**标准框架：**

1. **自动驾驶芯片标准研究背景**
   1. 汽车芯片分类（按照功能分类）（全体）（**华大汇总**）
      1. 计算芯片（CPU，GPU，FPGA等）
      2. 感知芯片 （光电 指纹 麦克风 MEMS等）
      3. 存储芯片 （中汽研）
      4. 通信芯片（蓝牙、wifi、V2X等）
      5. 能源芯片（电源、DC-DC、LDO等）
      6. 安全芯片 （华大）
   2. 汽车芯片现状（**华为汇总**）
      1. 计算芯片（地平线 华为 黑芝麻高通，**地平线汇总**）
      2. 感知芯片 （万集）
      3. 存储芯片（中汽研、紫光）
      4. 通信芯片（高通、万集）

目前主流汽车通信芯片均为4G/5G多模制式，支持的通信速率可高达数Gbps。典型的汽车联网SoC平台不仅仅支持多模蜂窝通信（2G/3G/4G和5G的SA/NSA模式），还集成支持了包括C-V2X PC5并发、DSDA、多模多频GNSS定位（包括北斗、GPS、Galileo和GLONASS系统）及增强（RTK/PPP、惯导、传感器增强等）、eCall/NG-eCall、信息安全等各种功能。芯片制程也已经采用了最先进的7nm工艺，并且正在进一步的向更高的5nm甚至3nm制程发展。目前主流芯片均已满足AEC-Q100的车规级要求。典型的汽车联网SoC平台包括高通推出的骁龙4G汽车平台和5G汽车平台，该平台已经被各大汽车厂商采用，相关产品已经商用。

车载蓝牙和Wi-Fi芯片平台通常被用来提供高品质的短距离车内以及汽车和手持终端之间的通信，提供包括无线汽车钥匙、手持终端与车机链接、多媒体播放、语音呼叫、车内热点、高清视频流媒体等多种应用和功能。主流蓝牙芯片方案已经支持最新的BT 5.x标准，Wi-Fi也已支持Wi-Fi 6（802.11ac）标准。芯片制程也已经采用了先进的14nm工艺，正在进一步的向更高的制程发展，并且主流芯片均已满足AEC-Q100的车规级要求。

* + 1. 能源芯片 （中汽研）
    2. 安全（华大、紫光、芯钛）
  1. 汽车芯片发展趋势（**华为汇总**）
     1. 计算芯片
     2. 感知芯片
     3. 存储芯片
     4. 通信芯片
     5. 能源芯片
     6. 安全芯片

1. **汽车芯片产业链现状** (**华为/中汽研**、其他补充，**华为汇总**)
   1. 汽车芯片产业链梳理
   2. 汽车芯片产业链现状
2. **汽车芯片技术要求** （**上汽大众汇总**，各家写需求）
   1. 汽车芯片技术要求（**中汽研、华为、上汽大众给出模板**）

**1）就环境温度等级要求（参照AEC-Q）**：

|  |  |  |
| --- | --- | --- |
| 等级 | 范围要求 | 测试时间 |
| 0 | -40°C—150°C | 150°C —1000小时，175°C—408小时 |
| 1 | -40°C—125°C | 125°C —1000小时，150°C—408小时 |
| 2 | -40°C—105°C | 105°C —1000小时，125°C—408小时 |
| 3 | -40°C—85°C | 85°C —1000小时，105°C—408小时 |

**2）功能安全等级（ISO 262626 和 GBT 34590）**：

安全等级ASIL按照三个维度进行具体评估，严重性、暴露性和可控性。

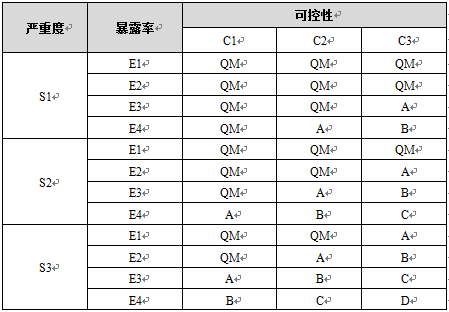
严重性，用SX表示，4个等级，S0无伤害；S1轻伤；S2重伤；S3致命伤害；

暴露性，用EX表示， 5个等级，E0是几乎不肯能暴露于危险中，E4是可能性极高。

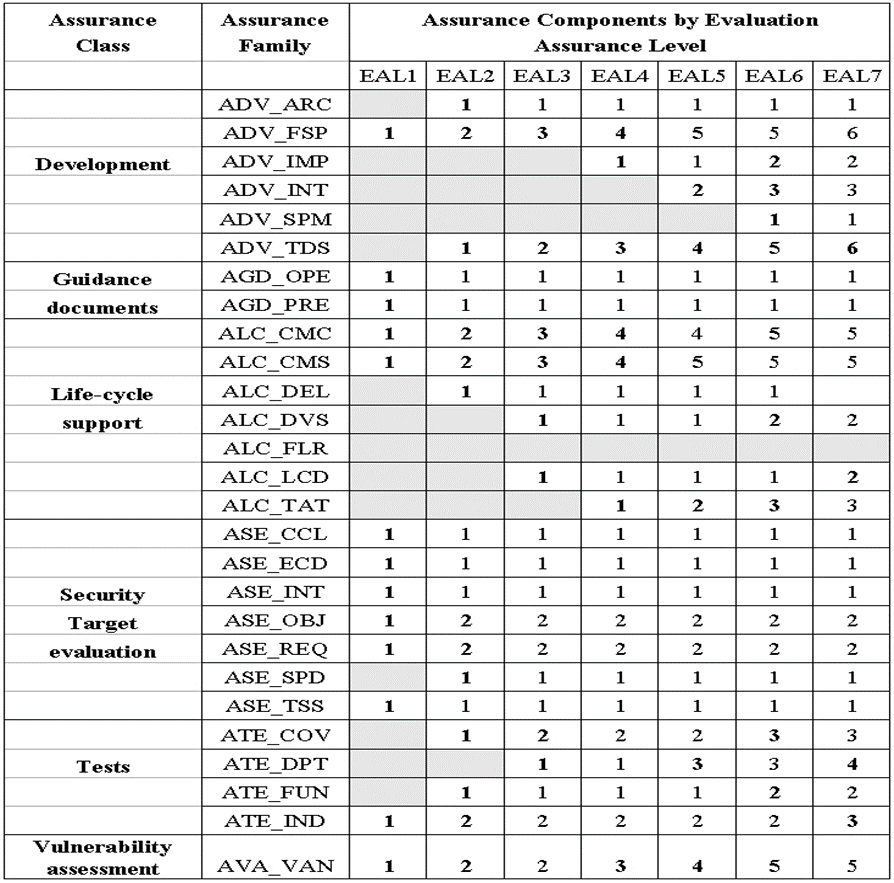
可控性，用CX表示，4个等级，最低C0可控，最高C3几乎不可控。

ASIL 等级分为A、B、C、D 四个等级，ASIL A 是最低的安全等级，ASIL D 是最高的

安全等级。除了这四个等级QM 表示与安全无关。评估结果范例表格如下图所示。



**4）信息安全（CC EAL，参照ISO15408 或 GB/T 22186）：**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全功能类 | 安全功能组件 | 编号 | 备注 | | |
| EAL3+ | EAL4+ | EAL5+ |
| FCS 类：密码支持 | FCS\_CKM.1 密钥生成 | 1 | √ | √ | √ |
| FCS\_COP.1 密码运算 | 2 | √ | √ | √ |
| FDP 类：用户数据保护 | FDP\_ACC.1 子集访问控制 | 3 | √ | √ | √ |
| FDP\_ACF.1 基于安全属性的访  问控制 | 4 | √ | √ | √ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 安全功能类 | 安全功能组件 | 编号 | 备注 | | |
| EAL3+ | EAL4+ | EAL5+ |
| FDP\_IFC.1 子集信息流控制 | 5 | √ | √ | √ |
| FDP\_ITT.1 基本内部传送保护 | 6 | √ | √ | √ |
| FDP\_SDI.1 存储数据完整性监  视 | 7 | ○ | √ | N/A |
| FDP\_SDI.2 存储数据完整性监  视和行动 | 8 | ○ | ○ | √ |
| FIA 类：标识和鉴别 | FIA\_UAU.1 鉴别的时机 | 9 | ○ | √ | √ |
| FIA\_AFL.1 鉴别失败处理 | 10 | ○ | √ | √ |
| FMT 类： 安全管理 | FMT\_LIM.1 受限能力 | 11 | √ | √ | √ |
| FMT\_LIM.2 受限可用性 | 12 | √ | √ | √ |
| FMT\_MSA.1 安全属性的管理 | 13 | √ | √ | √ |
| FMT\_MSA.3 静态属性初始化 | 14 | √ | √ | √ |
| FMT\_MTD.1TSF 数据的管理 | 15 | √ | √ | √ |
| FMT\_SMF.1 管理功能规范 | 16 | √ | √ | √ |
| FMT\_SMR.1 安全角色 | 17 | √ | √ | √ |
| FPT 类：安全功能保护 | FPT\_FLS.1 失效即保持安全状  态 | 18 | √ | √ | √ |
| FPT\_ITT.1 内部 TSF 数据传送  的基本保护 | 19 | √ | √ | √ |
| FPT\_PHP.3 物理攻击抵抗 | 20 | √ | √ | √ |
| FPT\_TST.1 TSF 测试 | 21 | ○ | √ | √ |
| FP T \_ R P L . 1 重放检测 | 22 |  |  |  |
| FRU：资源利用 | FRU\_FLT.2 受限容错 | 23 | √ | √ | √ |

**4）关键性能指标等进行说明；**

**举例见3.1.1 计算芯片**

* + 1. 计算芯片

**环境温度要求：GRADE 1**

**功能安全等级要求：ASIL-D**

**信息安全等级要求： EAL 5**

**关键性能指标：算力＞100tops，功耗＜20W，**

* + 1. 感知芯片
    2. 存储芯片
    3. 通信芯片
    4. 能源芯片
    5. 安全芯片

4 **标准适用性分析**（**中汽研汇总**）

4.1 标准现状及适用性分析

* 1. 车规芯片标准意义

5 **标准化建议**（**中汽研汇总**）

整体建议，可以有分步介绍，其中把高性能计算芯片和安全芯片作为优先实施方向