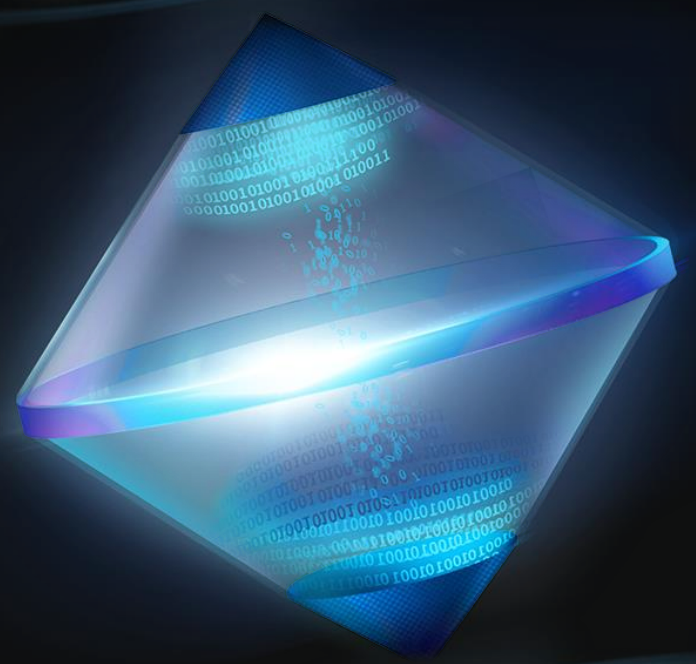
KCon

归源·智变

Returning to the source · Intelligent transformation

梅赛德斯.奔驰车机安全研究



演讲人：王启泽

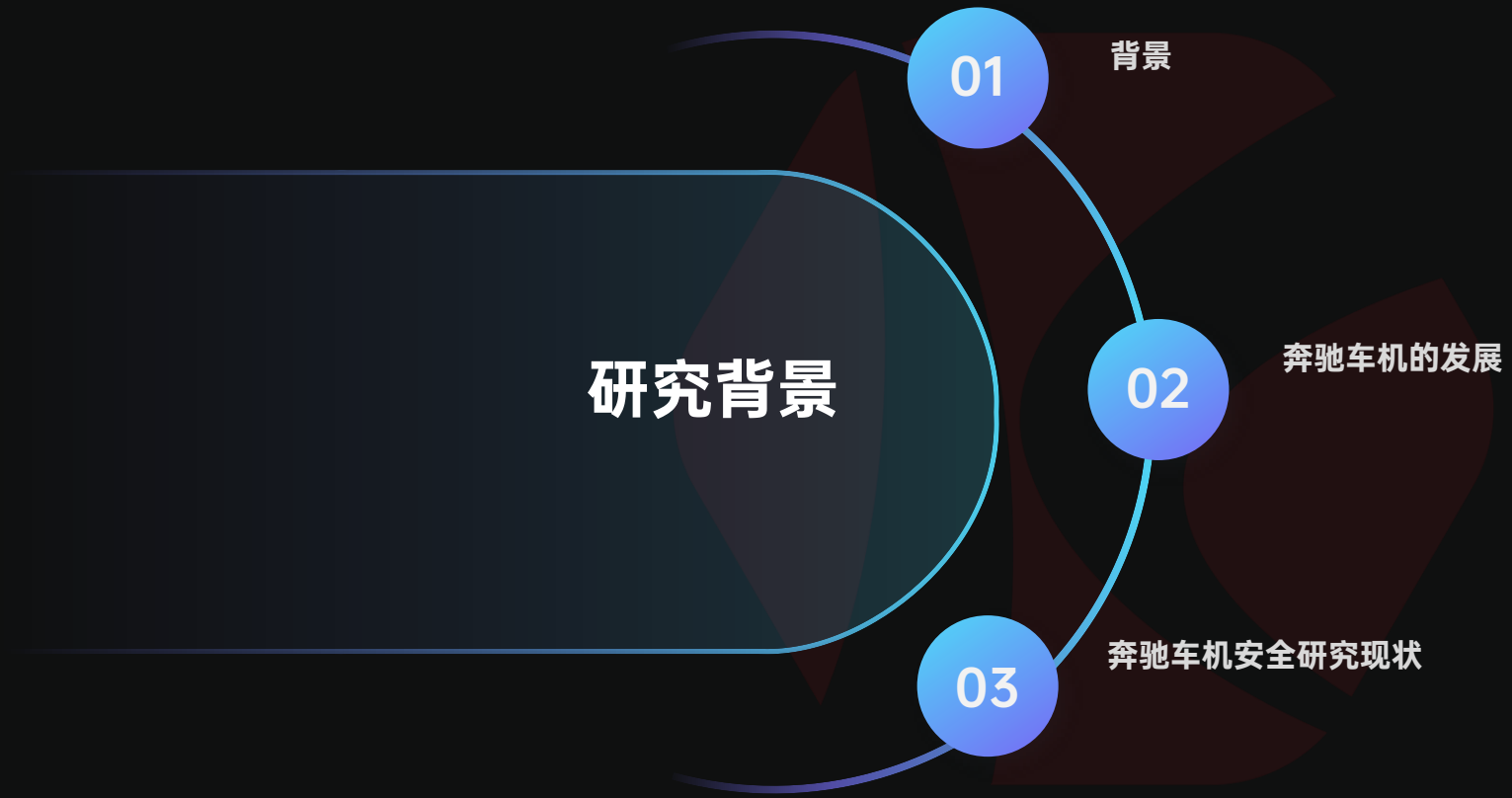
KCon

归源 · 智变

Returning to the source · Intelligent transformation

目录 / CONTENTS

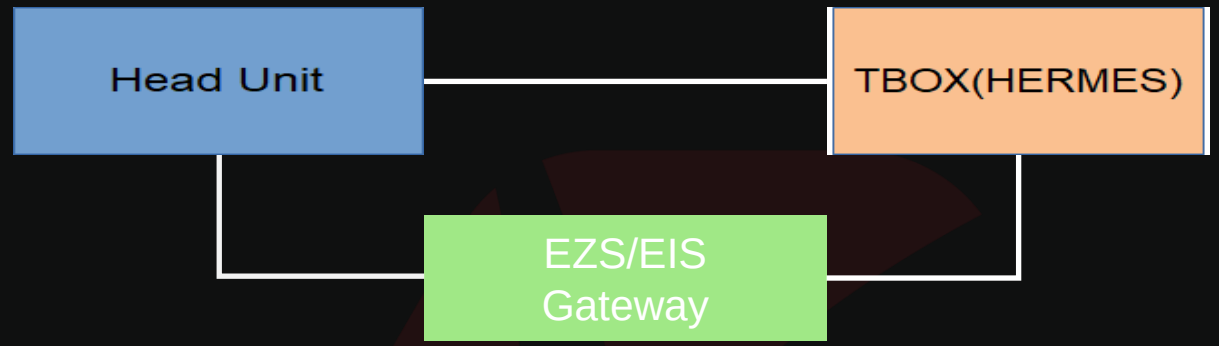
背景



汽车-时尚.科技

汽车信息安全

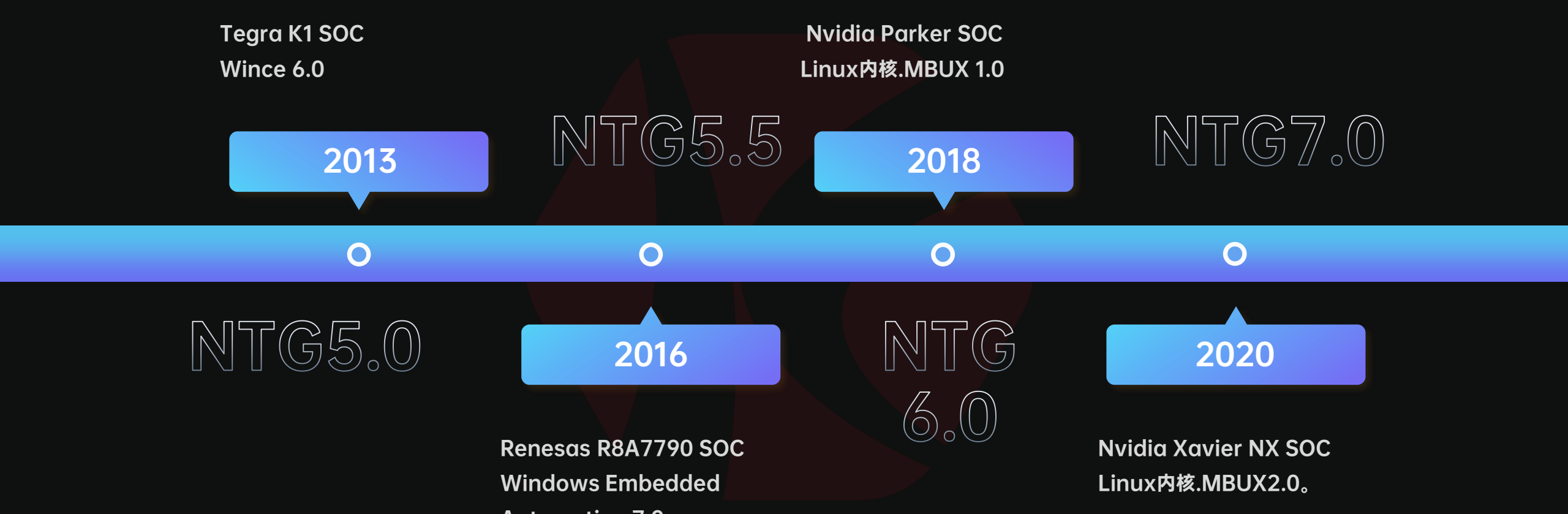
之前的研究



01 2020年360汽车安全团队发布了HERMES 1.1~2.1版本的研究成果。

2021年腾讯科恩实验室发布了HeadUnit6.0主机的研究成果。 02

奔驰车机的版本发展


Tegra K1 SOC
Wince 6.0
NTG5.0
2013
NTG5.5
2016
Renesas R8A7790 SOC
Windows Embedded
Automotive 7.0
Nvidia Parker SOC
Linux内核.MBUX 1.0
NTG 6.0
2018
NTG7.0
2020
Nvidia Xavier NX SOC
Linux内核.MBUX2.0。

奔驰车机发展迭代

HU5.5

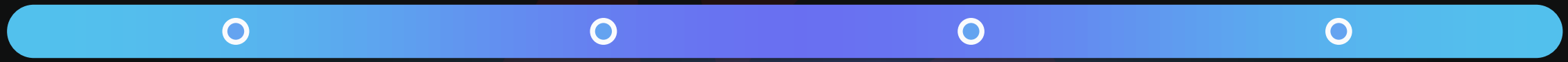
HU6.0

HU7.0

车机的安全防护

安全防护

这种加密及防护机制在那个时代是不多见的。



01

防盗及唤醒机制

02

磁盘加密

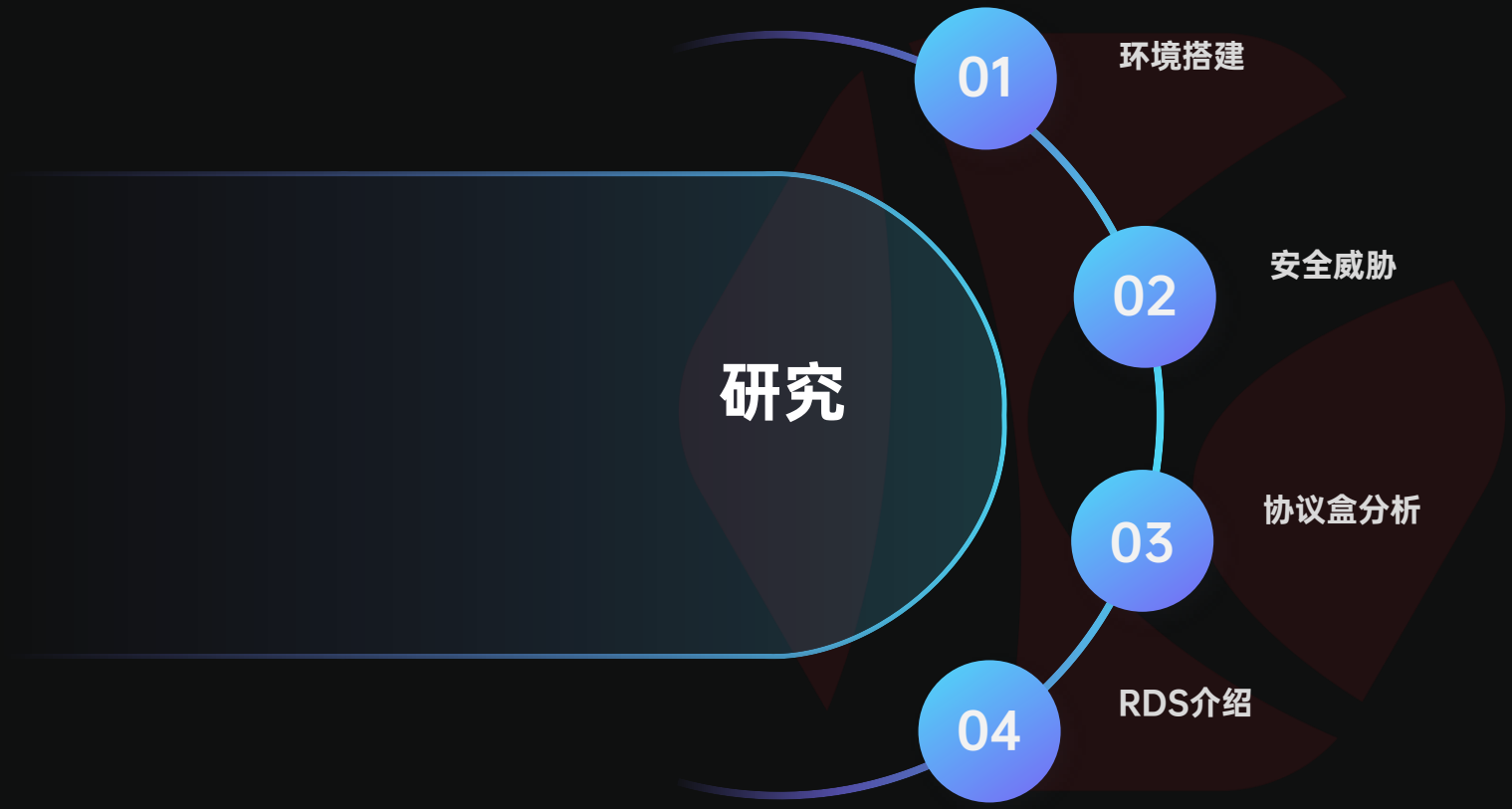
03

安全启动及
硬件加密

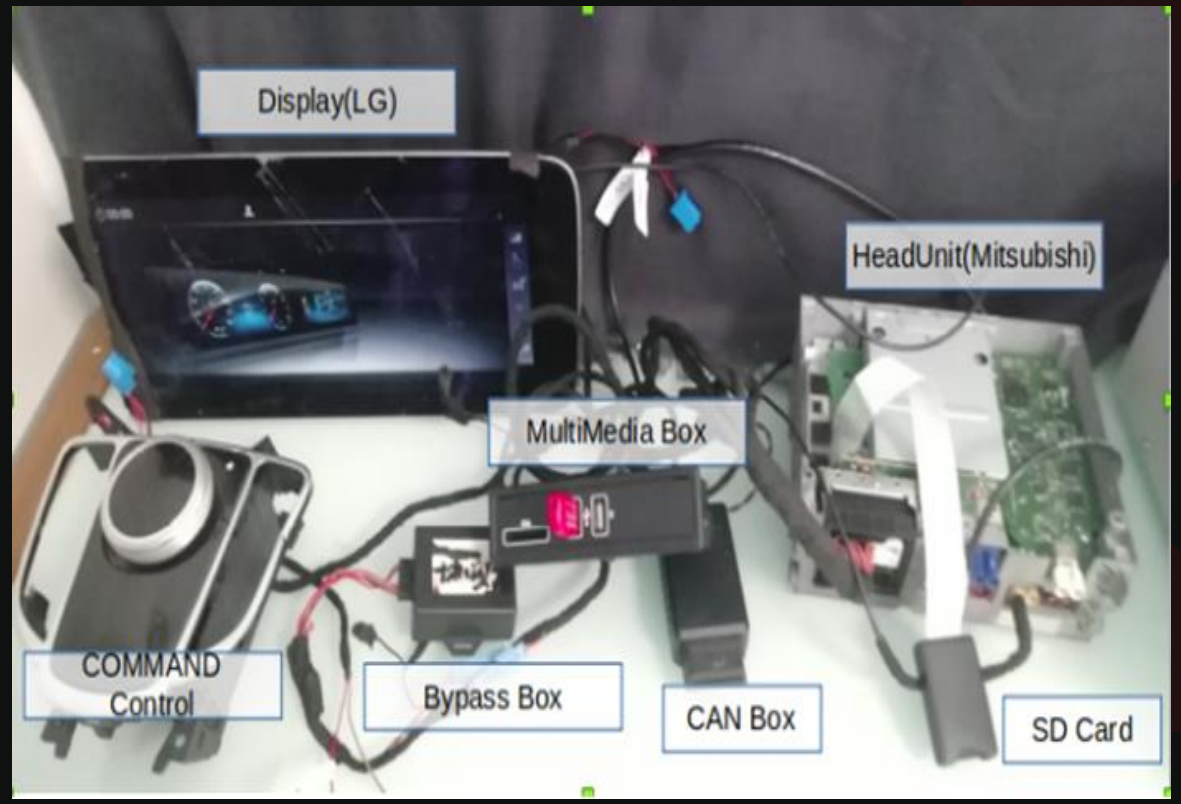
04

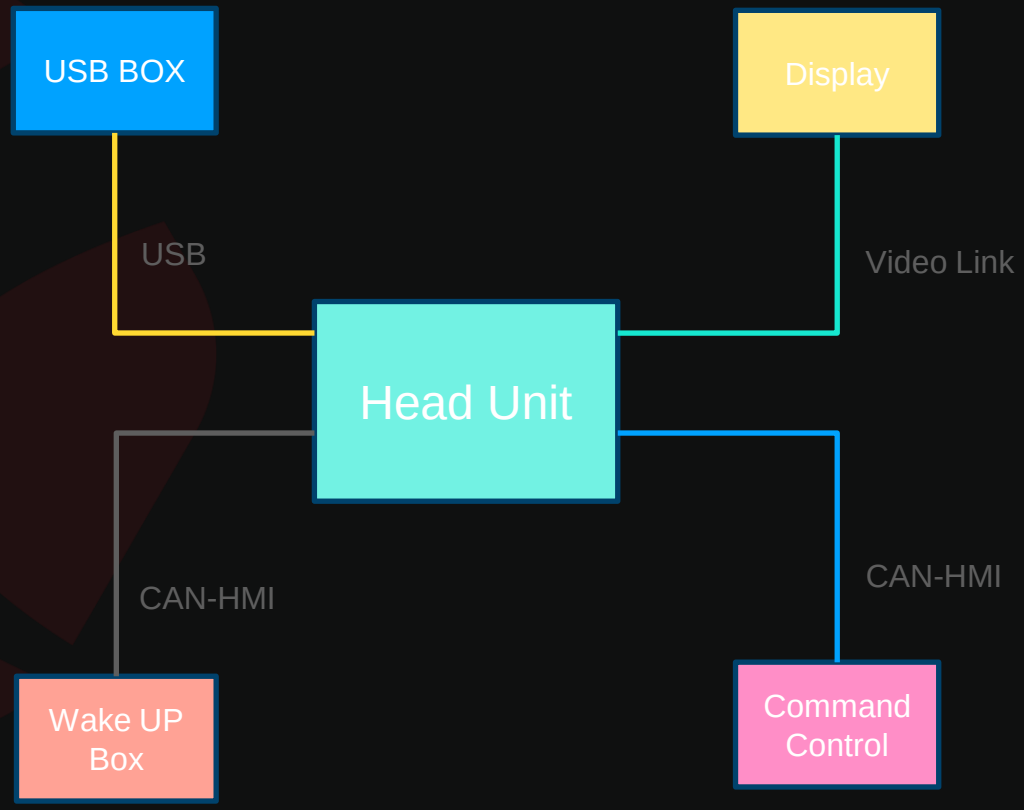
SD卡加密

研究



测试台搭建

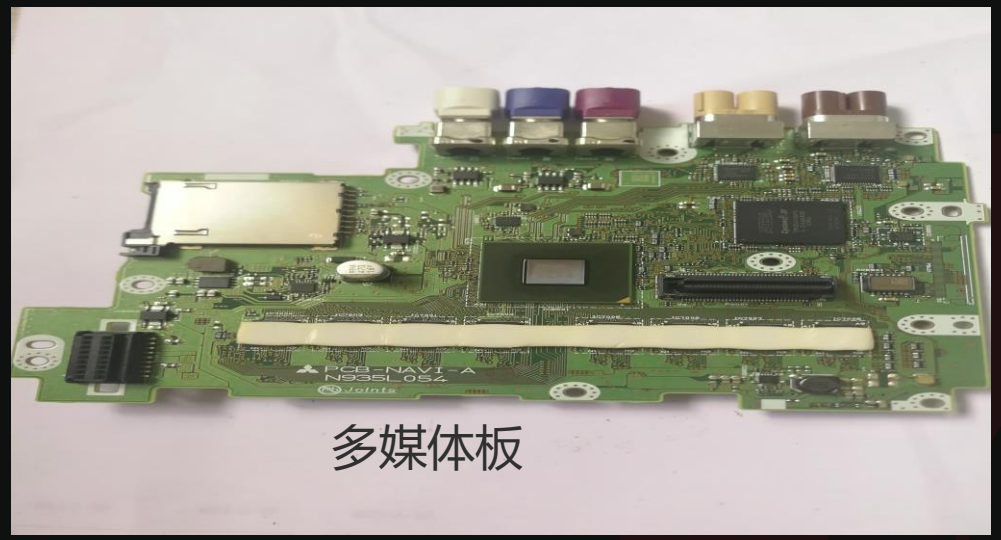

Display(LG)
HeadUnit(Mitsubishi)
MultiMedia Box
COMMAND Control
Bypass Box
CAN Box
SD Card


USB BOX
Display
USB
Video Link
Head Unit
CAN-HMI
CAN-HMI
Wake UP Box
Command Control

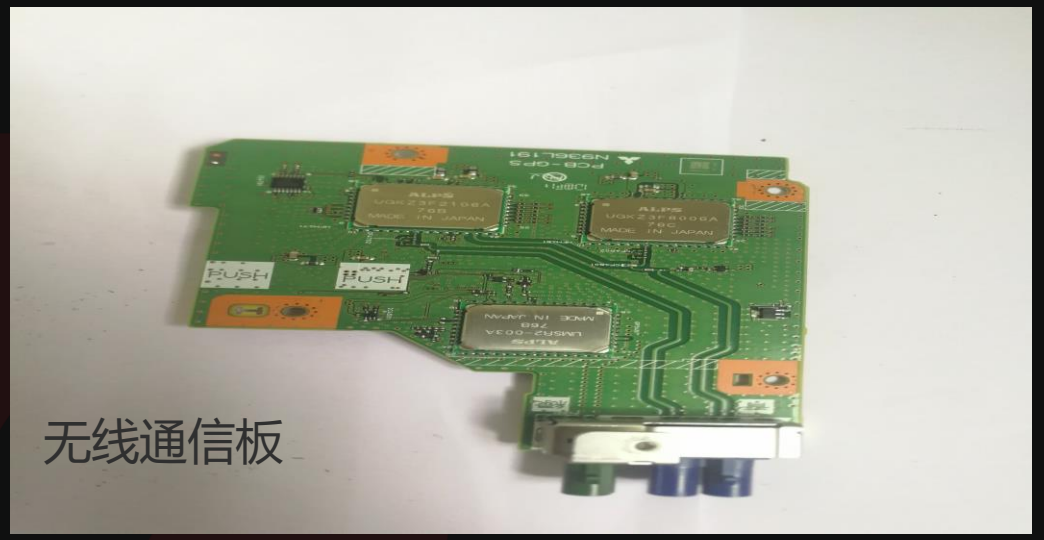
HU5.5车机外观


Mercedes-Benz
A 213 900 5219 / 001 Q1
HEADUNIT A-HIGH ECE
12V NEG GND MODEL : NR-213
MADE IN JAPAN
TRA
REGISTERED No.
ER40913/15
DEALER No.
DA0088122/12
OMAN-TRA
Connection and use of this communications equipment is permitted by the Nigerian Communications Commission
R-NZ
CE1731

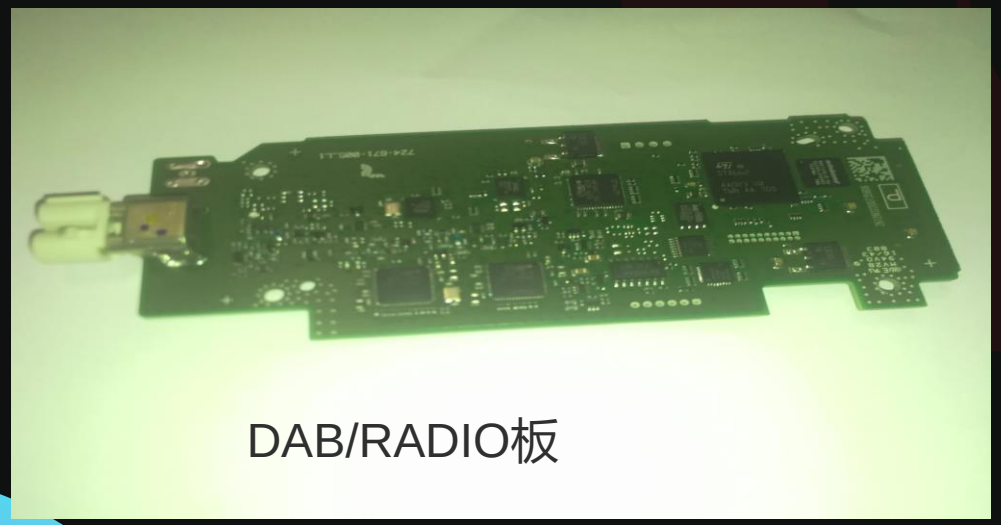
车机硬件模块



多媒体板



无线通信板



DAB/RADIO板

主板

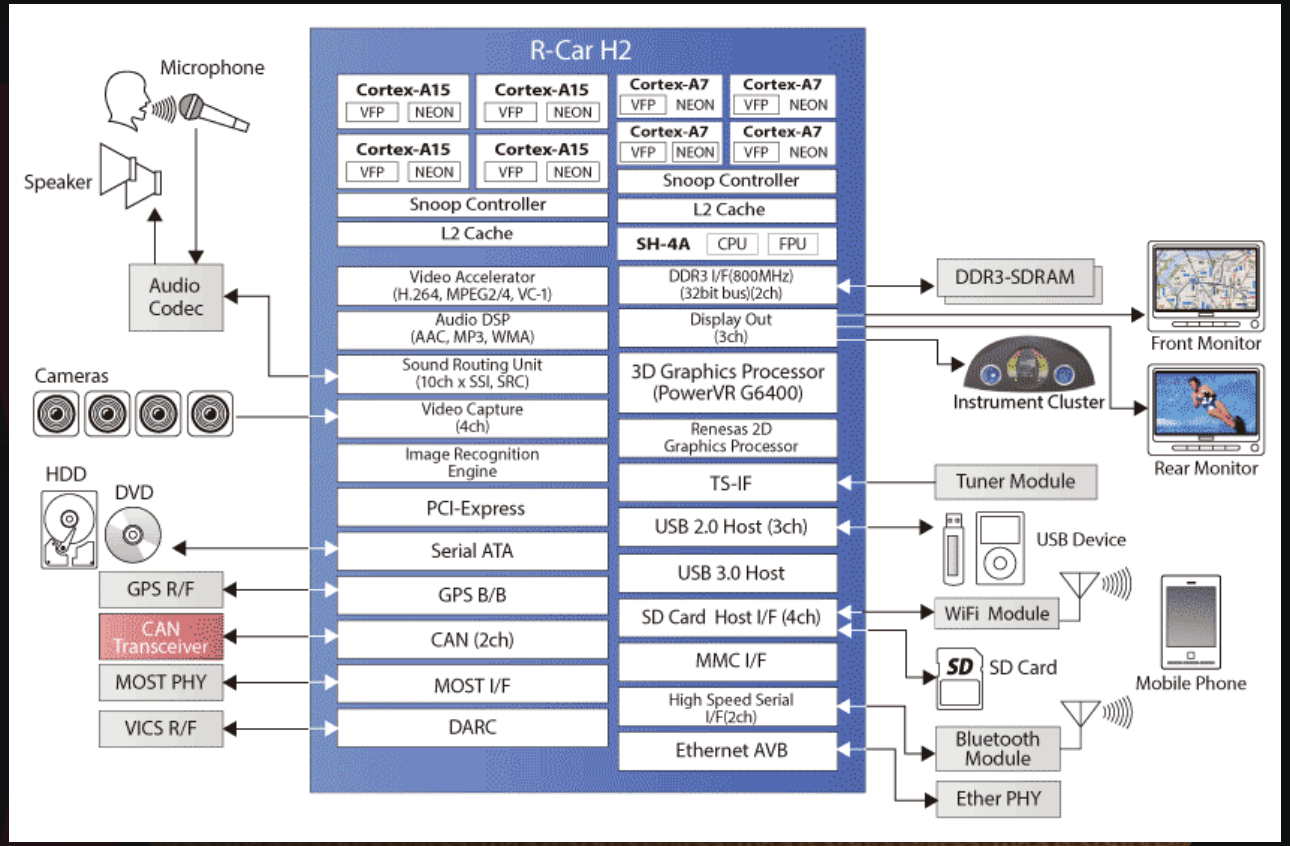
车机SOC

RCar-H2 SOC

Renesas(瑞萨) R8A7790，集成了SATA、GPS、CAN、SD、VIDEO、3D、USB、Ethernet、硬件加密

CPU架构

ARM 四核-A15，ARM 四核-A7，SH-4A(自研架构)



SD 卡介绍

SD卡协议

SD卡支持三种协议。

SD SPI、SD/UHS1、UHS2

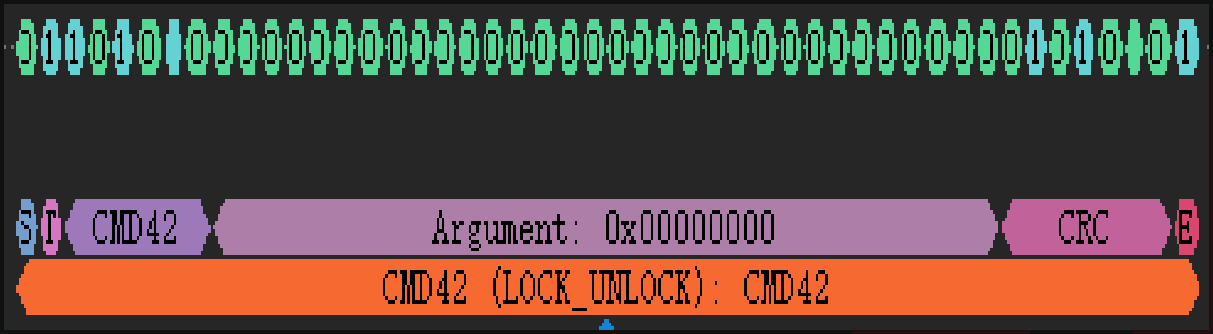
主要存储

存储背景图片、通讯录、本地化UI脚本、配置文件

加密保护

该SD卡是加密的，具体的算法是厂家自定义算法。系统启动时才动态加密。

SD 加/解锁命令介绍



Byte #	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Reserved (shall be set to 0)				ERASE	LOCK_ UNLOCK	CLR_ PWD	SET_ PWD
1	PWDS_LEN							
2	Password data							
...								
PWDS_LEN + 1								

功能

CMD42命令为SD卡设置密码，清除密码及解锁密码使用。

交互过程

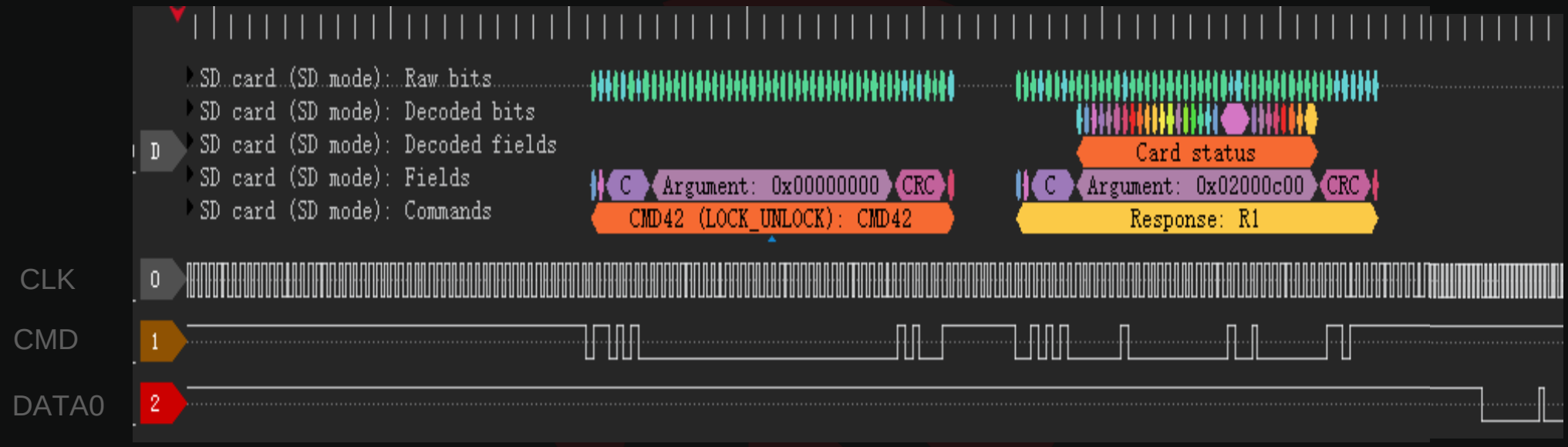
主机传送CMD42命令到SD卡。SD卡返回卡片状态。

主机传送后续的密码到SD卡，SD卡返回验证结果。

问题

密钥明文传输

逻辑分析仪



DATA0: BYTE0: 0000 0000 (bit2, unset, UNLOCK)
BYTE1: 0001 0000 (长度16)

车机SD卡目录结构

Air-HMI

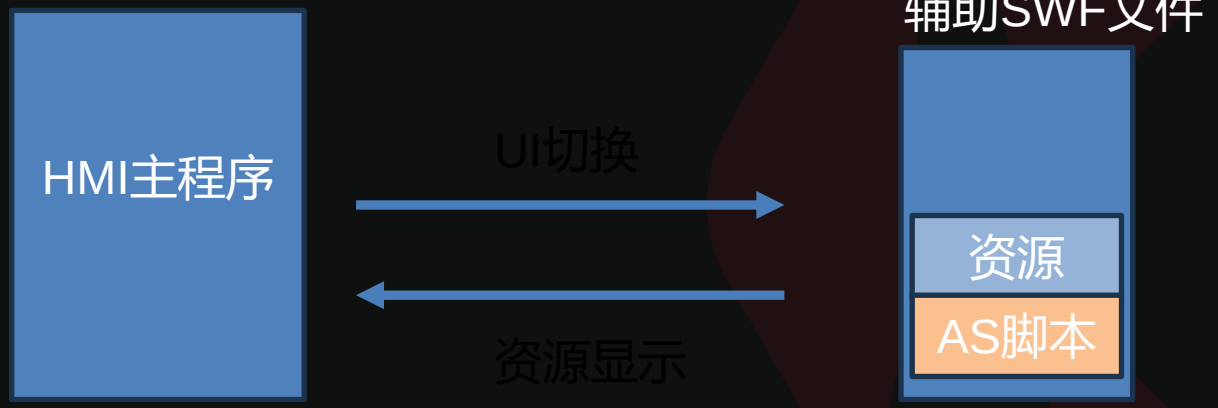
主要的UI程序

配置信息

浏览器、CarLife、无线、通信录

```
1|HWMHA:/data/data # ls /mnt/ext_sdcard/
Air-HMI                  DIAG       MLINK                        TTS
Android                  DTV        NBACKUP_FILE_FORMAT_VERSION  UAPApp
BIN                      Dictation  Others                       VCARD
BROWSER                  FIM        PartNumber                   VsIcc
Backup1                  HMI        Radio                        font
Backup2                  HMIManager RamdiskCache_ZIP             sms
CARPLAY                  HandsFree  SDS                          sysd
CarLife                  ICD        SD_SMB                       ucdef.dat
CommManager              ICO        SideA
CompatibilityInformation LOST.DIR   SideB
```

SWF文件



HMI主程序

每次启动时是从主磁盘中加载的。

辅助文件

启动时从SD卡中加载。

主机系统信息

磁盘

SD、UH30、RAMDISK、RAMDISK2ND、RAMDISK3RD、HDD、 HDD2 ~ HDD9

Wifi及蓝牙模块

CSR8311A12

CSR8311A08

网络接口

MEPV, NDCUFMP1, NDCUFMP4

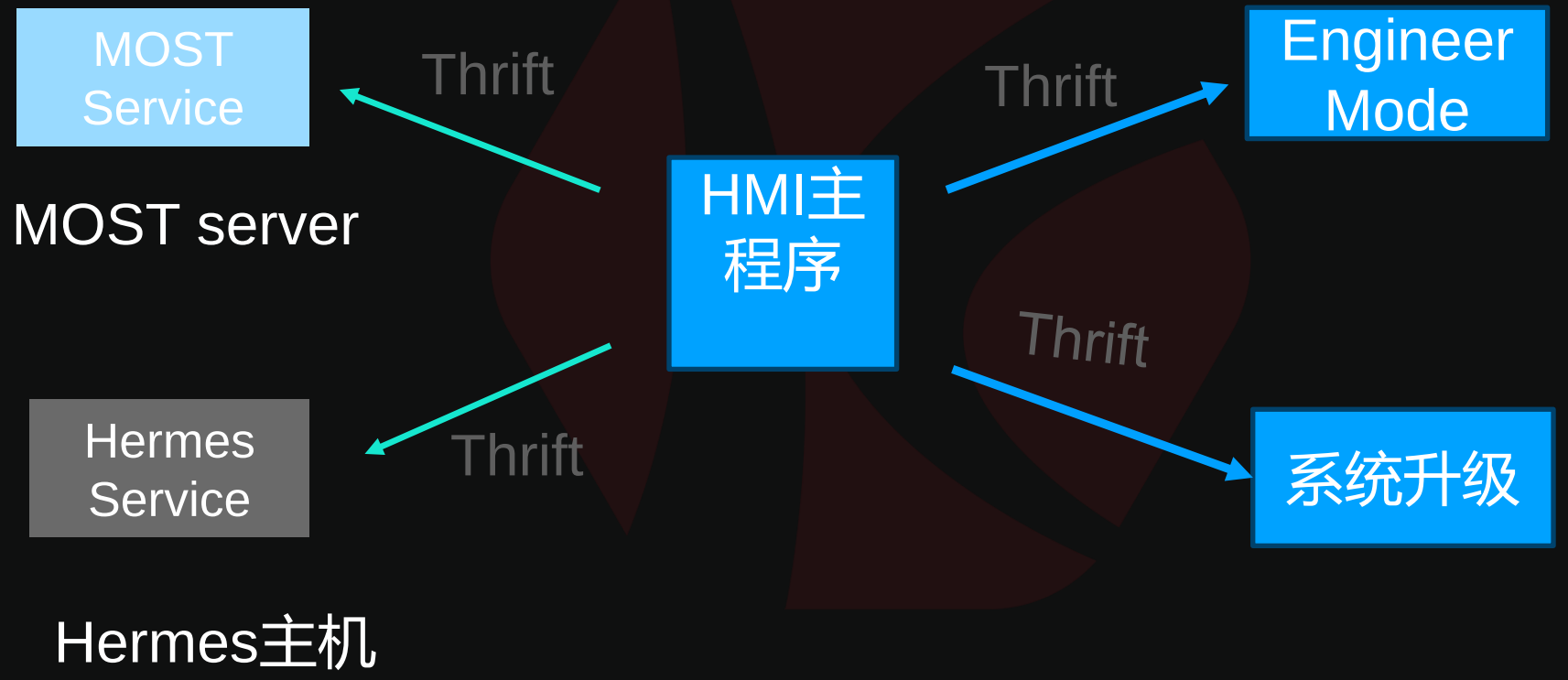
169.254.138.202,192.168.221.1(MGW), 192.168.220.1(HGW)

软件系统

系统：WINCE7.0

HMI： FLASH

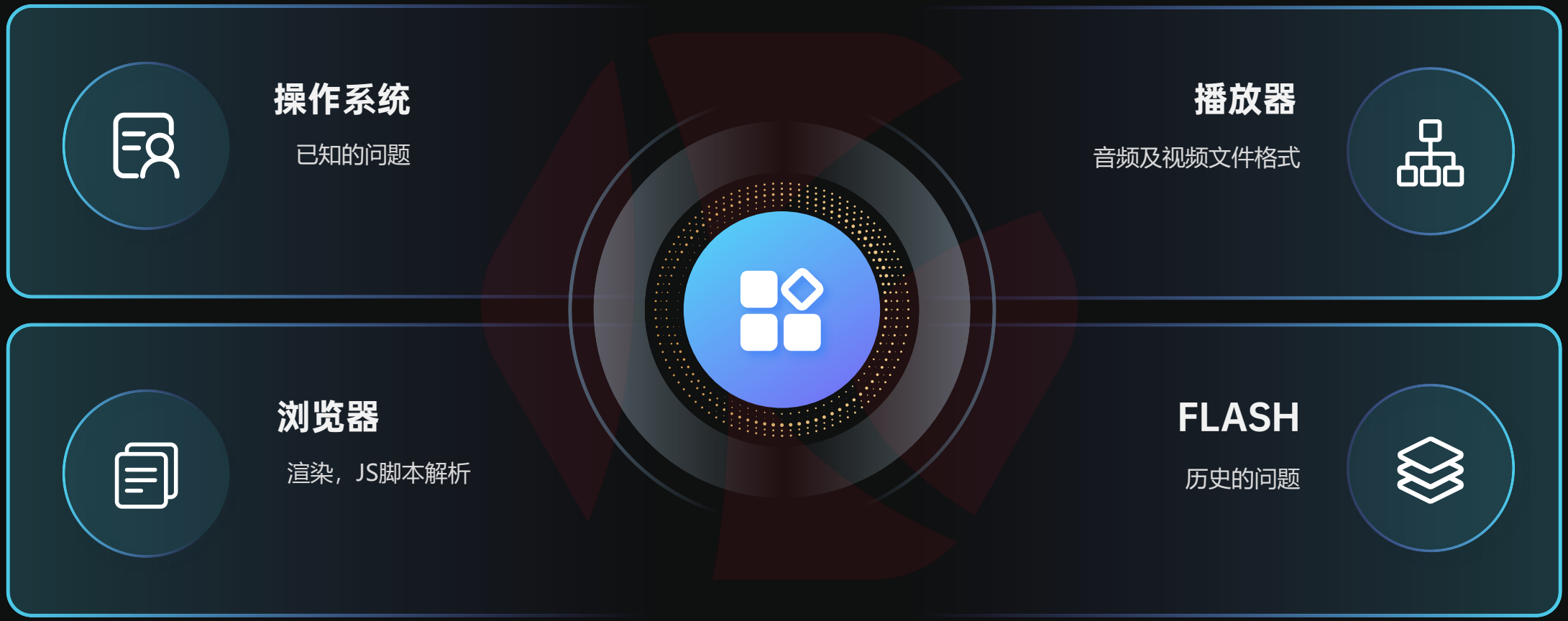
模块间调用


MOST Service
Thrift
Thrift
Engineer Mode
HMI主程序
Thrift
Thrift
Hermes Service
系统升级
MOST server
Hermes主机

调用工程模式


Engineering Mode
1. HU Information
2. MOST Information
3. History Information
4. SW Setting
5. HW Setting
6. Update
7. System Reset
End

安全威胁



第三方协议盒的功能

解防盗功能

如果定时没有收到CAN信号，则车机告警并停止工作。

唤醒功能

如果没有开机的时候没有收到CAN信号，则停止输出信号。

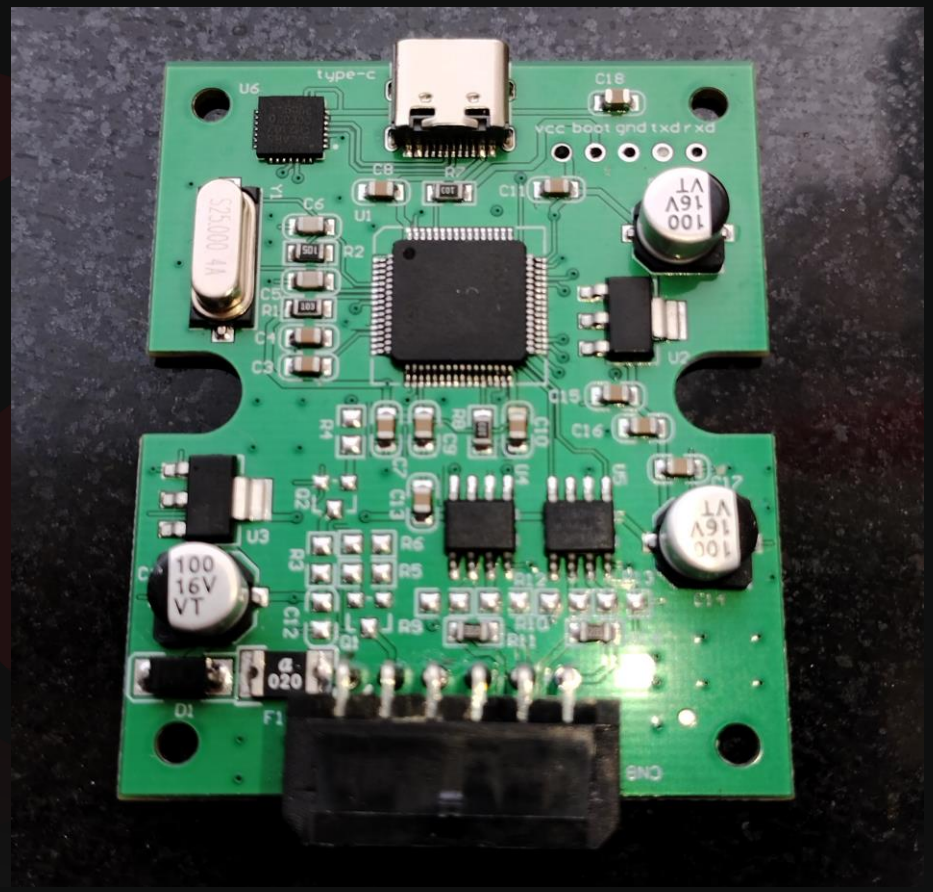
第三方协议盒拆解

STM32F105芯片

提供两路CAN接口

开放的调试口

VCC, BOOT, GND, TXD, RXD



CAN报文分析及自制协议盒

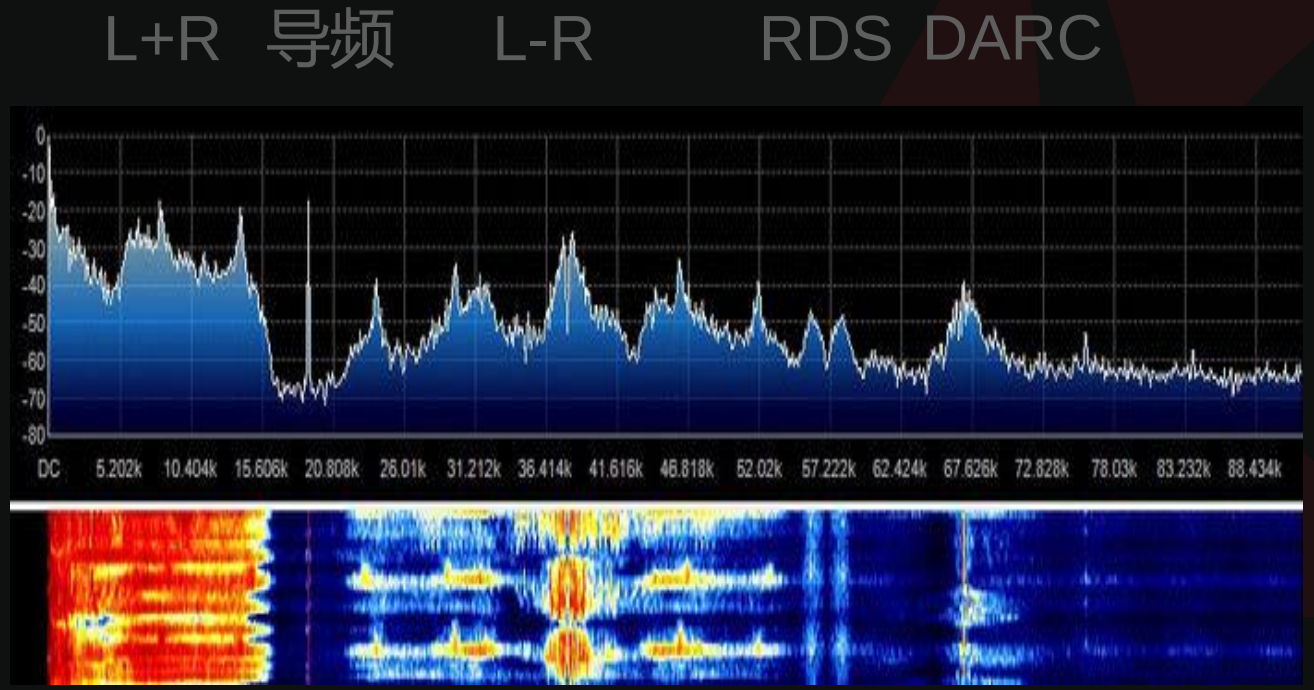
相关的CAN命令

共32条命令

复现协议盒

利用正点原子开发板的一路CAN接口

RDS介绍



无线数据广播系统

调频电台波段在87.5MHZ~108.0MHZ， 电台每个波段间隔100KHZ, 其中53KHZ用于传输音频信息。53K~100KHZ可以用于附加信息传递。

原理

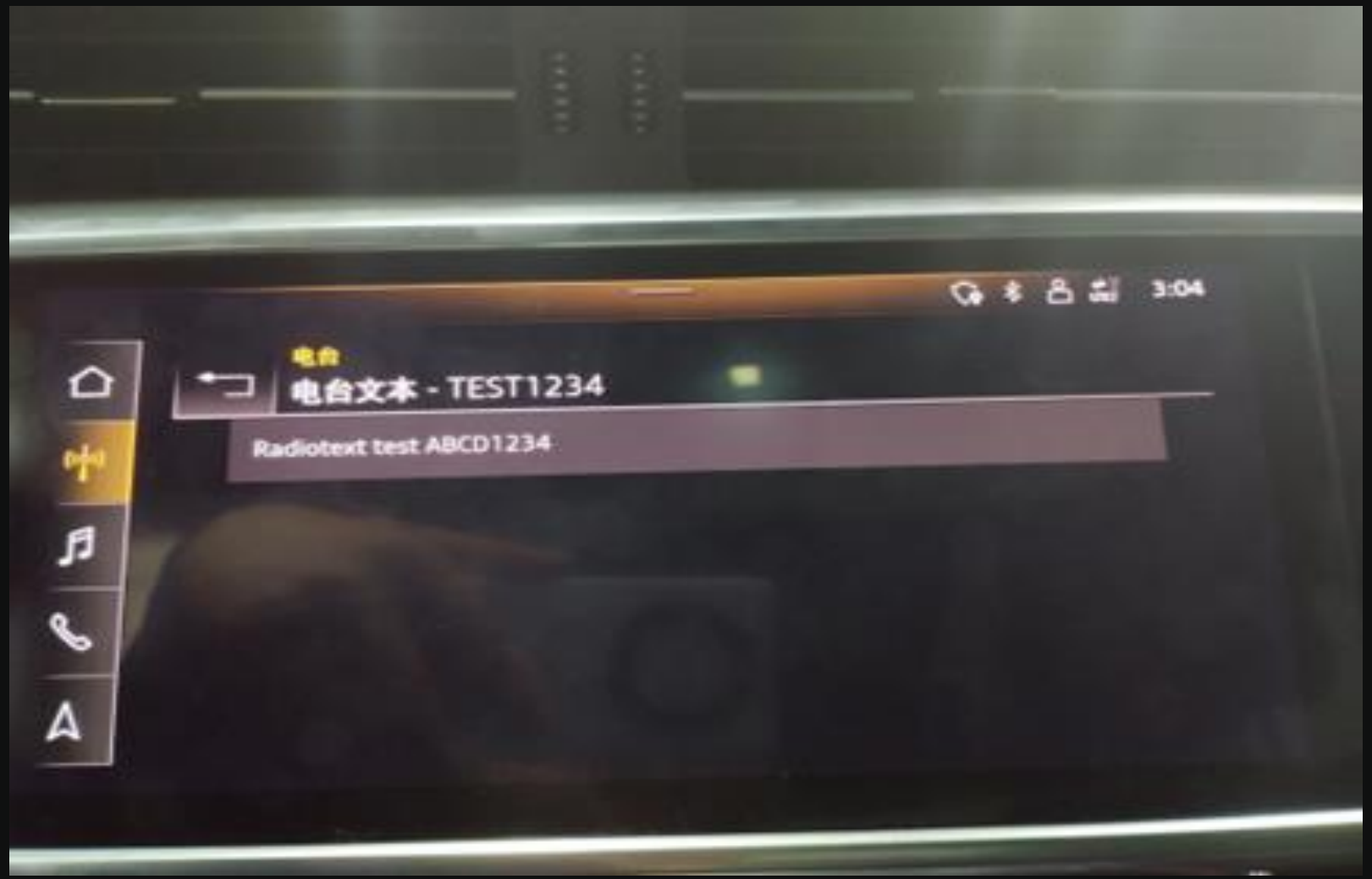
RDS系统是在商用调频发射机的57 kHz副载波上调制的双边带信号承载信息。

功能

RDS用于发送时间、无线电节目文本数据、节目类型、GPS位置、交通信息（TMC）等数据。

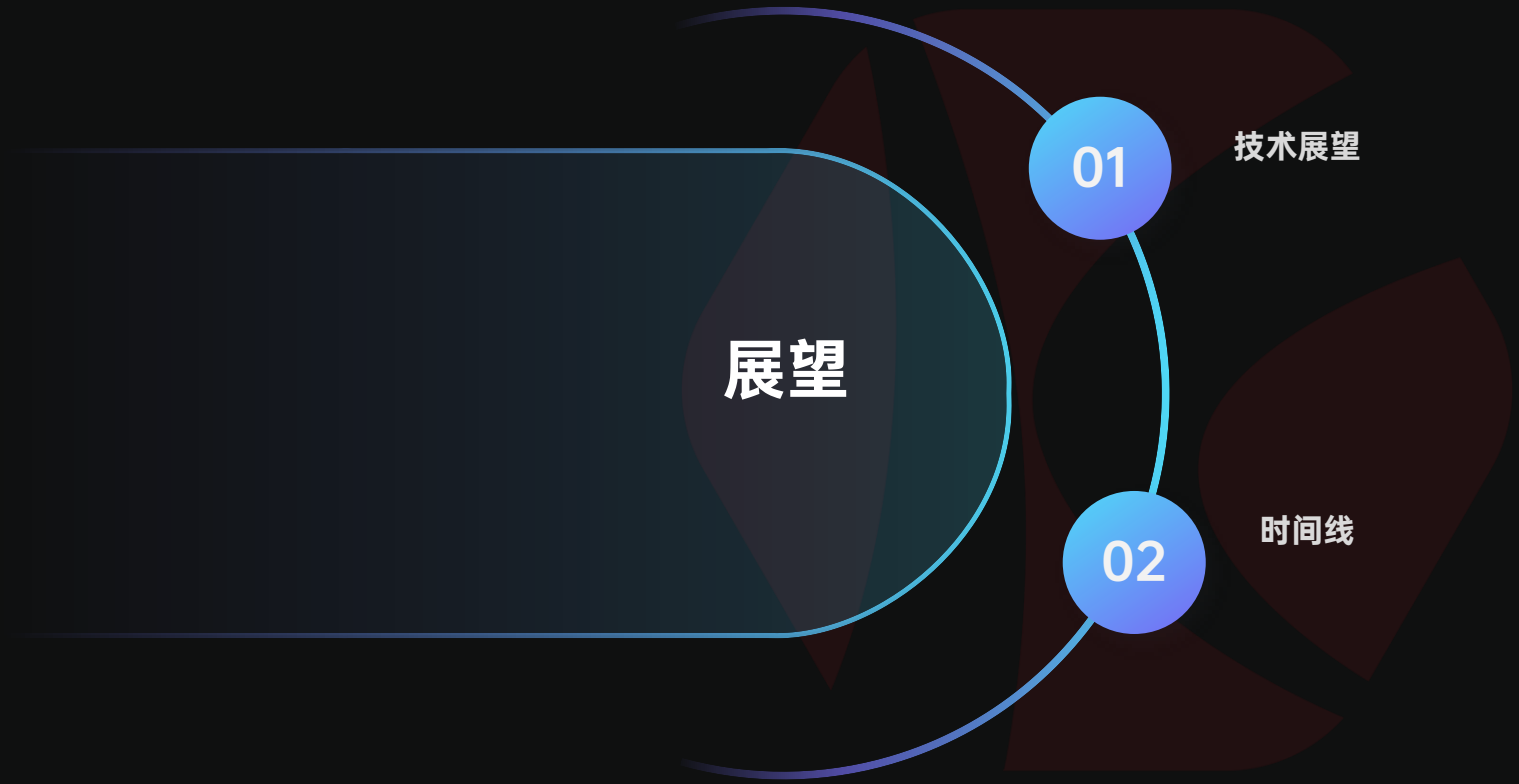
RDS-电台名称

RDS-电台文本

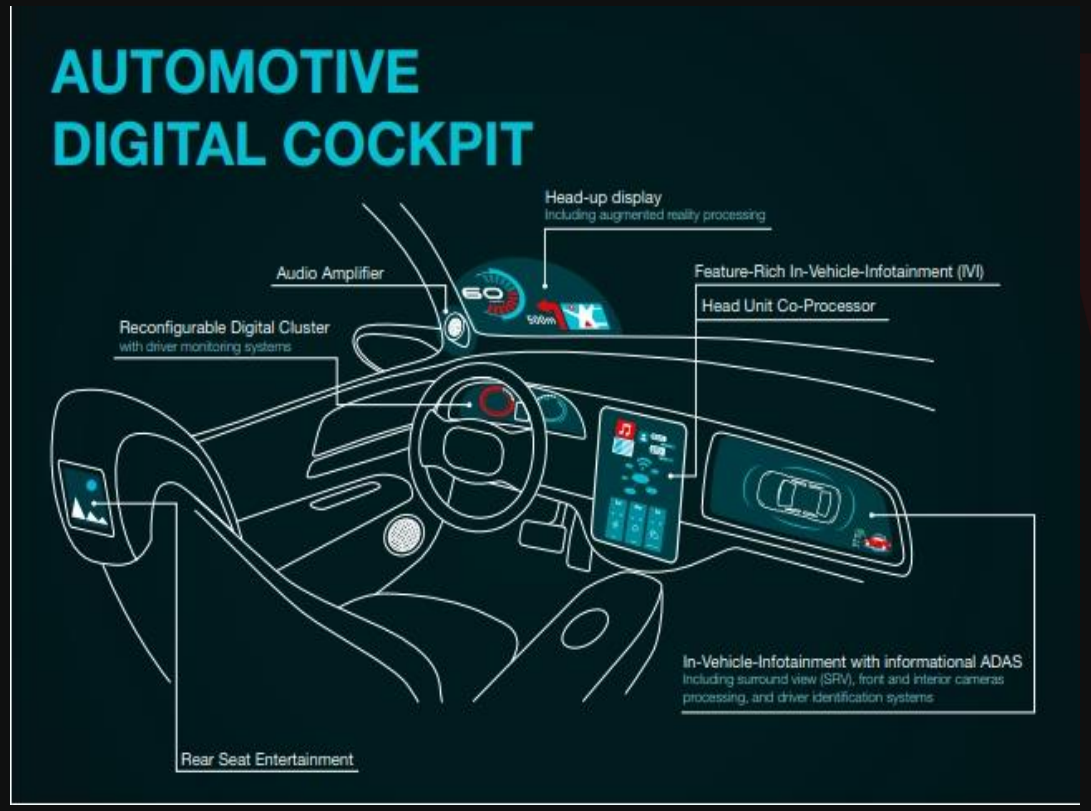


RDS-TMC

展望



智能座舱



图片来源： https://www.ti.com/lit/wp/spry307/spry307.pdf

云服务		
驾驶舱系统	娱乐系统	其他系统
感知交互		
应用软件系统层		
中间件		
虚拟层		
Linux/Android/QNX	TEE	
智能座舱芯片(SOC, SE, GPU)		

展望

新技术越来越应用到汽车上，汽车智能化，网联化发展。智能汽车将在我们的生活中扮演越来越重要的地位。

监管

监管的挑战

用户隐私保护、数据安全保护的监管需要

智能

新技术的挑战

时间线


时间线
2022.8
发现安全问题
2022.9
提交梅赛德斯.奔驰公司
2022.12
问题确认及修复
2023.8
KCON大会

KCon

归源·智变

Returning to the source · Intelligent transformation

感谢您的观看！

THANK YOU FOR YOUR WATCHING