火龙果 · 整理
uml.org.cn

# 智能驾驶功能安全

火龙果 · 整理
uml.org.cn

# 内容 & 观点

**智能驾驶Hazard Analysis**

- 智能驾驶分级定义已清晰提示Hazard
- Hazard Analysis可见智能驾驶 Level分水岭

智能驾驶 HARA and Safety Validation

智能驾驶 Safety Mechanism

Highlights: ISO 26262 Application

# 智能驾驶 Hazard Analysis

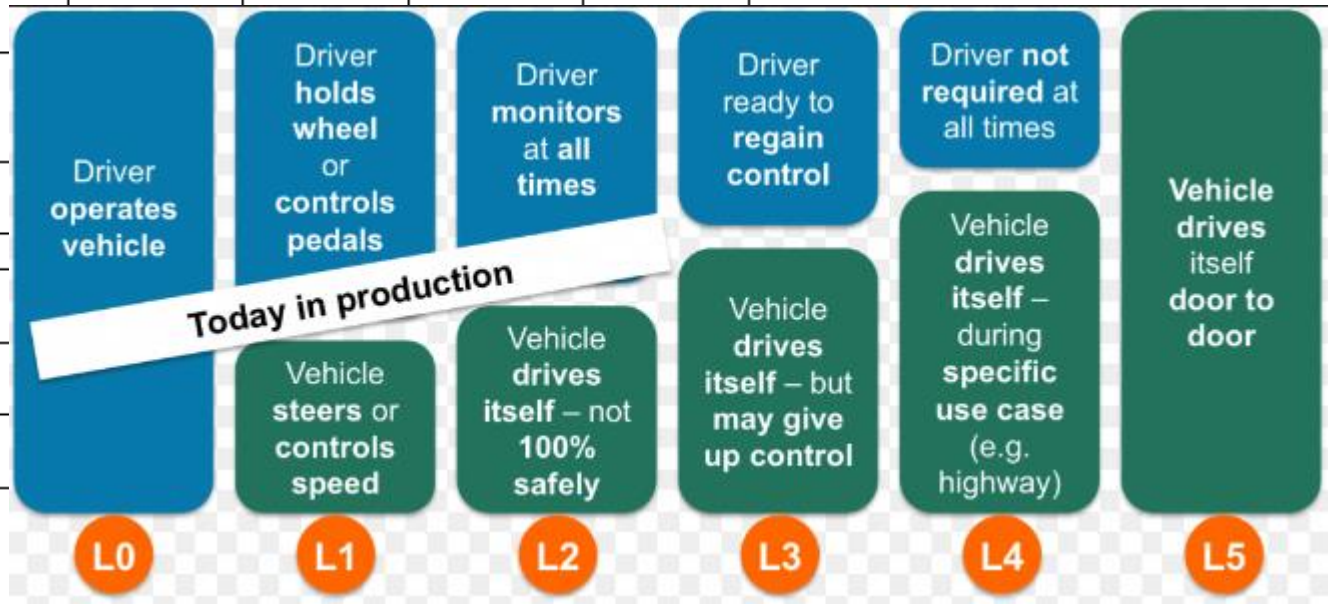
火龙果 · 整理
uml.org.cn

| | |
|---|---|
| 什么是智能驾驶？ | 智能驾驶 vs 传统汽车电子 |
| | SAE L0-L5定义 |
| 智能驾驶分水岭？ | 非L0系统 基础Hazard |
| | L1-L2 vs L3-L5 Hazard本质区别 |
| 各级别危害？ | SAE L1 – L5：分级Hazard Analysis |
| | 典型产品/功能定义/系统结构/事故实例 |

火龙果 · 整理
uml.org.cn

# 智能驾驶业界现状

| Operating Environment | System Function | Level | Status | 0–5 years | 5–10 years | 10–15 years |
|---|---|---|---|---|---|---|
| Highway | Traffic Jam Assist | 2 | Product announced for MY14 | ✔ | | |
| Highway | On-Center Driving w/ACC (limited steering authority) | 2 | Product | ✔ | | |
| Highway | Combined lateral/longitudinal control | 2 | | | | |
| Highway | On-Highway Platooning | 3 | | | | |
| Highway | Workzone Assistant | 2 | | | | |
| Highway | Emergency Stopping Assistant | 4 | | | | |
| City | Segregated Urban Automated Vehicles | 4 | | | | |
| City | Open Road Urban Automated Vehicles | 3 | | | | |
| All Roads | Automated Operation on All Road Types for Military Applications | 3 | | | | |
| Parking | Automated Valet Parking | 4 | Prototype | ✔ | | |




[NHTSA]

火龙果 · 整理
uml.org.cn

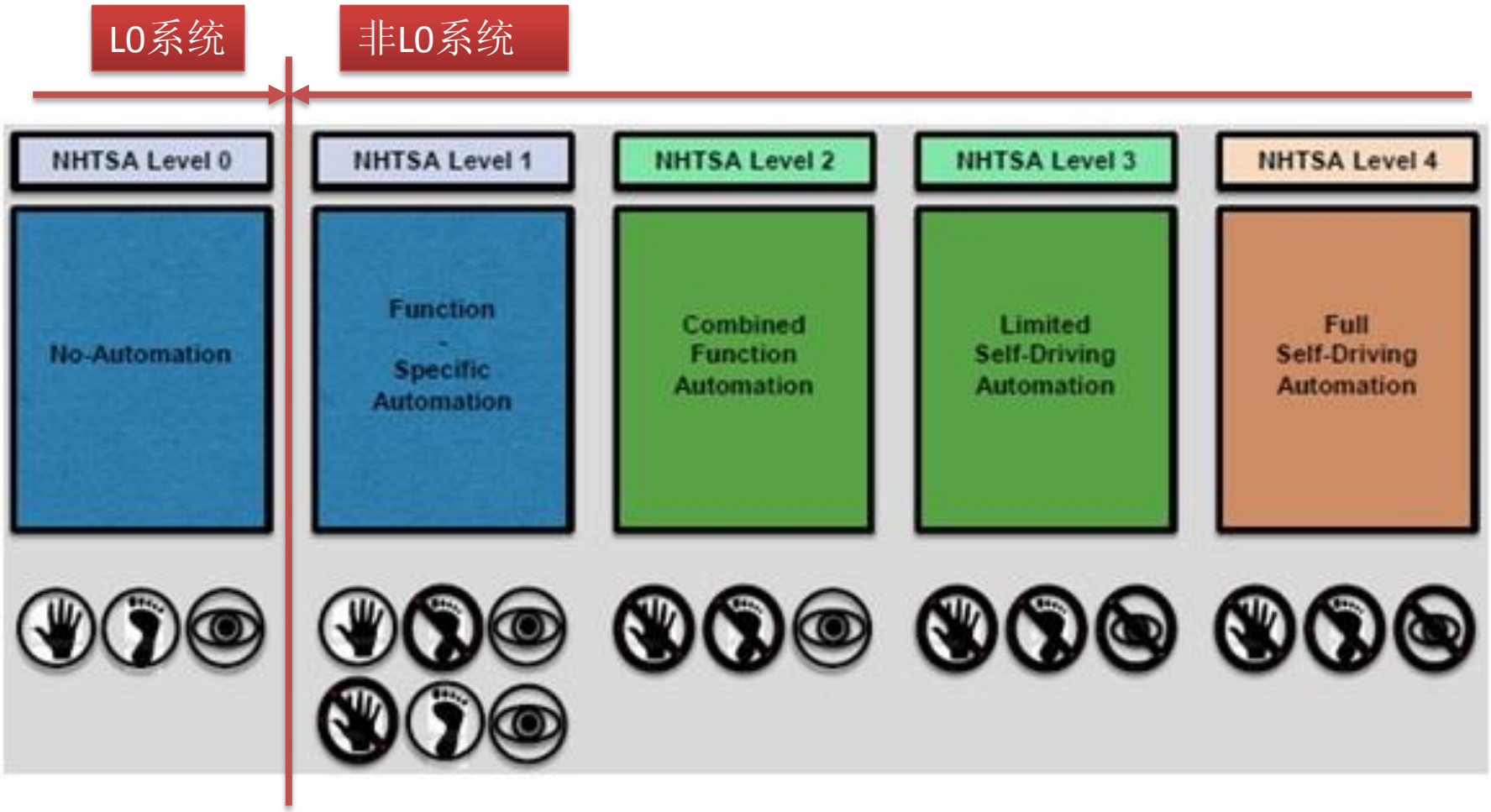
# SAE L0-L5定义

<table>
<tr><th colspan="2">自动驾驶分级</th><th rowspan="2">称呼（SAE）</th><th rowspan="2">SAE定义</th><th colspan="4">主体</th></tr>
<tr><th>NHTSA</th><th>SAE</th><th>驾驶操作</th><th>周边监控</th><th>支援</th><th>系统作用域</th></tr>
<tr><td>0</td><td>0</td><td>无自动化</td><td>由人类驾驶者全权操作汽车，在行驶过程中可以得到警告和保护系统的辅助。</td><td>人类驾驶者</td><td rowspan="2">人类驾驶者</td><td rowspan="3">人类驾驶者</td><td>无</td></tr>
<tr><td>1</td><td>1</td><td>驾驶支援</td><td>通过驾驶环境对方向盘和加减速中的一项操作提供驾驶支援，其他的驾驶动作都由人类驾驶员进行操作。</td><td>人类驾驶者<br>系统</td><td rowspan="4">部分</td></tr>
<tr><td>2</td><td>2</td><td>部分自动化</td><td>通过驾驶环境对方向盘和加减速中的多项操作提供驾驶支援，其他的驾驶动作都由人类驾驶员进行操作。</td><td rowspan="4">系统</td></tr>
<tr><td>3</td><td>3</td><td>有条件自动化</td><td>由无人驾驶系统完成所有的驾驶操作。根据系统请求，人类驾驶者提供适当的应答。</td><td rowspan="3">系统</td><td rowspan="3">系统</td></tr>
<tr><td rowspan="2">4</td><td>4</td><td>高度自动化</td><td>由无人驾驶系统完成所有的驾驶操作。根据系统请求，人类驾驶者不一定需要对所有的系统请求作出应答，限定道路和环境条件等。</td></tr>
<tr><td>5</td><td>完全自动化</td><td>由无人驾驶系统完成所有的驾驶操作。人类驾驶者在可能的情况下接管。在所有的道路和环境条件下驾驶。</td><td>全域</td></tr>
</table>

[NHTSA, SAE]

火龙果 · 整理
uml.org.cn

# SAE L0-L5定义



火龙果 · 整理
uml.org.cn

# L0/非L0系统基本特征

**L0系统**

- 智能驾驶未对人工控制回路造成直接变化

-仅以影响司机的方式参与控制回路

**非L0系统**

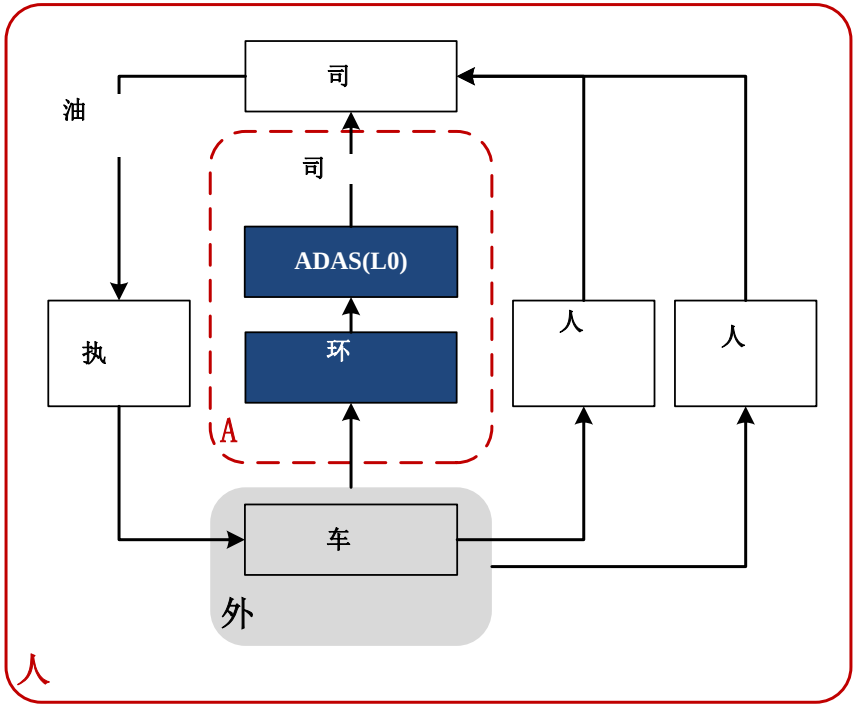
- 智能驾驶控制回路与人工控制共同直接作用于车辆

- 多控制源引入的控制冲突、控制缺失、切换延时

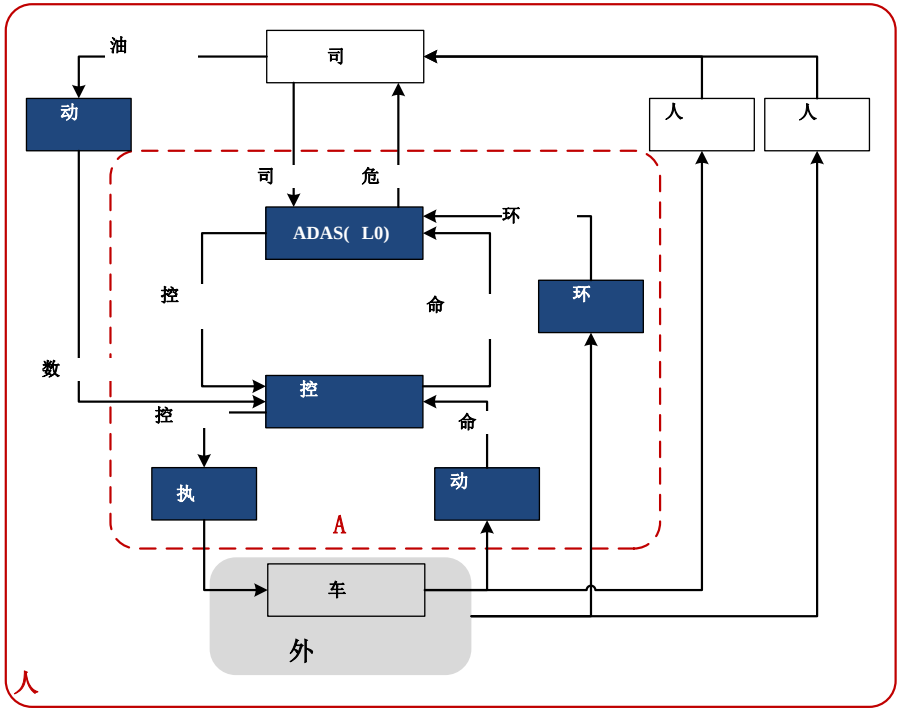
火龙果 · 整理
uml.org.cn

# L0/非L0系统典型控制结构

## L0系统

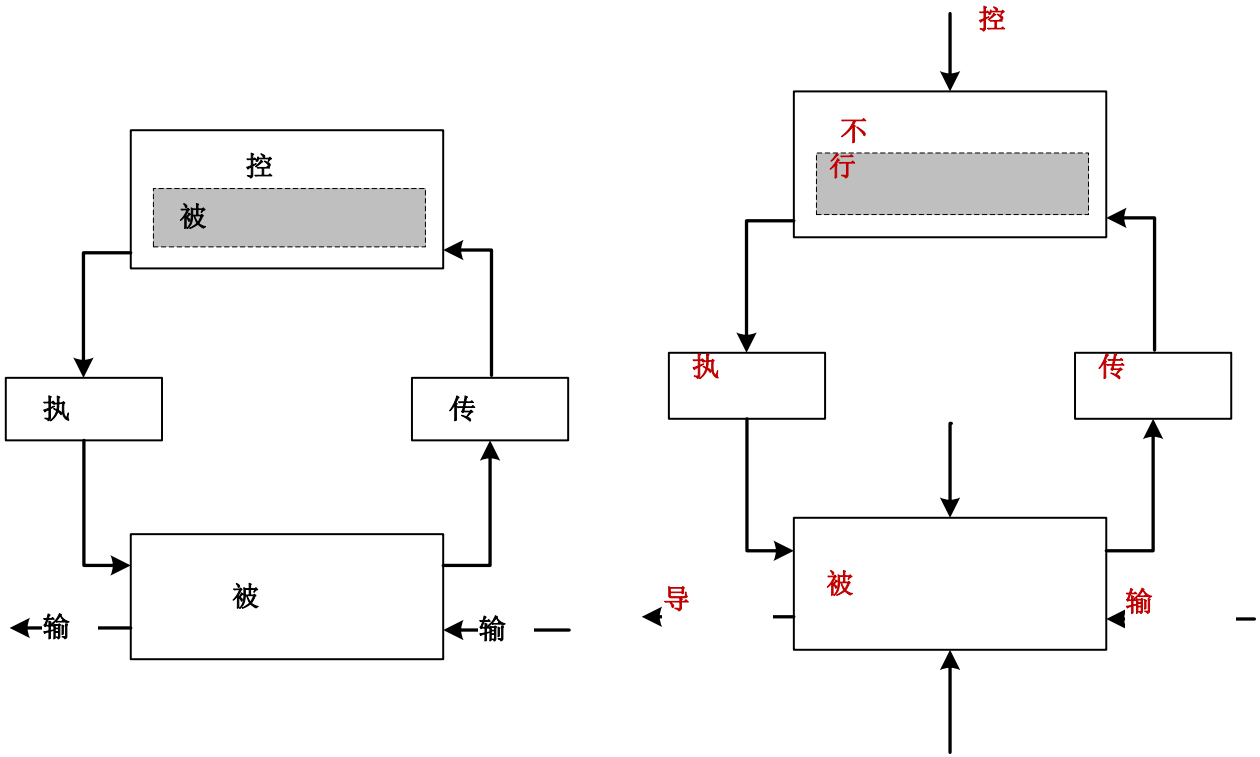



## 非L0系统



# 非L0系统Hazard分析-方法论

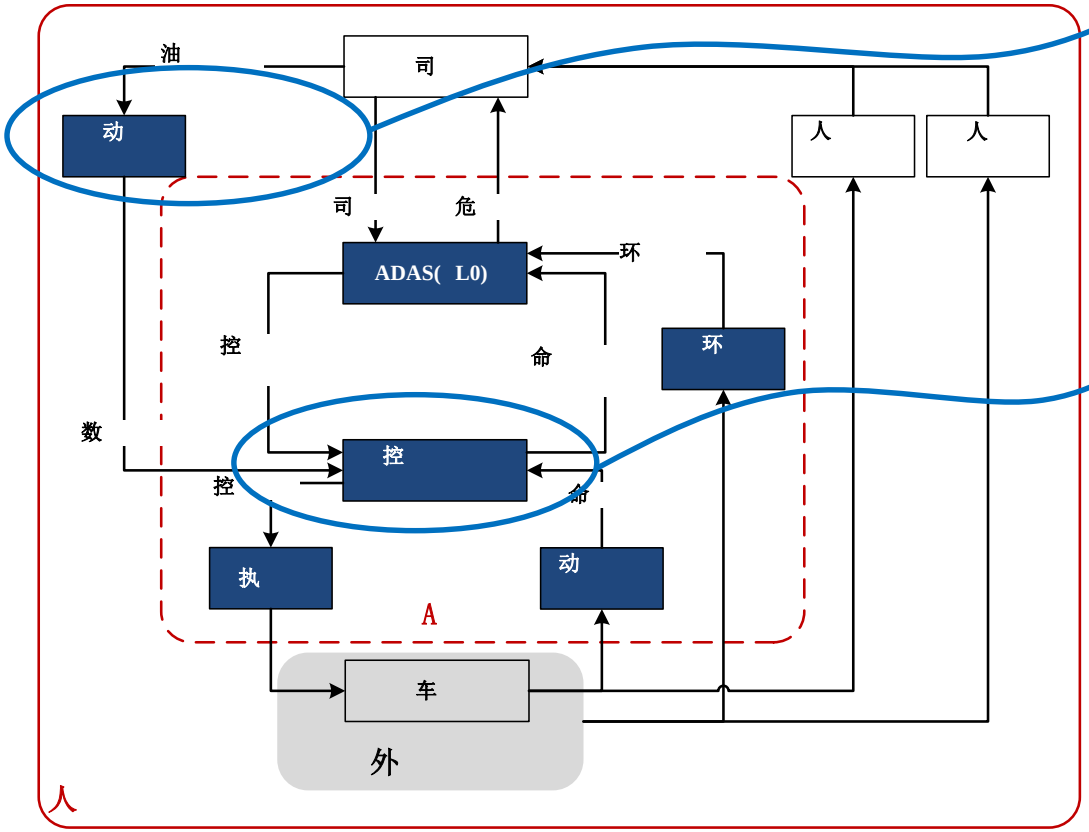
适用于耦合复杂控制系统的安全分析方法：STAMP




[Leveson, MIT]

火龙果 · 整理
uml.org.cn

# 非L0系统Hazard分析-顶层Hazard




**H1-1：** 司机、智能驾驶均未控制车辆

**H1-2：** 司机、智能驾驶控制命令冲突

**H1-3：** 车辆不按司机操作控制

**H1-4：** 人工控制切换延时

火龙果 · 整理
uml.org.cn

# 非L0系统Hazard分析-事故实例

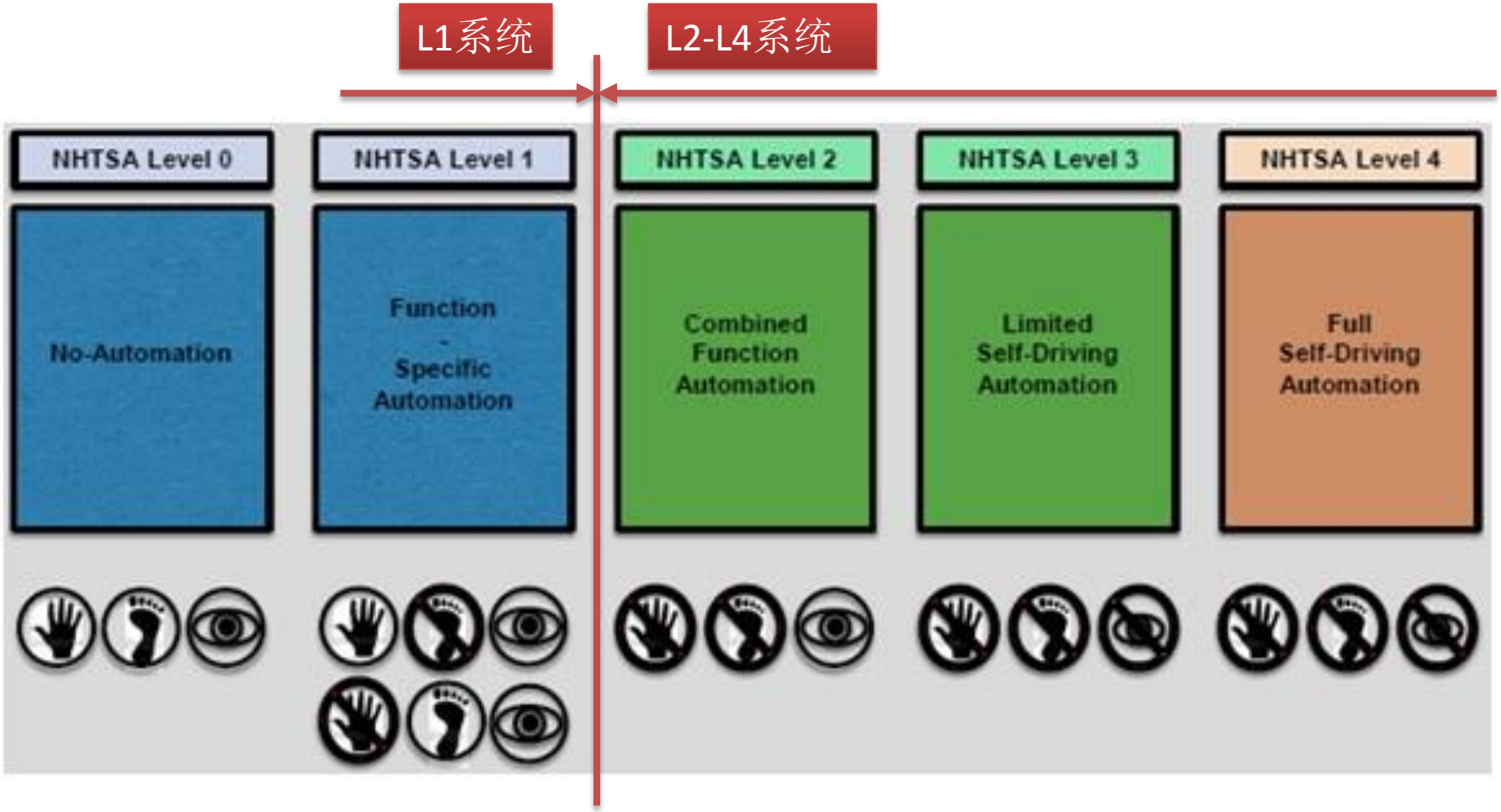
**2016.2.2：Denham, Buckinghamshire, UK：无法退出自动控制模式，司机致死**

| | |
|---|---|
| 车型 | Skoda Octavia |
| 智能驾驶类别 | Cruise control (L2) |
| 事故时速度 | 94mph |
| 事故场景 | 车辆被智能驾驶持续加速，司机无法退出自动模式，加速至94mph后与大卡车相撞 |
| 事故原因 | 1、智能驾驶意外加速<br>2、车辆不按司机操作控制 |

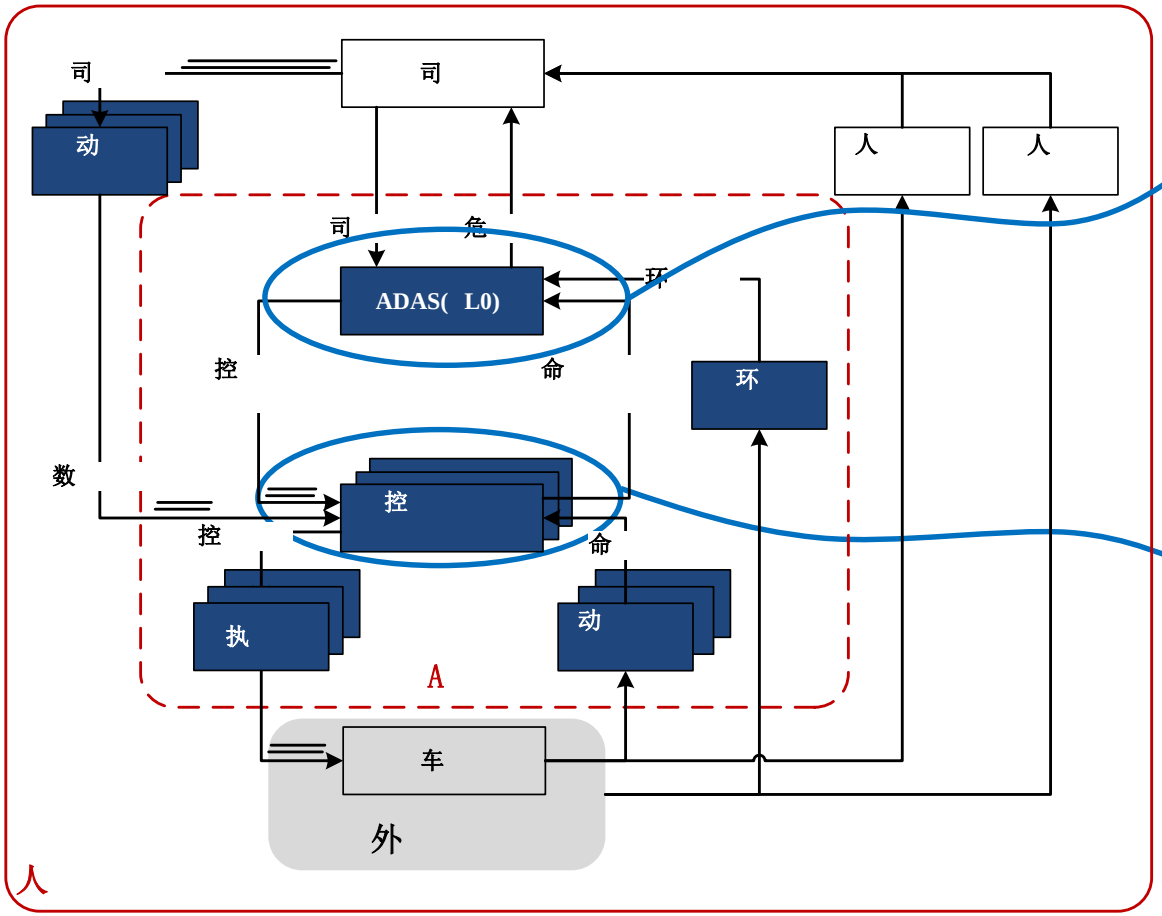
[Skoda driver decapitated after claiming car's cruise control was stuck]

火龙果 · 整理
uml.org.cn

# SAE L0-L5定义



# L2以上系统Hazard分析

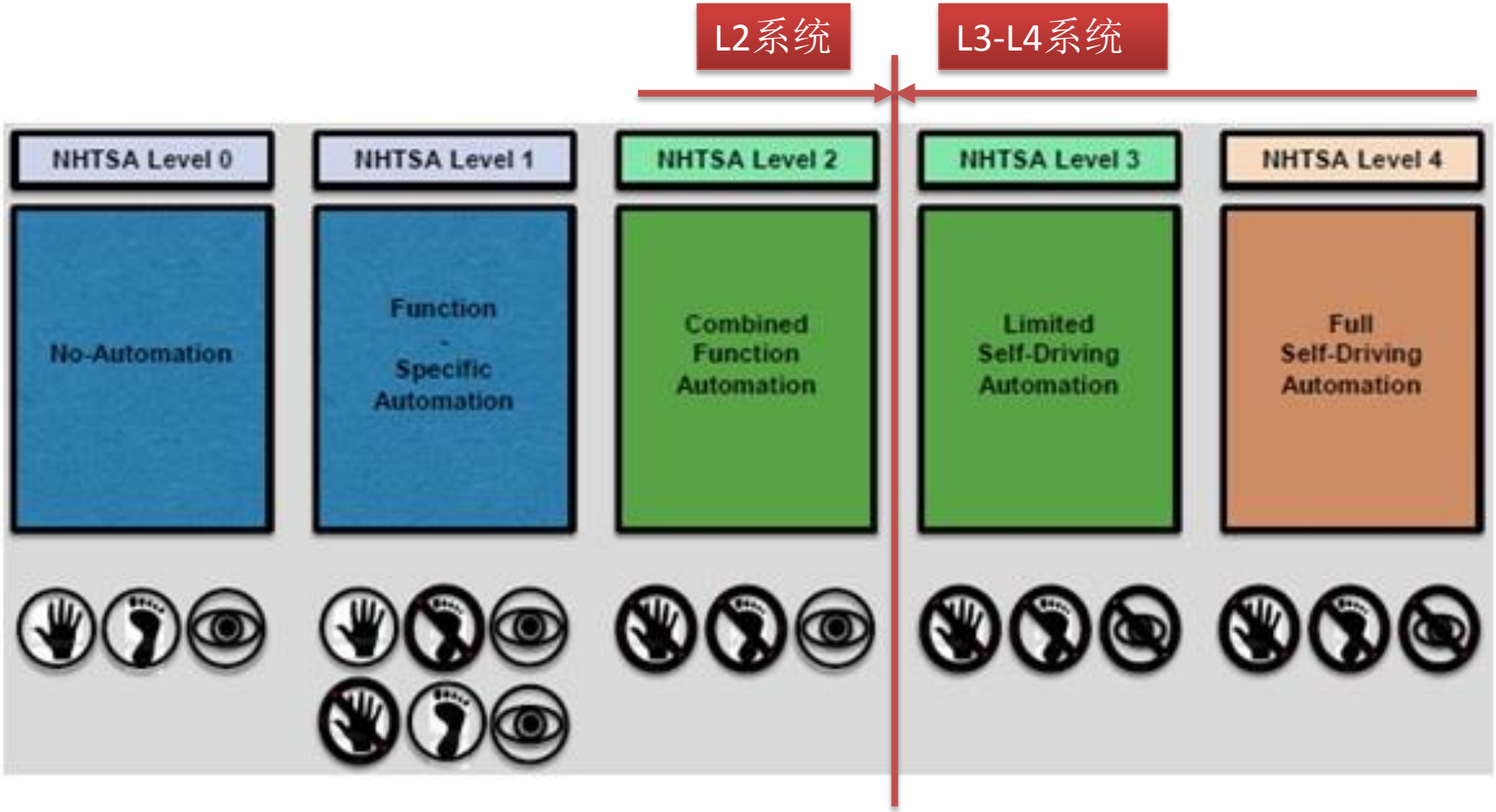



H2-1：加速/制动/转向命令冲突

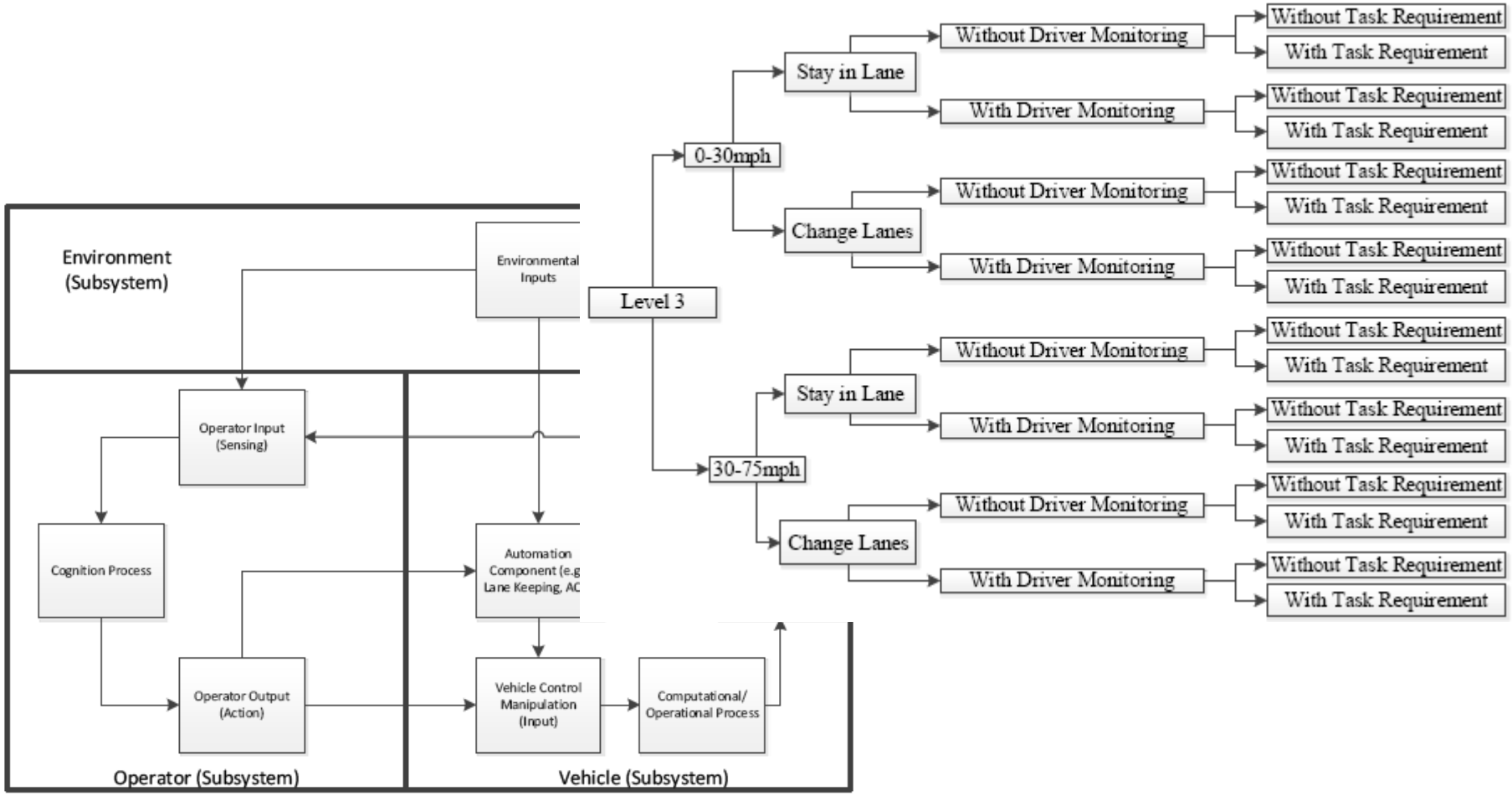
H2-2：加速/制动/转向控制状态不一致

火龙果 · 整理
uml.org.cn

# SAE L0-L5定义



# L2/L3系统的人因因素



火龙果 · 整理
uml.org.cn

# 内容 & 观点

智能驾驶 Hazard Analysis

**智能驾驶 HARA and Safety Validation**

- ISO26262 HARA标准可类比应用
- 部分Hazard需建立新的评估标准

智能驾驶 Safety Mechanism

Highlights: ISO 26262 Application

火龙果 · 整理
uml.org.cn

# 智能驾驶HARA and Safety Validation

| | |
|---|---|
| 功能安全已有的工具？ | ISO26262: HARA方法论 |
| | ISO 26262: Safety Validation |
| 能用于智能驾驶吗？ | S、E、C在智能驾驶中的应用类比 |
| | ISO 26262 HARA适用的Hazards |
| 足够吗？ | 环境感知的安全目标 |
| | Safety Validation标准 |

火龙果 · 整理
uml.org.cn

# ISO26262: HARA方法论

| | | C1 | C2 | C3 |
|---|---|---|---|---|
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| S3 | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

汽车安全完整度等级

[ISO26262]

火龙果 · 整理
uml.org.cn

# S、E、C在智能驾驶中的应用类比

| | Severity<br>严重度 | Exposure<br>驾驶场景频度 | Controllability<br>可控性 |
|---|---|---|---|
| 传统汽车电子 | - 通常由速度衡量<br>- 针对普适的人工驾驶场景，速度范围较宽，S等级跨度S1-S3. | - 危害在驾驶场景中暴露的频度<br>- 通常考虑其持续时间和发生频率。 | - 驾驶员/乘客/行人控制避免伤害的可能性<br>- 通常与特定事故类型相关 |
| 智能驾驶 | - **智能驾驶最高限速直接影响S等级**<br>- 例如仅用于低速情况的自动摆渡车。 | - 智能驾驶应衡量适用场景范围内的Exposure | **L2与L3的分水岭：**<br>**-L2系统对智能驾驶失效的可控性为C1；**<br>**-L3以上系统对智能驾驶失效的可控性为C3** |

火龙果 · 整理
uml.org.cn

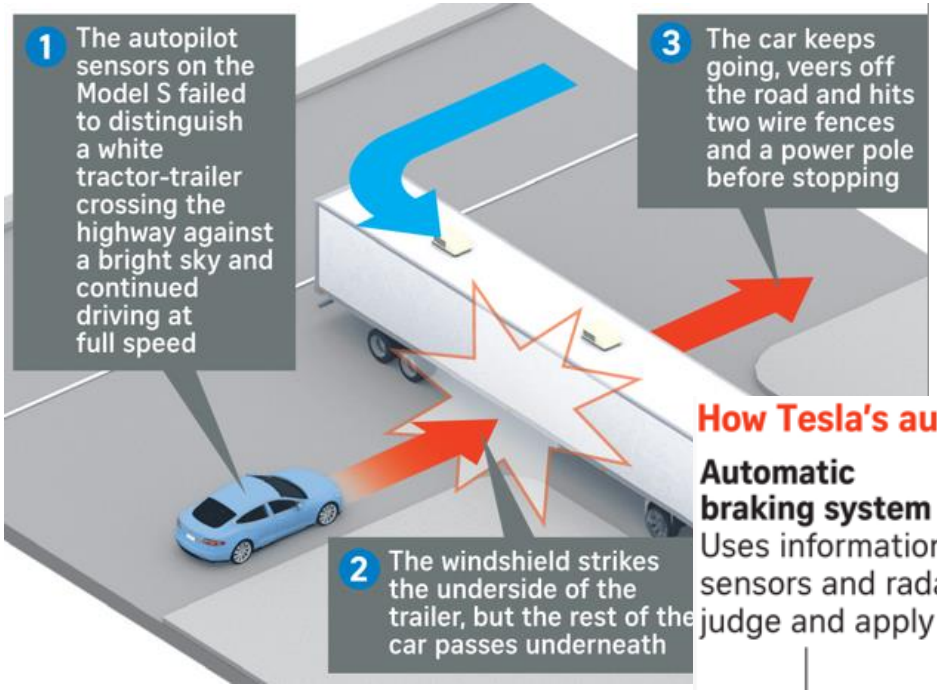
# S、E、C在智能驾驶中的应用类比

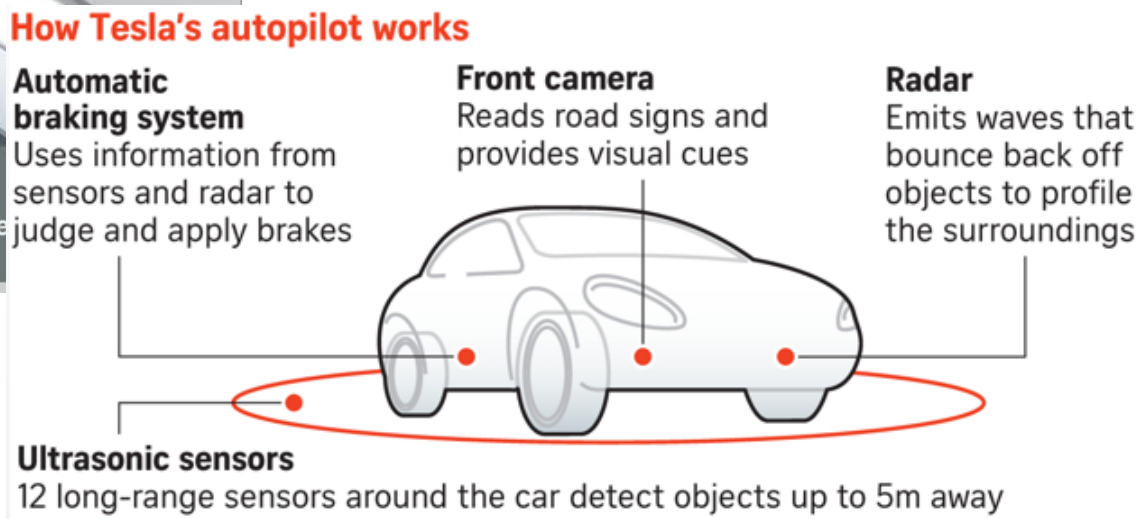
| ID | Malfunctions and hazards | Selected situations | E | Reason for E (for the 1st occurence only) | Consequences of hazardous events | S | Reason for S |
|---|---|---|---|---|---|---|---|
| LKAS_H1 | Providing of incorrect lane information in CAMERA | car moves forward; high speed and acceleration; Guardrail | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H2 | Providing of incorrect lane information in CAMERA | car moves forward; accelerated in a hazardous situations; Guardrail | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H3 | Providing of incorrect lane information in CAMERA | car moves forward; with middle speed manoeuvre in highway; Guardrail | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | Medium speed and more than 10% probability of AIS 5-6 |
| LKAS_H4 | Providing of incorrect lane information in CAMERA | car moves forward; with high speed manoeuvre in highway; Guardrail | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H5 | Loss of lane detection in CAMERA | car moves forward; high speed and acceleration; Guardrail | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H6 | Loss of lane detection in CAMERA | car moves forward; high speed and acceleration; Tunnel | 2 | Low probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H7 | Loss of lane detection in CAMERA | car moves forward; high speed and acceleration; Low stationary sunlight in the morning or evening | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |
| LKAS_H8 | Loss of lane detection in CAMERA | car moves forward; high speed and acceleration; fountains of water because of other cars | 4 | High probability | Collision with vehicle driving on neighbor lane or road's infrastructures | 3 | High speed and more than 10% probability of AIS 5-6 |

[TUV SUD, Eason Dong]

火龙果 · 整理
uml.org.cn

# 环境感知失效

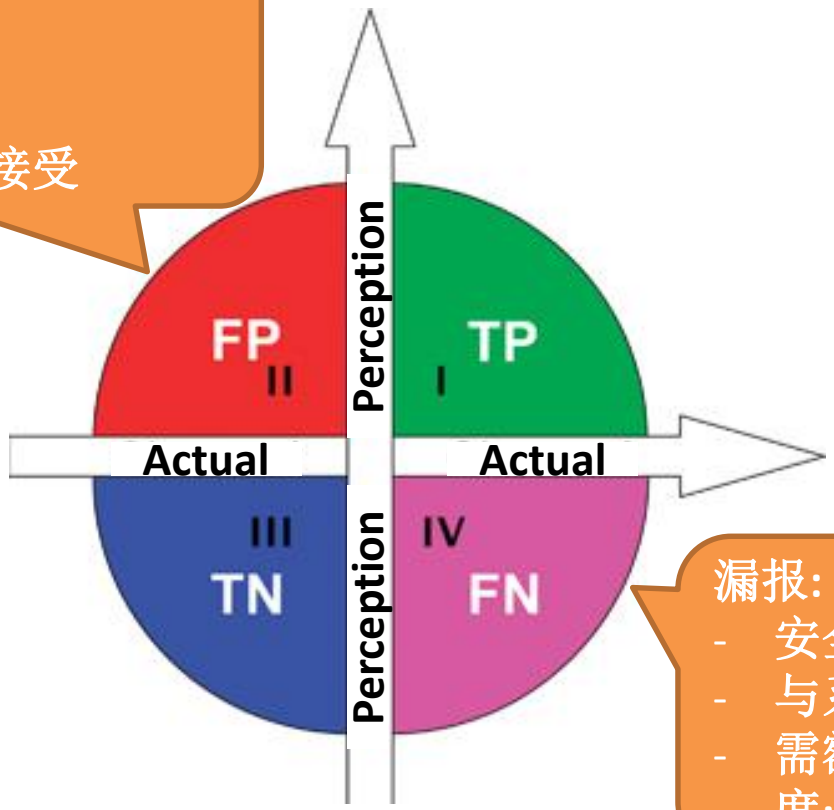


火龙果 · 整理
uml.org.cn

# 环境感知失效模式

虚警:
- 可用性失效
- 与用户体验相关
- 低于合理数值即可接受




漏报:
- 安全相关失效
- 与系统安全性能相关
- 需额外安全设计(概率可信度; 可达性分析等.)

火龙果 · 整理
uml.org.cn

# 环境预测失效模式

**难点：**

多种类、多姿态的移动障碍物

速度、方向预测

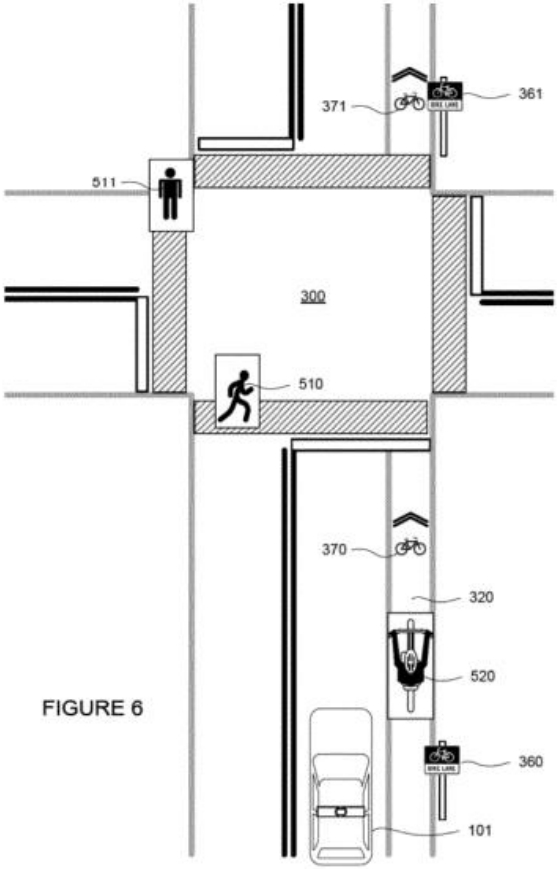



FIGURE 6

[google patent]

火龙果 · 整理
uml.org.cn

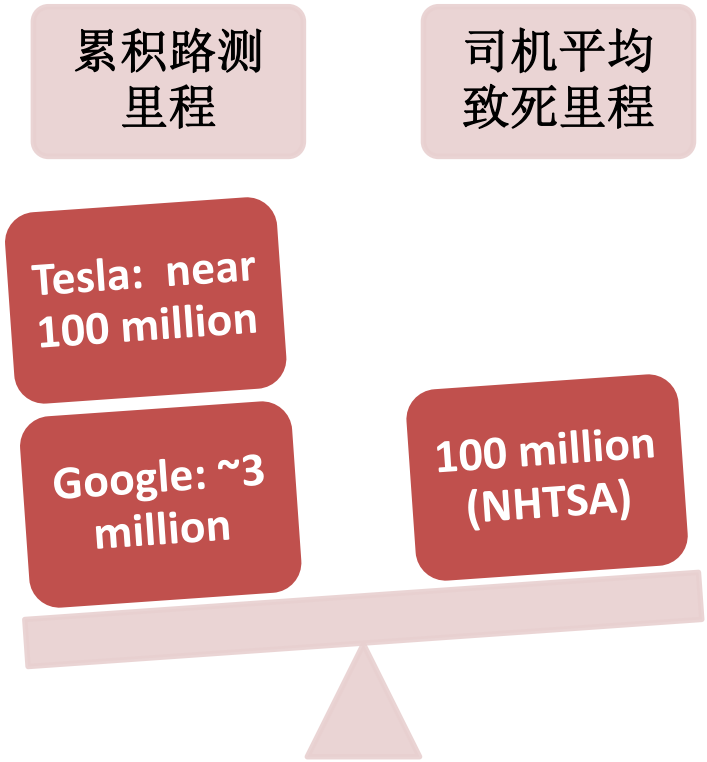
# 失效率指标及评估方式

**失效率指标：**

- 目前尚无标准政策
- ASIL 失效率定量值无意义
- 可对标人为失效概率
- 人因失效率约为10^-2

**评估方式：**

- 仿真测试
- 封闭路测
- 公共路测



火龙果 · 整理
uml.org.cn

# 内容 & 观点

智能驾驶 Hazard Analysis

智能驾驶 HARA and Safety Validation

**智能驾驶 Safety Mechanism**

- 不同智能驾驶级别→安全状态差异→安全设计差异
- 传统安全设计不足以防范智能驾驶风险

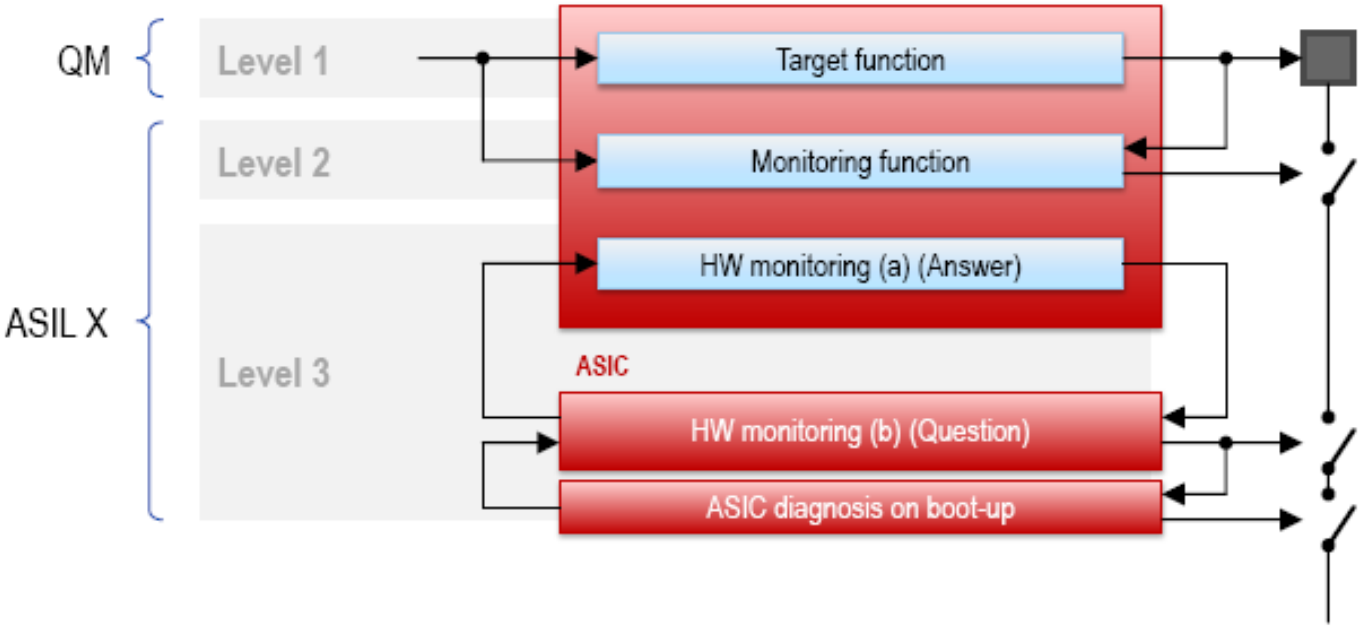
Highlights: ISO 26262 Application

火龙果 · 整理
uml.org.cn

# 智能驾驶 Safety Mechanism

| | |
|---|---|
| 危害产生原因？ | 部件失效 |
| | 软件失效 |
| | AI引入的新失效模式 |
| 怎样识别？ | 传感器失效模式、传感器能力识别 |
| | 基于概率的检测算法失效模式 |
| | 深度学习模型引入的失效 |
| 如何防范？ | Fail-safety: 不同level的安全侧定义 |
| | Fail-safety: 实时性要求 |

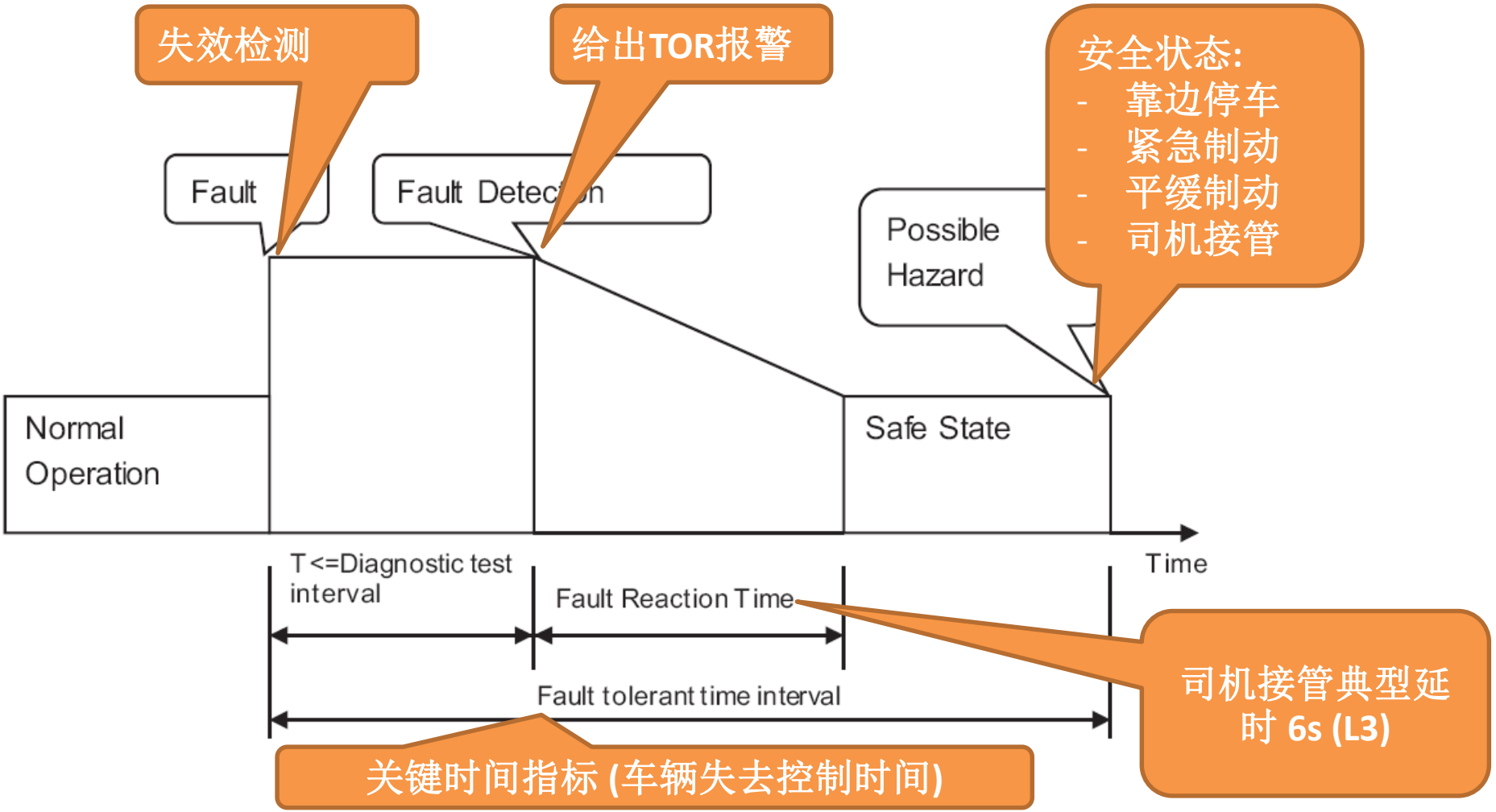
# 3-Level concept



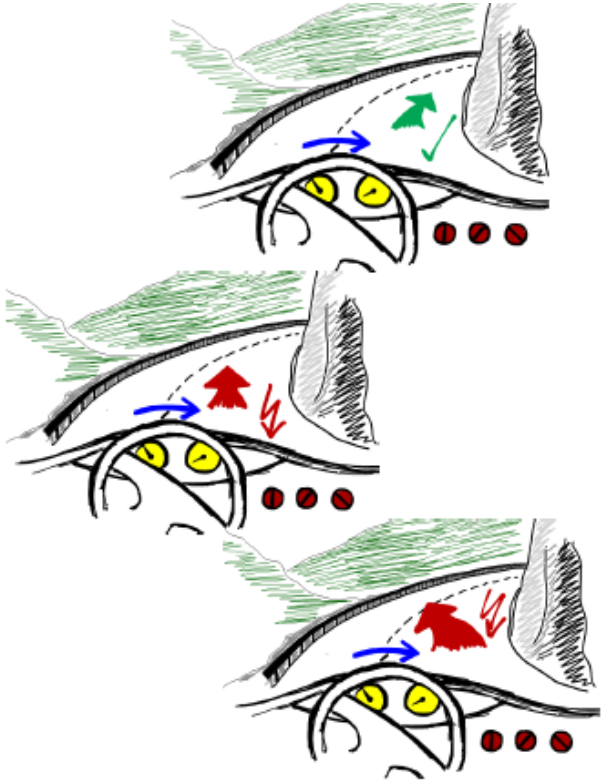

**3-Level concept在智能驾驶的应用挑战：**

- **Monitoring function**完整性的度量？
- 实施**Monitoring** 的硬件独立性？

# Safety mechanism: safe state



# 各级别智能驾驶的Fail-safety



- It is OK if the function works well
- It is NOT OK if the function works not at all
- It is NOT OK if the function works unintended

**Requirements:**

- There is a mechanism that detects failures
- There must be an alternative function that continues working
  - **Fail operational**: for a longer period of time
  - **Fail functional**: at least for a limited time

It is no option to quit the function!

- A fallback solution using other technologies is possible!
  → EPS can fall back to mechanics

**L1 & L2:**

- **Fail – takeover**

**L3:**

- **Fail – TOR**

**L4 & L5:**

- **Fail – operational**

[TUV SUD, Eason Dong]

火龙果 · 整理
uml.org.cn

# 内容 & 观点

智能驾驶 Hazard Analysis

智能驾驶 HARA and Safety Validation

智能驾驶 Safety Mechanism

**Highlights: ISO 26262 Application**

- 系统方法论对智能驾驶具有重要借鉴意义
- 挑战与局限：失效模式、人因影响、环境影响、软件规模……