|  |  |  |
| --- | --- | --- |
|  | ## | |
| ## | |  |
|  | |  |
|  | | | | | | |
|  | | | | | | |
|  | | | | | | |
| 团 体 标 准 | | | | | | |
|  | | | | | | |
|  | | | |  |  |  |
|  | | | |  | T/CSAEXX－20XX |  |
|  | | | |  |  |  |
|  | | | | | | |
|  | | | | | | |
| 车控操作系统功能安全要求 | | | | | | |
| **Functional safety requirements for**  **vehicle-controlled operating system**  Drafting guidelines for commercial grades standard of Chinese medicinal materials | | | | | | |

|  |  |  |
| --- | --- | --- |
|  | | |
|  | | |
| XXXX-XX-XX发布 |  | XXXX-XX-XX实施 |
|  | | |
| 中国汽车工程学会 **发布** | | |

目 次

[前 言 III](#_Toc5811)

[车控操作系统功能安全要求 4](#_Toc23204)

[1 范围 4](#_Toc12211)

[2 规范性引用文件 4](#_Toc1233)

[3 术语和定义 4](#_Toc9153)

[4 车控操作系统安全假设 5](#_Toc23176)

[4.1 范围假设 5](#_Toc28704)

[4.1.1目的 5](#_Toc25465)

[4.1.2边界范围 5](#_Toc1853)

[4.1.3目标环境 5](#_Toc5112)

[4.1.4功能属性 5](#_Toc29026)

[4.2 安全假设 5](#_Toc19268)

[5 车控操作系统安全要求 5](#_Toc12396)

[5.1功能软件安全要求 5](#_Toc3322)

[5.1.1环境模型 5](#_Toc26096)

[5.1.2规划模型 7](#_Toc5914)

[5.1.3控制模型 7](#_Toc30632)

[5.1.4基础服务 7](#_Toc16718)

[5.1.5数据流框架 7](#_Toc3102)

[5.1.6数据抽象 7](#_Toc14163)

[5.1.7应用软件接口 7](#_Toc18935)

[5.2 系统软件安全要求 7](#_Toc28591)

[5.2.1POSIX及其他接口 7](#_Toc22092)

[5.2.2实时安全域 7](#_Toc2332)

[5.2.3系统中间件及服务 7](#_Toc13027)

[5.2.4系统软件工具链 7](#_Toc19541)

[5.2.5操作系统内核 7](#_Toc25437)

[5.2.6虚拟化管理及板级支持包 7](#_Toc15645)

[6 车控操作系统验证和确认 7](#_Toc14470)

[6.1安全验证要求 7](#_Toc15550)

[6.2安全确认要求 8](#_Toc23403)

[7安全集成要求 8](#_Toc4441)

[附 录 A 9](#_Toc15845)

[附 录 B 10](#_Toc174)

[参考文献 11](#_Toc1208)

|  |
| --- |
|  |
| 前 言 |
|  |

本文件按照GB/T1.1－2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国智能网联汽车产业创新联盟提出。

本文件起草单位：清华大学苏州汽车研究院（相城）（第一牵头单位），国汽智控（北京）科技有限公司（第二牵头单位）。

本文件主要起草人：####各成员单位人员。

|  |
| --- |
| 车控操作系统功能安全要求 |
|  |

1 范围

本标准规定了智能网联汽车车载智能计算基础平台车控操作系统功能安全总体要求。

本标准适用于智能网联汽车车载智能计算基础平台车控操作系统功能安全的设计开发和产品评价。

按照V流程开发，本标准只针对软件安全要求和嵌入式软件测试进行定义和明确，软件安全架构设计、软件详细设计、软件实现、软件单元测试和集成测试不再本标准范围内。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

1. ISO 26262-2018 Road vehicles-Functional safety.
2. 34590

...

备注：必须是标准

3 术语和定义

下列术语和定义适用于本文件。

3.1

车控操作系统 vehicle-controlled operating system

运行于车载智能计算基础平台，支撑智能网联汽车的感知、决策、规划和控制等功能的安全可靠运行的软件集合。

3.2

系统软件 system software

车控操作系统中支撑自动驾驶功能实现的复杂大规模嵌入式系统运行环境。

3.3

功能软件 function software

车控操作系统中根据面向服务的架构设计理念，通过提取自动驾驶核心共性需求，形成自动驾驶各共性服务功能模块，高效实现自动驾驶功能开发的软件模块。

......

4 车控操作系统安全假设

4.1 范围假设

4.1.1目的

4.1.2边界范围

描述对外边界、接口和范围

该部分可以从各模块进行提炼和汇总

4.1.3目标环境

描述目标环境，比如集成与某个平台上，或需要的硬件资源有哪些；

该部分可以从各模块进行提炼和汇总

4.1.4功能属性

提供了哪些功能和具有某些相关属性

该部分可以从各模块进行提炼和汇总

4.2 安全假设

描述车控操作系统更高层级的软件要求，以便导出软件安全要求。

该部分可以从各模块进行提炼和汇总

5 车控操作系统安全要求

5.1功能软件安全要求

5.1.1环境模型

1. **安全假设**

安全目标：环境模型提供安全的环境检测和定位信息

安全等级：环境模型可实现最高安全等级为ASIL C

目 的：服务于搭载辅助驾驶或自动驾驶汽车的安全感知

边界范围：输入预留各类传感器通讯接口；输出预留进行处理加工融合后的目标信息给规划模块；

目标环境：集成与中央控制计算平台上或其他域控制器；

功能属性：提供雷达或摄像头相关感知信息，经环境模型校验和计算后，输出安全可靠的环境信息。

安全假设：来自于雷达或摄像头相关信号要增加端对端保护信号（对外部系统要求）

该部分最终可进行提炼和汇总到Part4

1. **输入信号校验**
2. 环境模型应对目标检测（动态和静态目标）中目标元数据的目标ID、各组信号数据类型和取值范围进行校验，当检测到目标ID错误、各组信号数据类型错误或取值范围超出目标范围时，发出无效标志位。

b）环境模型对道路结构信息（道路标线和停止线的识别信息）中车道线集合数组、车道线元数据、停止线集合数组和停止线元据的数据类型、取值进行范围校验，当检测到数据类型错误或取值范围超出目标范围时，发出信号无效标志位；其卡滞/丢失/延迟应能被检测，当检测到以上失效应发出相应故障标志位。

c）对定位信息进行校验，位信息漂移/卡滞/丢失/延迟应能被检测，当检测到以上失效应发出相应故障标志位。

d）常见环境模型输入信号探测方法 见附录B

……

1. **诊断处理：**

当相应信号无效标志位触发时，融合模块应采取默认值或进入相应安全状态。

对环境各类环境感知计算模块应增加独立冗余校验模块，以监控计算是否正确，若计算出错，应进入对应安全状态。

对融合模块应增加合理性检查，以校验各路信号是否一致，若不一致，应进入该环境模型的安全状态。

信号校验模块调度周期或运行时间应该被监控，探测其运行太频繁、运行过长等错误。

对于存储安全校验模块的内存应该被保护，免于非法读写访问。

.....

1. **安全机制：**

描述该模块的核心安全机制

可以增加图片+文字描述 或添加到附录中

....

1. **输出信号：**

环境模型对计算处理后的输出目标信号、道路信号、定位信号增加timeout、alive counter、CRC和valid状态等保护信息；

......

1. **安全状态：**

定义安全状态应使系统进入对应工况下的安全运行模式，比如：自动驾驶L3以下的工况车道内减速并提示驾驶员接管，L3及L3以上的工况冗余备份系统执行安全靠边停车。

.....

1. **对车控操作系统其他模块要求：**

描述为实现该模块功能的安全要求，其它系统需要满足的内容。

硬件需要支持memory protect功能，比如ECC或MPU。

规划模块输入信号要对来自于环境模块的输出信号进行端对端校验，以检测信号完整性

......

**7）其它：**

除以上内容外，可描述其它需要补充内容

5.1.2规划模型

描述该模块安全要求

5.1.3控制模型

描述该模块安全要求

5.1.4基础服务

描述该模块安全要求

5.1.5数据流框架

描述该模块安全要求

5.1.6数据抽象

描述该模块安全要求

5.1.7应用软件接口

描述该模块安全要求

5.2 系统软件安全要求

描述以下系统软件各模块安全要求

5.2.1POSIX及其他接口

车控操作系统需要兼容POSIX标准，支持广泛的POSIX API规范，并可以被诸如PSE(Product Safety of Electrical Appliance & Materials)等测试套件进行验证，提供标准的libc/libc++库。

5.2.2实时安全域

车控操作系统需具备高效的内核调度机制，支持可抢占优先级的程序调度。特别地，对于自动驾驶应用场景，操作系统内核的平均中断延迟和最差中断延迟均应控制在微秒级别。

5.2.3系统中间件及服务

车控操作系统需提必要的系统中间件及服务，包括图像、音频、网络、文件系统、多媒体等模块。关键组件需达到TUV莱茵ISO26262 ASIL D认证。

5.2.4系统软件工具链

C语言编译器，链接器，汇编器，链接器和镜像生成器需符合ISO 26262 TCL3标准。

5.2.5操作系统内核

车控操作系统内核需要有强大容错性，所有的进程相互隔离，某个进程崩溃不会影响到系统其它进程，并有多种方式可实现智能恢复。支持快速启动，以满足汽车电子中多种场合需求，如开机画面瞬显、快速启动倒车摄像头和CAN总线响应等。操作系统内核需达到TUV莱茵ISO26262 ASIL D认证。

提供主流32/64位多核车载处理器的板级支持包。

5.2.6虚拟化管理及板级支持包

提供虚拟化支持，包括虚拟机程序、虚拟驱动、SMMU和于Guest系统间通讯机制，提供图像、音频、网络、输入等设备的虚拟化支持。其中，虚拟化程序需达到TUV莱茵ISO26262 ASIL D认证。

提供主流32/64位多核车载处理器的板级支持包。

6 车控操作系统验证和确认

6.1安全验证要求

描述安全验证方法、测试要求等

6.2安全确认要求

描述安全确认相关要求

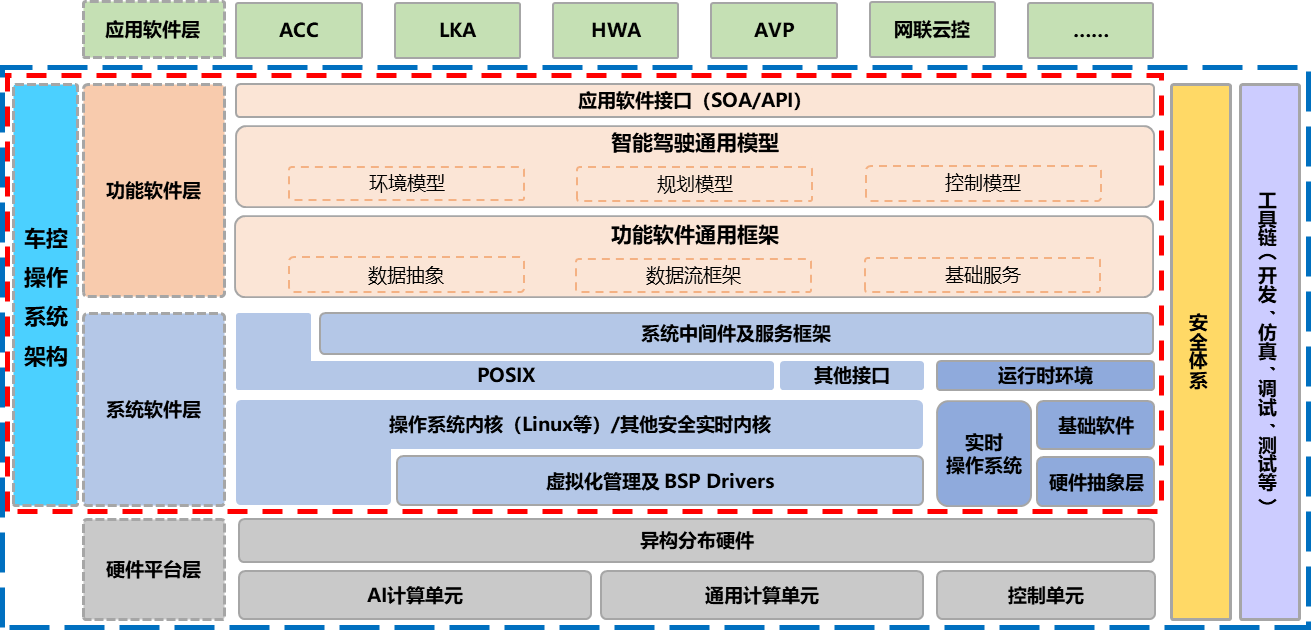
7安全集成要求

车控操作系统在全新特定环境下进行集成之前，需要确认全部假设在新环境下的有效性。若设与实际需求不一致需要启动变更管理流程，具体参加ISO 26262-8 Change management。

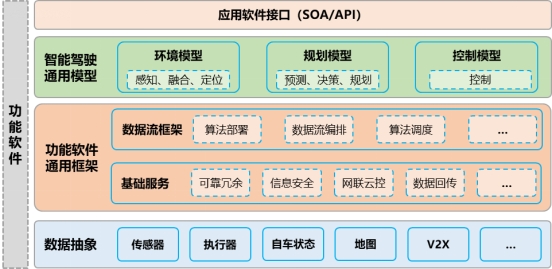
# 附 录 A

（规范性附录）

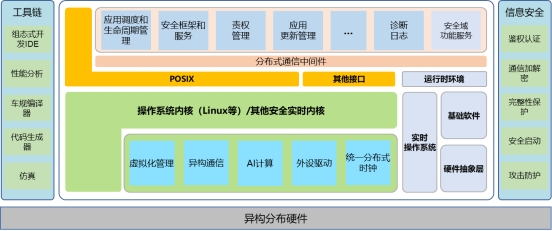
车控操作系统说明和架构



车控操作系统架构



功能软件架构



系统软件架构

# 附 录 B

环境模型输入信号探测方法

**摄像头的检测方法;**

1. 对于摄像头图像卡滞/丢失：对多帧图像进行像素点校验，如从IMU或wss读取车辆动态信息表示车辆仍在运动中而像素点完全重合，则为摄像头图像卡滞/丢失；摄像头的时钟源满足asil等级，检测其timestamp连续性，如果超过图像发送周期TBD ms 则判断其卡滞/丢失
2. 对于摄像头图像雪花（信号干扰）-sotif：可通过像素点重复率检验

**雷达检测方法：**

1. 雷达信号卡滞/丢失：判断多个物体距离信息无变动且自车处在运动状态；雷达时钟源满足asil等级，检测其timestamp连续性，如果超过图像发送周期TBD ms 则判断其卡滞/丢失
2. 检测漂移：雷达建立物体tracker的速度以及消失速度超出合理阈值

**定位检测方法：**

1. 丢失 - 检测信号无输入
2. 漂移：GNSS报送位置信息跳转速度超出自身车速阈值
3. 卡滞：GNSS位置报送重复坐标值，当从IMU或wss读取车辆动态信息表示车辆仍在运动中，且自身status信号丢失（非物体遮挡导致，如桥洞）

参考文献

1. ISO 42010—2011 Systems and software engineering-Architecture description.
2. ISO DIS 23150-2020 Road vehicles-Data communication between sensors and data fusion unit for automated driving functions.
3. ISO/PAS 21448-2019 Road vehicles-Safety of the intended functionality.
4. ISO 26262-2018 Road vehicles-Functional safety.
5. 《车控操作系统总体技术要求研究报告》
6. 《车控操作系统架构研究报告》