国家技术标准创新基地（汽车）
标准化技术文件

BASIC/TD 01—2025

汽车整车信息安全技术要求
应用指南

Technical requirements for vehicle cybersecurity

Guidelines

发布稿

本稿完成日期：2025 年 4 月

2025 - 04 - 30 发布

国家技术标准创新基地（汽车）　发　布

目　次

引　言

随着汽车智能化、网联化的不断发展与应用，车辆的信息安全问题日益严峻，一旦遭受网络攻击则可能导致用户个人信息泄露及远程入侵控车等严重后果，影响车辆用户的信息、财产、生命等多方面安全，甚至危害社会与国家安全。制定并实施强制性国家标准《汽车整车信息安全技术要求》为行业监管提供了明确的技术依据，划定了整车信息安全防护基线，保障了智能网联汽车产业健康可持续发展。

强制性国家标准《汽车整车信息安全技术要求》立足我国行业管理需求、产业发展实际和技术进步需要，并与国际法规充分协调，为智能网联汽车整体产业链“提质增效”提供支撑，于2024年8月23日由国家市场监督管理总局、国家标准化管理委员会批准发布。适用于M类、N类及至少装有1个电子控制单元的O类车辆，对于新申请型式批准的车型，自2026年1月1日起开始执行；对于已获得型式批准的车型，自2028年1月1日起开始执行。

基于标准要求编制本应用指南技术文件，旨在支撑GB 44495—2024《汽车整车信息安全技术要求》落地实施，提升汽车信息安全管理体系检查和车型检测试验的操作一致性程度，提供全面、系统的指导，确保标准的应用一致性。本应用指南分为两大部分，正文四个章节分别描述了总体原则、汽车信息安全管理体系、车型要求以及同一型式判定，附录给出总结文档模板，共包含十个附表，并给出详细的填写说明。

本应用指南由国家技术标准创新基地（汽车）组织，在工业和信息化部装备工业发展中心的指导下，由中国汽车技术研究中心有限公司牵头，协同多家整车企业、供应商企业、汽车行业检测机构等行业力量共同研究完成，在这里不一一列举，仅作诚挚的感谢！未来，随着技术的发展和实践经验日益丰富，本应用指南将根据实际需求持续迭代完善，再次衷心感谢参与编写的单位！

GB 44495—2024《汽车整车信息安全技术要求》应用指南

1 总体原则

本文件参照联合国UNECE R155《关于就信息安全与信息安全管理体系方面批准车辆的统一规定》及法规解释文件，旨在为标准的使用者进一步解释强制性国家标准GB 44495—2024《汽车整车信息安全技术要求》第5章、第6章、第7章和第9章的要求，并提供相关要求的要点解释和对应的证明文件。GB 44495—2024界定的术语和定义适用于本文件。

2 汽车信息安全管理体系

2.1 总则

检查人员通过查看车辆制造商信息安全管理体系的制度流程、附件表单以及对应的表单运行记录或证明材料，来判定被检查的信息安全管理体系是否全面、体系运行是否有效。针对检查要点中的每一项，满足对应检查准则的为该项符合，否则为该项不符合，存在一项不符合则整个体系检查不通过。

2.2 证明材料基本要求

2.2.1 在开展信息安全管理体系检查前，车辆制造商需提供汽车信息安全管理体系适用范围，明确体系适用的品牌。

2.2.2 车辆制造商需整理信息安全管理体系检查所需的证明材料清单，清单中至少需明确证明材料的文件名称、版本号和发布日期。证明材料清单需覆盖本次检查的信息安全管理体系所适用范围内的所有品牌、所有流程。

注：若存在多套体系流程独立运行，每套流程均需要准备制度文件和过程记录迎审。

2.2.3 若证明材料初始编制语言为非中文，需提供原文和对应的中文翻译，并申明两者的一致性，检查以中文版本材料为主。

注：制度流程类证明材料需提供完整的中文版本材料备查，表单以及对应的记录文件类材料可根据检查人员现场抽检结果进行现场翻译，现场翻译形式不限。

2.2.4 在开展信息安全管理体系检查过程中，车辆制造商需要提供证明材料清单所覆盖的所有材料。在信息安全管理体系检查结束后，车辆制造商需将检查要求的文档自留备查，备查文件由车辆制造商依照检测机构认可的方案进行防篡改处理（如盖章、签名软件等）。

2.3 汽车信息安全管理体系要点和证明材料

2.3.1

标准正文：5.1 车辆制造商应具备车辆全生命周期的汽车信息安全管理体系。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需覆盖全生命周期，全生命周期包括： --开发阶段 至少包含信息安全相关项定义、风险评估、信息安全需求、信息安全需求实施、信息安全需求验证和信息安全确认等信息安全活动 --生产阶段 至少包含生产控制计划制定、生产环节的控制措施 --后生产阶段 至少包含运维、终止支持和报废等信息安全活动	汽车信息安全管理体系相关的文件清单和体系文件
2	汽车信息安全管理体系文件需正式发布或受控	汽车信息安全管理体系文件正式发布或受控的证明材料

2.3.2

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立企业内部管理汽车信息安全的过程。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需明确汽车信息安全管理体系的组织架构及权责	包含汽车信息安全管理体系组织架构和职责分工的制度文件
		汽车信息安全管理体系组织架构中每个角色职责履行的活动记录
2	汽车信息安全管理体系需明确为保障汽车信息安全要求落地，提供足够的资源支持	包含信息安全资源投入承诺的制度文件
3	汽车信息安全管理体系需明确信息安全文化，并保证被指派信息安全角色和责任的人员具备履行相应足够的能力和意识	包含保障信息安全能力和意识的制度文件
		保障信息安全能力和意识的活动记录
4	汽车信息安全管理体系需明确体系持续改进机制	包含汽车信息安全管理体系持续改进机制的制度文件
5	汽车信息安全管理体系需明确汽车与信息安全相关的信息共享机制	信息安全相关的信息共享管理制度文件
6	汽车信息安全管理体系需明确对产品的信息安全变更管理、	汽车产品信息安全变更管理、需求管理、文档管理和配置管理制度文件或证明企业满足 ISO

	需求管理、文档管理和配置管理流程	9001、GB/T 19001、ISO/TS 16949、GB/T 18305等质量管理体系要求的证书
7	汽车信息安全管理体系需对影响汽车信息安全的工具进行管理 --工具管理对象为影响功能或组件信息安全的工具	汽车信息安全工具管理流程
		汽车信息安全工具管理记录

2.3.3

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到处置的过程，并确保车辆风险评估保持最新状态。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需明确信息安全相关项的相关性判定方法、定义要求	相关项的信息安全相关性判定方法和确定信息安全相关性活动要求的流程
		信息安全相关项的相关性判定、定义的记录
2	汽车信息安全管理体系需明确车辆信息安全风险评估方法论	车辆信息安全风险评估与威胁分析方法、指南或相关标准
		车辆信息安全风险评估与威胁分析记录
3	汽车信息安全管理体系需明确信息安全目标和信息安全声明制定和评审要求	信息安全目标和信息安全声明制定和评审流程
		信息安全目标和信息安全声明制定和评审记录
4	汽车信息安全管理体系需明确信息安全需求制定要求，需考虑 GB 44495—2024 第 7 章的要求	信息安全需求制定和评审流程
		信息安全需求制定和评审流程
5	汽车信息安全管理体系需明确信息安全风险跟踪机制	信息安全风险跟踪流程，确保车辆风险评估保持最新状态

2.3.4

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立用于车辆信息安全测试的过程。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需建立信息安全集成验证活动流程，包括活动的目的、计划、方案、结果等，至少包含测试活动	开展信息安全集成验证活动的流程
		开展信息安全集成验证活动的记录

2	汽车信息安全管理体系需建立信息安全确认活动流程，包括活动的目的、计划、方案、结果等，至少包含测试活动	开展信息安全确认活动的流程
		开展信息安全确认活动的记录
3	汽车信息安全管理体系需明确对信息安全测试过程中发现的问题进行处理的流程	信息安全测试问题处理流程
		信息安全测试问题处理记录

2.3.5

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布、上报等活动环节。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需制定漏洞管理制度，需包含漏洞收集、分析、报告、处置、发布、上报等活动环节 --报告 企业内部报告相关漏洞 --上报 外部上报至相关管理部门 --发布 参考《网络产品安全漏洞管理规定》七（三）条要求。对于需要产品用户（含下游厂商）采取软件、固件升级等措施的，应当及时将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供必要的技术支持	汽车漏洞管理流程
2	汽车信息安全管理体系需明确漏洞的信息收集流程	汽车漏洞信息收集流程
		汽车漏洞信息收集记录
3	汽车信息安全管理体系需明确漏洞的分析流程	汽车漏洞分析流程
		汽车漏洞分析记录
4	汽车信息安全管理体系需明确漏洞的内部报告流程	汽车漏洞内部报告流程
		汽车漏洞内部报告记录
5	汽车信息安全管理体系需明确漏洞的处置流程	汽车漏洞处置流程
		汽车漏洞处置记录

6	汽车信息安全管理体系需明确漏洞的外部上报流程	汽车漏洞外部上报流程
		汽车漏洞外部上报记录
7	汽车信息安全管理体系需明确漏洞的发布流程	汽车漏洞发布流程文件
		汽车漏洞发布记录

注：如车辆制造商在管理体系检查前尚未收集到汽车产品相关漏洞，可提供漏洞管理流程演练活动记录，演练活动无需真实执行漏洞上报和漏洞发布流程。

2.3.6

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：建立针对网络攻击提供相关数据并进行分析的过程，如通过车辆数据和车辆日志分析和检测网络攻击、威胁和漏洞。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需明确按照事件或一定频率对与网络攻击相关的车辆数据进行分析的流程	车辆网络攻击相关数据和车辆日志分析流程
2	汽车信息安全管理体系需明确对网络攻击、网络威胁和漏洞进行信息分析的流程	网络攻击、网络威胁和漏洞的信息分析流程
		网络攻击、网络威胁和漏洞的信息分析记录

2.3.7

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：建立确保对网络攻击、网络威胁和漏洞进行持续监控的过程，且车辆纳入监控范围的时间应不晚于车辆注册登记的时间。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需建立对网络攻击、网络威胁和漏洞进行持续监控的流程，包含信息收集、信息分析和结果处置	网络攻击、网络威胁和漏洞持续监控流程
2	汽车信息安全管理体系需明确车辆纳入监控范围的触发点的要求	包含纳入监控范围的触发点要求的流程

3	汽车信息安全管理体系需建立收集与其车型相关的网络攻击、网络威胁和漏洞相关信息的流程。收集流程需明确信息的监控来源、工具、告警阈值、频次等相关要求。监控日志记录保存不得少于 6 个月（180 个自然日）	与其车型相关的网络攻击、网络威胁和漏洞相关的信息收集流程
		与其车型相关的网络攻击、网络威胁和漏洞相关的信息收集记录

2. 3. 8

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在时限内得到处置的过程。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需建立一套完整的网络攻击、网络威胁和漏洞响应机制。其中网络攻击（事件）响应包含事件信息收集、事件信息分析、事件报告、事件处置流程、事件恢复流程、事后总结和监测。网络威胁响应包含处置机制。漏洞响应参考 2.3.5.	信息安全事件响应流程
		网络威胁处置机制
		网络威胁处置记录
2	汽车信息安全管理体系需建立信息安全事件信息收集流程	信息安全事件信息收集流程
		信息安全事件信息收集记录
3	汽车信息安全管理体系需明确信息安全事件的分级及其分级原则、不同级别事件的响应处置优先级要求和事件处置时限要求	信息安全事件分级流程
		信息安全事件分级判定记录
4	汽车信息安全管理体系需建立信息安全事件的内部报告流程	信息安全事件内部报告流程
		信息安全事件内部报告记录
5	汽车信息安全管理体系需建立信息安全事件的处置流程	信息安全事件处置流程
		信息安全事件处置记录
6	汽车信息安全管理体系需建立信息安全事件的恢复流程	信息安全事件恢复流程
		信息安全事件恢复记录

7	汽车信息安全管理体系需建立信息安全事件事后总结和监测的流程	信息安全事后总结和监测流程
		信息安全事后总结和监测记录（对事件的持续监控记录）

2.3.9

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：建立评估所实施的信息安全措施在发现新的网络攻击、网络威胁和漏洞的情况下是否仍然有效的过程。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需建立对新的网络攻击、网络威胁和漏洞的验证评估流程，评估所实施的信息安全措施有效性	对新的网络攻击、网络威胁和漏洞的评估流程（评估所实施的信息安全措施有效性）
		对新的网络攻击、网络威胁和漏洞的评估记录（评估所实施的信息安全措施有效性）

2.3.10

标准正文：5.2 汽车信息安全管理体系应包括以下内容-建立管理企业与合同供应商、服务提供商、车辆制造商子组织之间汽车信息安全依赖关系的过程。

要点和证明材料：

序号	要点	证明材料
1	汽车信息安全管理体系需建立涉及信息安全要求的供应商管理流程。	供应商（涉及信息安全要求）管理流程
2	汽车信息安全管理体系需对涉及信息安全要求的采购项目进行识别	涉及信息安全要求采购项目的识别要求
		涉及信息安全要求采购项目的识别记录
3	汽车信息安全管理体系需包含对供应商能力进行论证和评估的流程	供应商信息安全能力论证和评估流程
		供应商信息安全能力论证和评估记录，至少覆盖零部件（软硬件）供应商
4	针对与其供应商之间的互动、依赖关系和责任，车辆制造商需制定信息安全需求相关的报价流程	信息安全需求相关的报价请求（RFQ）流程
		信息安全需求相关的报价请求（RFQ）记录
5	为明确与其供应商之间的信息安全责任，汽车信息安全管理体系需建立信息安全接口协议并验证供应商信息安全活动符合性，包括信息安全活动、漏洞处置、安全	信息安全接口协议（CIA）或同等效力材料要求
		信息安全接口协议（CIA）或同等效力材料记录

	需求和冲突解决	

注：合同供应商、服务提供商、车辆制造商子组织的定义可参考ISO 21434等标准，至少需包括零部件软硬件供应商（可以对1级供应商提出要求，并要求其将要求分配给2级供应商）、车端应用服务提供商。

3 汽车信息安全车型要求

3.1 总则

3.1.1 在信息安全基本要求检测过程中，企业需要提供总结文档，并依照总结文档将检测要求的文档自留备查，备查文件由车辆制造商依照检测机构认可的方案进行防篡改处理（如盖章、签名软件等）。

注：总结文档需提供中文版本，备查文件可根据检查人员现场抽检结果进行现场翻译，现场翻译形式不限。

3.1.2 在信息安全基本要求检测过程中，检测人员应依据基本要求检测过程中确认的信息制定信息安全技术要求检测方案，并结合技术要求检测结果综合确认基本要求是否符合标准要求。在信息安全技术要求检测过程中，检测人员依据车辆信息安全基本要求检测时确定的检测方案开展检测。

3.2 汽车信息安全基本要求要点和证明材料

3.2.1

标准正文：6.1 车辆产品开发流程应遵循汽车信息安全管理体系要求。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商的信息安全管理体系需满足第 5 章要求，应有相关报告	证明车辆制造商满足第 5 章要求的检验报告（报告附件含体系文档清单）
2	车辆制造商需遵循第 5 章信息安全管理体系要求开展产品开发	车辆产品开发总结文档（可参考附录的总结文档参考模板，至少应形成文档清单）
		现场留存备查的文档（应和总结文档一致）

3.2.2

标准正文：6.2 车辆制造商应识别和管理车辆与供应商相关的风险。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商需依照企业管理体系要求，明确涉及信息安全活动的供应商，对供应商信息安全资质进行评审	该车型涉及信息安全活动的供应商清单
		该车型供应商信息安全能力评估报告
2	车辆制造商需依照企业管理要求，确保涉及信息安全活动的供应商依照管理制度要求开展信息安全活动，包括信息安全接口协议的签署、信息安全活动符合性评估等	该车型供应商信息安全接口协议、信息安全活动符合性评估记录或同等效力材料

3.2.3

标准正文：6.3 车辆制造商应识别车辆的关键要素，对车辆进行风险评估，并管理已识别的风险。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商需依照企业管理体系要求开展车辆信息安全相关项识别和风险评估， 包括资产识别等过程	该车型信息安全相关项识别清单和过程记录
		该车型风险评估分析报告或记录
2	车辆制造商需评估所识别的风险与第 7 章技术要求的相关性	证明车辆制造商梳理了所识别的风险与第 7 章相关性的文件

3.2.4

标准正文：6.4 车辆制造商应采取基于第7章要求的处置措施保护车辆不受风险评估中已识别的风险影响。若处置措施与所识别的风险不相关，车辆制造商应说明其不相关性。若处置措施不足以应对所识别的风险，车辆制造商应实施其他的措施，并说明其使用措施的合理性。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商需依照企业管理体系要求，制定信息安全声明和安全目标	该车型信息安全声明和信息安全目标清单
2	车辆制造商需依照企业管理体系要求，制定车辆信息安全需求	该车型信息安全需求规范
3	车辆制造商应采取基于第 7 章要求的处置措施保护车辆不受风险评估中已识别的风险影响	证明车辆制造商依照第 7 章的信息安全技术要求处置与之相关的风险的文件
4	若处置措施与所识别的风险不相关，车辆制造商应说明其不相关性	证明车辆制造商未采取的第 7 章要求的处置措施与所识别的风险不相关的证明材料
5	若处置措施不足以应对所识别的风险，车辆制造商应实施其他的措施，并说明其使用措施的合理性	证明车辆制造商对于第 7 章要求的处置措施不足以应对的风险，采取其他措施的证明材料

3.2.5

标准正文：6.5 如有专用环境，车辆制造商应采取措施，以保护车辆用于存储和执行后装软件、服务、应用程序或数据的专用环境。

要点和证明材料：

序号	要点	证明材料
1	如有专用环境，车辆制造商需针对相关风险实施完整的安全措施，并进行相关验证活动	该车型专用网络环境安全措施技术规范
		该车型专用网络环境安全措施验证记录

3.2.6

标准正文：6.6 车辆制造商应通过测试来验证所实施的信息安全措施的有效性。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商需按照管理体系要求，开展集成验证活动，通过测试开展的需保证测试结果的有效性	该车型信息安全集成验证方案
2		该车型信息安全集成验证活动报告
3		该车型信息安全集成验证活动过程的评审记录
4	车辆制造商需按照管理体系要求开展信息安全确认活动，通过测试开展的需保证测试结果的有效性	该车型信息安全确认活动方案
5		该车型信息安全确认活动报告
6		该车型信息安全确认活动过程的评审记录
7	集成验证活动和确认活动的对象应与公告准入车辆相一致	研发阶段测试对象与公告准入车辆相一致的证明材料或变更不影响信息安全的证明材料

3.2.7

标准正文：6.7 车辆制造商应针对车辆实施相应措施，以确保具备以下能力：

——针对车辆网络攻击的识别能力；

——针对与车辆相关的网络攻击、网络威胁和漏洞的监测能力及数据取证能力。

要点和证明材料：

序号	要点	证明材料
1	车辆需具备识别网络攻击的能力	该车型识别网络攻击的技术方案和验证/测试报告
2	车辆制造商需具备车辆相关的网络攻击、网络威胁和漏洞的监测能力及数据取证能力	车辆制造商网络攻击、网络威胁和漏洞的监测能力及数据取证能力的技术方案

3.2.8

标准正文：6.8 车辆制造商应使用公开的、已发布的、有效的密码算法，应根据不同密码算法和业务场景，选择适当的参数和选项。

要点和证明材料：

序号	要点	证明材料
1	如使用密码算法保护车辆，车辆制造商应使用公开的、已发布的密码算法或含以上算法的组合算法	核心业务场景（7.1 外部连接安全要求、7.2 通信安全要求、7.3 软件升级安全要求、7.4 数据安全要求相关的场景等）所使用的所有密码算法清单（如使用密码算法），包括算法类型和来源等证明密码算法属于公开密码算法的证据
2	如使用密码算法保护车辆，车辆制造商应根据不同密码算法和业务场景，选择适当的参数和选项	核心业务场景所使用密码算法的技术文档（如使用密码算法）

3.2.9

标准正文：6.9 车辆制造商应满足以下密码模块要求之一：

——采用符合国际、国家或行业标准要求的密码模块；

——未采用国际、国家或行业标准要求的密码模块，说明使用的合理性。

要点和证明材料：

序号	要点	证明材料
1	如使用密码模块保护车辆，车辆制造商所使用的密码模块，需满足国际、国家或行业标准要求，或提供说明采用非标密码模块的合理性	车型所使用的密码模块情况总结报告（如使用密码模块）
2		如功能组件使用国际、国家或行业标准要求的密码模块，须提供由车辆制造商或供应商或第三方检测机构出具的技术方案评审报告、检测报告或提供由认证机构出具的密码模块安全认证证书。功能组件至少包括中央网关、车载软件升级系统所在的零部件、具备蜂窝移动通信系统功能的零部件、驾驶辅助系统域控制器、自动驾驶域控制器、自动驾驶数据记录系统（DSSAD）、数字钥匙等
3		如核心功能组件使用非标密码模块产品，须提供由车辆制造商或供应商或第三方检测机构出具的检测报告或经过专家论证审查的证明材料

3.2.10

标准正文：6.10 车辆应采用默认安全设置，如WLAN的默认连接口令应满足复杂度的要求。

要点和证明材料：

序号	要点	证明材料

1	车辆制造商需采取措施保证车辆采用默认安全设置	车型相关的默认安全设置方案文件

3.2.11

标准正文：6.11 汽车数据处理活动中的数据车内处理、默认不收集、精度范围适用、脱敏处理、个人同意及显著告知等要求，应符合GB/T 44464—2024中4.2.2的规定。

要点和证明材料：

序号	要点	证明材料
1	车辆制造商应依照 GB/T 44464—2024《汽车数据通用要求》中 4.2.2 的规定处理个人数据	由具备资质的第三方检测机构出具的证明车型满足 GB/T 44464—2024《汽车数据通用要求》中 4.2.2 要求的检测报告，或委托开展 GB 44495—2024 第 6 章基本要求检测的检测机构在基本要求检测期间开展实车检测并出具该条款通过检测的报告

3.3　汽车信息安全技术要求要点和证明材料

3.3.1

标准正文：7.1.1.1 车端具备远程控制功能的系统、授权的第三方应用等外部连接系统不应存在由汽车行业权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞。

要点和要点解释：

序号	要点	要点解释
1	具备远程控制功能的系统	车端具备接收远程控制指令，对远程控制指令进行真实性和完整性校验的系统，通常为车机（IVI）、车载终端（T-BOX）等外部连接系统
2	授权的第三方应用	指通过授权的方式，在车辆生产之后，可以进行安装并为车主用户提供服务，所有预置的应用不算作第三方应用，只有在合法的应用商店下载且经过车辆制造商或指定代理审核机构审核并签名的第三方应用视为授权的第三方应用
3	处置	拥有合理处置时限的处置计划（与体系保持一致）也视为处置
4	汽车行业权威漏洞平台	汽车行业权威漏洞平台包括但不限于工业和信息化部网络安全威胁和漏洞信息共享平台车联网产品安全漏洞专业库 NVDB-CAVD 等政府主管部门认可的漏洞平台
5	6 个月前	从车辆到样（检测机构接收到正式测试车辆和正式检测材料）时开始计算的前 6 个月（180 个自然日）
6	高危及以上的安全漏洞	根据汽车行业权威漏洞平台的评分规则进行定义，漏洞扫描可以基于二进制软件包或者软件/开源软件清单（如 sbom 格式的数据包）进行扫描

3.3.2

标准正文：7.1.1.2 车辆应关闭非业务必要的网络端口。

要点和要点解释：

序号	要点	要点解释
1	网络端口	指的是车载以太网、蜂窝网络、WLAN 等外部通信通道所开放的对外通信协议端口
2	非业务必要的网络端口	不在车辆制造商提前出具的网络端口清单内，各个带有操作系统的零部件由外部可访问且没有明确的业务用途的网络端口

3.3.3

标准正文：7.1.2.1 应对远程控制指令信息进行真实性和完整性验证。

要点和要点解释：

序号	要点	要点解释
1	远程控制指令信息	车主用户通过无线通信通道传输的控制车辆功能和状态的指令信息，不包含蓝牙等近场控车指令信息

3.3.4

标准正文：7.1.2.2 应对远程控制指令设置访问控制，禁用非授权的远程控制指令。

要点和要点解释：

序号	要点	要点解释
1	远程控制指令信息	车主用户通过无线通信通道传输的控制车辆功能和状态的指令信息，不包含蓝牙等近场控车指令信息
2	非授权的远程控制指令	车端可接收，未经云端或车端授权允许执行的控车指令，如具备分享功能的钥匙、付费指令等指令

3.3.5

标准正文：7.1.2.3 应具备记录远程控制指令的安全日志功能，安全日志记录的内容至少包括远程控制指令的时间、发送主体、远程控制对象、操作结果等，留存相关的安全日志应不少于6个月。

要点和要点解释：

序号	要点	要点解释
1	远程控制指令的安全日志	指的是车辆执行远控指令（如开启空调、启动车辆、车门解闭锁等）记录的安全日志
2	留存相关的安全日志	安全日志可以在车端留存，也可以在云端留存
3	不少于 6 个月	以该条安全日志记录时间为起始时间，该条安全日志需至少在车端或云端留存不少于 6 个月（180 个自然日），期间不得以存储空间不足被覆盖或删除

3.3.6

标准正文：7.1.2.4 应对车端具备远程控制功能的系统进行完整性验证。

要点和要点解释：

序号	要点	要点解释
1	完整性验证	通过安全启动等方式保护具备远程功能的系统不被篡改

3.3.7

标准正文：7.1.3.1 应对授权的第三方应用的真实性和完整性进行验证。

要点和要点解释：

序号	要点	要点解释
1	授权的第三方应用	指通过授权的方式，在车辆生产之后，可以进行安装并为车主用户提供服务，所有预置的应用不算作第三方应用，只有在合法的应用商店下载且经过车辆制造商或指定代理审核机构审核并签名的第三方应用视为授权的第三方应用

3.3.8

标准正文：7.1.3.2 应对非授权的第三方应用的安装进行提示，并对已安装的非授权的第三方应用进行访问控制，限制此类应用直接访问系统资源、个人信息等。

要点和要点解释：

序号	要点	要点解释
1	非授权的第三方应用	指通过车辆制造商预留途径，由车主用户自行选择安装并为车主用户提供服务的第三方应用，该应用未经过车辆制造商或指定代理审核机构审核
2	直接访问系统资源、个人信息等	如车主用户授权，则可获取相关权限
3	安装	若系统支持安装，应明确具体安装路径和方式，若系统不支持安装，应提供声明文件
4	提示	提示方式包括在安装时以文字、图片等方式进行提示

3.3.9

标准正文：7.1.4.1 应对车辆外部接口进行访问控制保护，禁止非授权访问。

要点和要点解释：

序号	要点	要点解释
1	外部接口	车辆外部物理接口，包括 CAN 诊断口、以太网诊断接口、具备数据交互功能的 USB 接口/新能源汽

		车整车充电接口、SD 卡卡槽等接口

3.3.10

标准正文：7.1.4.2 应对车辆USB接口、SD卡接口接入设备中的文件进行访问控制，仅允许读写指定格式的文件或安装执行指定签名的应用软件。

要点和要点解释：

序号	要点	要点解释
1	指定格式	由车辆制造商根据实际使用场景定义的格式

3.3.11

标准正文：7.1.4.3 车辆应对USB接口接入设备中的病毒风险进行处置。

要点和要点解释：

序号	要点	要点解释
1	病毒	一种能够自我复制、传播，并对计算机系统造成损害或干扰其正常运行的程序或代码
2	进行处置	处置包括提示、拦截、隔离、删除或对病毒文件不执行

3.3.12

标准正文：7.1.4.4 通过诊断接口向车辆发送关键配置及标定参数的写操作指令时，车辆应采用身份鉴别或访问控制等安全策略。

要点和要点解释：

序号	要点	要点解释
1	关键配置参数	指的是车辆制造商经过风险评估分析得出的会影响行车安全、车主用户财产安全的参数，如制动参数、安全气囊展开阈值、动力电池参数等，通常由车辆制造商自行定义
2	标定参数	标定参数是指用于控制和优化汽车性能的各种设置和配置参数，通常由车辆制造商自行定义

3.3.13

标准正文：7.2.1 车辆与车辆制造商云平台通信时，应对其通信对象的身份真实性进行验证。

要点和要点解释：

序号	要点	要点解释
1	车辆制造商云平台	主要包括远程控车、OTA、远程诊断、远程监控、企业处理或存储个人信息的平台、PKI 等与车辆直接进行交互的云平台，法律、行政法规、强制性国家标准中另有规定的云平台除外

3. 3. 14

标准正文：7.2.2 车辆与车辆、路侧单元、移动终端等进行V2X直连通信时，应进行证书有效性和合法性的验证。

要点和要点解释：

序号	要点	要点解释
1	证书有效性	指车辆在进行 V2X 直连通信时，校验 V2X 证书的时间和范围的有效性，且未被伪造、篡改
2	证书合法性	指车辆在进行 V2X 直连通信时，校验 V2X 证书的签发机构是可信的，且证书未被撤销

3. 3. 15

标准正文：7.2.3 车辆应采用完整性保护机制保护除RFID、NFC之外的外部无线通信通道。

要点和要点解释：

序号	要点	要点解释
1	除 RFID、NFC 之外的外部无线通信通道	指移动蜂窝通信、WLAN、经典蓝牙、低功耗蓝牙、V2X 等非接触式的方式与车辆进行通信的通道
2	完整性保护机制	不限制实现方式，应用层或传输层皆可

3. 3. 16

标准正文：7.2.4 车辆应具备对来自车辆外部通信通道的数据操作指令的访问控制机制。

要点和要点解释：

序号	要点	要点解释
1	车辆外部通信通道	指移动蜂窝通信、WLAN、经典蓝牙、低功耗蓝牙、V2X、NFC、RFID 等非接触式的方式与车辆进行通信的通道，如车辆无法通过该类通道传输数据操作指令，对该类通信通道视为本条款不适用
2	访问控制机制	不限制实现方式，应用层或传输层皆可

3. 3. 17

标准正文：7.2.5 车辆应验证所接收的外部关键指令数据的有效性或唯一性。

要点和要点解释：

序号	要点	要点解释
1	外部关键指令数据	指通过移动蜂窝、WLAN、经典蓝牙、低功耗蓝牙、V2X、RFID、NFC 等非接触式的外部无线通信通道接收的关键指令数据，关键指令数据由车辆制造商基于标准要求和风险评估自行确认
2	有效性或唯一性	车辆需要确认接收到的数据是否符合预期的格式、协议和标准，或这些数据在规定时间范围内是否是唯一的

3. 3. 18

标准正文：7.2.6 车辆应对向车外发送的敏感个人信息实施保密性保护措施。

要点和要点解释：

序号	要点	要点解释
1	敏感个人信息	可参考 GB/T 44464—2024《汽车数据通用要求》中附表 A.2 个人信息分类分级示例表

3. 3. 19

标准正文：7.2.7 车辆应具备安全机制防御物理操纵攻击，至少具备与外部直接无线通信的零部件的身份识别机制。

要点和要点解释：

序号	要点	要点解释
1	与外部直接无线通信的零部件	指通过移动蜂窝通信、WLAN、经典蓝牙、低功耗蓝牙、V2X 等非接触式的方式与外部直接进行通信的零部件，通常为车机（IVI）、车载终端（T-BOX）和 V2X 控制器
2	身份识别机制	若存在异常部件连接告警，则须明示用户

3. 3. 20

标准正文：7.2.8 车辆与外部直接无线通信的零部件应具备安全机制防止非授权的特权访问。

要点和要点解释：

序号	要点	要点解释

1	与外部直接无线通信的零部件	指通过移动蜂窝通信、WLAN、经典蓝牙、低功耗蓝牙、V2X 等非接触式的方式与外部直接进行通信的零部件，通常为车机（IVI）、车载终端（T-BOX）和 V2X 控制器

3. 3. 21

标准正文：7.2.9 车辆应对内部网络进行区域划分并对区域边界进行防护。车辆内部网络跨域请求应进行访问控制，并遵循默认拒绝原则和最小化授权原则。

要点和要点解释：

序号	要点	要点解释
1	内部网络	车辆内部网络包括车载总线、车载以太网等
2	区域划分	从业务角度说明如何进行区域划分

3. 3. 22

标准正文：7.2.10 车辆应具备识别车辆通信通道遭受拒绝服务攻击的能力，并对攻击进行相应的处理。

要点和要点解释：

序号	要点	要点解释
1	对攻击的处理	包括对攻击数据包的拦截或丢弃，受影响系统的自动恢复、日志记录等
2	车辆通信通道	包括移动蜂窝通信、V2X、CAN 总线、车载以太网等

3. 3. 23

标准正文：7.2.11 车辆应具备识别恶意的V2X数据、恶意的诊断数据的能力，并采取保护措施。

要点和要点解释：

序号	要点	要点解释
1	恶意	非预期，不符合业务场景，由车辆制造商自行定义

3. 3. 24

标准正文：7.2.12 应具备记录关键的通信信息安全事件日志的功能，日志存储时长应不少

于6个月。

要点和要点解释：

序号	要点	要点解释
1	通信信息安全事件日志	关键的通信信息安全事件由车辆制造商根据风险评估的结果确定，风险评估需覆盖 GB 44495—2024 第 7 章 7.2.1~7.2.11 的场景
2	不少于 6 个月	以该条安全日志记录时间为起始时间，该条安全日志需至少在车端或云端留存不少于 6 个月（180 个自然日），期间不得以存储空间不足被覆盖或删除

3. 3. 25

标准正文：7.3.1.1 车载软件升级系统应通过安全保护机制，保护车载软件升级系统的可信根、引导加载程序、系统固件不被篡改，或在被篡改后，通过安全保护机制使其无法正常启动。

要点和要点解释：

序号	要点	要点解释
1	安全保护机制	车辆制造商应至少选择以下一种机制进行安全保护： 1. 系统启动时需进行完整性校验，完整性校验不通过则无法正常启动 2. 确保车载软件升级系统具备一系列的安全措施，如加密技术、身份认证、访问控制等，以防止未经授权的篡改

3. 3. 26

标准正文：7.3.1.2 车载软件升级系统不应存在由汽车行业权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞。

要点和要点解释：

序号	要点	要点解释
1	处置	拥有合理处置时限的处置计划（与体系保持一致）也视为处置
2	汽车行业权威漏洞平台	汽车行业权威漏洞平台包括但不限于工业和信息化部网络安全威胁和漏洞信息共享平台车联网产品安全漏洞专业库 NVDB-CAVD 等政府主管部门认可的漏洞平台
3	6 个月前	从车辆到样（检测机构接收到正式测试车辆和正式检测材料）时开始计算的前 6 个月（180 个自然日）
4	高危及以上的安全漏洞	根据汽车行业权威漏洞平台的评分规则进行定义，漏洞扫描可以基于二进制软件包或者软件/开源软件清

		单（如 sbom 格式的数据包）进行扫描

3. 3. 27

标准正文：7.3.2.1 车辆和在线升级服务器应进行身份认证，验证其身份的真实性，并在下载中断恢复时重新验证。

要点和要点解释：

序号	要点	要点解释
1	在线升级服务器	管理和下发无线升级任务的后台系统，不包括升级包下载服务器
2	身份认证	车辆与在线升级服务器通信时应对平台的身份来源进行校验，防止使用伪造的平台与车辆建立通信

3. 3. 28

标准正文：7.3.2.2 车辆应对下载的升级包进行真实性和完整性验证。

要点和要点解释：

序号	要点	要点解释
/	/	/

3. 3. 29

标准正文：7.3.2.3 应对在线升级过程中发生的信息安全事件日志进行记录，日志存储时长应不少于6个月。

要点和要点解释：

序号	要点	要点解释
1	不少于 6 个月	以该条安全日志记录时间为起始时间，该条安全日志需至少在车端或云端留存不少于 6 个月（180 个自然日），期间不得以存储空间不足被覆盖或删除

3. 3. 30

标准正文：7.3.3.1 若车辆使用车载软件升级系统进行离线升级，车辆应对离线升级包真实性和完整性进行验证。

要点和要点解释：

序号	要点	要点解释

/	/	/

3. 3. 31

标准正文：7.3.3.2 若车辆不使用车载软件升级系统进行离线升级，应采取保护措施保证刷写接入端的安全性，或验证升级包的真实性和完整性。

要点和要点解释：

序号	要点	要点解释
1	保护措施	可以通过设备认证或基于服务的认证方式来保护刷写接入端的安全

3. 3. 32

标准正文：7.4.1 车辆应采取安全访问技术或安全存储技术保护存储的对称密钥和非对称密钥中的私钥，防止其被非授权访问和获取。

要点和要点解释：

序号	要点	要点解释
/	/	/

3. 3. 33

标准正文：7.4.2 车辆应采取安全访问技术、加密技术或其他安全技术保护存储在车内的敏感个人信息，防止其被非授权访问和获取。

要点和要点解释：

序号	要点	要点解释
1	敏感个人信息	可参考 GB/T 44464—2024《汽车数据通用要求》中附表 A.2 个人信息分类分级示例表

3. 3. 34

标准正文：7.4.3 车辆应采取安全防御机制保护存储在车内的 VIN 等用于车辆身份识别的数据，防止其被非授权删除和修改。

要点和要点解释：

序号	要点	要点解释
1	用于车辆身份识别的数据	一般是指整车统一的，且是唯一的标识数据，一般是指 VIN 码。不包含各个零部件的 SN 号、发动机号等

3. 3. 35

标准正文：7.4.4 车辆应采取安全防御机制保护存储在车内的关键数据，防止其被非授权删除和修改。

要点和要点解释：

序号	要点	要点解释
1	关键数据	关键数据由车辆制造商根据风险评估结果自行定义

3. 3. 36

标准正文：7.4.5 车辆应采取安全防御机制保护存储在车内的安全日志，防止其被修改和非授权删除。

要点和要点解释：

序号	要点	要点解释
1	存储在车内的安全日志	仅适用于存储在车内的安全日志，如车辆不在本地存储安全日志，则不适用于本条款
2	防止其被修改	本条款旨在要求安全日志无法被任何车内用户（记录日志的用户除外）修改

3. 3. 37

标准正文：7.4.6 车辆应具备个人信息删除功能，该功能可删除的信息不应包括法律、行政法规、强制性国家标准中规定必须保留的个人信息。

要点和要点解释：

序号	要点	要点解释
1	个人信息	可参考 GB/T 44464—2024《汽车数据通用要求》中附表 A.2 个人信息分类分级示例表，且车辆保持正常运行所必须车辆 MAC 地址、设备序列号等信息不在本条款的要求范围内

3. 3. 38

标准正文：7.4.7 车辆不应直接向境外传输数据。

要点和要点解释：

序号	要点	要点解释
1	不应直接向境外传输数据	指车辆网络连接里，不存在直接连接境外 IP 的网络流量

4 汽车信息安全同一型式判定

4.1 总则

车型产品在满足标准9.1 信息安全直接视同判定条件时，可无需重新进行整车测试，但在发生如下变化时，需针对变化项提供补充的风险评估和验证确认证明材料（提供的证明材料参考标准6.3、6.4、6.6的要求）：

1. 车辆整车电子电气架构和信息安全处理措施采取4.2.2中列出的第二种场景进行视同判定；

2. 车辆中央网关的软件版本号变化但不影响信息安全；

3. 车辆车载软件升级系统软件版本号变化但不影响信息安全；

4. 车辆具备蜂窝移动通信系统功能的零部件软件版本号变化但不影响信息安全；

在不满足标准9.1 信息安全直接视同判定条件，但满足标准9.2 信息安全测试验证后视同判定条件时，可仅需对变更参数相关的技术要求进行补充测试。

4.2 信息安全直接视同判定条件要点及解释

4.2.1

标准正文：

如符合下述规定，则视为同一型式：

——汽车信息安全管理体系有效

要点和证明材料：

序号	要点	要点解释
1	有效	车辆制造商汽车信息安全管理体系满足如下两项要求其一时，视为管理体系有效： 1.该车型适用的车辆制造商信息安全管理体系经具备资质的第三方检测机构检验合格，具备由第三方检测机构出具的管理体系检验报告 2.该车型适用的车辆制造商信息安全管理体系可与其它车型的信息安全管理体系视同，并具备由第三方检测机构出具的视同报告

4.2.2

标准正文：

如符合下述规定，则视为同一型式：

——车辆整车电子电气架构相同且信息安全处置措施相同；

要点和证明材料：

序号	要点	要点解释
1	电子电气架构相同且信息安全处置措施相同	车辆满足如下两种场景其一时，视为车辆整车电子电气架构相同且信息安全处置措施相同： 1. 场景一-整车电子电气架构未发生任何变化 2. 场景二-整车电子电气架构发生轻微变化但同时满足如

		下 4 项要求： ① 车辆核心部件（中央网关、车载软件升级系统所在的零部件和具备蜂窝移动通信系统功能的零部件）数量及拓扑位置相同或减少（减少时需不影响车辆信息安全防护处置措施） ② 车内网络总线类型相同或减少 ③ 车内网络总线数量相同或减少（减少时需连同其上搭载的零部件整体减少），替换总线的场景除外 注：替换总线的场景是指相比原车型电子电气架构，新车型电子电气架构在移除某条总线的同时增加一条新的总线来保持总线数量不变，例如车辆制造商减少一条搭载燃油动力系统控制器总线的同时增加了一条搭载新能源动力系统控制器的总线。 ④ 具备诊断、刷写功能的对外接口（如 OBD、直流充电接口等）数量、拓扑位置及通讯协议相同

4.2.3

标准正文：

如符合下述规定，则视为同一型式：

——车辆中央网关的硬件型号和软件版本号（不影响信息安全的除外）相同；

要点和证明材料：

序号	要点	要点解释
1	中央网关的硬件型号相同	需为同一产品相同型号
2	中央网关的软件版本号相同（不影响信息安全除外）	指网关的信息安全需求和开发方案相同，且已通过验证，后续由于其他功能更新引起的软件版本变更，只需通过软件代码的漏洞扫描等方式验证无新增信息安全漏洞即可，此类变更视为不影响网关的信息安全

4.2.4

标准正文：

如符合下述规定，则视为同一型式：

——车辆车载软件升级系统硬件型号和软件版本号（不影响信息安全的除外）相同；

要点和证明材料：

序号	要点	要点解释
1	车载软件升级系统所在 ECU 的硬件型号相同	需为同一产品相同型号

2	车载软件升级系统所在 ECU 软件版本号相同（不影响信息安全除外）	指 ECU 的信息安全需求和开发方案相同，且已通过验证，后续由于其他功能更新引起的软件版本变更，只需通过软件代码的漏洞扫描等方式验证无新增信息安全漏洞即可，此类变更视为不影响车辆车载软件升级系统的信息安全

4.2.5

标准正文：

如符合下述规定，则视为同一型式：

——车辆具备蜂窝移动通信系统功能的零部件硬件型号和软件版本号（不影响信息安全的除外）相同；

要点和证明材料：

序号	要点	要点解释
1	具备蜂窝移动通信系统功能的零部件硬件型号相同	需为同一产品相同型号
2	具备蜂窝移动通信系统功能的零部件软件版本号相同（不影响信息安全除外）	指 ECU 的信息安全需求和开发方案相同，且已通过验证，后续由于其他功能更新引起的软件版本变更，只需通过软件代码的漏洞扫描等方式验证无新增信息安全漏洞即可，此类变更视为不影响具备蜂窝移动通信系统功能的零部件的信息安全

4.2.6

标准正文：

如符合下述规定，则视为同一型式：

——车辆无线通信方式所使用的协议类型、协议版本、接口类型、接口数量相同或减少；

要点和证明材料：

序号	要点	要点解释
1	无线通信方式	包含 WLAN、蓝牙、NFC、蜂窝通信、V2X 等

4.2.7

标准正文：

如符合下述规定，则视为同一型式：

——车辆外部接口的类型、数量相同或减少；

要点和证明材料：

序号	要点	要点解释
/	/	/

4.2.8

标准正文：

如符合下述规定，则视为同一型式：

——与车辆直接连接并产生数据交互的车辆制造商云平台IP地址或域名相同。

要点和证明材料：

序号	要点	要点解释
1	云平台 IP 地址或域名相同	云平台满足如下两种方案其一时，视为云平台 IP 地址或域名相同： 1. 与车辆直接交互并产生数据的云平台数量相同或减少，且交互的平台 IP 或域名未发生变更 2. 企业云平台发生升级、迁移等变更，只要其变更的云平台对应信息安全等级保护定级未发生变更且变更后的平台通过公安部等保认证，则视为未发生变更

附 录 A

（规范性）

总结文档模板

XX企业XX车型总结报告

一、 基本情况概述

企业名称:

车辆型号:

该车型研发遵循的体系：XXXXXXX（体系报告编号，详细的体系文件清单见附表一）

二、 信息安全相关供应商总结

概述依照XXX文件/使用XXX工具开展了XX车型信息安全相关供应商管理，共识别管理信息安全相关供应商XX家。（详细清单见附表二）

三、 车辆风险评估、处置方案总结

车辆产品开发总结文档-风险评估情况总结，包括输出物清单（详细清单见附表三）、网络拓扑结构简介、与7.4要求相关的零部件清单。（详细清单见附表四）

四、 专用环境总结

车辆专用环境概述，说明是否存在专用环境，如存在专用环境需逐项解释所使用的专用环境。（详细清单见附表五）

五、 车辆测试验证总结

车辆验证和确认情况概述，说明验证和确认的周期和时间节点，验证或确认的实施方式（测试/评审等），测试或评审报告清单。(详细清单见附表六)

六、 网络攻击/网络威胁/漏洞监测方案总结

网络攻击/网络威胁/漏洞监测方案总结包括两部分，一是针对此车型采取的网络攻击识别方案，简要说明网络攻击识别技术方案及覆盖的攻击类型；二是在企业层面采取的网络攻击、网络威胁和漏洞监测方案，简要说明使用的方法/

工具。（详细清单见附表七）

七、 密码算法总结

车辆密码算法总结，需对照 GB 44495—2024 第 7 章明确的四类核心业务场景（外部连接、通信安全、软件升级、数据安全），梳理各业务场景相关的密码算法，非核心业务场景相关的密码算法可不列出。(详细清单见附表八)

八、 密码模块总结

车辆密码模块总结，需至少明确车辆核心零部件上所使用的密码模块，包括密码模块类型和证明满足标准要求的方案（评审、检测或认证证书）。(详细清单见附表九)

九、 默认安全设置总结

默认安全设置总结包括是否存在默认安全设置，以及技术方案概述。(详细清单见附表十)

附表一：管理体系文件清单

（请参照管理体系检查时提交的文件清单，梳理该车型对应的管理体系文件清单，并注明版本）

序号	文件名称	文件编号	版本号
1	*汽车信息技术安全-网络安全管理体系（CSMS）政策*	*AAAAA*	*V1.3*

附表二：XXX 车型信息安全相关供应商清单

序号	供应商名称	供应商职责	是/否 开展供应商能力评估	供应商能力评估记录	是/否 签署 CIA 协议	供应商 CIA 协议
1	*ABC*	*负责 T-BOX 研发*	*是*	*XXX 车型供应商 ABC 评估报告*	*是*	*XXX 车型供应商 ABC CIA 协议*

（本清单中仅需列出零部件软硬件相关供应商，企业可对供应商名称等机密信息进行处理，例如使用企业内部供应商代码等非敏感唯一标识信息进行替代）

附表三：风险评估及处置文件清单

序号	文件名称	文件编号	版本号
1	*XXX 风险评估报告*	*AAAAAA*	*V1.3*
2	*XXX 安全需求*	*AAAAAB*	*V1.1*
3	*XXX 安全设计规范*	*AAAAAC*	*V1.3*

附表四：数据安全相关零部件清单

标准章节号	零部件名称
7.4.1	*T-BOX*
	.....
7.4.2	*T-BOX*
	.....
7.4.3	*车机（IVI）*
	.....
7.4.4	*BMS*
	.....
7.4.5	*网关*
	.....

附表五：专用环境清单

序号	专用环境名称	对应技术方案		
		技术文件名称	文件编号	文件版本
1	*沙箱*	*V1.3*	*AAAAA*	*V1.3*
2				
3				

附表六：验证和确认文件清单

序号	文件名称	文件编号	版本号
1	*XXX 验证测试报告*	*AAAAA*	*V1.3*
2	*XXX 确认测试报告*	*AAAAAA*	*V1.2*
3	*XXX 评审报告*	*AAAAAA*	*V1.4*

附表七：网络攻击/网络威胁/漏洞监测文件清单

序号	文件名称	文件名称	文件编号	版本号
1	*车型识别方案*	*XXX 方案*	*AAAAA*	*V1.3*
2		*XXX 方案*	*AAAAAA*	*V1.2*
3	*企业识别方案*	*XXX 方案*	*AAAAAA*	*V1.4*
4		*XXX 平台*	*ABCDE*	*V1.3*

（如通过平台等工具实现网络攻击/网络威胁/漏洞监测，需在文件名称列填写平台等工具的名称，文件编号填写工具编号，版本号填写工具相关版本信息）

附表八：密码算法清单

序号	业务场景	算法名称	算法类型	证明选择适当参数和选项的技术文档		
				文档名称	文档编号	版本号
1	*外部连接*	*RSA 2048*	*公开算法*	*XXX 方案*	*AAAA*	*V1.2*
2		*SM2*	*公开算法*			
3		*HHH*	*基于公开算法 RSA 2048 的私有算法*			
4		*AAA+SM2*	*组合算法*			
5	*通信安全*					
6						
7	*软件升级*					
8						
9	*数据安全*					
10						

（业务场景应至少包含应用指南中所列出的核心业务场景，车辆不具备该业务场景的除外，如不具备软件升级功能）

附表九：密码模块清单

序号	功能组件名称	密码模块		密码模块检测/审查报告		
		模块类型	模块形态	文档名称	文件编号	版本号
1	*T-BOX*	*标准密码算法模块*	*硬件*	*XXX 审核报告*	*AAAAA*	*V1.3*
2	*网关*	*标准密码算法模块*	*软件*	*XXX 检测报告*	*AAAAAA*	*V1.2*
3	*ADAS 域控制器*	*标准密码算法模块*	*硬件*	*XXX 证书*	*AAAAAA*	*V1.4*
4	*车机（IVI）*	*非标准密码算法模块*	*硬件*	*XXX 审查报告*	*AAAA*	*V1.3*

（功能组件应至少覆盖应用指南中所列出的核心功能组件，车辆不具备该功能组件的除外，如车辆不具备 ADAS 功能，不存在对应的域控制器。如某核心功能组件上未使用密码算法模块，也需在清单中列出，并标识无密码模块。以上示例仅供参考，不代表某一功能组件必须使用某种类型的密码模块类型，也不代表某类密码模块一定要提供某类证明材料）

附表十：默认安全设置

序号	默认安全设置	默认安全设置实现技术方案		
		文档名称	文件编号	版本号
1	*WIFI 默认安全口令*	*XXX 信息安全生产规范*	*AAAAA*	*V1.3*
2				
3				

填写说明

1、本模板仅供参考，企业实际文档名称和格式无需和模板保持一致，企业可根据实际情况酌情进行调整。

2、本模板中所有斜体字为注释或编制样例，用于辅助企业理解，正式提交版文件中请删除注释和编制样例。

3、本模板附表中所述的“文档”不限于纸制/电子版的文件，企业可根据实际情况进行填写并调整模板，例如企业通过软件平台开展车型产品风险评估时，可填写软件平台的相关信息和该车型风险评估结果等信息在软件平台内检索查询的方式。

4、所有“文档”的名称、编号和版本号须与现场被查的材料保持一致（文件编号指某文件记录的唯一性标识，企业可根据文档管理的实际情况填写该列内容）。

附 录 B

（规范性）

确定测试对象的方法

检测人员依据 GB 44495—2024《汽车整车信息安全技术要求》逐项确认各个条款的相关测试对象。对于第 7.2.7 条、第 7.2.8 条、第 7.4.1 条、第 7.4.2 条、第 7.4.3 条、第 7.4.4 条、第 7.4.5 条和第 7.4.6 条（以下统称“上述条款”），检测机构可采用如下联合抽选的方式确定测试控制器，具体方式如下：

①联合抽选条款确认

从上述条款中选择测试对象为多个控制器的条款，将其整理为“联合抽选条款清单 X_1”；

②测试控制器抽选

基于“联合抽选条款清单 X1”整理“测试控制器清单 S1”，通过随机抽选方式从清单 S1 中随机抽选测试控制器 A1（测试控制器 A1 需保证与送检车辆对应零部件的信息安全处置措施相同）。

③覆盖度验证及测试执行

若测试控制器 A1 可以完全覆盖“联合抽选条款清单集 X1”，则依据 GB 44495—2024《汽车整车信息安全技术要求》针对测试控制器 A1 执行相关测试并判定；

若测试控制器 A1 未完全覆盖“联合抽选条款清单 X1”，则针对上述条款中未覆盖条款整理“联合抽选条款清单 X2”和对应的“测试控制器清单 S2”，通过随机抽选方式从清单 S2 中随机抽选测试控制器 A2（测试控制器 A2 需保证与送检车辆对应零部件的信息安全处置措施相同），若测试控制器 A2 可完全覆盖“联合抽选条款清单 X2”，则依据 GB 44495—2024《汽车整车信息安全技术要求》针对测试控制器 A1 和 A2 执行相关测试并判定；

本程序循环执行直至“联合抽选条款清单 X1”被完全覆盖。

【注】所有确定测试零部件的记录均需按标准要求形成可追溯的原始记录。