附件4

HJ

中华人民共和国国家环境保护标准

HJ □□□□.3—20□□

重型车远程排放监控技术规范

第 3 部分：车载终端技术要求及测量方法

Technical specifications of remote emission supervision system for heavy-duty vehicles

PART3: On-board terminal technical requirements and measurement methods

（征求意见稿）

20□□-□□-□□发布　　20□□-□□-□□实施

生　态　环　境　部　　发布

目 录

前 言

为贯彻《中华人民共和国环境保护法》和《中华人民共和国大气污染防治法》，防治装用压燃式及气体燃料点燃式发动机的汽车排气对环境的污染，规范车辆远程排放监控技术，改善空气质量，制定本标准。

本标准分为五个部分：

——第1部分：总则；

——第2部分：平台技术要求；

——第3部分：车载终端技术要求及测量方法；

——第4部分：通讯协议及数据格式；

——第5部分：监管技术规范。

本部分为本标准的第3部分。

本部分规定了重型车远程排放监控系统车载终端的技术要求，包括功能要求、性能要求、试验方法、检验规则、标志标识以及运输存储安装要求，适用于安装应用在重型车上用于采集、存储和传输车辆OBD信息和发动机排放数据的设备装置。

本标准由生态环境部大气环境司、法规与标准司组织制订。

本标准起草单位：中国环境科学研究院、中国汽车技术研究中心有限公司、智联万维（北京）网络信息科技有限公司、唐山市环境监控中心。

本标准生态环境部20□□年□□月□□日批准。

本标准自20□□年□□月□□日实施。

本标准由生态环境部解释。

重型车远程排放监控技术规范

第 3 部分：车载终端技术要求及测量方法

1 适用范围

本标准规定了重型车远程排放监控系统车载终端的技术要求，包括功能要求、性能要求、试验方法、检验规则、标志标识以及运输存储安装要求。

本标准适用于安装应用在重型车上用于采集、存储和传输车辆OBD信息和发动机排放数据的设备装置。

2 规范性引用文件

本标准引用了下列文件或其中的条款。凡是未注明日期的引用文件，其最新版本适用于本标准。

GB 17691—2005 车用压燃式、气体燃料点燃式发动机与汽车排气污染物排放限值及测量方法（中国III、IV、V阶段）

GB 17691—2018 重型柴油车污染物排放限值及测量方法（中国第六阶段）

GB/T 2423.18 环境试验 第2部分：试验方法 试验Kb：盐雾，交变(氯化钠溶液)

GB/T 4208 外壳防护等级（IP代码）

GB/T 28046.1 道路车辆 电气及电子设备的环境条件和试验 第1部分：一般规定

GB/T 32960.2 电动汽车远程服务与管理系统技术规范 第2部分：车载终端

GB/T 32960.3 电动汽车远程服务与管理系统技术规范 第3部分：通讯协议及数据格式

HJ □□□□.4 重型车远程排放监控技术规范 第4部分：通讯协议及数据格式（制订中）

ISO 9001 质量管理体系

ISO 14001 环境管理体系

GM/T0008 安全芯片密码检测准则

GM/T0009 SM2密码算法使用规范

3 术语和定义

GB 17691—2018确定的以及下列术语和定义适用于本标准。

3.1

数据防篡改基础信息备案 data tamper-proof basic information filing service

用于完成安全信息、车载终端、车辆信息的数据防篡改基础信息备案。

3.2

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码兑换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

3.3

密钥 key

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

3.4

公钥 public key

在某一实体的非对称密钥对中，能够公开的密钥。

3.5

私钥 private key

在某一实体的非对称密钥对中，只应由该实体使用的密钥。

注 1：正常情况下，私钥不应泄露。

注 2：在非对称签名体制的情况下，私钥定义签名变换。而在非对称加密体制的情况下，私钥定义解密变换。

3.6

安全芯片 security chip

一类专用芯片，对存储保护采用了专门的逻辑电路设计保护，有效的防止攻击者通过物理复制和波形探测来拷贝内部数据，可以利用保存在其中的私钥对数据进行加密或签名，但无法将私钥读出。

3.7

安全芯片标识 ID security chip ID

芯片ID为芯片生产厂商生产的安全芯片唯一标识，由三位芯片型号标识符和车辆生产企业自定义的最多十三位字符组成，用来绑定安全芯片的公私钥对。

3.8

首次定位时间 time to first fix,TTFF

导航接收机通电后获得的正确定位的时间。

3.9

重捕时间 re-get time

卫星信号短暂中断后，导航接收机重新捕获卫星信号并确定其当前位置的时间。

3.10

实时动态 real - time kinematic，RTK

载波相位差分技术，是实时处理两个测量站载波相位观测量的差分方法，将基准站采集的载波相位发给用户接收机，进行求差解算坐标。

4 一般要求

4.1 重型车车载远程在线监控终端应具备本标准第 5 章规定的功能，并能满足第 6 章规定的性能要求，能够确保在车辆全寿命期内，按 HJ □□□□.4 规定的通讯要求进行数据发送。

4.2 应按第 7 章规定的测试方法，对车载终端进行功能和性能测试，并将测试报告向生态环境主管部门公开。

5 功能要求

5.1 车载终端的自检、时间、日期和 OBD 信息采集

应符合GB 17691—2018第Q.5.1、Q.5.2和Q.5.3的要求。

5.2 发动机数据采集

5.2.1 车载终端应能采集发动机排放相关数据。安装在符合GB 17691—2018重型车上车载终端采集的数据见表1，采集频率至少应为1Hz。安装在符合GB 17691—2005 第五阶段的重型车和安装在排气后处理系统改造车辆上的车载终端应至少采集表1中规定的数据。

表1 车载终端采集的数据

数据项	安装在符合第六阶段重型车上的车载终端	安装在符合第五阶段重型车上的车载终端	安装在排气后处理系统改造车辆上的车载终端
车速	√	√	√
大气压力(直接测量或估计值)	√	√	×
发动机最大基准扭矩	√	√	×
发动机净输出扭矩（作为发动机最大基准扭矩的百分比），或发动机实际扭矩/指示扭矩（作为发动机最大基准扭矩的百分比，例如依据喷射的燃料量计算获得）	√	√	×
摩擦扭矩（作为发动机最大基准扭矩的百分比）	√	√	×
发动机转速	√	√	×
发动机燃料流量	√	√	×
NOx 传感器输出	√	√（如适用）	√
SCR 入口温度	√	√（如适用）	√
SCR 出口温度	√	√（如适用）	√

数据项	安装在符合第六阶段重型车上的车载终端	安装在符合第五阶段重型车上的车载终端	安装在排气后处理系统改造车辆上的车载终端
DPF 压差	√	√（如适用）	√
进气量	√	√	×
反应剂余量	√	√（如适用）	×
油箱液位	√	√（如适用）	√（如适用）
发动机冷却液温度	√	√	×
经纬度	√	√	√
累计里程	√	√（如适用）	√（如适用）

注：安装在符合GB 17691—2005第五阶段的重型车上的车载终端，若该车辆未采用SCR技术则涉及SCR及尿素相关参数可不上传。

5.2.2 对于采用三元催化器后处理技术的车辆，车载终端应采集表2规定的数据，第六阶段车辆采集频率为1Hz。

表2 车载终端采集的数据（采用三元催化技术的车辆）

数据项	采用三元催化器技术的车辆采集参数
车速	√
大气压力(直接测量或估计值)	√
发动机最大基准扭矩	√
发动机净输出扭矩（作为发动机最大基准扭矩的百分比），或发动机实际扭矩/指示扭矩（作为发动机最大基准扭矩的百分比，例如依据喷射的燃料量计算获得）	√
摩擦扭矩（作为发动机最大基准扭矩的百分比）	√
发动机转速	√
发动机燃料流量	√
三元催化器下游 NOx 传感器输出	√
前氧传感器输出	√
后氧传感器输出	√
进气量	√
油箱液位	√
发动机冷却液温度	√
经纬度	√

数据项	采用三元催化器技术的车辆采集参数
累计里程	√

5.2.3　车辆生产企业应确保车载终端采集和上传的数据与车辆实际数据一致。

5.3　车辆注册（防篡改信息备案）

5.3.1　安装在符合GB 17691—2018的重型车上的车载终端应按HJ □□□□.4规定的通讯协议，按图1规定向国家平台进行注册。

5.3.2　注册信息为HJ □□□□.4规定的防篡改备案信息，包括安全芯片标识ID、储存在安全芯片中的公钥和车载终端通过OBD读取的车辆VIN。

5.3.3　注册信息应通过安全芯片中存储的私钥添加数据签名后提交。

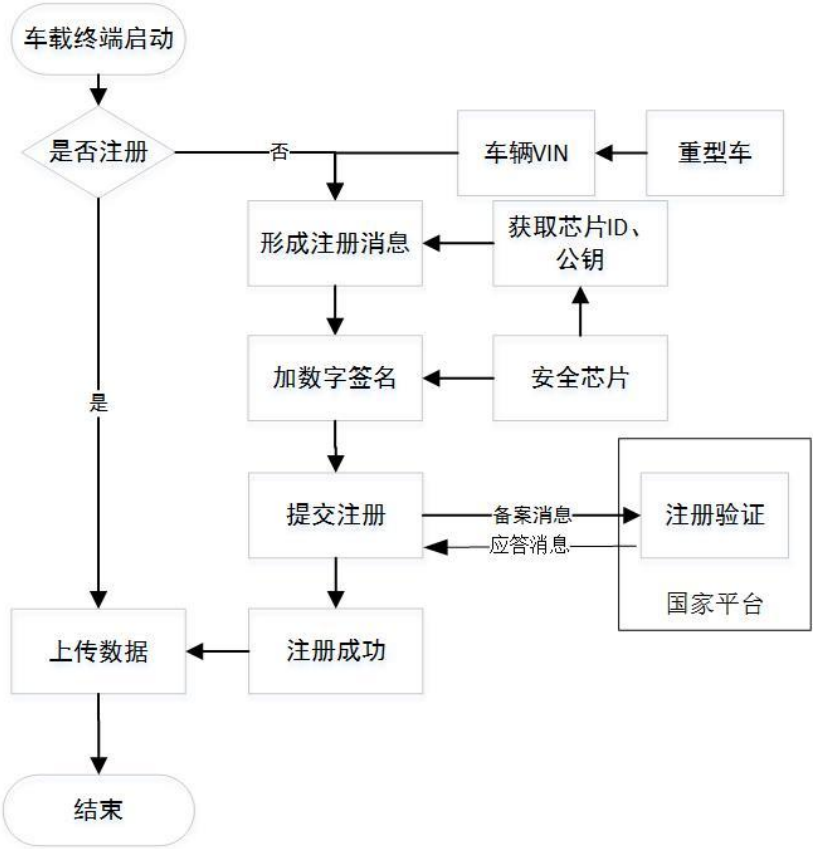

图 1 注册流程

5.3.4　车载终端应按HJ □□□□.4规定的协议接收国家平台下发的注册结果。

5.4　数据上传功能

5.4.1　终端注册成功后，将采集的数据添加数字签名，按HJ □□□□.4规定的通讯协议进行上传（如图2）。OBD信息至少24 h内上传一次，发动机数据流信息至少10 s上传一次。

5.4.2　第5.3.3和5.4.1规定的数字签名应遵循GM/T 0009规定的要求，每个完整的数据包进行一次签名，签名应使用保存在安全芯片中的私钥进行。

5.4.3　发动机启动后60 s内必须开始传输数据，发动机停机后可以不传输数据。

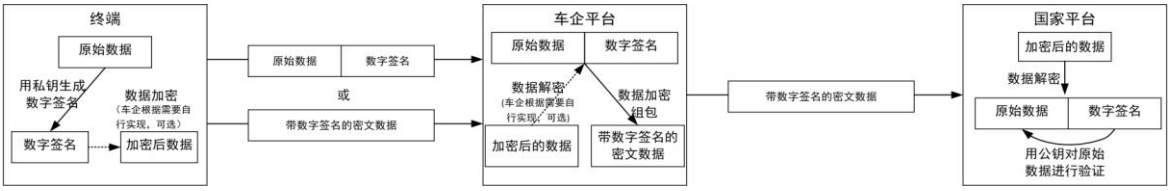

图 2 数据上传流程

5.4.4 安装在符合GB 17691—2005第五阶段的重型车上的车载终端，宜采用HJ □□□□.4规定的通讯协议进行数据上传。发动机数据流信息应至少30s上传一次，OBD信息应至少24 h内上传一次。

5.5 安全芯片要求

5.5.1 安装在符合GB 17691—2018的重型车上的车载终端安全芯片应具备一个唯一的标识ID。

5.5.2 安全芯片中应存储芯片ID和密钥（公钥和私钥），密钥应由安全芯片生产企业进行注册。芯片ID和公钥可以读取，私钥不可读不可改，应防止密钥泄露。

5.5.3 安全芯片生产厂家应具备完善的质量保证体系，通过ISO 9001质量管理体系和ISO 14001环境管理体系认证。

5.5.4 安全芯片安全等级应满足GM/T 0008安全等级2级要求，且应具备商用密码产品型号证书。

5.5.5 产品安全保证级别不低于EAL4+级要求。

5.5.6 安全芯片密钥长度应为256 bit。

5.5.7 通过安全芯片中的私钥进行数字签名的速度应不小于50 次/s。

5.6 数据补发

当数据通信链路异常时，车载终端应将上报数据进行本地存储。在数据通信链路恢复正常后，在发送上报数据的同时补发存储的上报数据。补发的上报数据应为恢复通讯时刻前5×24 h内，通信链路异常期间存储的数据，数据格式与上报数据相同，并标识为补发信息上报（0x03）。

5.7 数据存储

数据存储应符合GB 17691—2018 中Q.5.5的要求。

5.8 定位功能

车载终端应能提供GB/T 32960.3中规定的定位信息。精度要求应满足：

a) 水平定位精度不应大于5 m；

b) 最小位置更新率为1 Hz。

c) 定位时间：

1) 冷启动：从系统加电运行到实现捕获时间应不超过120 s；

2) 热启动：实现捕获时间应小于10 s。

5.9 防拆除功能

车辆生产企业应具有车载终端防拆除技术措施，确保车载终端不被恶意拆除。

当车载终端故障或拆除时，车辆应激活驾驶员报警系统，并尽可能向国家平台按照HJ □□□□.4规定的通讯协议发送拆除报警信息，报警信息包括拆除状态、拆除时间和定位经纬度信息。

5.10 安全策略

5.10.1 车载终端应按GB 17691—2018中 Q.4的要求提供技术可行的安全策略，保证产品各种性能和功能处于安全范围内。

5.10.2 车载终端应具备数据安全系统。

6 性能要求

6.1 按 GB 17691—2018 附录 Q.7 规定，车载终端的电气适应性能、环境适应性能和电磁兼容性能应符合 GB/T 32960.2 中 4.3.1-4.3.3 的要求。

6.2 可靠性性能

车载终端使用寿命应不低于10年。

6.3 盐雾防护性能

车载终端在参照GB/T 2423.18规定的严酷等级(5)进行四个试验循环后，正常功能应没有降低（例如，密封功能，标志和标签应清晰可见），功能状态应达到GB/T 28046.1定义的C级。

6.4 外壳防护性能

车载终端应至少满足GB/T 4208中规定的IP54的防护等级，对于安装在驾驶舱外的车载终端，应至少满足GB/T 4208中规定的IP65的防护等级，试验后车载终端所有功能应处于GB/T 28046.1定义的A级。

6.5 定位性能

6.5.1 仿真定位精度

首次定位时间：冷启动：TTFF≤120s；热启动：TTFF≤10s。

位置更新频率：车载终端应能自动、连续更新位置信息，频率至少为 1Hz。

6.5.2 整车导航定位精度

整车导航定位精度测试采用高精度（误差在2 cm以内）的RTK差分定位接收机作为基准，整车行驶时间超过15 min后，对车载终端的定位轨迹误差求平均值，在HDOP≤3或PDOP≤4的情况下，要求误差在5 m以内。

7 测试方法

7.1 终端测试内容

每个型号的车载终端，都应进行附录A规定的终端功能和性能测试，以及附录C规定的安全性测试，测试项目和测试方法见表3。

表3 终端测试内容

试验内容	技术要求	试验方法
连接检查	5.1	附录 A.3.1.1
时间和日期	5.1	附录 A.3.1.2
数据采集	5.1 和 5.2	附录 A.3.1.3
数据存储	5.7	附录 A.3.1.4
数据补发	5.6	附录 A.3.1.5
导航定位性能测试	5.8 和 6.5.1	附录 A.3.1.6
电气适应性	6.1	附录 A.3.2.1
环境适应性	6.1	附录 A.3.2.1
电磁兼容适应性	6.1	附录 A.3.2.1
可靠性	6.2	附录 A.3.2.2
盐雾防护性能	6.3	附录 A.3.2.3
外壳防护性	6.4	附录 A.3.2.4
信息安全测试	5.10	附录 C
卫星导航安全测试	5.10	附录 C

7.2 整车测试内容

每个型号的车载终端，应安装到整车上，进行附录B规定的整车远程监控测试，测试项目和测试方法见表4。

表4 整车测试内容

试验内容	技术要求	试验方法
通信直连测试	HJ □□□□.4	附录 B.4.1
通信转发测试	HJ □□□□.4	附录 B.4.2
整车导航定位精度测试	6.5.2	附录 B.4.5

8 实施要求

标准自发布之日起实施。

在GB 17691—2018标准6b阶段正式实施后，定位精度应满足GB 17691—2018规定的精准定位要求。

附 录 A

（规范性附录）

车载终端试验方法

A.1 概述

本附录规定了进行远程排放管理车载终端功能和性能检测的方法。

A.2 环境准备

提前准备4套车载终端、相应的线束及配套接插件等，1套用于验证车载终端各项功能的工具。

A.3 车载终端测试方法

A.3.1 功能测试

A.3.1.1 连接检查

车载终端接上电源后，按生产企业提供的产品说明书检查车载终端是否工作正常，并查看是否满足GB 17691—2018附录Q.5.1规定的自检功能，然后检查车载终端是否能正常连接到检测平台，并有数据上传到平台。

A.3.1.2 时间和日期检查

车载终端应能提供时间和日期。车载终端应能以时、分、秒或hh:mm:ss的方式记录时间；应能以年、月、日或yyyy/mm/dd的方式记录日期。与标准时间相比时间误差24 h内 ±5s。

A.3.1.3 数据采集检查

通过检测平台，检查上报数据频率、采集数据频率和数据内容是否满足GB 17691—2018附录Q.5.3、Q.5.4和Q.6.3的要求。

A.3.1.4 数据存储功能检查

检查车载终端的数据是否满足GB 17691—2018附录Q.5.5的要求。同时根据连续传输10 min的数据量来计算车载终端是否满足至少7天的存储要求。

A.3.1.5 数据补发检查

人为制造车载终端通信异常故障，之后恢复通信后通过检测平台查看是否有补发数据，且满足GB 17691—2018附录Q.6.4.5.5。

A.3.1.6 卫星导航定位性能仿真测试

A.3.1.6.1测试方法

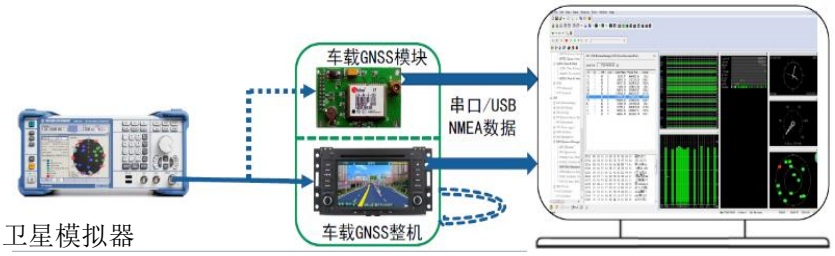

图 A.1 仿真测试示意图

仿真测试采用卫星系统GNSS模拟器，模拟器应可同时模拟产生最多24颗卫星动态信号，并支持模拟汽车路径规划，为了和真实环境中卫星数目比较接近，模拟7-8颗恒定载噪比（42~44）质量的卫星。

首次定位时间：从待测件开机开始计时，直至其定位正确停止计时。分别进行冷启动和热启动，得到两种模式下的启动时间。冷启动，需使待测件连续7天不加电；热启动，需使待测件正常工作情况下，断电60 s，再重新启动。

位置更新频率：待测件以文件形式输出定位结果，查看时间间隔为t，则位置更新频率为1/t。

A.3.1.6.2判定指标

a) 首次定位时间：

——冷启动：TTFF≤120s；

——热启动：TTFF≤10s。

b) 位置更新频率：更新频率≥1Hz。

A.3.2 性能测试

A.3.2.1 车载终端电气适应性能试验、环境适应性能试验和电磁兼容性能试验应按照GB/T 32960.2第5.2.1-5.2.3条要求进行。

A.3.2.2 可靠性试验

车载终端使用寿命应不低于10年，可靠性试验方法采用GB/T 32960.2附录A温度交变耐久寿命试验方法。

A.3.2.3 盐雾防护性能试验

车载终端盐雾性能按照GB/T 2423.18规定的严酷等级(5)的试验方法进行试验。

A.3.2.4 外壳防护性试验

车载终端按照GB/T 4208中规定的相应防护等级的试验方法进行。

附 录 B

（规范性附录）

重型车远程排放监控系统协议及定位测试

B.1 概述

本附录规定了车载终端数据通讯协议和平台间数据转发协议以及整车定位精度的检测方法。

B.2 环境准备

按以下要求进行测试环境的准备：

1）连接线：准备天线与功分器之间、功分器与基准接收机/待测件之间的连接线。

2）天线：准备接收卫星信号天线。

3）功分器：准备至少有两路输出的低损耗功分器。

4）基准接收机：确认基准接收机工作额定电压及供电方式；确保测试过程中存储基准路径数据并能够导出处理。

5）待测件供电：确认待测件工作额定电压及供电方式；确保测试过程中存储待测件解算路径数据并能够导出处理。

6）测试车辆：准备有足够空间及供电接口（或蓄电池）给基准接收机、待测件或功分器（有源）供电的测试车辆。测试车辆车顶能够安装卫星天线及与差分基站之间通信的通信天线，且配有相应的车载终端。

B.3 试验场地

在测试道路上布置RTK差分基站，供RTK差分定位接收机使用。RTK差分基站放置点经过测绘局测绘得到准确位置信息。在差分基站覆盖范围内，包含开阔场地及建筑物遮挡场地，测试车辆可做加减速、拐弯等行驶模式。

B.4 重型车远程排放监控系统通信及定位测试方法

B.4.1 直连测试

通过车辆点火进行登入登出（三次），数据补发，车辆行驶等测试步骤将数据直接上传到数据测试平台，进行数据校验，检测数据是否符合HJ □□□□.4中规定的协议格式。

B.4.2 转发测试

通过车辆点火进行登入登出（三次），数据补发，车辆行驶等测试步骤将数据上传到企业平台，再通过企业平台将数据转发到数据测试平台，进行数据校验，检测数据是否符合HJ □□□□.4中规定的协议格式。

B.4.3 整车导航定位精度测试

图 B.1 路测原理示意图

整车导航定位精度测试采用高精度（误差在2 cm以内）RTK差分定位接收机作为基准，测试车辆作为载体，车载卫星天线接收的卫星信号用功分器分配给基准接收机及待测件定位模块，以车速10~80 km/h在试验场地行车15min，待测件定位模块定位轨迹与基准接收机的定位轨迹作差，得到待测件定位模块的定位误差。对定位轨迹误差求平均值，验证是否满足规定指标。

附 录 C
（规范性附录）
车载终端安全性测试

C.1概述

本附录规定了GB 17691—2018附录Q.4安全策略以及本标准5.1.4导航定位安全的检测方法，本附录的检测方法满足GB 17691—2018的附录Q.7.7的测试要求。

C.2 样件准备

C.2.1测试样件能够上电运行，能够正常通讯。

C.2.2测试样件具备导航定位功能。

C.2.3测试样件能够输出或者通过远程查看入侵日志和入侵响应。

C.2.4测试样品能够实现SM2加密算法。

C.3渗透测试方法

C.3.1测试设备

渗透测试的设备如下：

1）异常指令发送设备；

2）信号连接设备；

3）测试控制电脑。

C.3.2测试方法

C.3.2.1审查生产企业提交的文档，检查车载终端是否具有对从管理平台接收的操作指令进行安全检测、并提供相应防护措施的机制。

C.3.2.2基于正常的获取排放及其相关数据要求，建立车载终端需要处理、来自管理平台的正常操作指令集，以及不少于100个样本的异常指令集，检测车载终端是否具有检测出其中95%以上异常指令的能力，且误报率能够小于1%、在攻击开始后10s内能够发现并启动防护措施。

C.3.2.3对车载终端进行安全检测，检测车载终端是否存在可能影响排放及相关数据在采集、存储与传输等环节的脆弱性。

C.3.3评价指标

C.3.3.1响应时间：被测样件输出第一条检测到的异常指令，如在攻击开始时间后10s（包含10s）以内，测试通过；大于10s或者未检测到异常指令，测试失败。

C.3.3.2被测样件输出全部检测到的异常指令，如检测出异常指令比例大于（包含）95%测试通过，如否，测试不通过。

C.3.3.3在满足C.3.3.2的情况下，比对检测结果与异常指令对应情况，如果正确率大于（包含）99%测试通过，否则测试失败。

C.4导航定位安全性测试方法

C.4.1测试设备

导航定位安全性测试设备如下：

1）导航定位信号模拟设备；

2）信号模拟设备被测样件连接线；

3）交换机；

4）干扰信号模拟设备；

5）控制电脑；

6）结果记录电脑。

C.4.2测试方法

C.4.2.1待测样件在特定干扰信号功率水平条件下，持续保持定位信息的连续输出，测试验证终端是否具备一定的抗干扰能力。特定干扰信号至少包含GNSS同频点单音干扰信号。

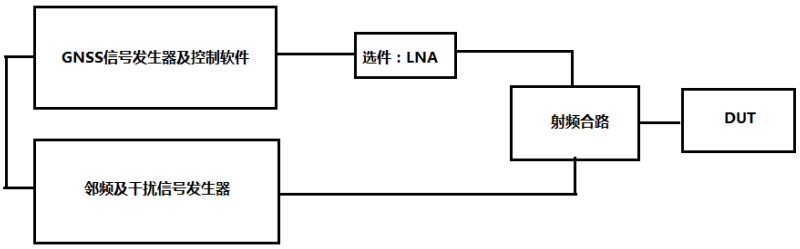

图 C.1 干扰测试拓扑

C.4.2.2带 GNSS功能的车载终端在接收到卫星段的异常信号时，检查接收机能否正确响应。

C.4.3评价指标

C.4.3.1被测样件在特定干扰条件下导航定位信号信噪比均值变化小于5%测试通过，否则测试不通过。

C.4.3.2被测样件在特定星数且含有欺骗卫星信号条件下的定位位置与真实位置的差值的绝对值小于1米，测试通过，否则测试不通过。

C.5密码算法实现安全性测试方法

C.5.1测试设备

密码算法安全性测试设备如下：

1）侧信道信号采集分析系统；

2）高级示波器；

3）电磁采集探头；

4）故障信号注入系统；

5）电磁辐射发生器；

6）电磁场探头；

7）测试结果记录电脑。

C.5.2测试方法

C.5.2.1 检测厂家提供设计和说明文件或相关国密认证证书。

C.5.2.2 通过SM2算法验签工具，使用厂家声明的密码算法对至少100条凭证信息添加数字签名。通过接口测试验证其国密算法SM2使用正确性；由测试送样人员提供公钥、签名R值、签名S值、签名使用的ID及签名后数据。

C.5.2.3 通过侧信道采集分析系统借助电磁采集探头对样品签名处理及传输过程进行侧信道分析监听或破解，查看签名内容是否在加密硬件内进行，如是则测试通过，否则测试不通过。

C.5.3评价指标

C.5.3.1 样品的芯片如具备GM/T 0008 规定的安全等级第2级的检测报告复印件，且样品具备商用密码证书复印件则通过检测，否则不通过。

C.5.3.2 参加验签的数据正确率不低于99%则检测通过，否则不通过。

C.5.3.3 测试样品使用硬件加密，且无法获得加密芯片私钥测试通过，否则不通过。