推荐性国家标准
《汽车信息安全通用技术要求》
(征求意见稿)
编制说明

标准起草项目组

2020年5月

汽车信息安全通用技术要求(征求意见稿)

编制说明

一、工作简况

(一) 任务来源

本项目是根据国家标准委[2019]11号文《关于下达2019年第一批推荐性国家标准计划的通知》(计划项目编号20191065-T-339,标准项目名称《汽车信息安全通用技术要求》)进行制定。

(二) 工作过程

任务下达后,汽标委智能网联汽车分标委组织成立标准起草项目组并面向工作组成员单位公开征集成员,经综合考虑,确定吉利汽车研究总院和华为技术有限公司为牵头单位,在此基础上明确了任务和分工,积极开展标准的前期预研等工作。

2018年3月~5月:初步研究确定标准的基本框架。

2018年6月~10月:明确标准的定位和撰写思路,梳理标准框架内容。

2018年11月~12月:讨论确定标准范围和技术要求的编写原则。

2019年1月~6月:明确按照安全维度分项列出技术要求,并完成标准初稿。

2019年7月~10月:在初稿的基础上,按章节分小组讨论,根据组内意见迭代多个草案版本。

2019年10月~12月:标准内容在项目组内达成一致,并面向工作组征求意见。

2020年1月~5月:根据工作组成员的意见,更新标准草案,并形成征求意见稿,向社会征求意见。

1. 汽车信息安全通用技术要求项目组第一次会议

2018年5月,在广州召开项目组第一次会议,会议主要成果如下:

- 1) 按照需要抵抗信息安全威胁强度和威胁造成的影响来定义信息安全的等级标准,汽车信息安全划分为L1-L4四个等级;
- 2) 从物理安全、系统软件安全、应用软件安全、网络与通信安全和数据与隐私安全等五个层次分别提安全要求;
- 3) 明确不同安全等级的区别,例如对应的安全资源需求及防御效果提升程度;

4) 完成汽车信息安全通用要求标准框架。

2. 汽车信息安全通用技术要求项目组第二次会议

2018年10月，在天津召开项目组第二次会议，会议主要成果如下：

- 1) 本标准规范的定位是解决产品的信息安全可评估性问题，目标是定义用于产品安全评估/认证的通用信息安全要求；
- 2) 本标准规范将以信息安全抽象框架为逻辑主线开展写作，分别从技术防护、安全管理和安全评估三个维度定义产品的信息安全要求；
- 3) 各参与单位根据分工情况，开展标准写作，起草单位将根据计划组织会前的邮件和电话会议讨论，提高面对面会议的效率，所有会议讨论将以提案的形式进行讨论。

3. 汽车信息安全通用技术要求项目组第三次会议

2018年12月，在北京召开项目组第三次会议，会议进行了汽车信息安全防护等级划分方法论专题研讨，华为、吉利、大陆电子和戴姆勒四家单位做了专题的研究报告，目标是使技术防护等级要求的划分更加严谨和客观，使未来的产品安全评估更加可度量性。会议主要成果如下：

- 1) 基于本标准的定位、时间上和等级划分本身的工作难度上的考虑，起草组决定放弃技术防护等级划分方法论的研究和制定，本标准的技术防护要求均不做等级区分，本标准以最高的防护目标定义共性的原则性的技术要求，暂时先不涉及产品开发流程的要求和交付件要求；
- 2) 重新明确标准范围：以概念性的网联汽车模式为对象，识别其面临的信息安全威胁，定义通用的汽车信息安全模型，根据识别的安全威胁和信息安全防护的原则性要求作为需求驱动，来定义通用安全技术要求；
- 3) 重新定义文档的写作逻辑框架和各单位分工。

4. 汽车信息安全通用技术要求项目组第四次会议

2019年6月，在无锡召开项目组第四次会议，会议中牵头单位输出了通用技术要求的初版草案，初步定义了标准的框架结构和通用技术要求的参考框架和对安全对象。各成员单位对草案达成初步共识，为后续的工作奠定基础。会议主要成果如下：

- 1) 明确标准突出“面向产品可评估性的纲领性技术要求”，淡化指导性质和推导过程，需符合国家主管部门的最新要求。会议决定对重构标准框架，标准正文包括安全分析框架、安全设计原则要求、各个安全对象的安全保护需求等，其他内容包括威胁、

技术措施建议等均作为资料性附录；

- 2) 有关戴姆勒提出的采用 WP29 文档主体内容作为通用技术要求的建议，希望戴姆勒按照 UNECE/WP29/GRVA 的思路采用从上到下的形式整理文档，作为另一种可能的架构及文稿选择；
- 3) 安全对象分层分类按照吉利的提案分车外系统，通信通道和车内系统；
- 4) 针对安全对象重新编写安全技术要求，分析安全对象应具备的安全属性，并根据安全属性进行分类阐述；
- 5) 本标准正文的各要求不涉及安全管理，只定义技术要求，需要在标准范围中给予明确说明；
- 6) 安全威胁举例只关注安全威胁，不涉及安全风险描述，建议以车辆视角进行威胁描述；
- 7) 本标准只涉及车与其外部生态系统通信的接口，车外 APP，后端服务器等相关安全内容不做要求；
- 8) 关于增加测试章节内容，会议结论是不建议在本标准中增加，希望成立一个新的项目来承担整车的安全测试。理由：
 - a) 本标准不是面向整车的技术要求，而是通用的技术要求；
 - b) 通用性要求是比较高层级的要求，测试验证是可执行的要求，中间存在很大的鸿沟。

5. 汽车信息安全通用技术要求项目组第五次会议

2019 年 7 月，在西安召开项目组第五次会议，会议首先在初稿草案的基础上，各成员单位统一确定了编写通用技术要求的思路。明确了通用技术要求主要的范围为提炼出网联汽车的共性的信息安全技术要求，安全威胁分析不在标准的范围之内，标准注重于共性的技术要求，而不是开发的流程和过程的要求。会议主要结论如下：

- 1) 会议决定以现有 V0.2 版本草案为基础，在标准附录中应该包括威胁和措施内容，正文中包含标准框架图。本标准包含以下内容：范围、规范性引用文件、术语和定义、标准框架图、通用模型、原则要求、技术要求和附录，其中附录中包括威胁和措施。
- 2) 牵头单位将在 7 月 25 日前，根据这次会议的修改意见，完成刷新标准草案，命名为 V0.4 版本，作为下次（电话）会议的提案基准版本。

- 3) 为了提供效率，会议决定将分成三个专题修订小组并行对 V0.4 版本进行修订，各专题小组负责统一本领域的意见，各小组牵头可以以电话会议、邮件讨论和面对面讨论方式组织组内成员进行修订，并输出最终更新结果。
- 4) “算法公认原则”和“安全协议公认原则”不易执行，由大陆电子王奕负责更新，需要解决实际应用情况和当前安全监管的原则性要求的平衡问题。
- 5) 戴姆勒草案中的面向车产品的具体要求，可以采纳到通用技术要求中。具采纳条款需由 C 组讨论。
- 6) 4.1 节的安全框架章节，第一段有关安全框架想解决什么问题，不应该出现标准正文，可改成陈述句后放入引言或者编制说明。
- 7) 中国软件测评中心提案细节部分由于时间关系没有进行讨论，后续再 V0.4 版本上再进行修订。

其中分组情况如下：

- a) A 组：负责属于术语部分的修订，由 360 来组织大家修订，尽量引用已有 GB 的定义，当前标准没有定义的，以本标准的实际情况来定义。
- b) B 组：安全框架部分和车生态系统的简化图，其中安全框架部分由 360 来组织，八个维度和安全对象的分类要保留，不需要箭头（根据 ICT 安全标准定义经验，框架性的国际上基本不用箭头）。车生态简化图有尹杨负责牵头刷新，刷新重点是突出以车为中心，车外通信还是保留远距离和近距离通信的分类，使之和技术要求部分一致。
- c) C 组：负责具体技术要求部分修订，由 PSA 牵头各车企，还是按照八个维度进行展开，不涉及的技术维度无需列出。

6. 汽车信息安全通用技术要求项目组第六次系列会议

根据项目组各成员单位的提案，各小组分别组织会议讨论标准的相应章节，A 组完成了术语和定义的具体内容讨论和更新。B 组完成了标准整体框架的讨论和更新，包括标准章节架构，信息安全参考框架和汽车参考模型。C 组完成了标准中关于技术要求的讨论和更新。包括原则性要求，系统性防御策略要求和保护维度技术要求。同时协同处理各小组相关联的问题。

7. 汽车信息安全通用技术要求项目组第七次会议

2019 年 11 月，在杭州召开项目组第七次会议，会议中项目组各单位最后处理相应的提

案准备标准面向工作组内开始公开征集提案。会议主要成果如下：

- 1) 更新范围的表述，使其更加简洁明了，需要更新 3.1.1 汽车信息安全的定义；
- 2) 3.2 缩略语更新，删除 Wifi 和 APP 定义，并更新 NFC 定义；
- 3) 更新 4.1 安全参考框架的概念的表述，更改 4.1 安全对象分类，先 a. b. c 在 1. 2. 3；
- 4) 4.3.3 更新纵深防御表述，删除最后一句话关于纵深防御的分类；
- 5) 删除原附录 A.1 关于密码的推荐，同时附录需要在正文中提及，后续确认链接到正文中。

（三）主要参加单位和工作组成员及其所做的工作等

本标准由十余家单位共同起草。在本标准的制定过程中，多次组织行业专家进行了研讨，得到了相关单位的支持、协助与配合，取得了大量建设性意见、建议。

二、国家标准编制原则和确定国家标准主要内容

（一）标准编制原则

本标准编制遵循如下原则：

- 1) 本标准编写符合 GB/T1.1《标准化工作导则》的规定；
- 2) 在项目组内对标准内容广泛征求意见，并在会上和电话中充分讨论；
- 3) 起草过程充分考虑国内外现有相关标准的统一和协调；
- 4) 标准的要求充分考虑了国内当前的行业信息安全技术水平。

（二）标准主要内容

本标准规定了汽车信息安全通用技术要求，包括原则性要求、系统性防御策略要求和保护维度技术要求。本标准主要条款说明如下：

1) 引言

在引言中说明了编写本标准的原因以及汽车信息安全与其他行业信息安全的差别，提出了信息安全的参考框架。

信息安全参考框架不是技术要求，而是本标准的编写思路，介绍了技术要求和每个对象的保护维度的相互关系，有助于对标准内容的理解。

2) 1 范围

本标准规定了汽车信息安全的保护对象和技术要求，适用于 M 类、N 类汽车整车及其电子电气零部件。

本标准落脚于汽车信息安全的通用技术要求，注重提出通用的、共性的汽车信息安全技

术要求。所以本标准不包括信息安全工程的流程要求和威胁分析等内容。

3) 5 安全保护对象

本标准的标准化对象是汽车信息安全，汽车是一个复杂的系统，各子系统的信息安全要求存在差异，为了更加合理的提出技术要求，对保护对象进行了分类，主要依据如下：

- a) 采用有整体到局部的分类方法，最后对细分子对象提出技术要求，这样既列出通用的技术要求，同时由覆盖了汽车包含的对象。
- b) 将汽车作为对象分为车内系统、车外系统和车外通信三类子保护对象。车内系统又可分为软件系统、电子电气硬件、车内数据和车内通信。这样既能对车内零部件所包含的共性内容（软件、硬件、数据）提要求，同时能对将车内零部件连接起来的车内通信提要求。针对分类后的子保护对象，因其通用的属性可以合理列出相关的通用技术要求。
- c) 车外通信考虑到攻击通信因距离的难易不同，以通信距离作为分类依据。车外远距离通信主要包括蜂窝通信和卫星通信，车外近距离通信主要包括 OBU、WIFI、NFC、蓝牙等，分别提出相应技术要求。

4) 条款 6.1 原则性要求和 6.2 系统性防御策略要求

在信息安全的实践的过程，行业归纳出一些通用的原则性要求和防御策略，用于指导产品设计以及实现，确保产品的信息安全。本标准基于汽车的特性归纳总结了六个原则性要求和三个防御策略要求，作为基础性和指导性的技术要求，确保汽车信息安全设计和实现时的合理性。

5) 条款 6.3 保护维度技术要求

传统信息安全行业一般考虑 CIA 三个安全维度，但是考虑到 CIA 不能完整规范汽车信息安全要求，考虑到汽车信息安全的特殊性，最后归纳为八个信息安全保护维度。

针对各保护对象的自身情况提出对应的技术要求，如果与某个维度不相关，就直接省略这个维度的技术要求。

6) 条款 6.3.1.1.4 可用性要求

定义功能安全等级高的软件应支持防 DoS/DDoS 攻击，目前标准对防 DoS/DDoS 的具体量化的能力以及应该达到什么程度没有具体的要求，只是要求支持防 DoS/DDoS 攻击。

7) 条款 6.3.1.1.5 访问可控性要求

软件系统本身应具有权限控制的管理机制，在各个应用场景，应验证其权限。

8) 条款 6.3.1.3 数据安全保护

本标准考虑的数据安全主要为安全重要参数，同时有列出安全重要参数的保护要求。个人信息由于已有相关的法律法规要求，在本标准中没有涉及。各功能业务产生的数据也没有包含在标准中，主要基于以下考虑：

- a) 各功能业务产生的数据各不相同，并不具有通用和共用性。
- b) 各功能业务产生的数据跟功能业务的威胁分析有关，而标准的安全对象的通用性，从而导致无法定义相应的各个维度的安全技术要求。

9) 条款 6.3.1.3.1 保密性要求

安全重要参数传输时，不应以明文形式存在。在存储时，有的安全重要参数可用明文存在安全的环境中，所以对于安全重要参数的存储只要求存在安全的环境中，没有要求不能以明文的形式存在。

10) 条款 6.3.1.3.2 完整性要求

本条款的对象为安全重要参数，安全重要参数的完整性具有重要，所以技术要求为安全重要参数应支持完整性校验。

11) 条款 6.3.1.3.3 可用性要求

安全重要参数应防止丢失、防误删除等以确保其可用性，可以采用备份或者专用空间存储。

12) 条款 6.3.1.4 车内通信的保护要求

本条款以及对车外通信的技术要求，都是基于通信功能在汽车上的应用，是从通信功能为切入点提出的相关的要求，具体要求的实现需要通信 ECU 进行相应配合。

13) 章节 6.3.2.1.4 车外远距离通信的可用性要求

可用性要求中关于车外远距离通信应支持抗无线干扰，没有具体规定抗无线干扰具体需要的量化的要求以及应该达到的程度，只是要求应支持抗无线干扰。

14) 章节 附录

本标准为促进主机厂对各对象的信息安全威胁的理解和认识，决定把各个安全对象的威胁举例放在附录，以供参考。

三、主要试验（或验证情况）分析

本标准是技术要求标准，不涉及试验内容。

四、标准涉及的专利情况

本标准不涉及专利问题。

五、预期达到的社会效益等情况

随着目前汽车智能化网联化的快速发展,同时汽车电子电气系统越来越复杂以及电子电气零部件的增多,导致汽车信息安全的薄弱点和可能面临的威胁急剧增加。

《汽车信息安全通用技术要求》作为汽车信息安全的第一批通用的技术要求标准,为所有的汽车整车及其零部件都提供通用的信息安全技术要求,为其信息安全的开发,提供了通用的技术指导和要求,特别对于没有专门标准进行信息安全规范的产品均可以参考此标准。

《汽车信息安全通用技术要求》标准可以为所有零部件及整车的信息安全设计提供指导,筑牢汽车信息安全基线,推动整个汽车产业健康发展;为汽车信息安全产业的监管提供基础的技术依据,支撑政府主管部门进行行业管理;作为汽车信息安全领域的基础性标准,可以支持其他的信息安全标准的制定。

六、采用国际标准和国外先进标准的情况

本标准没有采用国际标准。

本标准制定过程中未查到同类国际、国外标准。

本标准水平为国内先进水平。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准与我国现行有关法律、法规和强制性国家标准不矛盾。

八、重大分歧意见的处理过程和依据

无。

九、标准性质的建议说明

鉴于本标准在《国家车联网产业标准体系建设指南(智能网联汽车)》中的项目定位与规划。根据标准化法和有关规定,建议本标准的性质为推荐性国家标准。

十、贯彻标准的要求和措施建议

1. 首先应在实施前保证本标准文本的充足供应,使每个制造厂、设计单位以及检测机构等都能及时获得本标准文本,这是保证新标准贯彻实施的基础。

2. 本次制定的《汽车信息安全标准通用技术要求》不仅与生产企业有关,而且与设计单位、检测机构等相关。对于标准使用过程中容易出现的疑问,专业标委会有义务进行必要的解释。

3. 可以针对标准使用者，如制造厂、质量监管等相关部门，有侧重点地进行标准的培训和宣贯，以保证标准的贯彻实施。

十一、废止现行相关标准的建议

无。

十二、其他应与说明的事项

无。