报告编号:

检　验　报　告

整车信息安全

产品名称 _____

产品型号 _____

委托单位 _____

检验类别 验证检验

注　意　事　项

1.报告无“检验检测专用章”或“试验专用章”无效。

2.未经本检验中心批准，不得部分复制本检验报告。复制报告未重新加盖“检验检测专用章”或“试验专用章”无效。

3.报告无主检、审核、批准人签字无效。

4.报告涂改无效。

5.对检验报告若有异议，请以书面形式通知本检验中心总师室受理。

6.送样检验仅对样品负责。

7.委托方（客户）对样品及提供的数据和信息的真实性承担责任。

8.报告中未注资质认定标志时，仅供委托方（客户）内部使用，不具有对社会的证明作用。

检验单位地址电话:
地　　址：
电　　话：
邮政编码：

委托单位地址电话:
地　　址:
电　　话:
邮政编码:

目　　录

报告编号：

检 验 报 告

检验结论：

样品名称		商标	----
型号规格		检验类别	验证检验
委托单位			
生产企业			
送 样 者		送样日期	
样品数量		生产日期	
检验依据		检验项目	
检 验 结 论	签发日期：		
备注			

批准： 批准　　审核： 审核　　主检： 主检

检 验 报 告

1.任务来源及目的

受----委托，对其提供的SVW73025CK型轿车样品进行汽车信息安全管理要求、车辆信息安全一般要求、车辆信息安全技术要求的检验，考核其检验结果是否符合GB XXXXX《汽车整车信息安全技术要求》的要求。

检验任务单编号为：

2.检验依据

2.1 方法依据

依据GB XXXXX《汽车整车信息安全技术要求》规定的方法进行检验。

2.2 判定依据

依据GB XXXXX《汽车整车信息安全技术要求》规定的要求进行判定。

3.样品情况

3.1 来样方式：送样

3.2 样品数量： 辆

样品情况：

序号	项目名称	项目参数
1	车辆型号	
2	车辆识别码	
备注	----	

4.检验项目：

序号	检 验 项 目	样 品 编 号
1	汽车信息安全管理体系要求	
2	信息安全一般要求	
3	信息安全技术要求	

5.检验时间及地点

检 验 报 告

6.检验结果

6.1 汽车信息安全管理要求

序号	检验项目	标准要求		检验结果	符合性判定
1	汽车信息安全管理要求	车辆生产企业应建立车辆全生命周期的汽车信息安全管理体系。		车辆生产企业建立了车辆全生命周期的汽车信息安全管理体系。	符合
2		汽车信息安全管理体系中应涵盖必要流程，以确保充分考虑安全风险。		汽车信息安全管理体系涵盖了必要流程，可以确保充分考虑安全风险。	符合
3		车辆生产企业应建立车辆生产企业内部管理信息安全的流程。		车辆生产企业建立了车辆生产企业内部管理信息安全的流程。	符合
4		车辆生产企业应建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到适当处置的流程，并确保车辆风险评估保持最新状态。		车辆生产企业建立了识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到适当处置的流程，可确保车辆风险评估保持最新状态。	符合
5		车辆生产企业应建立用于车辆信息安全测试的流程。		车辆生产企业应建立了用于车辆信息安全测试的流程。	符合
6		车辆生产企业应建立针对车辆的网络攻击、网络威胁和漏洞的监测及响应流程。	建立漏洞管理流程，明确漏洞收集、分析、报告、处置、发布等活动环节。	车辆生产企业建立了漏洞管理流程，明确了漏洞收集、分析、报告、处置和发布环节。	符合
7			建立针对网络攻击提供相关数据并进行分析的流程。	车辆生产企业建立了针对网络攻击提供相关数据并进行分析的流程。	符合
8			建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在合理的时限内得到处置的流程。	车辆生产企业建立了确保已识别的网络攻击、网络威胁和漏洞得到响应，且在合理的时限内得到处置的流程。	符合
9			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流程。	车辆生产企业建立了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流程。	符合
10			建立确保对网络攻击、网络威胁和漏洞进行持续监控的流程。	车辆生产企业建立了确保对网络攻击、网络威胁和漏洞进行持续监控的流程。	符合
11		车辆生产企业应建立管理车辆生产企业与合同供应商、服务提供商、车辆生产企业子组织之间信息安全依赖关系的流程。		车辆生产企业建立了管理车辆生产企业与合同供应商、服务提供商、车辆生产企业子组织之间信息安全依赖关系的流程。	符合

检 验 报 告

6.2 车辆信息安全一般要求

序号	检验项目	标准要求	检验结果	符合性判定
1	车辆信息安全一般要求	车辆产品开发流程应遵循汽车信息安全管理体系要求。	车辆产品开发流程遵循了汽车信息安全管理体系要求	符合
2		车辆产品开发流程中应识别和管理车辆与供应商相关的风险。	车辆产品开发流程中已识别和管理车辆与供应商相关的风险。	符合
3		车辆产品开发流程中应识别车辆的关键要素，对车辆进行详细的风险评估，合理管理已识别的风险。风险评估应考虑车辆的各个要素及其相互作用，并进一步考虑与任何外部系统的相互作用。	车辆产品开发流程中已识别车辆的关键要素，对车辆进行详细的风险评估，合理管理已识别的风险。风险评估已考虑车辆的各个要素及其相互作用，并进一步考虑与任何外部系统的相互作用。	符合
4		车辆产品开发流程中应采取基于第 7 章、第 8 章、第 9 章、第 10 章的信息安全技术要求处置措施保护车辆不受风险评估中已识别的风险影响。	车辆产品开发流程中已采取基于第 7 章、第 8 章、第 9 章、第 10 章的信息安全技术要求处置措施保护车辆不受风险评估中已识别的风险影响。	符合
5		如有专用环境，则车辆生产企业应采取相应适当的措施，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。	无专用环境。	符合
6		车辆产品开发流程中应通过适当和充分的测试来验证所实施的信息安全措施的有效性。	车辆产品开发流程中已通过适当和充分的测试来验证所实施的信息安全措施的有效性。	符合
7		车辆生产企业应针对车辆实施相应措施，以识别和防御针对该车辆的网络攻击、网络威胁和漏洞，并为车辆生产企业在识别与车辆相关的网络攻击、网络威胁和漏洞方面提供监测能力，以及为分析网络攻击、网络威胁和漏洞提供数据取证能力。	车辆生产企业已针对车辆实施相应措施，以识别和防御针对该车辆的网络攻击、网络威胁和漏洞，并为车辆生产企业在识别与车辆相关的网络攻击、网络威胁和漏洞方面提供监测能力，以及为分析网络攻击、网络威胁和漏洞提供数据取证能力。	符合
8		车辆应采用符合国际通用、国家或行业标准要求的密码模块。若使用的密码模块未采用国际通用、国家或行业标准要求，则应说明其使用的合理性。应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和场景，选择适当长度和有效的密钥。	车辆采用符合国际通用、国家或行业标准要求的密码模块。使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；根据不同密码算法和场景，选择适当长度和有效的密钥。	符合
9		车辆应采用默认安全设置。	车辆采用默认安全设置。	符合

6.3 车辆信息安全技术要求

6.3.1 车辆外部连接安全要求

6.3.1.1 外部连接一般安全

序号	检验项目	标准要求	检验结果	符合性判定
1	外部连接一般安全	车辆远程控制系统、授权的第三方应用等外部连接系统应不存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。	使用漏洞扫描工具对车辆外部连接系统、授权的第三方应用进行漏洞扫描测试，其中车辆外部连接系统存在权威权威漏洞平台 6 个月前公布的高危及以上的安全漏洞：CVE-2023-21250、CVE-2023-21096、CVE-2022-27568，对照车辆生产企业提交的漏洞处置方案清单，确认车辆生产企业提交的漏洞处置方案清单中覆盖该漏洞。	符合
2		车辆应关闭不必要的网络端口。	使用端口扫描设备查看被测样品所开放的端口，并将开放的端口列表与提交的车辆业务列表进行对比，车辆开放非必要的网络端口：22、23、5555、8080。	不符合

6.3.1.2 远程控制系统安全

序号	检验项目	标准要求	检验结果	符合性判定
1	远程控制系统	应对远程控制系统的指令信息进行真实性和完整性验证，并应具备验证失败的处理能力。	在 ROOT 测试手机上安装远程控车应用，并尝试设置代理使用抓包工具进行抓包，可以进行抓包。使用工具拦截远程控车时的指令报文，并对其进行篡改，篡改后发送该报文，车辆未响应该报文。	符合
2		应对远程控制系统的指令设置访问控制，禁用非授权的远程控制指令。	在 ROOT 测试手机上安装远程控车应用，并尝试设置代理使用抓包工具进行抓包，可以进行抓包。使用工具拦截远程控车时的指令报文，并按照该指令的应用场景和使用权限文件或说明，构造超出权限的控制指令，发送该报文，车辆未响应该报文。	符合
3		应具备远程控制系统的安全日志记录功能，安全日志记录的内容至少包括远程控制指令的日期、时间、发送主体、远程控制对象、操作结果。	检查远程控车日志文件，包含远程控制指令的日期、时间、发送主体、远程控制对象、操作结果；检查远程控车安全日志的记录时间跨度，所提供的日志的时间跨度不少于 6 个月。	符合
4		应对车端具备远程控制功能的系统的程序和配置数据进行完整性验证。	车端具备远程控制功能的系统为 TBOX，无法提供关于安全刷写或安全更新的设计方案及测试验证材料。	不符合

6.3.1.3 第三方应用安全

序号	检验项目	标准要求	检验结果	符合性判定
1	第三方应用	应对授权的第三方应用的真实性和完整性进行验证。	尝试对企业提供的第三方应用：酷我音乐进行篡改并重新打包签名，无法进行安装。	符合
2		应对非授权的第三方应用的安装运行进行提示，并对已安装的非授权的第三方应用进行访问控制，此类应用应不超出访问控制权限的访问系统资源、个人信息等。	尝试安装并执行非授权的第三方应用 ES 文件浏览器，车辆进行提示，不能安装成功。	符合

6.3.1.4 外部接口安全

序号	检验项目	标准要求	检验结果	符合性判定
1	外部接口安全	应对外部接口进行访问控制保护。	使用非授权的用户或工具访问车辆的外部接口，不能成功建立连接，不能访问相应的信息。	符合
2		应对从 USB 接口读取和写入的文件进行读写控制，只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。	将存储了媒体文件和指定签名的应用软件的移动存储介质连接到车辆 USB 接口，车辆可以执行媒体文件，无法执行指定签名的应用软件。	符合
3		应具备抵御 USB 接口接入设备中的病毒程序和携带病毒的媒体文件/应用软件的能力。	在具备 USB 接口的移动存储介质中注入病毒文件，将移动存储介质连接到车辆 USB 接口，尝试执行病毒文件，车辆系统能检测出移动存储介质中的病毒文件，未执行病毒文件。	符合
4		通过诊断接口发送车辆关键参数的写操作请求时，应采用身份鉴别或访问控制等安全措施。	通过 CAN 诊断接口发送车辆关键参数和标定数据的写操作请求，不能写入成功，采用了身份鉴别等安全措施。	符合

6.3.2 车辆通信通道安全要求

序号	检验项目	标准要求	检验结果	符合性判定
1	通信通道安全	车辆与车辆生产企业云平台通信时，应对其通信对象的身份真实性进行验证。	车辆与车辆生产企业云平台远程控车云平台通信采用公共网络环境进行通信，使用安全通信协议 TLS V1.2。	符合
2		车辆与车辆、路侧单元、移动终端等进行直连通信时，应进行证书有效性和合法性的验证。	被测车辆不涉及 V2X 功能。	符合
3		车辆应采用完整性保护机制保护外部通信通道。	车辆外部通信通道包括移动蜂窝通信、WLAN、蓝牙，均已采用完整性保护机制保护。	符合
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。	车辆外部通信通道包括移动蜂窝通信、WLAN、蓝牙，均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。	符合
5		车辆应验证所接收的关键指令数据的有效性或唯一性。	车辆外部关键指令涉及的通信通道包括移动蜂窝通信、蓝牙、射频钥匙、总线，尝试录制各通信通道的指令并进行重放，重放后车辆不响应，车辆各通信通道均已验证所接收的关键指令数据的有效性或唯一性。	符合
6		车辆应对发送的敏感个人信息实施保密性和完整性保护措施。	车辆向外传输敏感个人信息的通信通道包括移动蜂窝通信、WLAN，均已对发送的敏感个人信息实施保密性和完整性保护措施。	符合
7		车辆与外部直接通信的零部件应具备身份识别机制。	使用和测试车辆与外部直连通信零部件功能、型号相同且能正常工作的零部件车机，替换安装在整车相同的位置，启动车辆，替换的零部件正常工作，车辆没有异常部件连接告警提示。	不符合
8		车辆与外部直接通信的零部件应具备安全机制防止非授权的系统特权访问。	车辆与外部直接通信的零部件系统存在多种权限用户，尝试对非特权用户进行提权，无法提权成功。	符合
9		车辆内部网络应划分安全区域，并实现安全区域之间的隔离，对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。	车辆内部网络使用逻辑隔离措施，发送不符合策略的数据帧到指定的目的端口，车辆未接收到相应的数据帧。	符合
10		车辆应具备在拒绝服务攻击结束后恢复正常使用或处于安全状态的能力，并对攻击数据包进行相应的处理。	测试设备对 CAN 总线发起大于 80%总线负载率的拒绝服务攻击，在拒绝服务攻击时，车辆未受攻击的 CAN 通道通信性能和预设的功能未受到影响。	符合
11		车辆应具备识别恶意的 V2X 数据、恶意的诊断数据等的能力，并采取保护措施。	依据 CAN 诊断通信规则，构造并向车辆发送恶意的诊断消息数据，车辆鉴别并拒绝响应。	符合
12		车辆应对关键的通信信息安全事件进行日志记录。	构建并触发车辆关键通信信息安全事件拒绝服务攻击，车辆按照通信信息安全日志记录机制记录该事件；检查日志记录时间跨度，所提供的日志时间跨度不少于 6 个月。	符合

6.3.3 车辆软件升级安全要求

6.3.3.1 软件升级一般安全要求

序号	检验项目	标准要求	检验结果	符合性判定
1	软件升级一般安全要求	车载软件升级系统应具备安全启动的功能，应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，或被篡改后无法正常启动。	被测车辆不能提供车载软件升级系统（TBOX 的可信根、引导加载程序、系统固件）的安全保护机制的安全证明文件，不能合理证明车载软件升级系统具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。	不符合
2		车载软件升级系统应不存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。	车载软件升级系统不存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞。	符合

6.3.3.2 在线升级安全要求

序号	检验项目	标准要求	检验结果	符合性判定
1	操作系统安全启动	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。	车辆和在线升级服务器通信采用公共网络环境进行通信，使用安全通信协议 TLS V1.2。	符合
2		车载软件升级系统应对下载的在线升级包进行真实性和完整性校验。	构造被篡改破坏的在线升级包，将该升级包下载到车载端，尝试执行软件升级，车辆未执行升级。车载软件升级系统对下载的在线升级包进行了真实性和完整性校验。	符合
3		车载软件升级系统应记录在线升级过程中发生的失败事件日志。	车载软件升级系统记录了在线升级过程中发生的失败事件日志。	符合

6.3.3.3 离线升级安全要求

序号	检验项目	标准要求	检验结果	符合性判定
1	操作系统更新	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校验。	构造被篡改破坏的离线升级包，将该升级包传输到车载端，尝试执行软件升级，车辆未执行升级，车载软件升级系统对下载的离线升级包进行了真实性和完整性校验。	符合
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，并校验离线升级包的真实性和完整性。	车辆使用车载软件升级系统进行离线升级。	符合

6.3.4 车辆数据代码安全要求

序号	检验项目	标准要求	检验结果	符合性判定
1	车辆数据代码安全	车辆应安全地存储对称密钥和私钥，防止其被非授权访问和获取。	车辆具备密码存储功能的关键零部件为 TBOX，TBOX 使用硬件 HSM 安全的存储对称密钥和私钥。被测车辆无法提供硬件安全模块安装位置说明文档。	不符合
2		车辆应采取访问控制技术、加密技术等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。	车辆涉及敏感个人信息存储的关键零部件为车机，车机使用加密技术安全的存储敏感个人信息。	符合
3		车辆应采取安全防御机制保护存储在车内的 VIN 和用于身份识别的数据，防止其被非授权删除和修改。	尝试通过软件分析工具和诊断工具分别篡改 VIN，无法篡改成功。车辆采取了安全防御机制保护存储在车内的 VIN 和用于身份识别的数据，防止其被非授权删除和修改。	符合
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。	尝试通过软件分析工具篡改车辆关键数据，无法篡改成功，车辆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。	符合
5		车辆应采取安全防御机制保护存储在车内的安全日志，防止其被非授权删除和修改。	尝试通过软件分析工具篡改车辆安全日志，无法篡改成功，车辆采取安全防御机制保护存储在车内的安全日志，防止其被非授权删除和修改。	符合
6		车辆应具备个人信息清除功能及防恢复机制，便于在转售、租借或报废时清除个人信息。	测试车辆具备个人信息清除功能，使用测试车辆个人清除功能清除车辆内存储的个人信息，个人信息被完全清除。	符合
7		车辆不应直接向境外传输数据。	开启车辆移动蜂窝网络，依次模拟测试车辆各项预装的数据传输功能；使用网络数据抓包工具进行抓包，解析通信报文数据，包含境外 IP 地址。	不符合

7.附录

图 1 样品照片

图 2 试验照片

----以下空白----