TC260-PG-20246A

网络安全标准实践指南

—— 一键停止收集车外数据指引

(v1.0-202412)

全国网络安全标准化技术委员会秘书处

2024 年 12 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：小米汽车科技有限公司、中国电子技术标准化研究院、岚图汽车科技有限公司、北京汽车研究总院有限公司、国家计算机网络与信息安全管理中心、上海机动车检测认证技术研究中心有限公司、众链科技（北京）有限公司

本文件主要起草人：姚相振、郝春亮、单渤凯、杨思佳、林小栋、李国强、张骁、郭登海、王秉政、丁翠、林文涛、张钧、王金奎、范乐君、陈燕呢、申任远、滕添益、赵梓健、韩昭、王寒生。

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

为防止智能网联汽车的车外数据收集状态难以被察觉，导致车辆可能收集大量重要数据和敏感个人信息的情况发生，业界有各种方案在探索实践中。本文件提出一种较为便捷的一键停止收集车外数据功能实践指引，一方面通过设置物理按键的方式关闭各类车载摄像头、雷达等传感器，实现一键停止收集车外数据的功能；另一方面通过汽车的车外状态标识，向重要敏感区域的管理人员告知车辆处于暂停收集车外数据的安全状态，降低其管理难度。

本文件面向的智能网联汽车，尤其是装有高清摄像头、激光雷达、4D 毫米波雷达等传感器，对车外数据有精准收集和分析能力的车辆。对于已定型、不具备相应精度传感器、不具备精准收集和分析能力的车辆，仅供参考。

目　录

1 范围

本文件给出了在装有车载摄像头、雷达等传感器的智能网联汽车上设置一键停止收集车外数据功能的指引。

本文件适用于汽车制造企业、自动驾驶研发企业以及相关零部件或服务提供商设计、研发、制造具有车外数据收集功能的智能网联汽车（不包括主驾无人的高级别自动驾驶汽车）；也适用于重要敏感区域的管理机构对进入该区域内汽车的数据收集状态进行判断；还可为第三方测评机构开展智能网联汽车车外数据停止收集功能的有效性和安全性测试评估提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 4094　汽车操纵件、指示器及信号装置的标志

GB/T 41871-2022　信息安全技术 汽车数据处理安全要求

GB/T 44373-2024　智能网联汽车 术语和定义

3 术语和定义

GB/T 41871-2022 界定的以及下列术语和定义适用于本文件。

3.1 智能网联汽车

智能网联汽车是指具备环境感知、智能决策和自动控制，或与外界信息交互，乃至协同控制功能的汽车。

[来源：GB/T 44373-2024, 3.1]

3.2 车外数据

通过车载摄像头、雷达等传感器从汽车外部环境收集的道路、建筑、地形、交通参与者、机动车车牌等数据，以及其经处理产生的数据。

注：交通参与者是指参与交通活动的人，包括机动车、非机动车、其他交通工具的驾驶人与乘员，以及其他参与交通活动的相关人员。

3.3 一键停止收集

通过设定按键便捷地使车外数据收集装置处于关闭状态。

3.4 关闭状态

设备处于断电状态，或不感知周围环境的状态。

注：关闭状态包括设备处于断电状态或设备仍然保持供电，但是处于低功耗模式下的待机状态。以机械式激光雷达为例，当进入不感知周围环境的状态时，电机和激光发射器均停止工作，不具备数据收集能力。

4 停止收集车外数据流程

一键停止收集车外数据功能通过关闭各类车载摄像头、雷达等传感器（示例见图 1），实现停止收集车外数据的管控。

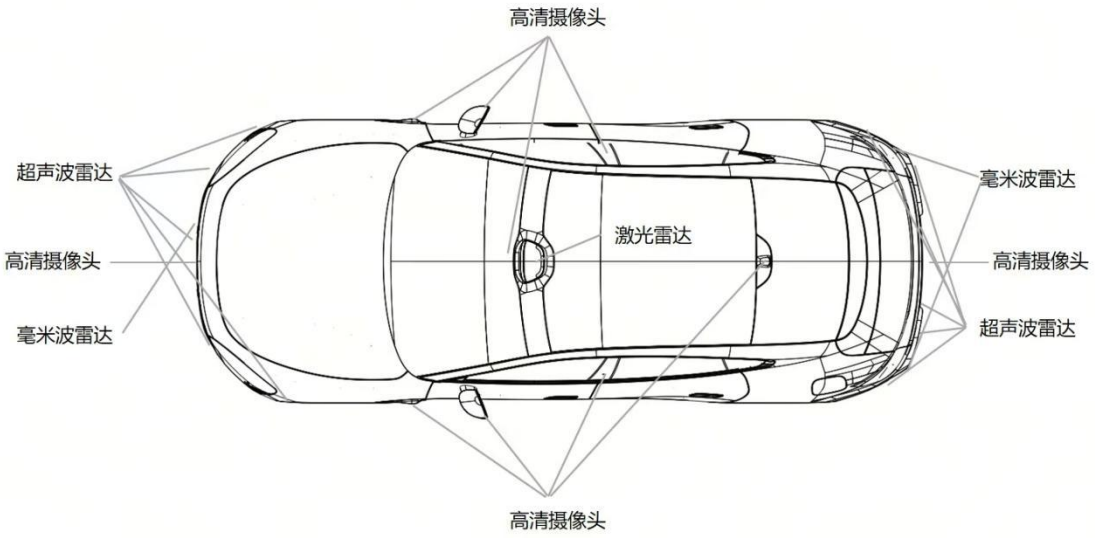

图 1 智能网联汽车外部传感器

一键停止收集车外数据功能基本运行逻辑见图2,运行流程如下:

a）点击按键触发功能启用;

b）传递功能开启信号至相关传感器，包含摄像头、雷达等;

c）传感器进行响应，返回关闭状态信号;

d）接收到功能启用、传感器关闭状态信号后，相关联功能禁用，对应的指示标识启用，进入停止收集车外数据状态。

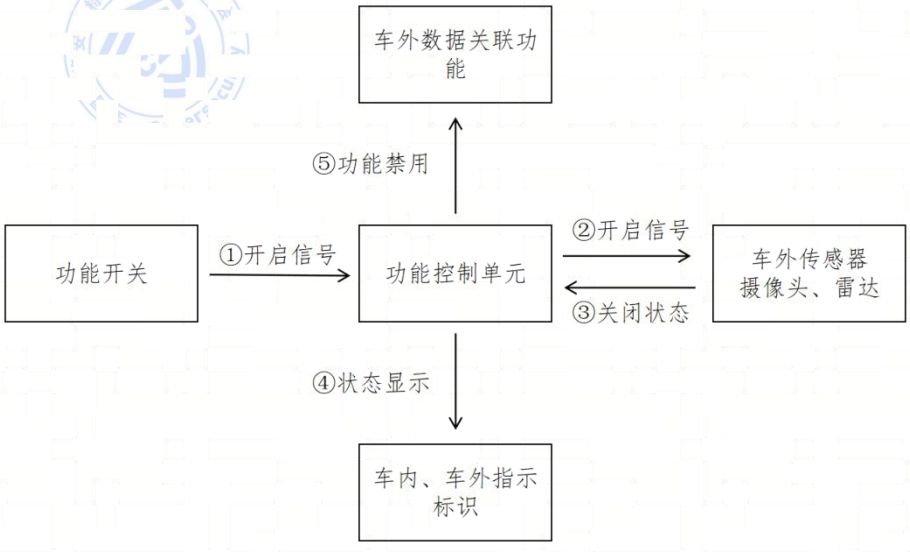

图 2 停止车外数据收集流程简图

5 基本要求

5.1 功能要求

一键停止收集车外数据功能应满足:

a）应具有专门的开关用于进入或退出停止收集车外数据状态。该开关应处于座舱内驾驶人方便操作的位置，不宜位于驾驶人以外其他乘员可操作的位置，测试方法见附录 B.1;

注：按键包括按键、旋钮等实体开关，按键设置位置可参考附录 A。

b）汽车处于停止收集车外数据状态时，传感器的数据收集应符合文件第六章要求，车内和车外均应按本文件第七章要求进行展示提示，测试方法见附录 B.2;

c）汽车处于停止收集车外数据状态时，汽车驻车期间（包含锁止并离开车辆后）以及下次车辆启动仍应保持停止收集车外数据的状态;

d）开启一键停止收集车外数据功能前，应采用显著方式向驾驶人告知关联影响，确保行车安全。

注 1：关联影响指一键停止收集车外数据功能触发后，相关辅助驾驶功能被禁用的情况。
注 2：考虑到行车安全，车辆达成某一车速限值时，一键停止收集车外数据功能不生效。

5.2 信息安全要求

一键停止收集车外数据功能应采取适当的信息安全措施，以规避非预期操作风险，相关要求如下，测试方法见附录 B.3。

a）整车应对功能开关指令进行完整性保护;

b）整车应对发送的功能开关指令进行安全保护，包括对发送功

能开关指令的对象进行身份认证、权限校验，避免车外远程发送的恶意操作指令生效。

6 停止收集

6.1 触发方式

触发一键停止收集车外数据功能可通过以下方式实现。

a）实体开关

由实体开关触发且应设置防误触机制。

示例：设置专用一键停止收集车外数据的按键，长按 2S 触发。

b）采取实体开关和显示面板交互方式组合

触发实体开关，并在大屏确认是否进入停止收集车外数据的状态。

示例：触发实体开关，大屏向驾驶人告知开启功能产生的关联影响，包含辅助驾驶功能被禁用、车速受限等，驾驶人点击二次确认后，功能启用。

6.2 摄像头

汽车处于停止收集车外数据状态时，应使车载摄像头处于关闭状态。

示例：车载摄像头可包括前/后远视摄像头、周视摄像头、环视摄像头等。

6.3 雷达

汽车处于停止收集车外数据状态时，应使雷达处于关闭状态。

示例：普通毫米波雷达可不关闭，激光雷达、4D 毫米波雷达等能精确进行障碍物形状分析且能精确测距的雷达应关闭。

6.4 其它

汽车处于停止收集状态时，应关闭其它收集车外数据的传感器。

6.5 解除方式

a）再次触发一键停止收集的开关；

示例：再次按压或旋钮触发一键停止收集的开关。

b）驾驶人触发开关解除停止收集状态时，车机屏幕应提示用户，用户点击确认则退出，用户点击取消则继续处于停止收集状态。

示例：车机屏幕提示可为“请遵循相关法律法规要求，注意保护车外数据安全”。

7 状态标识

7.1 停止收集状态标识

a）为便于敏感区域管理人员准确识别汽车的数据收集状态，应设置车外数据收集状态的车外指示标识，标识应符合以下要求：

1） 有明显的车外指示标识指示汽车处于停止收集车外数据状态；车外标识展示样例可参考附录A。

2） 驻车期间（包含锁止并离开车辆后），车外指示标识应持续工作；

3） 工作指示标识如图3所示，标识颜色宜为蓝色，其长度不宜小于15mm、宽度不宜小于15mm；

图 3 工作指示标识

4） 工作指示标识在车外的可见范围见附录C。在可见区域边界范围内（区域由车辆前端横向平面、距车前2m的横向平面，及距车辆中心两侧各2m的纵向平面组成，高度为地面以上1m到3m范围内），能观察到车外工作指示标识

工作状态；

5） 车外工作指示标识也可采用其他形式，可有效达成上述条款中提示效果即可。

b）为便于驾驶人在座舱内准确识别车外数据的收集状态，应设置车外数据收集状态的车内指示标识，标识应符合以下要求：

1） 有明显的车内指示标识指示汽车处于停止收集车外数据状态；

2） 车内指示可采用图3，也可通过其他方式向驾驶人显著告知当前处于停止收集车外数据的状态，相关要求应符合GB 4094《汽车操纵件、指示器及信号装置的标志》。

7.2 收集状态标识

宜设置明显的车内、车外指示标识指示汽车处于收集车外数据状态。

附录 A

（资料性）

车内一键关闭功能按键及车外展示指示灯位置样例

车内停止收集功能按键可位于车内后视镜区域的双闪灯按键旁，样例见图 A.1。

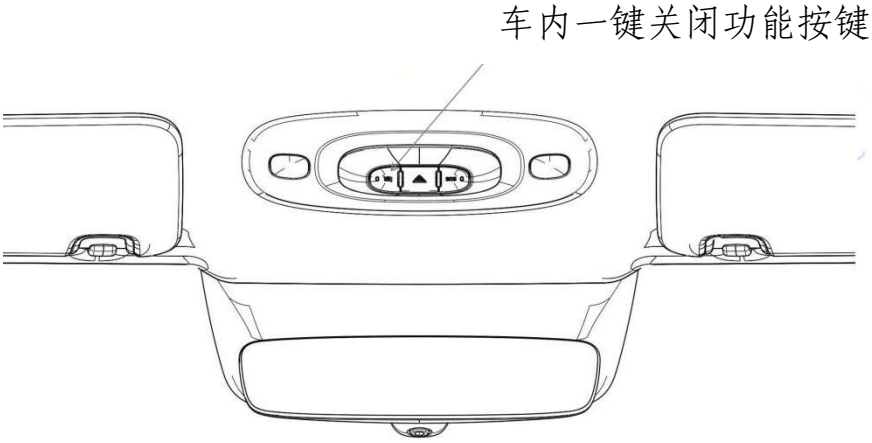

图 A.1 车内关闭车外数据功能按键位置样例

为便于敏感区域车外数据管理，汽车处于停止收集车外数据状态时，车外展示指示灯可位于汽车前挡风玻璃中间位置，样例见图 A.2。

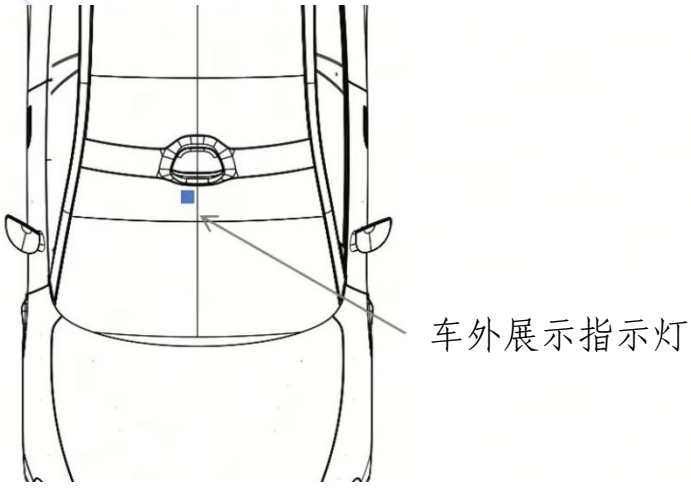

图 A.2 车外展示指示灯位置样例

附录 B

（规范性）

车外数据一键停止收集车外数据测试方法

B.1 一键停止收集车外数据功能测试方法

a）开关机制测试方法：

1） 检查座舱内是否通过实体按键、旋钮或以实体按键、旋钮和车载显示面板交互等方式，设置了便捷的车外数据停止收集开关；

2） 检测人员于驾驶员位置落座，测试是否能方便地操作一键停止收集车外数据的开关；检查完成后，更换至座舱其他各个位置并尝试操作此开关，确认是否能够方便地进行操作；

3） 尝试开启车外数据一键停止收集车外数据的开关，检查此开关是否设置了防误触机制；

4） 尝试关闭开关，检查车机是否以车载显示面板弹窗等方式，对于退出停止收集车外数据的状态进行二次确认；

5） 保持开关开启，车辆下电并重新上电，检查车辆是否仍处于停止收集车外数据的状态。

b）停止收集车外数据状态测试方法：

1） 触发停止收集车外数据开关，使车辆进入不收集车外数据的状态；依次尝试使用涉及车外数据处理的功能，确

认功能是否能正常使用；

2） 解除停止收集车外数据开关，使车辆退出不收集车外数据的状态；检查车辆收集车外数据的传感器是否恢复正常工作。

B.2 车外和车内指示标识展示测试方法

a）车外指示标识可见范围测试方法：

1） 人工检测：开启一键停止收集车外数据功能后，测试人员于本指南附录C所规定的区域内变更位置，观察车外指示标识是否保持可见的状态；

2） 设备检测：开启一键停止收集车外数据功能后，使用相机及相机支架于本指南附录C所规定的区域内变更位置及高度，观察车外指示标识是否保持可见的状态；

3） 经人工检测和设备检测，车外指示标识都保持可见的状态，视为符合要求。

b）车外指示标识持续可见测试方法：

1） 驻车状态持续可见：开启一键停止收集车外数据功能后，触发驻车状态5分钟，车内人员锁车并离开车辆，使用B.2中所述人工检测方法和设备检测方法，确认指示标识是否持续可见；

2） 行驶状态持续可见：开启一键停止收集车外数据功能后，车辆缓慢行驶、倒车5分钟，使用B.2中所述设备检测方

法，确认指示标识是否持续可见；

3） 在驻车状态、行驶状态下，车外指示标识都持续可见，视为符合要求。

c）一键停止收集车外数据的车内状态告知测试方法如下。若至少存在一种告知方式，视为符合要求。

1） 测试人员进入车内，观察是否在仪表盘或车载面板位置显示指示标识；

2） 通过语音方式告知停止收集状态。

B.3 信息安全测试方法

a）完整性测试方法如下：

1） 使用测试工具对功能开关和车外数据收集装置间的通讯进行数据抓包；

2） 录制数据包内容；

3） 修改录制的数据包内容，例如原指令为关闭一键停止收集车外数据指令，修改为开启功能指令；

4） 使用测试工具模拟功能开关向车外数据收集装置发送修改的功能开发指令，查看开启状态；

5） 功能未发生状态变化，视为符合要求。

b）身份认证测试方法如下：

1） 使用测试工具对功能开关和车外数据收集装置间的通讯进行数据抓包；

2） 录制数据包内容;

3） 使用测试工具模拟功能开关向车外数据收集装置发送录制的数据包内容（功能开发指令），查看功能开启状态;

4） 功能未发生状态变化，视为符合要求。

附录 C

（规范性）

车外工作指示标识可见范围

停止收集车外数据工作状态指示标识可见范围见图 C.1。

a）X 向：车辆最前端向前 2m 范围内；

b）Y 向：以 Y 基准平面为准，±2m 范围内；

c）Z 向：以地平面为准，1m~3m 范围内。

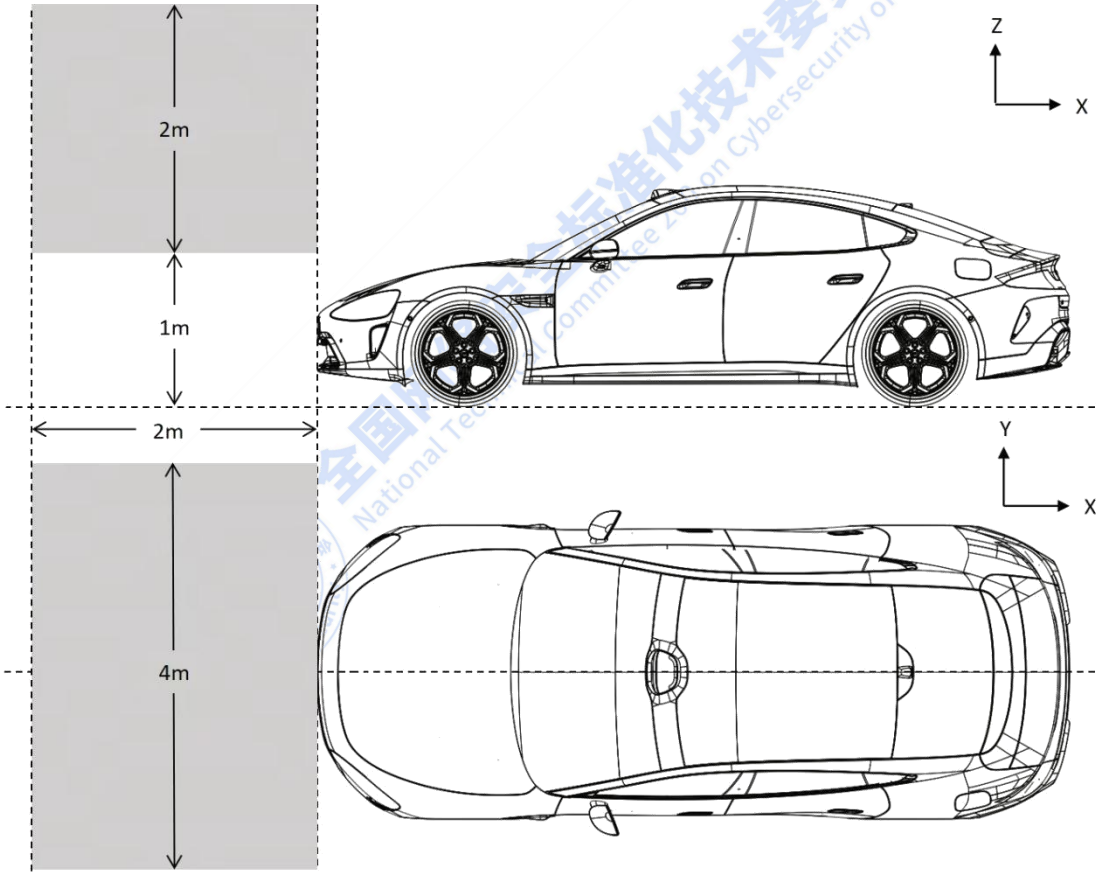

图 C.1 车外工作指示标识可见范围