环境测试在上位机平台上执行，测试工具软件选取可考虑以下因素：

1. 自动代码生成，可将常用的软件搭建模型转换为高效、确定且简明易读的C语言代码；
2. 代码覆盖度分析，针对代码执行过程的动态分析，找出从未被执行的代码段。要求自带代码覆盖度分析功能，或留有接口覆盖度分析的工具接入；
3. 测试机制，能够使用多种测试机制、测试手段对代码进行测试，留有不同的接口可用于模型或代码进行信号连接，构成如MIL、SIL、PIL等测试环境；
4. 代码生成效率，测试工具能够对模型或代码效率进行分析，简化模型和代码的复杂度，通常一个5M大小的环境模型编译时间不应超过10分钟；
5. 自动化程度，测试工具的选取应具有一定的通用性和自动化功能，提高测试的效率；
6. 可扩展性，工具本身预留充足接口便于进行二次开发；
7. 用于测试的代码情况。由于上位机上开展测试的代码有可能并非完整代码，需要考虑用于测试的这部分代码里是否含有服务层代码，若有则在选择测试软件时应考虑是否应具备将服务层发送的数据转换为信号的功能；
8. 符合相关的质量标准和功能标准。这一项可根据实施方在这方面的要求进行考虑，如开发流程需要开展或已经开了ISO26262的认证，那么需要考虑是否符合ISO26262标准对验证工具软件的要求，若开发上采用了AUTOSAR架构，则需要考虑是否支持AUTOSAR标准软件部分的测试。
9. 测试执行工具；

测试设备本身也需要依托于测试上位机的工具软件来开展测试，测试设备的工具软件应至少满足以下要求：

1. 测试采用的软件应至少支持Windows, Mac, Linux等系统中的一种或多种操作系统，支持C、C++、Python、.NET语言接口；
2. 支持使用可视化的图形建模工具搭建环境模型；
3. 具备数据分析和环境模型转换为运行代码的功能，具备标准的第三方软件接口。能够满足多任务、多用户的测试开发需求；
4. 测试软件应能支持实时测试和在线标定、配置和控制I/O接口，提供操作界面，实现测试自动化，出具测试报告的功能；
5. 测试软件应具备多种数据类型格式的实时导入和存储功能，支持向量、数组、结构体等多种形式的数据写入和存储。存储的数据可以进行格式转化和二次开发。

4.3 测试实施阶段要求

测试实施阶段除了测试执行本身外，还包括对功能描述文档的前期处理以及测试设计方面的要求。

4.3.1 对测试需求的分析要求

对测试需求的分析为可选内容，若测试准备阶段提供的描述文件，指向清晰，条目化清晰可不做测试需求的分析。

开展测试需求分析的目的是在于将测试需求条目化、识别测试接口、明确每条测试需求的测试用例设计要求以及在有可能的情况下提取非功能性质量要求。

1. 条目化；

根据功能描述文件进行条目化工作，从文档中将相对独立的功能描述内容提取出来构成一个单独的条目，同时明确该功能的前置条件。

1. 测试接口；

根据功能描述文件与接口描述文件识别条目化后的功能涉及的输入接口、输出接口。

若两份描述文件由不同部门编写，则可能遇到两份文件中接口描述名词不一致的情况，若无法短时间内修正，那么应在描述测试接口时应明确注明该接口所接收的额外信息来源。

1. 用例设计要求；

根据测试目的以及功能本身可能带来的影响，针对条目化的内容逐一编写用例设计要求，在设计时除了考虑对测试设计方法选用的要求外，还可参考4.3.3对不同等级进行要求

1. 非功能性质量要求。

非功能性要求需同时参考功能描述文档内容间的联系以及外部政策法规要求。比如功能描述文档中提出了有高低压互锁功能，但没有明确其断开时间，那么可根据政策法规提出性能要求——“当发生高低压互锁故障时，要求1秒以内断开高压”。再比如当功能描述文档中提出了绝缘检测功能，但未明确其对驾驶员的显示要求，那么可根据法规要求提出安全性要求——“在绝缘检测发生时需要发出可在仪表显示的信号”。

4.3.2 基于需求的测试用例设计要求

本标准要求在设计测试用例的同时对测试用例进行编号，编号规则需与前端功能描述文档或测试分析文档的编号规则有一定的相似性。若控制器为平台化开发，则需要在用例的最后附加上针对项目应用的标识号。

测试用例除了包含编号外，应有不超过32个字符的，容易辨识、与相关阅读者形成共识的英文或英文缩写来表达该用例所指向的测试内容。

测试用例具体测试内容的格式上应包含前置条件、输入变量及其数值、预期结果。

测试用例在编写后应进行评审，评审应由对功能了解的开发人员以及编写用例的测试人员共同参与，在评审完成后需及时编写会议纪要进行签批确认，或对于该次会议的评审范围进行当场修改并于一致通过后结束会议。

本部分内容主要依据黑盒测试方法和新能源汽车中可能出现的功能提出。

在使用下述测试用例设计要求之前，除了根据功能本身的重要程度之外，还可根据开发团队所使用的工具情况、流程实际执行情况以及以往在测试端的软件质量表现来选取采取何种等级的用例设计。

相同的测试条件在不同的功能模块中，根据重要程度不同采用的设计测试方法也不同。本标准将功能的重要程度分为三类：重度，中度，轻度。

重要程度的定义如下：

——重度：影响整车安全的功能，或容易出现问题的中度功能；

——中度：影响车辆使用体验（包括驾驶体验）的功能，或不容易出现问题的重度功能；

——轻度：人体无法直接感受，或不容易出现问题的中度功能。

目前新能源汽车车载控制器软件功能定义描述的内容，主要可分为以下几类：

1. 阈值类；
2. 查表类；
3. 触发条件类；
4. 延迟触发类；
5. 分支类；
6. 故障类；
7. 枚举类；
8. 多状态跳转类；
9. 迭代控制类；
10. 公式类；
11. 配置类。

不同测试点应按照输出有效与无效相互交错的方式进行排序，即有效、无效、有效、无效，相互交替顺序执行。

4.3.2.1 阀值类测试用例的设计方法

应用表3列出的阈值类需求描述设计测试用例。

表3阈值类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | | AX≤B |
| 不同重要程度的测试点： | 重度 | X分别取值A、A+精度值、B、B+精度值、AB中间值、起作用的A的最小值、起作用的B的最大值 |
| 中度 | X分别取值A、A+精度值、B、B+精度值、AB中间值 |
| 轻度 | X分别取值A、A+精度值、B、B+精度值 |
| 测试技术及方法： | 等价类、边界值 | |

参考表4提供测试用例实例设计阈值类测试用例

表4阈值类需求功能实例

|  |  |
| --- | --- |
| 功能描述： | 当电机转速>电机超速限制值(12000rpm，精度60)，则MCU进入零转矩控制模式 |
| 测试点： | 电机转速=11940rpm，MCU未进入零转矩控制模式 |
| 电机转速=12000rpm，MCU未进入零转矩控制模式 |
| 电机转速=12060rpm，MCU进入零转矩控制模式 |

4.3.2.2 查表类测试用例的设计方法

查表类测试用例设计方法包括二维查表及一维查表，以二维查表为例内容如下：

表5查表类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | | 二维查表 (直线代表表格边界,×代表测试的数值点) |
| 不同重要程度的测试点： | 重度 | 有特征点的也需要选取特征点及其前后的点作为测试点 |
| 中度 | 有特征点的也需要选取特征点及其前后的点作为测试点 |
| 轻度 | 有特征点的也需要选取特征点及其前后的点作为测试点 |
| 测试技术及方法： | 等价类、边界值 | |

4.3.2.3 触发条件类测试用例的设计方法

应用表6列出的触发类条件的需求描述设计测试用例。

表6 触发条件类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | 满足条件1、条件2、条件3，即实现某功能，条件之间为逻辑运算符建立联系  以条件1&&条件2&&条件3为例 | |
| 不同重要程度的测试点： | 重度 | 1.满足条件1且满足条件2且不满足条件3，不实现该功能  2.满足条件1且不满足条件2且满足条件3，不实现该功能  3.不满足条件1且满足条件2且满足条件3，不实现该功能  4.每个条件都满足，实现该功能  5.确定功能可以重复触发 |
| 中度 | 1.满足条件1且满足条件2且不满足条件3，不实现该功能  2.满足条件1且不满足条件2且满足条件3，不实现该功能  3.不满足条件1且满足条件2且满足条件3，不实现该功能  4.每个条件都满足，实现该功能  5.确定功能可以重复触发 |
| 轻度 | 1.选取任意条件不满足，不实现该功能  2.每个条件都满足，实现该功能 |
| 测试技术及方法： | MCDC覆盖、判定覆盖 | |

4.3.2.4 延迟触发类测试用例的设计方法

应用表7列出的延迟触发条件类需求描述设计测试用例。

表7延迟触发条件类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | 满足一些单条件或条件组合且持续时间>=T,实现此功能。 | |
| 不同重要程度的测试点： | 重度 | 1.满足条件1，持续时间<T，不实现此功能。  2.不满足条件1，持续时间>=T，不实现此功能。  3.达到前置条件，满足条件1，持续时间T1 < T，再重新进入前置条件，满足条件1，持续时间T2 < T，在此期间均不实现此功能，其中T1 + T2 >= T  4.满足条件1，持续时间>=T，实现此功能,同时观察在后续的T时间内该功能现象未消失或符合预期。 |
| 中度 | 1.满足条件1，持续时间<T1，不实现此功能。  2.不满足条件1，持续时间>=T1，不实现此功能。  3.达到前置条件，满足条件1，持续时间<T1，再重新进入前置条件，满足条件1，持续时间<T1不实现此功能，其中T1 + T2 > T  4.满足条件1，持续时间>=T，实现此功能,同时观察在后续的0.5T时间内该功能现象未消失或符合预期。 |
| 轻度 | 1.满足条件1，持续时间<T1，不实现此功能。  2.不满足条件1，持续时间>=T1，不实现此功能  3.满足条件1，持续时间>=T，实现此功能。 |
| 测试技术及方法： | 等价类、边界测试 | |

4.3.2.5 故障类测试用例的设计方法

应用表8列出的故障类需求描述设计测试用例。

表8故障类需求描述

|  |  |
| --- | --- |
| 描述： | 满足条件1（或为组合条件）则触发故障。 |
| 不同重要程度的测试点：（重度、中度、轻度相同） | 1.不满足条件1，故障现象未触发。  2.满足条件1，触发故障现象。  3.恢复故障。  4.再次满足条件1，触发故障现象。 |
| 测试技术及方法 | 等价类、强度测试 |

4.3.2.6 枚举类测试用例的设计方法

应用表9列出的枚举类需求描述设计测试用例。

表9枚举类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | X信号有N种输入值，之后导致Y信号有3种及以上的输出值或组合 | |
| 不同重要程度的测试点： | 重度 | 1.测试X信号的N种输入值 |
| 中度 | 2.测试X信号的N种输入值 |
| 轻度 | 1.将Y信号的输出情况列出  2.测试每个输出的其中1个有效等价的X输入值 |
| 测试技术及方法 | 真值表、等价类 | |

4.3.2.7 多状态跳转类测试用例的设计方法

应用表10列出的多状态跳转类需求描述设计测试用例。

表10多状态跳转类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | 2个及以上的状态描述，且存在状态跳转路径的情况 | |
| 不同重要程度的测试点： | 重度 | 1.将状态转换为状态树  2.按照MCDC以及路径覆盖的方式编写测试用例，若条件中存在非布尔型的输入量，则还应按阈值类测试中重度的取值方式覆盖取值 |
| 中度 | 1.将状态转换为状态树  2. 按照MCDC的方式编写测试用例，若条件中存在非布尔型的输入量，则还应按阈值类测试中中度的取值方式覆盖取值 |
| 轻度 | 1.将状态转换为状态树  2. 按照判定覆盖的方式编写测试用例 |
| 测试技术及方法： | 状态转换、等价类、边界测试、MCDC覆盖、路径覆盖、分支覆盖 | |

4.3.2.8 迭代控制类测试用例的设计方法

应用表11列出的迭代控制类需求描述设计测试用例。

表11迭代控制类需求描述

|  |  |
| --- | --- |
| 描述： | 迭代控制变量 |
| 不同重要程度的测试点：（重度、中度、轻度相同） | 1.操作1获得该变量的值并记录A  2.操作2基于记录的值A获得记录值B  3.操作3基于记录值B获得记录值C  3.清除该记录值（根据具体情况验证）重新重复1）、2） |
| 测试技术及方法： | 状态转换 |

4.3.2.9 公式类测试用例推荐的设计方法

应用表12列出的工时类需求描述设计测试用例。

表12公式类需求描述

|  |  |  |
| --- | --- | --- |
| 描述： | 以数学公式的方式给出的需求，有N个变量作为输入 | |
| 不同重要程度的测试点 | 重度 | 1.选取公式的输出变量的最大值、最小值，以及需要重点考察的输出值作为预期结果。  2.根据所选的数值反推N个变量的输入值作为输入，观察实际结果和预期结果是否符合  3.固定其他N-1个变量为任意值，但固定后不能导致公式本身为常数，剩余1个自变量取值最大值、最小值、以及在最大和最小之间取3个点，若该变量取值范围跨越0，则3个点中应包含零点、零点以上的点和零点以下的点。  4.重复步骤3）直至所有变量均被测试一遍  5.将N个变量均取值为0进行测试 |
| 中度 | 1.固定其他N-1个变量为任意值，但固定后不能导致公式本身为常数，剩余1个自变量取值最大值、最小值、以及在最大和最小之间取3个点，若该变量取值范围跨越0，则3个点中应包含零点、零点以上的点和零点以下的点。  2.重复步骤1）直至所有变量均被测试一遍  3.将N个变量均取值为0进行测试 |
| 轻度 | 1.固定N-1个变量为任意值，但固定后但固定后不能导致公式本身为常数，剩余1个自变量取任意值。  2.重复以上步骤直至所有变量均被测试一遍  3.将N个变量均取值为0进行测试 |
| 测试技术及方法 | 错误推测,边界测试 | |

当变量为查表值或变量之间还有其他关联关系时（如同为查表值，且查表所依赖输入量存在相似内容），在取值时可能会因为关联变量的原因而受到限制，此时可观察数据情况尽量选取有意义的值进行测试。

4.3.2.10 配置类测试用例设计方法

应用表13列出的配置类需求描述设计测试用例。

表13配置类需求描述

|  |  |
| --- | --- |
| 描述： | 该功能应平台化软件在没有配置不起作用时 |
| 不同重要程度的测试点：（重度、中度、轻度相同） | 1.配置的功能按照需求进行测试  2.未配置功能运行之前与其配套的用例库中的1个包含某项功能有效等价类的测试用例观察其输出是否无任何反应 |
| 测试技术及方法： | 等价类 |

4.3.3 基于经验的测试设计

考虑到测试无法穷尽的固有属性，保证一定的测试自由度有助于发现问题。本标准不提出具体的基于经验的测试方法以及其具体实践办法，但要求功能测试应有一定的自由度，应采取一定的基于经验的测试设计，如探索性测试、错误推测、场景测试。

1. 探索性测试。如基于输入观察输出，并根据输出值决定之后改如何操作，同时可根据经验判断输出是否合理，以此发现缺陷并对功能描述文档进行补充；
2. 错误推测。利用已有经验及缺陷数据，创建缺陷列表，而后针对缺陷列表逐一验证，以此确保所设想程序可能出现的问题不存在或已被修复；
3. 场景测试。基于经验罗列用户可能出现的使用场景，而后针对场景逐一验证，以此确保用户在绝大多数情况下使用不会出现问题。

4.3.4 基于安全的测试宜

安全规划需要从需求阶段开始介入后再进行安全设计、实现和测试。对于新能源汽车车载控制器软件安全性测试的要求，宜在安全性测试的同时需要兼顾对性能的考察，按照软件关键等级可要的分为两类，分别是车载控制类控制器、车载辅助类控制器。车载控制器安全性测试，按照测试阶段可划分为：单元测试（软件测试）、部件测试（软硬件集成测试）、系统测试；按照测试类型可划分为：功能安全测试、网络安全测试；按照安全层级可划分为：控制类网络安全和辅助类网络安全。

为满足机密性、完整性、可用性、可控性的要求，按车载控制器类型、测试类型和阶段规划的安全测试推荐方案如表14。

表14安全测试推荐方案

|  |  |  |  |
| --- | --- | --- | --- |
| 车载控制器类型 | 测试阶段 | 测试类型 | |
| 功能安全测试 | 网络安全测试 |
| 车载控制类控制器 | 单元测试 | √ | √ |
| 部件测试 | √ | √ |
| 系统测试 | √ | √ |
| 车载辅助类控制器 | 单元测试 | √ | √ |
| 部件测试 | √ | √ |
| 系统测试 | √ | √ |

4.3.4.1对功能安全测试的宜

安全性测试需求来自对控制器的失效模式分析和对车辆影响的DFMEA。本标准参考

ISO 26262《道路车辆功能安全》于软件功能安全测试提出要求，保证测试人员能够正确识别安全性要求。

本标准汽车功能安全分为主动安全（涉及ABS(防抱死制动系统)、ESC（电子稳定性控制系统）、AEBS（紧急制动系统）、EBS（电子制动系统）、胎压监测(TPMS)、驾驶辅助系统（ADAS）、自动泊车辅助(APA)、自动驾驶(SPA)、远程车辆报警(RVA)、远程车辆诊断(RVD)、远程车辆控制(RVC)等）和被动安全（涉及安全气囊二次保护、碰撞预警、座舱挤压防护、疲劳提醒等）。推荐识别汽车失效的方法，以及罗列目前汽车失效场景，依据失效场景衍生的安全性测试内容，分解为不同测试阶段达到功能安全测试要求。应用图3所示的方法识别汽车的失效。汽车常见的失效场景见表15。

图3识别汽车失效方法图

安全目标

安全状态

安全性测试

容错/报警

失效模式

安全需求分解

功能安全需求

表15为汽车常见失效场景

|  |
| --- |
| 场景 |
| 维修时整车高压上电，人员触电 |
| 车辆发生碰撞后，发生高压短路，引发着火 |
| 车辆发生碰撞后，安全气囊未及时弹出，引发人员伤亡 |
| 车辆制动助力丧失\减小引发交通事故 |
| 车辆坡道驻车后，重新起动，引发驾驶员或行人事故 |
| 车联网数据泄露，引发驾驶员或乘客遭遇犯罪事件 |

以常见失效场景为例，衍生安全性测试内容，示例如表16：

表16根据失效场景确认安全测试要求

|  |  |
| --- | --- |
| 场景 | 安全测试内容 |
| 失效模式 | 维修时整车高压上电，人员触电 |
| 安全目标 | 避免维修时高压上电，人员触电 |
| 安全状态描述 | 断开高压，提醒相关人员 |
| 功能安全需求 | 整车处于维修模式时无法上高压或整车处于上高压状态时不进行维修操作 |
| 安全需求分解 | 整车控制器收到维修模式指令后，禁止闭合继电器；  整车控制器检测到继电器端电压超过阈值时，禁止发送允许维修信号； |
| 容错/报警 | 发生闭合继电器的潜在故障时发送报警信息； |
| 安全性测试 | 整车控制器是否可正常接收维修模式指令；  整车接收到维修模式指令后，容错时间内是否可发送出禁止闭合继电器指令；  继电器在接收到整车发送的维修模式指令后，容错时间内是否进行闭合操作；  整车接收到维修模式指令后，发生闭合继电器的潜在故障时是否在容错时间内发送报警信息；  ……. |

本标准将控制器类型分为车载控制类和车载辅助类，并针对这两大类控制器的分级测试进行功能安全测试的要求，具体要求见表17。

表17功能安全测试要求

|  |  |  |
| --- | --- | --- |
| 车载控制器类型 | 测试阶段 | 功能安全测试要求 |
| 车载控制类控制器 | 单元测试 | 静态分析  动态分析 |
| 部件测试 | 结合等价类划分及边界法，根据表15分析失效场景，按表16制定安全测试内容，并执行测试 |
| 系统测试 | 结合等价类划分及边界法，根据表15分析失效场景，按表16制定安全测试内容，并执行测试 |
| 车载辅助类控制器 | 单元测试 | 静态分析  动态分析 |
| 部件测试 | 结合等价类划分及边界法，根据表15分析失效场景，按表16制定安全测试内容，并执行测试 |
| 系统测试 | 结合等价类划分及边界法，根据表15分析失效场景，按表16制定安全测试内容，并执行测试 |

另外，一定负荷的压力测试也可以暴露车载控制器潜在功能安全风险，压力测试主要是指重复执行某动作来实现对车载控制器的测试。通过模拟控制器长时间的工作状态来检查控制器的潜在安全风险。按照一般车辆使用寿命、使用环境及使用频率，可计算和规划出负荷压力测试所要执行的次数。

…………………………………（2）

式中:

H为年均使用日估算

T为日均使用次估算

t为矫正因子，一般可取为。

其中H和T按照公式(2)和(3)计算：

…………………………………（3）

式中：

Y为车辆平均使用年限，通常；

N为常量，

a为年使用矫正因子，一般取，

…………………………………（4）

式中：

X为车载控制器日均工作频次，可根据具体控件使用频次确定，通常按车辆日均使用3小时估算。

b为环境因子，一般取, 其中TH为车辆使用高温温度值，TL为车辆使用低温温度值，通常, 。

压力测试一般在系统测试后进行。

4.3.4.2对网络安全测试的宜

考虑到互联网/车联网的安全风险对现代汽车的要求越来越高，本标准也将对这部分内容进行要求。车载控制器网络安全隐患主要有：欺骗、篡改、抵赖、信息泄露、拒绝服务及权限提升等。推荐的测试方法有：确定信任边界、识别数据流、识别入口点、识别出口点，按下表18逐层分解，实施网络安全测试。

表18车载控制器测试分层分解解析表

|  |  |  |  |
| --- | --- | --- | --- |
| 安全测试要求 | 单元测试 | 部件测试 | 系统测试 |
| 代码审计 | √ |  |  |
| 软件反编译 | √ |  |  |
| 软件剥壳 | √ |  |  |
| 渗透测试 |  | √ | √ |
| 输入输出验证 |  | √ |  |
| 身份验证 |  | √ |  |
| 授权管理 |  | √ |  |
| 加密、解密 |  | √ |  |
| 安全配置 |  |  | √ |
| 敏感数据处理 |  | √ | √ |
| 日志审计 |  |  | √ |
| 会话管理 |  |  | √ |
| 异常管理 |  |  | √ |
| 漏洞扫描 |  |  | √ |
| 空口抓包分析 |  |  | √ |

4.3.4.3车载控制器的安全漏洞划分

智能网联管道相关控制器作为智能网联组件，为满足智能网联产品特征而衍生的软件安全性测试需求，直接涉及用户数据安全、用户隐私、用户财物安全等，间接涉及自动驾驶异常导致的人身安全。

针对识别的安全漏洞，按引起后果的严重性确定漏洞等级。漏洞等级依不同程度分为3段，分别是低危、中危、高危，下表19为漏洞等级的说明。

表19漏洞等级说明

|  |  |
| --- | --- |
| 漏洞等级 | 说明 |
| 高危 | 资产重大损失，业务中断，较大的财务损失等严重影响 |
| 中危 | 资产系统损失，业务受到损害，中等的财务损失等影响 |
| 低危 | 业务系统较小损失，并且立即可以受到控制，较小或忽略不计的财务损失等影响 |

针对车载控制器的安全漏洞问题及数量，划分安全等级如表20。

表20安全系统等级及内容描述

|  |  |
| --- | --- |
| 安全等级 | 内容描述 |
| 不安全系统（符合任何一个条件） | 1. 存在1个及以上高危或3个以上中危问题。 2. 直接获取核心系统权限的漏洞，包括但不限于任意代码执行，远程命令执行，缓冲区溢出，存储漏洞，敏感信息泄露，后台账号密码泄露（包括弱口令），重要系统源代码泄露，SQL注入获取系统权限漏洞等。 3. 核心系统业务逻辑的漏洞，包括但不限于交易支付逻辑漏洞，获取任务账号管理权限漏洞，越权增删或查改其他用户资源信息，未授权访问重要系统后台，重要系统任意文件读取和下载漏洞核心接口逻辑检验漏洞等。 4. 核心业务数据泄露的漏洞，包括但不限于核心DB的SQL注入漏洞，可获取大量用户身份信息，订单信息，资金交易信息的接口权限校验漏洞等。 |
| 一般安全系统（符合任何一个条件） | 1. 存在1个中危或3个低危以上的问题。 2. 普通的信息泄露，包括但不限于客户端明文密码储存等。 3. 需要用户交互方可影响的漏洞，包括但不限于反射性XSS，非敏感操作的CSRF等。 |
| 安全系统（符合任何一个条件） | 1. 最多存在3个低危的问题。 2. 不涉及安全问题的功能缺陷。 3. 无法复现，或者不能反映出漏洞影响的问题。 |

根据系统安全测试结果，修复安全问题或漏洞，并进行回归测试，确保安全问题或漏洞得到修复，且并未引入新的安全问题，以此达到安全系统等级。

4.3.5 测试执行

4.3.5.1 测试记录

1. 测试结果数据：即测试用例执行后的结果，除了实际测试结果外，还应包含测试时间信息、测试执行人员信息；
2. 测试日志：详细记录测试过程的文档，包括待办事项及其完成情况、当天完成的测试范围、发现的测试问题、上报问题的时间、开发人员接收问题的时间、解决问题的时间（若未解决应转接至第二天的待办事项）、异常事件记录等；

其中异常事件包括：测试时间计划变更、测试用例变更、测试范围变更、测试输入变更、开发/测试约定内容未达成、不可抗拒力（设备无征兆损坏、停电、上级领导介入导致等）。

若在测试开始前测试计划已具备任务模板，则可不填写测试日志。但若测试时间超过8个工作日时，无论有无模板均需填写测试日志。

测试日志在无需外界介入推进测试进度时，可不发送，但需要在结束后应与其他测试输出物一起归档。

1. 测试问题记录需包含以下内容：

测试问题报告标识符：为该测试问题报告规定唯一的标识符。

摘要：概述问题，标识涉及发现问题的测试项，并指出其严重级别。

问题描述：包含测试项的编号、问题编号、输入描述及相关操作、预期结果、实际结果、测试问题分析、修改意见、日期和时间、问题状态、解决方案等。

附录B为一种推荐的问题记录模板。

4.3.5.2 测试全过程数据信息监测

在测试的过程中应加入对部分数据的全程监测测试。比如未定义的数据被发送，未定义的数据字段被赋值，数据发送周期异常等信息。

若需要进行处理的数据量存在处理压力，宜采用先记录后分析的方式开展；在PC上用于进行数据分析的程序与测试执行用的软件应为并行运行的关系。

4.4 测试结束阶段要求

4.4.1 测试报告

4.4.1.1 测试报告概述

测试报告是由测试工作组提交的最终测试结果报告，主要内容包括对测试对象功能及其它质量特性的综合评价、详细测试结果描述以及测试环境描述等。

4.4.1.2 测试报告要求

测试报告应包含但不限于以下内容和要求：

1. 测试报告标识符：为该测试报告规定唯一的标识符，至少应包含测试开始日期、被测项目标识；
2. 测试输入信息：须包含被测对象版本信息（若有硬件也应注明硬件信息）、被测对象所依附的输入物版本信息；
3. 测试结论：应明确标明测试后该软件的质量状态与测试目的差异；
4. 测试内容：应建立功能描述文档与测试用例的对应追溯，或者其他用以表明测试范围、测试深度的内容；
5. 测试环境：
6. 应包含测试环境拓扑图；
7. 应包含测试环境软硬件配置信息，包括测试设备名称、型号等标识信息。

4.4.2 测试总结

4.4.2.1 测试总结概述

测试总结指定测试活动的结果并根据这些结果进行评价。

4.4.2.2 测试总结要求

测试总结应包含但不限于以下内容和要求：

1. 测试总结报告标识符：为该测试总结报告规定唯一的标识符；
2. 摘要：
3. 总结对测试项的评价，标识已完成测试项，标注版本/修订级别及执行测试活动所处的环境；
4. 对于每个测试项，如果存在测试计划、测试日志、测试报告、问题报告，则可作为相关信息的引用文档。
5. 差异：报告测试项与设计说明之间的全部差异，与测试计划的全部差异，并详细说明每种差异产生的原因；
6. 测试充分性评价：应根据测试计划中规定的测试充分性准则对测试过程做出评价，确定未作充分测试的特征或特征组合，并说明理由；
7. 结果汇总：汇总测试的结果，标识已解决的所有时间，并总结其解决方案，标识尚未解决的所有问题；
8. 评价：对每个测试项（包括其限制）进行总体评价，该评价应以测试结果和测试项级别的通过准则作为依据，可以包含对失败风险的估计；
9. 活动总结：总结主要的测试活动，总结资源消耗数据，例如：人员的总体配置水平、每个主要测试活动所花费的时间；
10. 批准：记录测试过程中涉及的所有人员的姓名和职务，并为审批人员签名和日期留出位置。

5. 测试问题管理

5.1问题状态

发现问题的人员需要将问题录入问题库。问题登记后，提交前可以编辑，补充问题记录的信息。

一个问题从提出到关闭，测试人员和开发人员需要跟踪问题的状态。

问题的状态一般分为Open（打开的）、Fixed（已修复的）、Rejected（被驳回的）、Verified（验证通过的）、Closed（关闭的）、Reopen（再次打开）、Deferred（延期处理）：

1. Open（打开的）：当某个问题被发现的时候，测试人员需要与项目负责人沟通以确认发现问题的有效性确认问题后进行记录，并将问题的状态设为“Open”。开发人员开始处理问题的时，状态设置保持为“Open”，这表示开发人员正在处理这个问题；
2. Fixed（已修复的）：当开发人员进行处理并认为已经解决问题之后，将问题的状态设置为“Fixed”并将其提交给开发组的负责人，由开发组的负责人将问题反馈给测试组；
3. Verified（验证通过的）：测试人员得到已修复的问题和新的软件版本，经过相同的步骤测试后如判定问题已经修复，将问题改为验证通过；
4. Rejected（被拒绝的）：开发人员接收问题后进行确认，如果确认符合功能描述或者经过与开发人员的讨论之后认可问题无效，开发组负责人可将问题的状态设置为“Rejected”；
5. Closed（已关闭的）：测试人员经过再次测试确认问题已经被解决，或者问题已经被判定为被拒绝状态，经与开发人员达成一致意见后测试组的负责人将问题的状态设置为“Closed”；
6. Reopen（再次打开）：如果经过再次测试发现问题仍然存在，测试人员将问题再次传递给开发组，并将问题的状态设置为“Reopen”；
7. Deferred（延期处理）：开发人员和测试人员评审问题后确定不在本轮测试计划内进行修改的问题，需要将其设置为“Deferred”。

5.2问题确认

当一个问题被提出之后，测试人员需要将其提交给开发人员。开发人员需确认问题有效性并对已确认的问题进行修改。

当开发人员发现符合符合正常功能描述，或者经过与开发人员的讨论之后认定问题无效，开发组负责人将问题的状态设置为“Rejected”。如果开发人员确认问题，需要对问题进行分析和修改。

5.2.1测试问题分配规则

问题由测试人员传递至开发人员后，需要定位该问题的责任人。一般有两种分配方式。

a) 测试人员分配问题；

测试人员已知该问题的责任人员，可直接将问题的负责人指定为具体负责相关软件模块的工程师，由该工程师修改问题；

1. 开发人员分配问题；

测试人员不知悉责任人员。测试人员需要把问题负责人指定为开发组的负责人。由开发组负责人把问题传递给具体的工程师负责修改。

5.3测试问题修改

测试问题传递至开发人员后，开发人员需要对问题进行修改并定义问题的解决方法。开发人员需要定义问题产生的原因，判定修改涉及的文件、源代码、配置、脚本等。

定位问题后，开发人员需要针对问题修改造成问题的代码、配置或脚本等。开发人员修改完成后将生产新的软件版本，并把问题状态改为“Fixed”并传递回测试人员。

5.4测试问题关闭验证

测试问题经开发人员修改后提交至测试人员，测试人员需要按照一定的规则对修改过的问题进行验证和关闭处理。

5.4.1问题关闭规则

1. 测试人员对“Fixed”已修复状态的问题进行回归测试，测试步骤应当按照记录的步骤进行重现，确认问题已解决后，关闭问题；
2. 对于状态为“Rejected”即开发人员驳回的问题。若测试人员对开发人员的回复不存在异议，可以直接将问题状态改为“Closed”关闭；若测试人员对开发人员的回复存在异议，则需进行测试问题评审，评审可以闭关的问题，也可以评审问题关闭状态信息，具体要求如下：
3. 测试人员确认问题已经解决后，关闭问题；
4. 回归测试验证不通过的问题，应驳回给开发人员，问题状态为“Reopen”即重新打开；
5. 对于被开发人员拒绝的问题，需要进行测试问题评审，评审为问题则需要修改问题状态为“Reopen”重新打开，评审为非问题则可以修改问题状态为“Closed”关闭。

5.5测试问题评审

开发人员拒绝修改的问题，需要根据一定的要求进行评审，评审过程在满足公开、有效的基础上开展并形成对于测试问题的定性及对应的处理决议。

5.5.1问题评审人员要求

针对“Rejected”状态且测试人员和开发人员存在异议的问题，可以对测试问题提出评审，评审人员通常为测试负责人、开发负责人、项目经理以及熟悉产品和行业，能够评价项目进展问题并提出解决办法的专家担任。

5.5.2问题评审流程要求

测试问题的评审应满足以下要求：

1. 评审由测试人员发起，与项目经理协商后，确定评审时间和评审人员；
2. 确定评审时间后，提前将需评审的问题进行整理并发送给相关评审人员；
3. 评审会议上对问题清单进行一一评审，并在创建测试问题评审表；
4. 测试人员参照测试问题评审表对问题状态进行修改。

5.5.3问题评审结论要求

测试问题的评审结论应满足以下要求：

1. 评审人员需要对“Rejected”状态的问题进行判断。若确定为非问题需将问题状态改为“Closed”，并标注说明确认为非问题的原因。若确认为问题，将问题状态改为“Reopen”并指派给相应的开发人员或者将问题状态更改为“Deferred”；
2. 评审人员判定为“Deferred”的问题，需标注说明延期处理原因；
3. 评审人员在问题“Deferred”即延期修改后，需要约定时间将问题重新打开，并将问题状态更改为“Reopen”，并指派给相应的开发人员进行修改。

**5.6测试问题跟踪**

测试问题处理过程中未能及时关闭的问题需要进行跟踪管控，按照评审决议及时进行相应的处理，避免因为该类问题处理不当对软件功能造成不良影响。

5.6.1问题延期处理办法

对于轻微级别的问题，如果开发人员设置为“Deferred”状态，测试人员在验证时，需要将问题状态修改为不做处理，可关闭相关问题。

在测试过程中，由于技术或者时间因素导致的需要延期处理的问题，作为本次任务的遗留问题（原则上只包括严重和中等级别的问题）。

5.7测试问题总结

测试过程中发现的所有问题都应进行总结和管理，并在此基础上形成规范流程改善方案，杜绝同类问题的出现并提高测试的有效性。

5.8问题分析

测试问题的分析可考虑以下几个维度的内容：

1. 问题分布分析；

可以表格的形式列出问题所在软件模块的分布情况，然后根据二八原则判断分析系统的主要问题集中区域，并给出文字说明。

1. 问题产生的原因；

分析问题产生的原因，为进一步改进软件开发过程提供依据。

1. 功能问题严重级别分布；

可根据问题的严重级别以堆积图的形式表示出各模块的问题分布情况，并加以具体文字描述。

1. 测试效率。

在不同阶段对不同模块、人员设计的用例进行分析，统计发现问题所需的最少用例长度。

6. 测试人员能力要求

6.1汽车业软件测试知识基础框架体系概述

汽车软件知识框架体系的建立需上层领导支持，同时还需要大量具有汽车背景知识和软件背景知识的人员。本标准对汽车控制器功能测试基础人员提出了如下图4所示的进阶式要求：



图4汽车业软件测试知识框架体系

6.2体系所依据的标准和规范

本部分所述体系（见上图4）建立在被实践证明有效的过程和标准之上，主要基于软件测试标准ISO/IEC/IEEE 29119以及ISTQB/CSTQB国家软件测试工程师资质认证等标准。并参考了针对汽车行业的标准和规范，例如ISO 26262（道路车辆-功能安全）、Automotive SPICE（汽车软件过程改进与能力测定）、AUTOSAR（AUTomotive Open System Architecture）以及MISRA 2012（Motor Industry Software Reliability Association 汽车产业软件可靠性协会规范）等。

6.3体系的基础

除标准和规范外，需要在整个体系内使用统一的术语表、正确定义概念、统一正确的理念（质量、测试等），保证培训的一致性。本部分所用术语可参照本文第3章术语和定义。

6.4体系的内容

根据汽车软件测试知识框架体系的要求，测试体系分为X1-测试助理，X2-基础级测试以及X3-汽车软件测试基础，本标准对不同的体系等级分别提出了具体的要求。

6.4.1测试助理职责

X1-测试助理级别主要包含作为测试助理员所应具备的基础，例如，IT基本概念和基础知识（软件、硬件、操作系统、通讯网络），同时还要需具备较好的实践动手能力，可搭建和配置测试工程的测试接口、部署测试工具、操作测试工具。此外，基本的软硬件工具应用功能也需有所掌握，例如，利用给定的硬件和软件以及工具，能够按照要求搭建测试环境、部署测试工具和工具驱动器、连接设备网络、安装测试软件等。又例如，能进行有效配置管理（包括版本管理、协同管理等），以及对开发过程有所了解。

6.4.2基础级测试

X2-基础级测试属于进入测试的入门级模块，此模块系统涵盖了软件测试的基本概念、理论和方法，包括测试管理和工具支持等知识。主要内容如下：

1. 测试基础：测试的定义及测试的目的；
2. 测试的基本原则和过程，测试的心理学；
3. 软件全生命周期的测试：针对不同的软件开发模型，测试的不同级别和测试的不同类型；
4. 静态测试技术：静态技术，评审过程；
5. 测试设计技术：测试设计技术的类型，基于规格说明或黑盒测试技术，基于结构或白盒的技术，以及基于经验的测试；
6. 测试管理：测试组织结构，测试计划和估算，测试过程的监督和控制，配置管理，风险管理基础，事件管理基础；
7. 测试工具的支持：测试工具的类型，如何有效选择和使用工具。

**注1：**本部分的具体内容可参看ISTQB/CSTQB基础级大纲。

6.4.3汽车软件测试基础

X3-汽车软件测试基础是从一般的软件测试基础（X2 基础级测试）过渡到专门的汽车软件测试基础。主要内容如下：

1. 绪论：汽车系统开发面临的挑战，汽车产品开发过程，标准的影响，测试工程师在发布过程中的贡献和参与；
2. 电子/电气测试标准：Automotive SPICE的要点，ISO26262 要点，AUTOSAR 要点，电子/电气标准之间的比较，电子/电气测试级别的比较；
3. 在虚拟环境中的测试：汽车测试环境，闭环系统与开环系统，模型在环系统（MiL），软件在环系统（SiL），硬件在环系统（HiL）；
4. 汽车专业测试（静态）：MISRA 2012指南，需求质量的评审；
5. 汽车专业测试（动态）：条件测试，背靠背测试，失效植入测试，基于需求的测试，选择适当的测试技术。

X3模块是以X2为基础的，宜在学习和掌握了X2模块后再学习X3模块。

**注1：**本部分的具体内容可参看ISTQB/CSTQB作为基础级附加模块“汽车软件测试工程师”大纲。

7. 供应商控制器管控要求

7.1控制器供应商测试实施方法

7.1.1委托第三方测试机构进行测试

供应商不具有完整的组织项目并实施软件系统验收测试的能力，需要委托具有一定行业影响力的第三方软件评测机构进行测试，出具测试报告。

7.1.2委托第三方测试机构审查

供应商具有完整的组织项目并实施软件系统验收测试的能力，自身进行软件测试，出具测试报告，但为确保测试的真实性和覆盖度，需要委托具有一定行业影响力的第三方软件评测机构进行测试报告审核，并针对某一具体功能项进行抽查测试，出具测试有效性评估报告。

7.2第三方测试机构资质要求

7.2.1第三方测试机构企业定位

第三方测试机构为中国汽车行业具有广泛影响力的综合性技术服务机构，具有“独立、公正、第三方”的企业定位。

7.2.2人员团队要求

1. 具有针对测试需求的专业的软件功能测试团队，团队人数不少于5人；
2. 测试人员应该独立设置的岗位，有明确的岗位定义和职责范围；
3. 应有涵盖岗位工作的考核体系，并有方法衡量人员能力是否达标；
4. 测试人员应有一定的职业发展路线规划；
5. 测试人员能力需符合本标准第7章规定的相关要求；
6. 测试团队应不少于10款新能源车型控制器测试经验。

7.2.3测试环境要求

1. 测试环境符合本标准4.2.7规定的相关要求；
2. 具有独立的软件功能测试实验室，实验室面积不小于40平米；
3. 实验室配置专业的功能测试设备，能够覆盖新能源汽车车载控制器测试需求；
4. 具有标准化测试环境搭建流程，并有与之对应的测试环境搭建说明手册；
5. 针对每一类可测试控制器应有明确的测试环境搭建所需数据参数的需求清单；
6. 具备测试管理平台，能够实现测试资源管理，测试资源状态应对供应商可视，更新周期小于7天。

7.2.4测试设计与执行能力要求

1. 在测试开始之前应将测试需求条目化，同时识别各自的风险等级；
2. 针对每一类控制器设计完善的入口准则，规范化定义测试所需的设计输入信息，包括输入信息的类型、内容、版本及其输入模板等；
3. 具有专业的测试用例设计方法进行测试用例开发，测试用例设计方法参考本标准4.3.2、4.3.3、4.3.4的相关要求；
4. 对需求文档的覆盖应有用例设计规格说明书，该说明书中规定了针对不同情况的测试覆盖方法；
5. 条目化的需求与测试用例间需形成对应关系，并可随时查阅；
6. 所有用例都应设置风险等级，用例执行顺序应遵从风险等级从高到低；
7. 具有测试评审环节，包括设计输入信息的评审以及测试用例的评审；
8. 应有测试执行过程中的应急预案，预案中应有可行的预备方案；
9. 应有冒烟测试环节；
10. 需有测试日志，在记录预定内容完成情况的同时也应记录其他异常事件；
11. 具有完善的风险管机制，能够应对测试实施过程中的异常事件；
12. 具有完善的测试出口准则，规范化定义所开展的测试任务的结束条件。

7.3控制器供应商第三方委托测试的要求

7.3.1控制器供应商样件管理要求

供应商在软件开发生命周期中，为便于追溯每版软件所经历过的测试情况及其发展情况，应在供应商内部建立一套完善的样件管理体系，版本管理主要包括如下内容：

1. 功能增长计划的管理。编制功能增长表列出详细的功能开发计划，便于第三方测试机构识别各阶段的测试样件所具备的功能，针对已实现的功能展开测试；
2. 软硬件版本的管理。供应商在释放每一版软件，推荐采用如下方式提交版本信息：
3. 在控制器软件内部填写软件、硬件版本信息，测试人员通过诊断或者总线通信获取对应版本信息；
4. 样件交付时附带软硬件变更说明书，详细说明软件、硬件与上一版之间的差异项和变更内容；
5. 软件配置的管理。释放的每一版软件需附带与软件对应的配置信息，对测试样件的功能配置进行详细说明。

7.3.2控制器供应商测试输入物的要求

供应商委托第三方测试需提供完整的测试输入物，输入物主要包括如下内容：

1. 控制器功能描述文档。按照功能进行功能描述文档条目化，对条目化后的功能需与主机厂进行会议确认，评估功能描述文档是否满足设计要求以及测试需求，最终冻结后释放给第三方测试机构；
2. 控制器接口描述文档。主要针对控制器硬线接口定义、接口参数特性进行详细描述；
3. 总线通信矩阵及数据库。主要针对控制器进行总线数据监测及网络仿真；
4. 诊断协议及诊断数据库。主要针对控制器诊断通信进行控制；
5. 控制器标定数据库及标定工具。主要针对控制器进行标定控制；
6. 故障定义及故障识别、处理策略。主要针对控制器的故障逻辑策略进行详细描述；
7. 两套待测控制器。需提供满足测试系统闭环调试的样件；
8. 待测控制器对应接插件。带插针接插件，预留1.5M线束。

7.3.3控制器供应商项目时间要求

1. 供应商项目定点后，进行控制器需求确认，第三方测试机构在供应商开发需求确认后切入项目，进行前期测试环境搭建以及测试用例开发相关工作；
2. 供应商与主机厂确认控制器测试验证时间计划及不同阶段软件开发目标，给第三方测试机构确认下达测试任务；
3. 供应商确保测试持续到车型上市，上市后保存测试环境3个月。

7.3.4控制器供应商项目测试计划要求

1. 供应商项目测试计划主要依据主机厂车型开发计划来制定，测试计划制定需与主机厂和第三方测试机构共同协商，最终确认若干具体阶段安排软件的定版测试；
2. 若在相邻的阶段软件版本没有正式版本更新，或者在上一阶段软件完成冻结，则无需安排测试，但需提供确认书发予主机厂，由主机厂专业部门确认，知会测试部门。

7.3.5控制器供应商测试问题管理要求

供应商测试问题管理符合本标准第5章规定的相关要求。

7.3.6控制器供应商测试整改要求

1. 供应商在每一个阶段测试完成后，针对第三方测试机构的提交的问题清单进行评估，要求三天之内完成问题反馈和确认；
2. 供应商在问题确认后组织内部相关人员进行问题整改方案讨论，要求三天之内完成问题整改方案及整改计划的制定；
3. 供应商在问题整改完成后按计划释放对应的回归测试软件，由第三方测试机构进行回归测试。

7.4委托第三方测试机构测试流程

7.4.1第三方测试机构定点

供应商在确认委托第三方测试机构测试需求后，进行第三方测试机构调研，针对第三方机构行业影响力、规模、人力资源、设备资源、项目经验等各方面进行综合评估，委托定点。

第三方测试机构资质审核按照本标准7.2规定的条件执行。

定点第三方机构需经过主机厂认可，不符合主机厂要求的第三方测试机构不能定点。

7.4.2项目启动

7.4.2.1测试团队组织架构确认。

供应商和第三方测试机构共同确认双方项目成员结构及分工。

7.4.2.2测试计划制定

供应商、第三方机构、主机厂共同协商测试计划，确认测试开展的具体阶段和测试时间，测试计划制定符合本标准7.3.4规定的相关要求。

7.4.2.3测试问题管理方案制定

供应商、第三方机构、主机厂共同协商共同确认测试管理方案，包括测试计划管控、测试问题管控，测试异常事件处理应急备案等，测试管理方案制定符合本标准第5章规定的相关要求。

7.4.2.4项目工作模板制定

包括项目需求文档模板、项目交付文档模板、项目管理文档模板的制定，由供应商、第三方机构、主机厂三方共同协商确认。

7.4.3测试输入物交付及审核

供应商须按照本标准7.3.2的要求进行输入物的搜集和准备，在委托第三方机构测试项目启动后2周内完成释放。

第三方测试机构对输入物进行审核，审核问题以问题清单的形式反馈给供应商，供应商针对问题清单进行确认以及回复，并进行文档更新。

7.4.4测试用例开发

第三方测试机构进行测试用例开发工作，测试用例设计开发方法参考本标准4.3.2、4.3.3、4.3.4的相关要求。

测试用例开发完成后需进行测试用例评审，由供应商、主机厂、第三方测试机构共同参与评审工作，第三方测试机构根据评审会议问题清单进行测试用例更新及完善。

7.4.5测试环境开发

7.4.5.1测试台架搭建

主要进行控制器与测试设备之间映射连接，一方面建立信号列表描述控制器和设备之间的资源分配关系，另一方面根据信号列表实现二者的硬线连接。

7.4.5.2测试环境开发

第三方测试机构提供测试环境模型开发所需数据参数的需求清单，供应商负责搜集释放相关数据参数，第三方测试机构进行测试环境模型开发及参数化，测试环境开发符合本标准5.2.7规定的相关要求。

7.4.5.3系统集成调试

基于测试软件开发测试界面，通过设置典型工况对测试环境进行系统集成调试，利用控制器标定工具实现测试系统参数优化。

7.4.6测试执行

按照测试计划，供应商在规定的测试阶段下达测试任务，提供对应的控制器软件。

第三方测试机构拿到测试样件后，针对控制器的主要功能进行冒烟测试，确认能够满足测试要求后执行完整的功能测试，否则，将样件退回。

测试执行过程符合本标准4.3.5规定的相关要求。

7.4.7测试报告交付

每一阶段测试完成后，第三方测试机构需提交报告给供应商及主机厂，测试报告符合本标准4.4.1 规定的相关要求。

测试报告释放后，供应商组织电话会议与主机厂、第三方测试机构针对测试问题进行评审确认，确认是问题的，反馈整改方案及整改计划。

7.4.8回归测试

供应商针对测试问题需按照整改计划进行软件修复，软件修复后下达回归测试任务，释放对应的整改软件以及软件修复说明文件。

第三方测试机构评估回归测试需覆盖的测试内容，进行回归测试，提交回归测试报告，测试报告符合本标准4.4.1 规定的相关要求。

7.4.9测试结束

符合下述要求的可以结束测试：

1. 预定的测试内容全部测试完成，并且软件完整解决所有测试问题；
2. 预定的测试内容全部测试完成，软件问题未完全解决，但供应商与主机厂协商做了偏差认可；
3. 被测对象功能发生重大变更，导致本次测试继续下去的意义丧失时，可以终止测试；
4. 因第三方测试机构的其他原因导致测试无法开展，如设备损坏短期无法修复。

测试结束阶段符合本标准4.4规定的相关要求。

7.5委托第三方测试机构审查流程

7.5.1第三方测试机构定点

第三方测试机构定点按照本标准7.4.1的要求进行。

7.5.2第三方测试机构审查计划制定

供应商在项目定点后，选定第三方测试机构，与主机厂三方一同进行协商，共同制定控制器测试计划。

第三方测试机构根据实际工作内容及工作量进行评估，确定测试审查计划。

7.5.3测试输入物交付

供应商须按照本标准7.3.2的要求进行输入物的搜集和准备，在委托第三方机构审查项目启动后2周内完成释放。

7.5.4第三方测试机构审查测试用例

供应商完成测试用例开发后，将测试用例释放给第三方测试机构，第三方测试机构针对测试用例进行评审，评估测试用例覆盖度及完整性，评估结果以测试用例评审报告的形式交付给主机厂和供应商。

7.5.4.1测试用例评审内容包括:

1. 功能需求覆盖完整性；
2. 测试用例设计方法合理性；
3. 用例结构设计的规范性。

7.5.4.2测试用例评审报告内容包括:

1. 测试用例有效性等级评估；
2. 测试用例改进宜。

7.5.5第三方测试机构测试环境开发

按照7.4.5要求开发控制器测试环境，测试环境满足抽查测试需求。

7.5.6第三方测试机构抽查测试

控制器供应商应按照测试计划提交测试报告，第三方测试机构与主机厂协商选定报告中的某一功能点进行抽查测试，验证测试报告的真实性。

抽查测试结束后，第三方测试机构根据测试结果提交抽查测试结论。若抽查结果不满足要求，主机厂有权拒绝接收该批次样件，并对供应商做相应的处罚。

7.5.7第三方测试机构审查结项

预定的审查内容全部完成，供应商交付的软件符合审查要求。

当供应商出现重大质量问题，严重偏离审查要求，主机厂终止合作。

8. 自动化测试框架推荐

8.1自动化测试框架概述

推荐在开发模式未迭代开发，或在未来有较多维护性测试的情况下开展测试自动化工作，测试自动化本身包含大量的工作内容，若所形成的用例、脚本、程序复用度较低时，不推荐开展测试自动化工作。

测试自动化若使用商业工具，可遵循商业工具的说明书开展工作，工具本身的好坏可能会影响自动化程度、效率、重用性，并非所有的自动化商业工具均需达成效果一致。

若使用自建测试框架的方式开展自动化，可参考以下推荐的一个自动化测试框架，该自动化测试框架目前实现了某主机厂电机控制器、电池控制器和整车控制器功能测试的完全自动化执行。

8.2任务准备

本标准将自动化测试框架涉及的具体信号操作、文件读取、信息读取、过程检查的函数均列入到该类目下。

8.2.1配置文件

设置控制器的测试类型。不同的控制器因其功能算法差异在其达到其预设功能初始化条件的方式是也存在差异，需准备测试整体执行过程中或者测试结束后测试环境复位时需要操作的信号路径，便于后续8.3.3.3环境初始化调用。

同时若控制器功能测试涉及其他无法在环境模型中搭建的信号接口，也可在此处给出接口变量列表，便于在测试开始前进行检查。



图5自动测试系统框架

8.2.2检查函数

在自动化测试开始前，为保证测试开始之后所有测试用例正常运行，需要对所使用的测试接口进行检查，可单独编写检查函数来完成此工作。

8.2.3路径函数

为尽可能的迅速，减少程序执行的延时，需要在测试开始前将所使用到的信号路径尽解析为当前测试设备或测试工具最快的访问格式，若只涉及一种测试设备或测试工具，无需编写路径函数进行路径转换。

8.2.4写入函数

该函数可根据所选择的测试设备种类、工具种类、测试接口种类的不同自动选择执行相应的写入方式。

8.2.5读取函数

该函数可根据所选择的测试设备种类、工具种类、测试接口种类的不同自动选择执行相应的读取方式。

8.2.6测试接口种类

新能源汽车车载控制器测试接口的种类不同，所需配置文件存在差异。本标准罗列了8种可能的测试接口

1. 诊断；

即汽车控制器的诊断功能接口，如UDS诊断

1. 标定；

如CCP、XCP

1. 故障注入；

对控制器硬线接口对地、对电源、悬空等操作的指令接口，通常由硬件在环测试设备供应商提供故障注入的操作接口和操作方式

1. 程序刷写；

对控制器进行程序的刷写工作，在某些功能测试时需要进行该操作，如OTA。

1. EEPROM操作；

在开展特定功能测试时可能会涉及到清除故障记录、原始计数等操作，有可能需要通过操作EEPROM来完成。

1. 网络通讯；

如CAN、车载以太网

1. 数字/模拟信号；

如DIG、ADC等

1. 模型接口。

环境模型中的可用于测试操作的接口。

8.3任务初始化

8.3.1测试工程加载

加载预先准备完毕的测试工程(如有则包含必要的测试环境模型)。

8.3.2用例列表生成

将需要运行的测试用例按照预设规则进行存放，并通过程序获取该用例集的完整列表。

8.3.3任务参数导入

导入与本次测试任务相关的配置内容

8.3.4测试前置检查

对本次测试所需要使用到的变量、文件进行检查，防止在测试过程中出现异常导致测试失效。

8.4任务执行

8.4.1用例初始化

测试用例的初始化主要涉及到测试用例信息的提取分组，访问路径的生成等活动。

8.4.1.1用例信息提取分组

提取用例中涉及到测试表达的所有信息，并存放在已定义的结构体中，尽可能的将执行用例所需要的数据放置于可快速读取的位置。

8.4.1.2信号最快访问路径生成

根据所使用的测试设备品牌、类型，将路径转换为可快速访问的格式。

8.4.2用例执行

测试用例的执行环节可参考下表示例：

表20测试用例序列举例

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 发送的信号名称 | | 测量的信号名称 | | |
| 时间序列（s） | TX1 | TX2 | RX1 | RX2 | RX3 |
| 0 | 发送方法 | 发送方法 | 测量方法 | 测量方法 | 测量方法 |
| 时间操作 | 发送方法 | 发送方法 | 测量方法 | 测量方法 | 测量方法 |
| 时间操作 | 发送方法 | 发送方法 | 测量方法 | 测量方法 | 测量方法 |

每行代表一个测试步骤。测试步骤数量没有限制，测量方法以及发送方法处可缺省，缺省时不作任何处理。

上表中TX1、TX2表示待发送数值的信号名称，可用实际名称替代，RX1、RX2、RX3表示待测量的信号名称，可用实际名称替代。

测试用例执行时先判断在当前测试步骤中，被采用的时间操作类型，0点被视为测试初始化状态。本标准罗列8种时间操作：

1. 绝对时间：绝对时间指时间轴上的某一个指定时间点，该点在时间轴上的具体位置与前一个时间0点相关，如绝对时间数值为18，则表示该点距离设定的时间0点的距离为18s；
2. 限定触发：指限定在某段时间内一定会有测量方法约定的某一个或多个测量信号数据，当在限定时间内获取到该数据则跳转到下一个测试序列，若超出限定时间均未获取到该数据则会判定该行测试不通过，同时跳转到下一个测试序列，跳转发生时将跳转的时间作为新的时间0点。比如限定触发时间为9，TX1的发送方法为定值2，RX1在该行的测试方法为定值1，那么则表示发送1次TX1=2，之后在9s内会收到RX1==1的情况，但不确定是9s内接收的具体时间，也可能未接收，这时判定为不通过；
3. 持续等待：指在限定的时间内一直都存在测量方法约定的某一个或多个信号的测量数据，若有不等同于约定的测量数据则判定为测试不通过，但会持续运行到约定时间结束才跳转到下一个测试序列。比如持续等待时间为9，TX1的发送方法为定值2，RX1在该行的测试方法为定值1，则表示发送1次TX1=2，之后在9s内会持续收到RX1==1的情况，若9s内有1次RX1~=1的情况，则判定为不通过；
4. 持续发送持续等待：指在限定的时间内不断的执行发送方法，并且一直都存在测量方法约定的某一个或多个信号的测量数据，若有不等同于约定的测量数据则判定为测试不通过，但会持续运行到约定时间结束才跳转到下一个测试序列。比如，时间为9，TX1的发送方法为随机值2~3之间，RX1在该行的测试方法为大于1，则表示在9s期间不断的使TX1信号在2~3之间取值，同时在9s内RX>1，若存在RX1<=1的情况则判定为不通过；
5. 随机绝对时间：等同于绝对时间，只是时间取值为指定的范围内的随机值，这种方法适用于同一用例反复运行的情况，通过多次运行可获得不同的测试效果；
6. 随机限定触发：等同于限定触发，只是时间取值为指定的范围内的随机值，这种方法适用于同一用例反复运行的情况，通过多次运行可获得不同的测试效果；
7. 随机持续等待：等同于持续等待，只是时间取值为指定的范围内的随机值，这种方法适用于同一用例反复运行的情况，通过多次运行可获得不同的测试效果；
8. 随机持续发送持续等待：等同于持续发送持续等待，只是时间取值为指定的范围内的随机值，这种方法适用于同一用例反复运行的情况，通过多次运行可获得不同的测试效果。

所有时间方法在具体使用时可用自定义的字母或其他符号来表示，并作为计算机识别的标识符。执行时在时间操作的框架下，先运行写入函数，再运行读取函数。

写入和读取时涉及到的操作有：

发送方法基于本人先前的模型自动生成发明专利，每个待发送的信号均有两种取值，仿真值和手动值，仿真值是指环境模型闭环运算出来的数值，而使用手动值时则会屏蔽仿真值发送指定的任意数值。

发送方法有：

1. 常数手动值：发送一个定值；
2. 两数值间的随机值：在两个数值之间发送一个随机值；
3. 数组间的随机值：在某一个数组内选取一个元素作为数值发送；
4. 给定概率的随机值：在两个数值之间取随机值，并在这两个数间再划定一个范围，并给这个范围内的数一个概率，这样在这两个数值间取值时，划定范围内的数被取值可能会满足设定的概率；
5. 按默认梯度变化：发送值按默认的梯度变化到给定值；
6. 在给定时间内梯度变化：发送值在给定的时间内变化到给定值；
7. 按给定的步长梯度变化：发送值按照给定的某一定时间指定变化数值量变化，直到给定值；
8. 恢复仿真值：将手动值赋值复位，并重新使用仿真值发送。

所有发送方法在具体使用时可用自定义的字母或其他符号来表示，并作为计算机识别的标识符。

测量方法：

测量方法的表达分为测量数据取值、测量判断逻辑关系，由选定的测量数据取值与测量判断逻辑关系来构成测量方法。

测量数据取值：

1. 存储：当选定为该类取值时，不做测量且不需再选定测量判断逻辑关系，但会将该点数据保存以备之后判断使用，可存储任意多个点；
2. 读取：读取之前存储的数据，可读取存储的任意位置；
3. 常数值：发送一个定值；
4. 两数值间的随机值：在两个数值之间选取一个随机值发送；
5. 数组间的随机值：在某一个数组内取一个元素作为数值发送；
6. 给定概率的随机值：在两个数值之间取随机值，并在这两个数间再划定一个范围，并给这个范围内的数一个概率，这样在这两个数值间取值时，划定范围内的数被取值可能会满足设定的概率。

测量判断逻辑关系：

大于、小于、全等于、不等于、大于等于、小于等于

所有测量方法在具体使用时可用自定义的字母或其他符号来表示，并作为计算机识别的标识符。

8.4.3用例结束

8.4.3.1测试数据生成

将测试所得到得原始数据记录并导出文件。

8.4.3.2报告信息生成

提取原始数据记录中生成测试报告所需要的信息，并存放于指定位置，等待其他测试用例运行完成。

8.4.3.3环境初始化

检查当前的被测控制器情况是否可用于后续测试，如SOC状态是否过低，测试环境上是否仍有车速等状态检查。如有与期望不符的情况，则应采取相应措施进行恢复。

8.5任务结束

8.5.1测试报告生成

根据既定的模板根式生成报告

8.5.2测试结束

生成所有的文件图标以及存储、上传其余测试信息。

附 录 A

（资料性附录）

测试周期构成方式

A.1产业化项目测试

A.1.1判定方法：满足以下任一的条件，按照产业化项目测试执行

a)：已有签批版本的平台化功能定义（在其他项目测试过）在全新项目中应用；

b)：参数变更的功能模块数>=5个(推荐值)。

A.1.2测试周期计算方法：

测试周期 = 冒烟测试0.5天 + 全功能完整测试1天 + 再测试2天 + 回归测试2天

其中的再测试第1天完成50%的问题关闭，第2天完成剩余问题关闭。

A.2功能变更测试

A2.1判定方法：满足以下条件，按照功能变更测试执行

在签批版平台化功能定义基础上，有新增加或逻辑变更的某个功能的子功能项。

A.2.2测试周期计算方法：

测试周期 = 环境搭建（可能存在）0.5天 + 冒烟测试0.5天 + 功能变更测试（根据变更范围大小） + 全功能完整测试1天 + 再测试1天 + 回归测试1天

A.3新功能测试

A.3.1判定方法：满足以下条件，按照新功能测试执行

在已测试过的项目基础上增加一个全新功能模块。

A.3.2测试周期计算方法：

测试周期 = 环境搭建（可能存在）0.5天 + 冒烟测试0.5天 + 新功能测试(根据功能大小) + 再测试1~2天（根据功能复杂程度） + 回归测试1天

A.4 参数变更测试

A.4.1判定方法：满足以下条件，按照参数变更测试执行

被测对象描述文件不变，只有配置参数变更，并且参数变更功能定义模块数< 5个（推荐值）。

A.4.2测试周期计算方法：

测试时间 = 冒烟测试0.5天 + 修改项测试0.5天 + 再测试1天 + 回归测试1天

**附 录 B**

（资料性附录）

问题记录模板

测试问题报告标识符：为该测试问题报告规定唯一的标识符。

摘要：概述问题，标识所涉及的有问题的测试项，指出其严重级别。

问题描述：给出测试项的编号、问题编号、输入描述及相关操作、预期结果、实际结果、测试问题分析、修改意见、日期和时间、问题状态、解决方案等。

以下为必选记录信息：

1. 测试问题的编号，标识问题唯一性的标识
2. 测试用例标号，发现该问题的用例，如果多个用例均发现该测试问题，选择最具代表性的用例。
3. 问题发现时间，问题发现的日期或更详细的时间
4. 软件版本信息
5. 故障描述，包含测试步骤、预期结果、实测结果
6. 问题原因
7. 解决方案
8. 提报人、责任人、排除人、关闭人

以下记录信息经过实践被证明对问题解决有帮助：

1. 问题严重等级，该问题发生后可能带来的后果分级
2. 发生频次，描述该问题在用车过程中可能被触发的频次
3. 拟排除日期，在问题被确认之初责任人承诺排除日期
4. 实际关闭日期，问题最终被关闭的日期

以下为经实践被证明对优化开发过程有帮助：

1. 发现阶段，该问题在首轮验证、再测试、回归测试中的具体发现阶段
2. 故障引入阶段，该问题在整个开发过程中何时被引入
3. 故障类型，故障本身所带的特征属性，可以按功能分类、所属业务科室分类、原因分类，针对不同的分类将用以进行不同的优化
4. 重复出现次数，该问题重复发生的次数