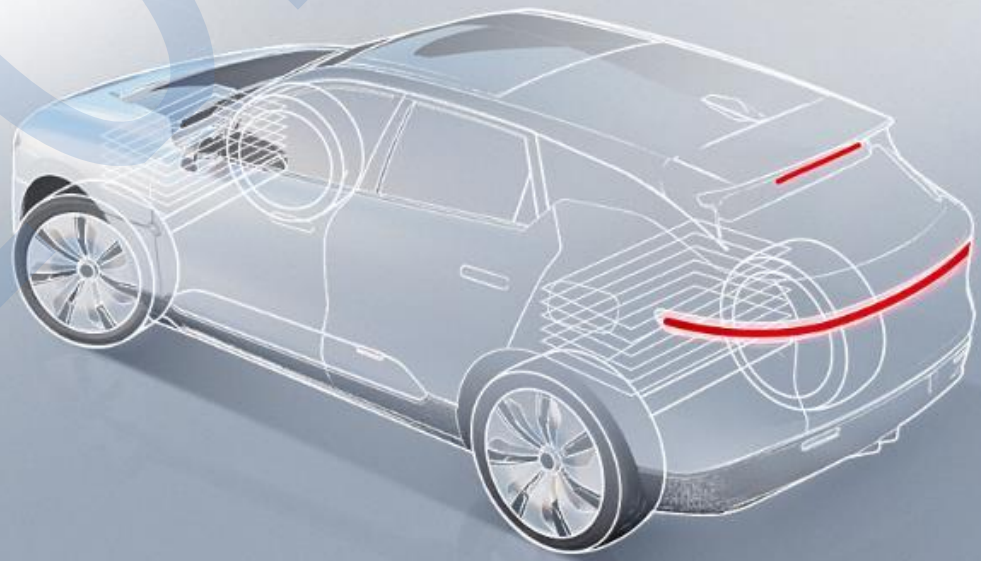
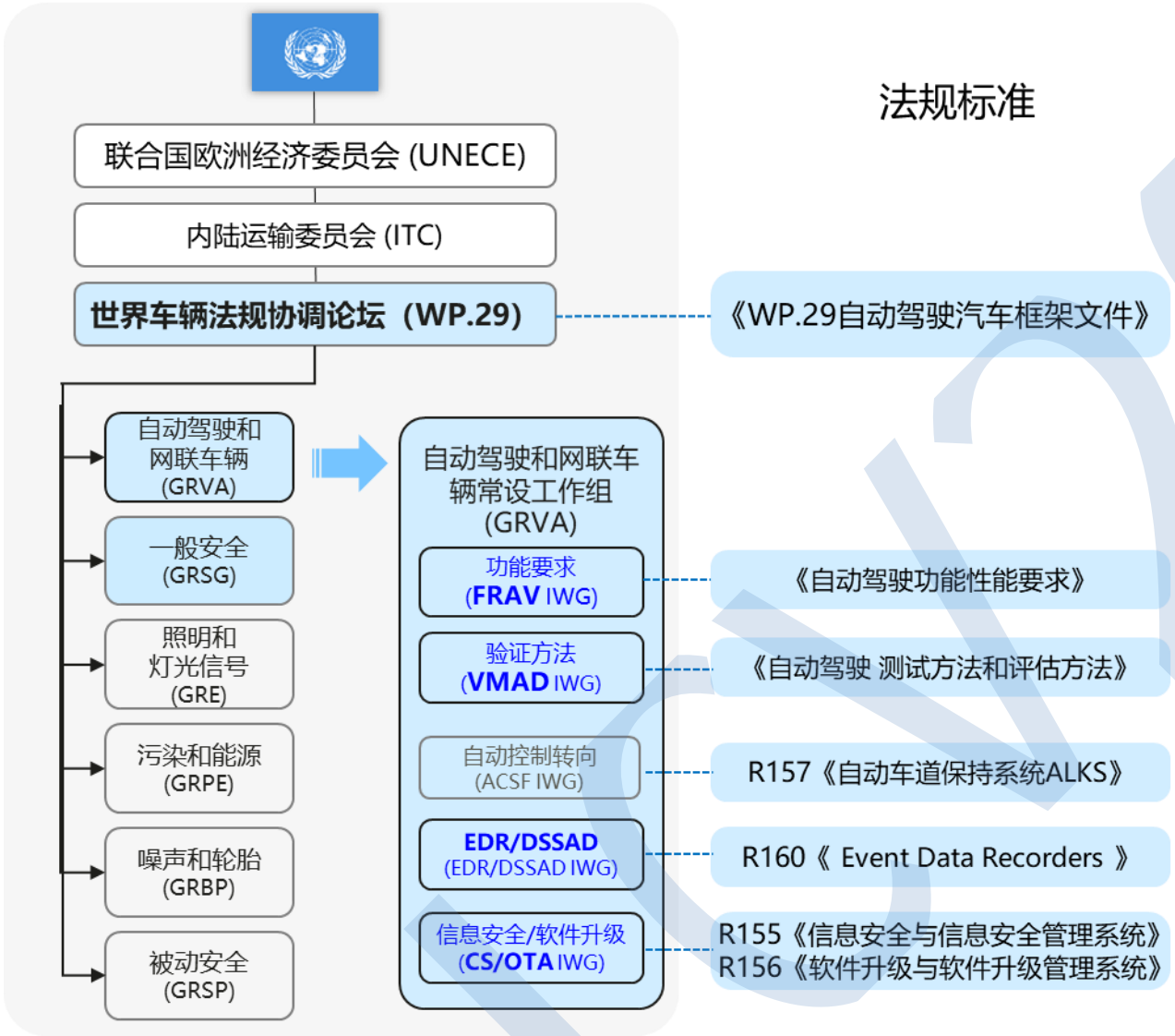
智能驾驶安全标准体系

万蕾
华为智能汽车解决方案
2021.07.07



HUAWEI

联合国智能网联法规：双V 确保 Safety & Security



法规标准

《WP.29自动驾驶汽车框架文件》

《自动驾驶功能性能要求》

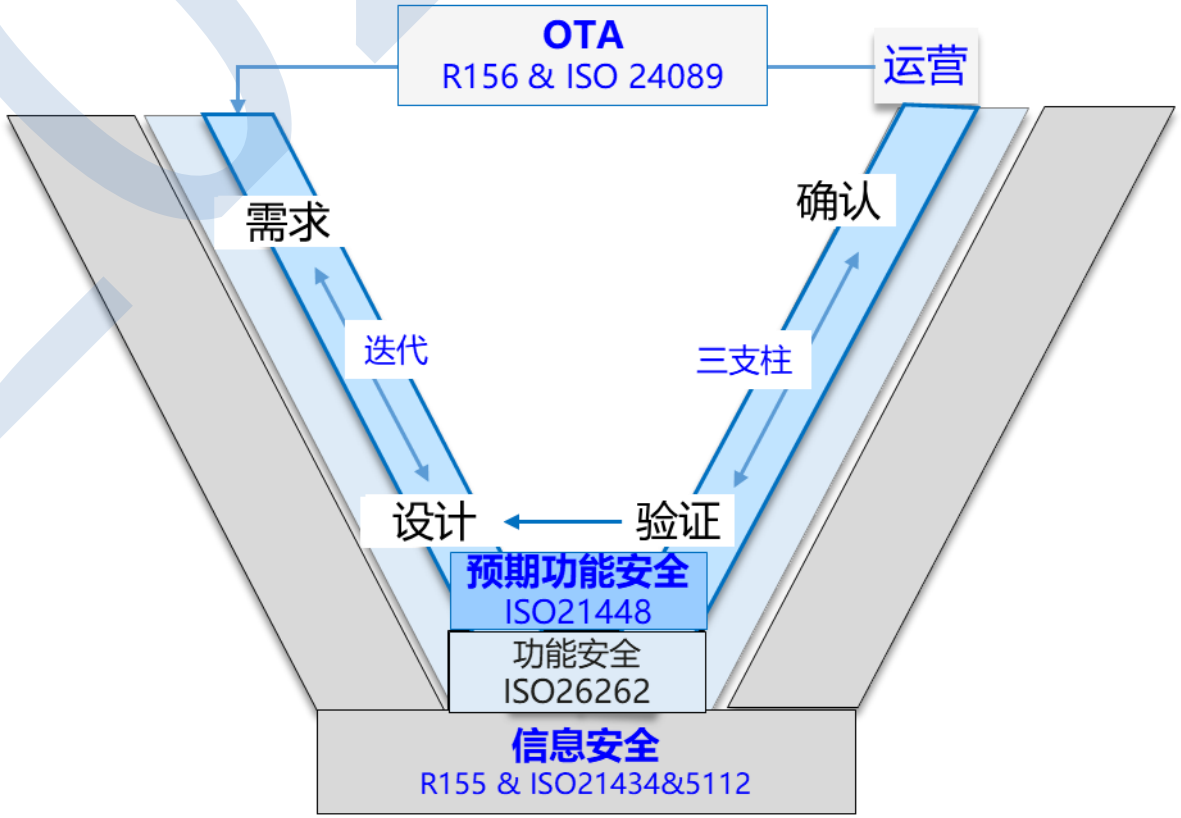
《自动驾驶 测试方法和评估方法》

R157《自动车道保持系统ALKS》

R160《 Event Data Recorders 》

R155《信息安全与信息安全管理系统》
R156《软件升级与软件升级管理系统》

自动驾驶车辆安全法规
双V 确保 Safety & Security



HUAWEI

自动驾驶标准热点

	ISO	SAE INTERNATIONAL	NTCAS 全国汽车标准化技术委员会 National Technical Committee of Auto Standardization	其他
Safety	功能安全FuSa ISO 26262 **预期功能安全SOTIF** ISO 21448	**自动驾驶等级方法** SAE J3016 STPA方法 SAE J3187	**FuSa & SOTIF** • GB/T 34590 修订 • GB/T 预期功能安全	IEEE **ADS 车辆行为模型假设** IEEE P2846
V&V	**ADS 场景构建** ISO 3450X	ADS 路测指导 SAE J3018	**三支柱体系** • GB/T 自动驾驶仿真试验方法及要求 • GB/T 自动驾驶场地测试方法及要求 • GB/T 自动驾驶开放道路测试方法及要求 • GB/T 自动驾驶通用技术要求 • GB/T 设计运行条件ODC	ASAM **ADS 仿真** • Open-Drive • Open-Scenario • Open-CRG
Security	**信息安全工程** ISO 21434	信息安全指导书 SAE J3061	**信息安全** • GB/T 道路车辆 信息安全工程 • GB/T 汽车网关信息安全技术要求及试验方法 • GB/T 车载信息交互系统信息安全技术要求及试验方法	
OTA	**OTA** ISO 24089		**OTA** 汽车软件升级技术要求	

注：STPA-System Theoretic Process Analysis；CRG-Curved Regular Grid

SOTIF标准（ISO 21448）定义

- **预期功能安全**（safety of the intended functionality， SOTIF）是指**由于功能不足（insufficiencies）引发的不合理风险**
- SOTIF和传统功能安全（FuSa）主要区别是危害事件的触发因素不同：**faults (FuSa) vs. insufficiencies (SOTIF)**

危害来源		
FuSa	**功能故障（faults）**	
SOTIF	**不足**	**specification insufficiency 规范不足** • 整车级规范不足 • 子系统/部件/EE元器件规范不足
		performance limitation 性能局限 • 子系统/部件/EE元器件性能局限
		合理可预见的误用（reasonably foreseeable misuse）
		可能导致安全隐患影响车辆决策的远程操作/协助/通信

SOTIF范畴

R&D相关流程阶段	设计	验证	确认	运营
机器相关行为&能力	感知判断	决策规控	执行	记录
人相关行为&界面	HMI	接管	DMS	MRM

SOTIF vs. FuSa

对比项	FuSa	SOTIF
危害根因	电子电气系统**故障** （随机硬件故障和系统性故障）	功能**不足**（insufficiency） （规范不足、功能局限、合理误用）
对象	所有**E/E**系统	复杂传感/决策/执行的E/E系统，重点**ADAS/ADS**
HARA分析	分析危害的严重/概率/可控程度，给出**ASIL**评级	• 沿用危害的严重/概率/可控程度分析 • 侧重于**Trigger Condition**的识别，如：环境、传感器性能、算力限制、HMI设计等
设计开发	• **正向开发**流程 • 原则：安全目标（safety goal）和ASIL等级	• **迭代开发**流程； • 原则：将更多**未知场景转为已知**，减少危害场景，同时控制危害场景的风险在可接受级别
测试验证	• 基于**确定性故障**类型 • 测试方法：**故障集注入测试**	• 基于**已知和未知场景**测试 • 测试方法：**三支柱**（封闭道路测试、开放道路测试、**模拟仿真**）
运行维护	传统售后，如：4S店维修/升级	• **OTA** 承担重要角色

*参考ISO DIS 21448

HARA分析

FuSa: 部件故障

以“安全气囊失效”为例

严重度	可控性 / 概率	C1~2	C3
S1~2	E1~4	QM/ ASIL-B	QM/ ASIL-B/C
S3	E1~3	QM/ASIL-B	ASIL-C
	E4	ASIL-B/C	ASIL-D

评级 → ASIL D

SOTIF: 传感器性能局限

以“碰撞翻车的白色卡车”为例

触发条件:

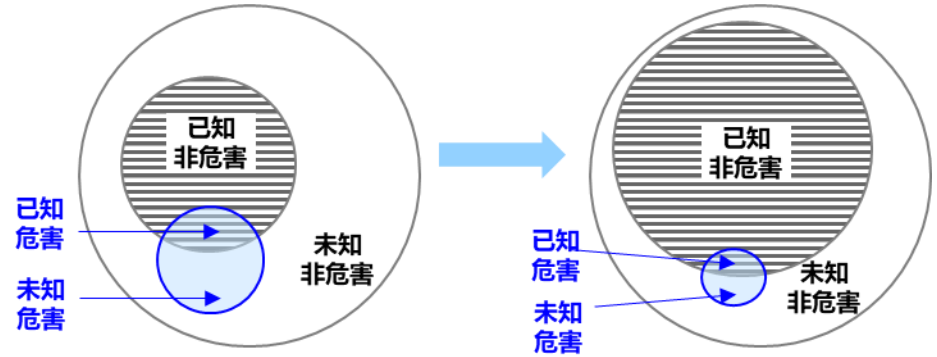
外: 强光+白色车顶镜面效果

内: 只有视觉传感器，无距离测量

危害事件:

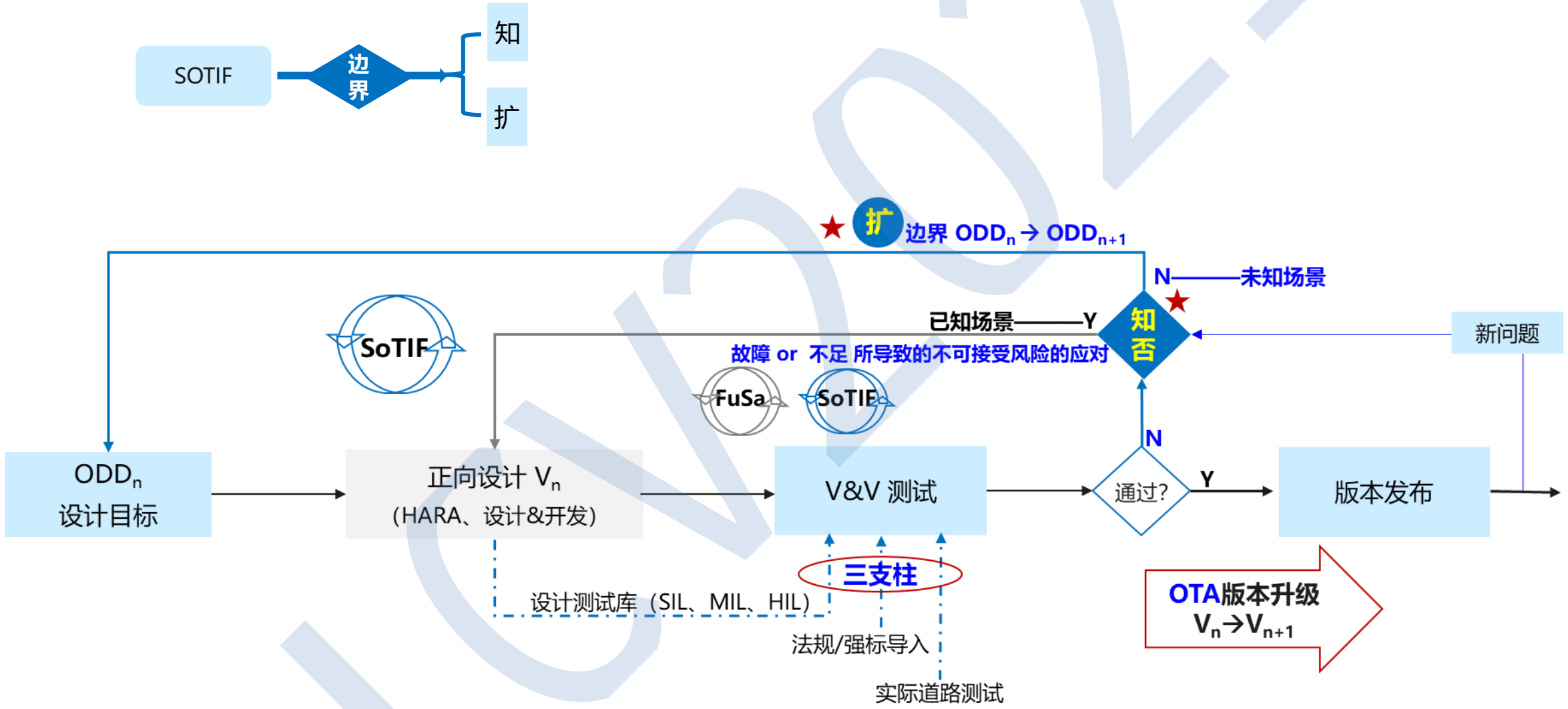
将白色车顶误识别为天空/云朵，未能识别障碍物，发生正面碰撞

从未知场景→已知场景



HUAWEI

SOTIF vs. FuSa：知/否



SOTIF：未知→ 潜在危害

潜在危害事件

外部：复杂多样的环境

目标复杂多样


两轮车


代步车

…

自然环境不确定性


傍晚


雾霾

…

行为复杂多样


横穿马路


逆行者

…

社会环境不确定性


白卡车→蓝天白云


红灯笼→红绿灯

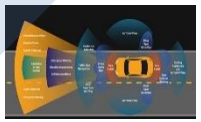
…

内部：系统设计不足 & 人/机认知差异

规范不足
Specification insufficiency

- 未充分考虑行人横穿、逆行等场景，无法正确应对
- 未考虑交通信号灯规范的变更，无法识别和解析新式红绿灯指示

性能局限
Performance limitation



- 视觉传感器对光照敏感，在强光下对目标识别准确率降低
- 机器学习算法对于未训练的目标识别与分类效果较差
- 制动系统在湿滑路面下制动效果减弱

合理误用
Reasonable Misuse

- 系统自动驾驶模式界面混淆，驾驶员不清楚人驾还是机驾
- 驾驶员在城区场景下，误触发仅在高速场景下使用的自动驾驶功能

HUAWEI

注：部分图片来自网络

SOTIF案例分析 —— 知/否

案例--2018年Uber 无人车致命事故:

2018年3月18日21:58左右，基于2017版Volvo XC90的改装Uber自动驾驶测试车，在“自动驾驶模式”下，撞上Mill大道的行人，当时她正推着自行车横穿一条多车道马路，且没有遵守交规走人行横道。此时车上的安全员正在用手机观看视频。经过一年多调查，最终美国检方宣布：Uber不承担刑事责任，当时在驾驶位的安全员需被进一步调查。

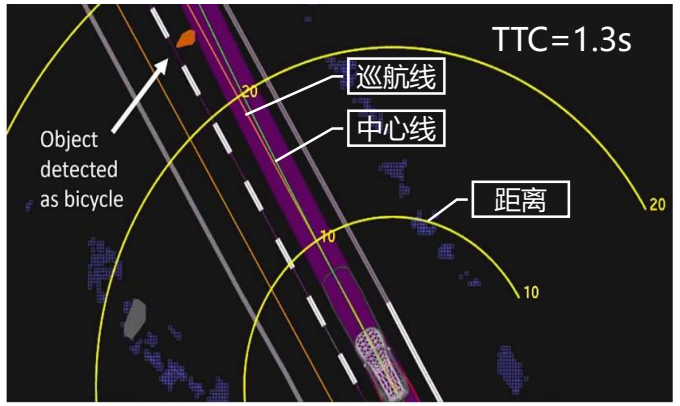
案例中主要危害来源分析:

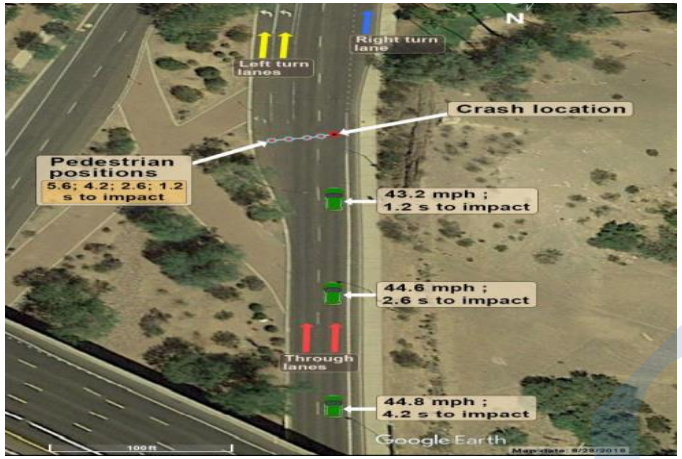
性能局限 **Performance limitation**		• **夜晚**，感知系统**未正确识别“pedestrian”**，在碰撞前5.2s识别到有目标，但在“unknown” “vehicle” “bicycle”之间摇摆； • **频繁更改识别结果导致系统无法准确计算其行驶轨迹**，一直在“静止”和“移动”之间摇摆，也没有意识到她处在与车辆碰撞的路线中； • 设计**未考虑到不守规则、横闯马路的行人**；
合理误用 **Reasonable Misuse**		• 事发时，司机正用手机看视频，未关注路况； • 在驾驶员将视线移开道路时，没有提醒功能；
规范不足 **Specification insufficiency**	AEB被关闭	• AEB被关闭，但**系统执行逻辑没有更改**，在遇到碰撞风险时仍会要求AEB提供辅助； • 紧急事件发生时，在刹车前设置了不必要的“action suppression” 缓冲时间

HUAWEI

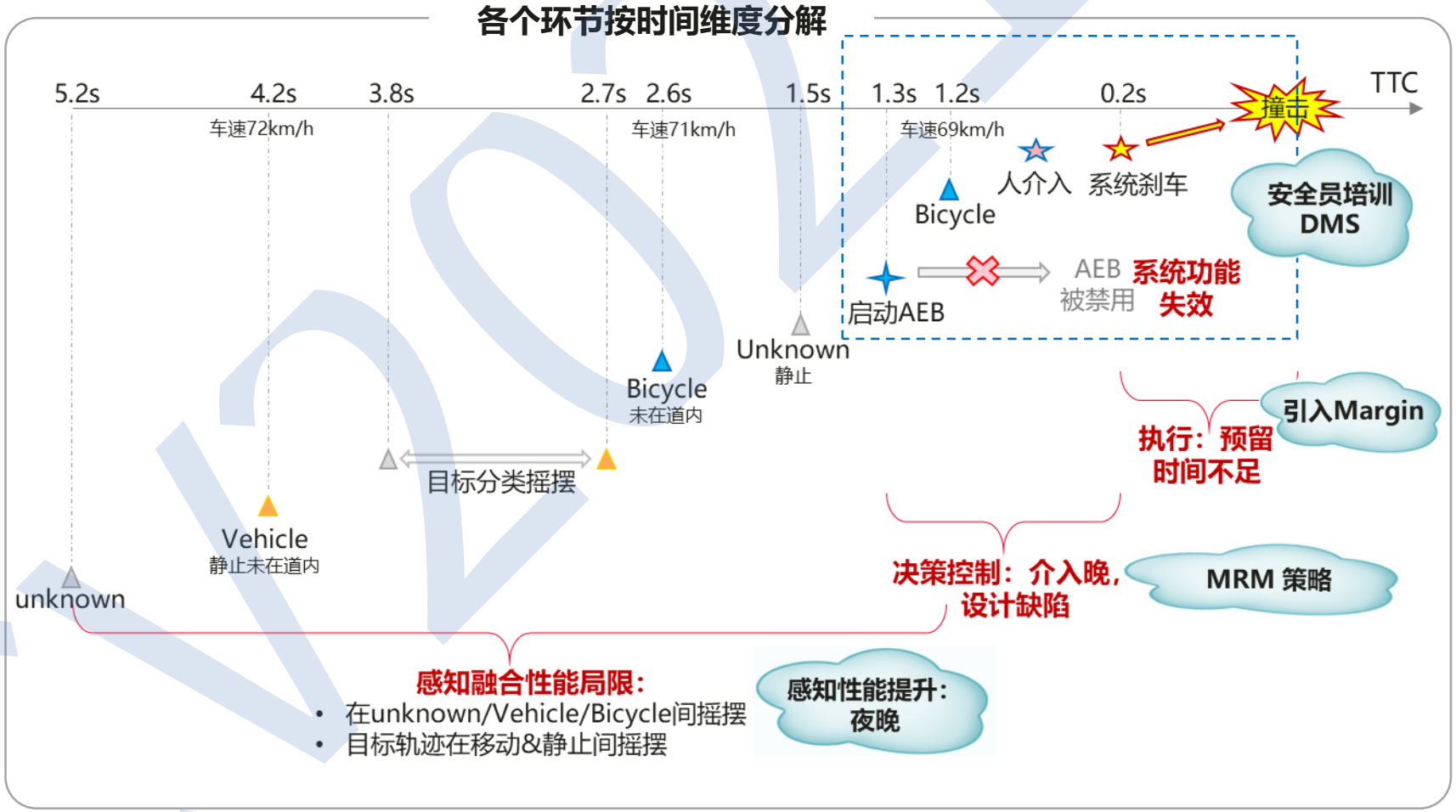
注：图片来自网络

SOTIF案例分析 —— Hazard应对涉及多个环节，需设计Margin





注：摘自美国国家运输安全委员会（National Transportation Safety Board，NTSB）报告；TTC：Time-To-Collision

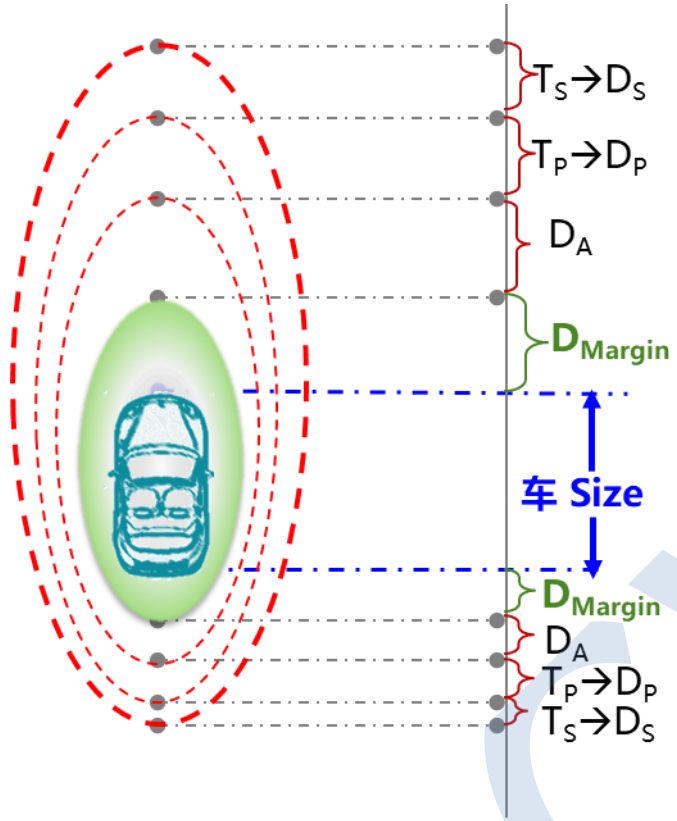


感知 → 规划/决策 → 控制 → 执行

$t_p + \delta_p$　$t_d + \delta_d$　$t_c + \delta_c$　$t_e + \delta_e$

- 每个环节都为未知环境预留处理时间margin
- 面对“未知环境”，降低车速，增大TTC，允许更长的端到端处理时延

智能驾驶：传统基于空间的安全域的痛点→ 安全时间域 STD



影响因素：
- 速度、算力、算法复杂度、
- 传感器工作范围、转向/制动性能、
- 决策规控策略、车型、外部环境因素

传统基于空间的安全域的痛点

度量不统一	设计评估复杂	不同车型影响

安全时间域：Safety Time Domain (STD)

STD定义

针对自动驾驶系统，在**时间域定义统一的安全模型**，来表征功能范围、安全边界、安全距离、路权、车辆的安全处置行为等安全相关概念，以用于自动驾驶车辆的安全设计和评估。

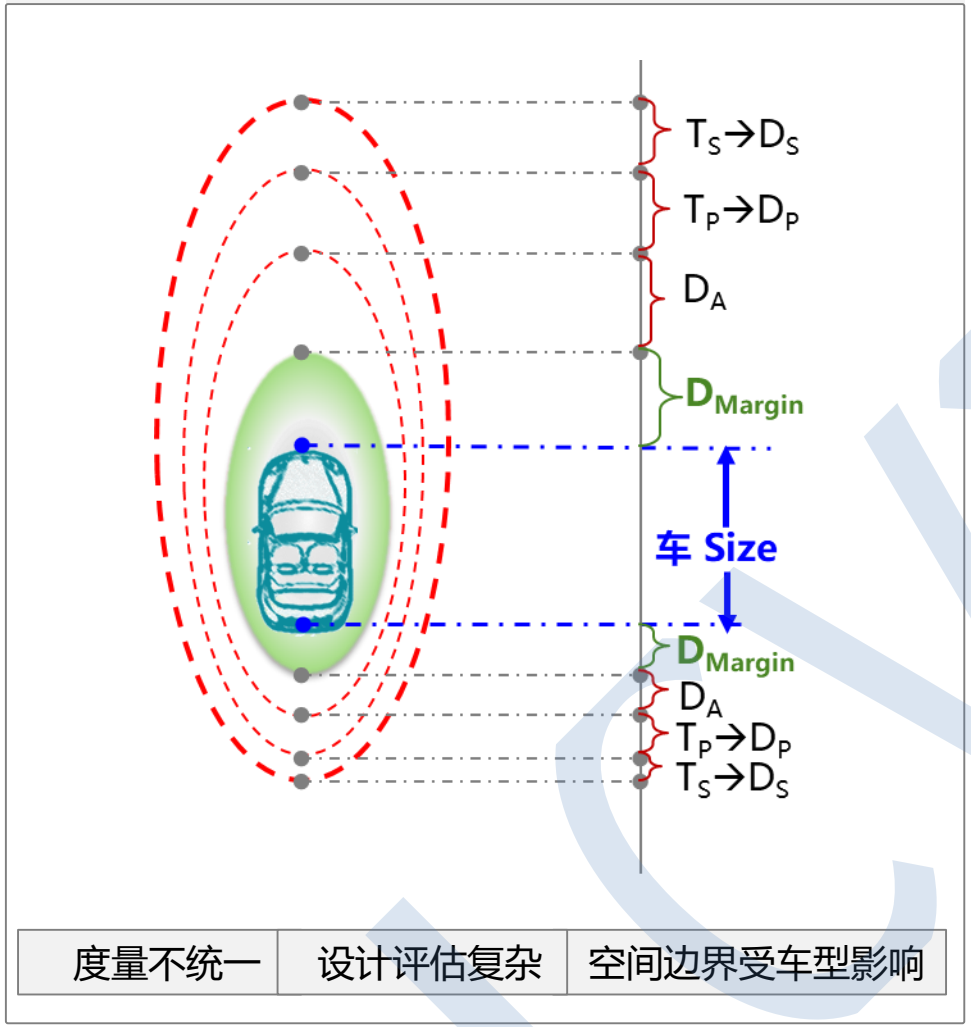
设计原则 $SBR \leq \Sigma \{FR_n, n = 1 \sim N\}$

- Function Range（**FR**）：AEB，BSD 等功能的作用范围
- Safety Boundary Requirement（**SBR**）：安全边界要求；车基于自身反应时间/刹车/防撞等能力，所允许的能保证自身安全性的最小边界范围

HUAWEI

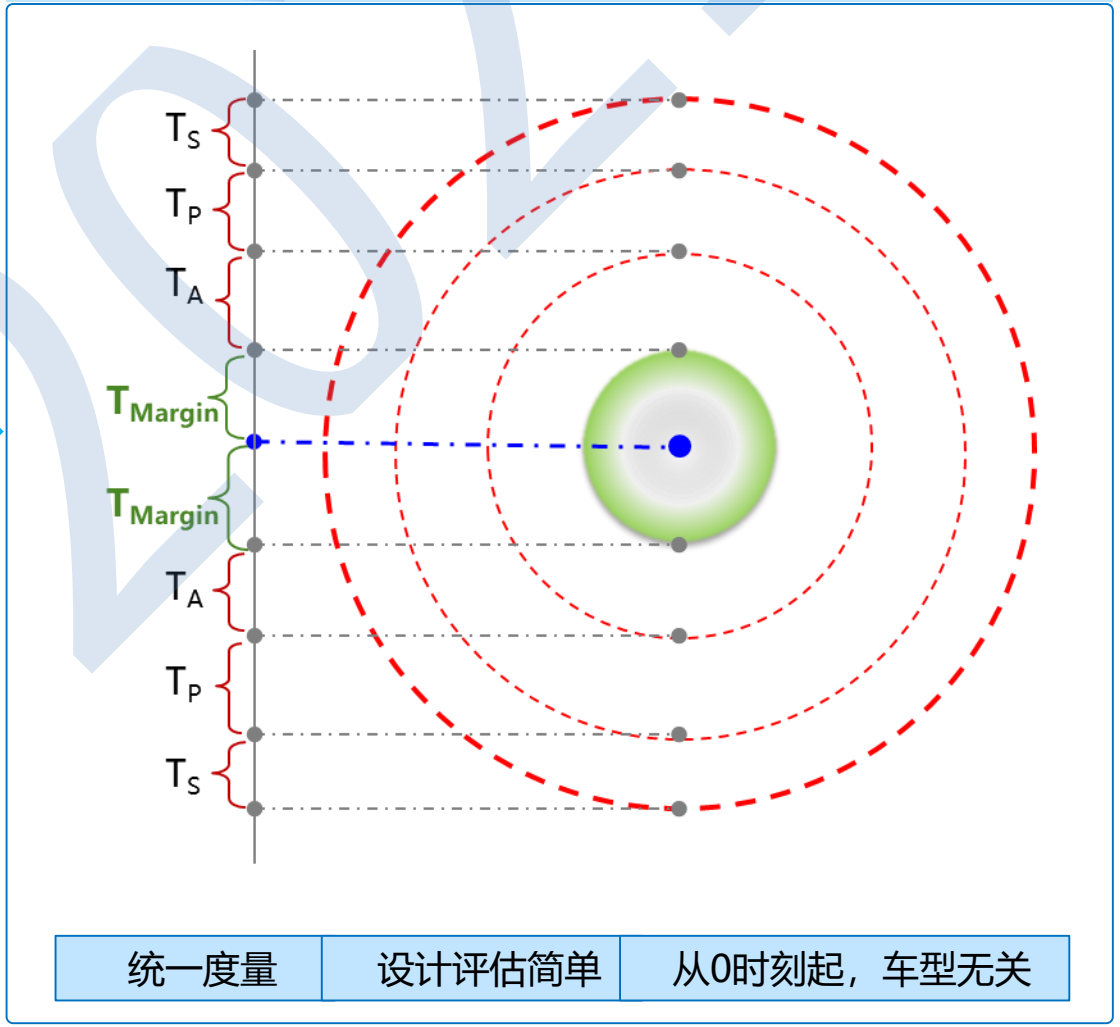
STD定义：安全时间域——统一度量

传统：安全空间域



度量不统一	设计评估复杂	空间边界受车型影响

STD: 安全时间域

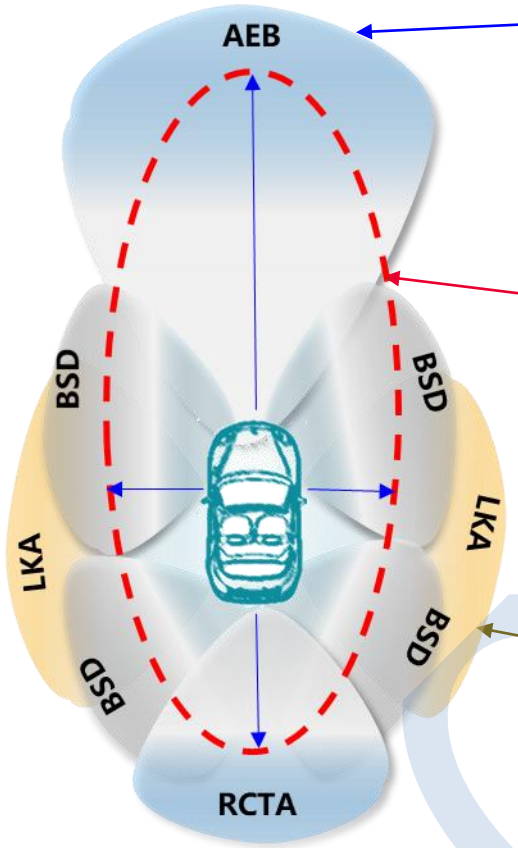


统一度量	设计评估简单	从0时刻起，车型无关

HUAWEI

STD定义：安全时间域——安全边界要求 & 功能范围

传统: 安全空间域



各向异性：受速度影响 | 空间边界受车型尺寸影响

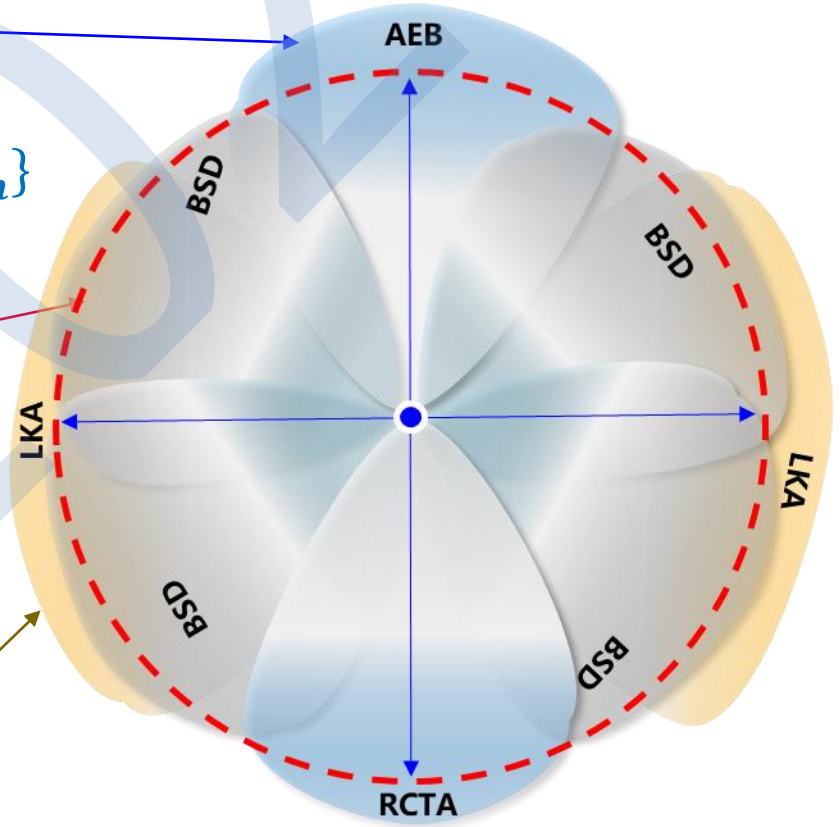
FR_{AEB}：AEB功能范围

设计原则：$SBR \leq \sum_{n=1}^{N} \{FR_n\}$

SBR：安全边界要求

FR_{LKA}：LKA功能范围

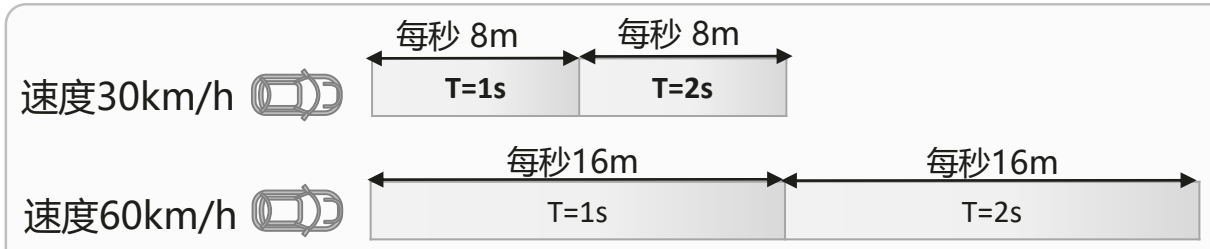
STD: 安全时间域



各向同性：各向典型速度不同 | 从0时刻起，车型无关

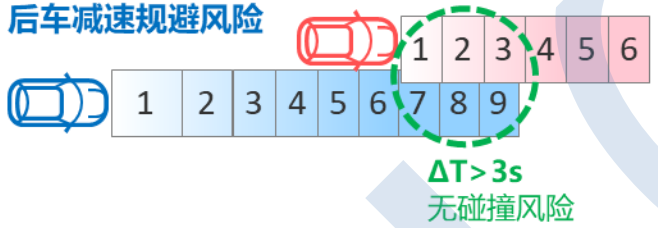
HUAWEI

多交通参与者交互场景下的STD

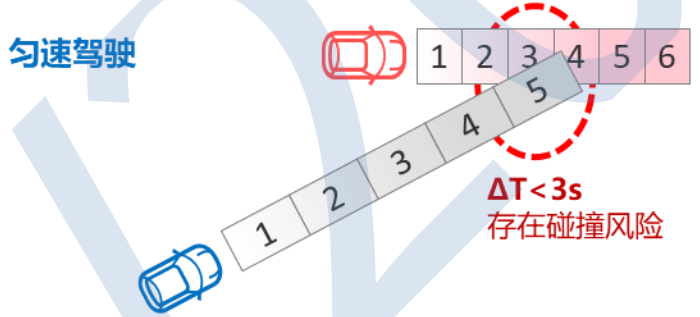


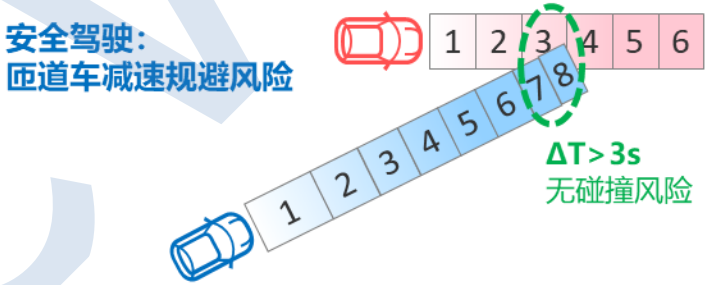
时间域路径（Route - time domain）：
基于交通参与者当前的**速度与加速度**，将T（T=#N s）到达预期路径上各点的时间值赋给预期路径

Case 1：同向行驶

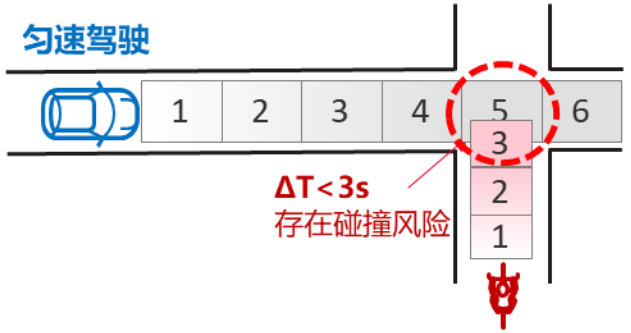


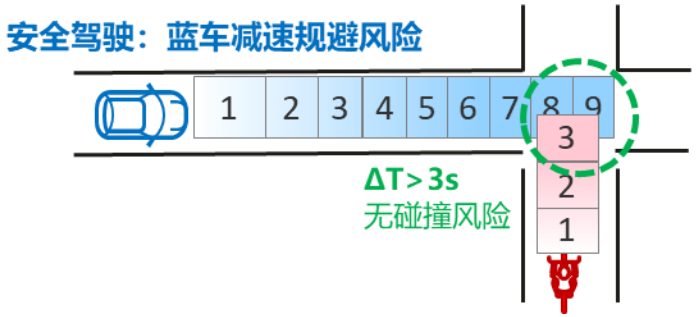
Case2：匝道





Case3：交叉路口





潜在碰撞风险：不同交通参与者的时间域路径若存在交叉区域，且多交通参与者在交叉区域处的时间差属于危险时差区间，则存在潜在碰撞风险

数字交规：机器（自动驾驶汽车）看得懂

模糊语义明确化 | **参数取值有理有据** | **方便转为机器语言执行**

人类驾驶：主观，灵活性 ⟹ **自动驾驶：客观，可量化**

《道交法实施条例》，机动车超车时，

- 应当提前开启左转向灯、变换使用远、近光灯或者鸣喇叭。
- 后车应当在确认有充足的安全距离后，从前车的左侧超越，
- 在与被超车辆拉开必要的安全距离后，开启右转向灯，驶回原车道。

[提前多少时间开启？]

[充足的安全距离是多少？]

[必要的安全距离是多少？]

STD安全距离模型：

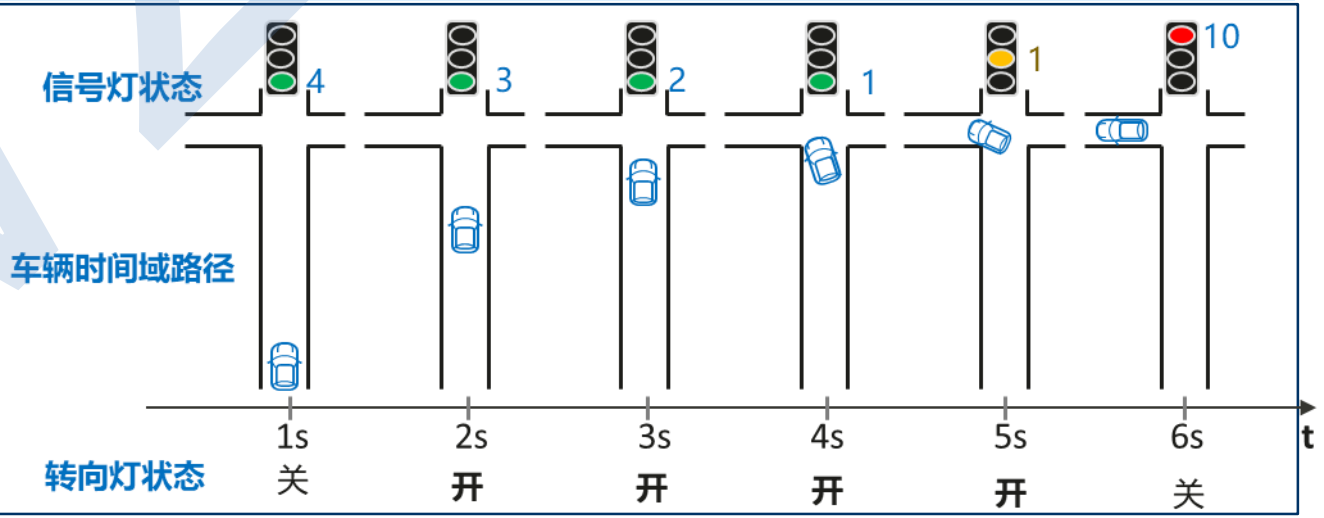
- 不同车速下，安全距离不同。
- 将安全在时间域定义，更符合机器判断逻辑

基于机器特点，在“安全时间域”定义“数字化交规”

很多交规都是建立在时间基础上的，如：

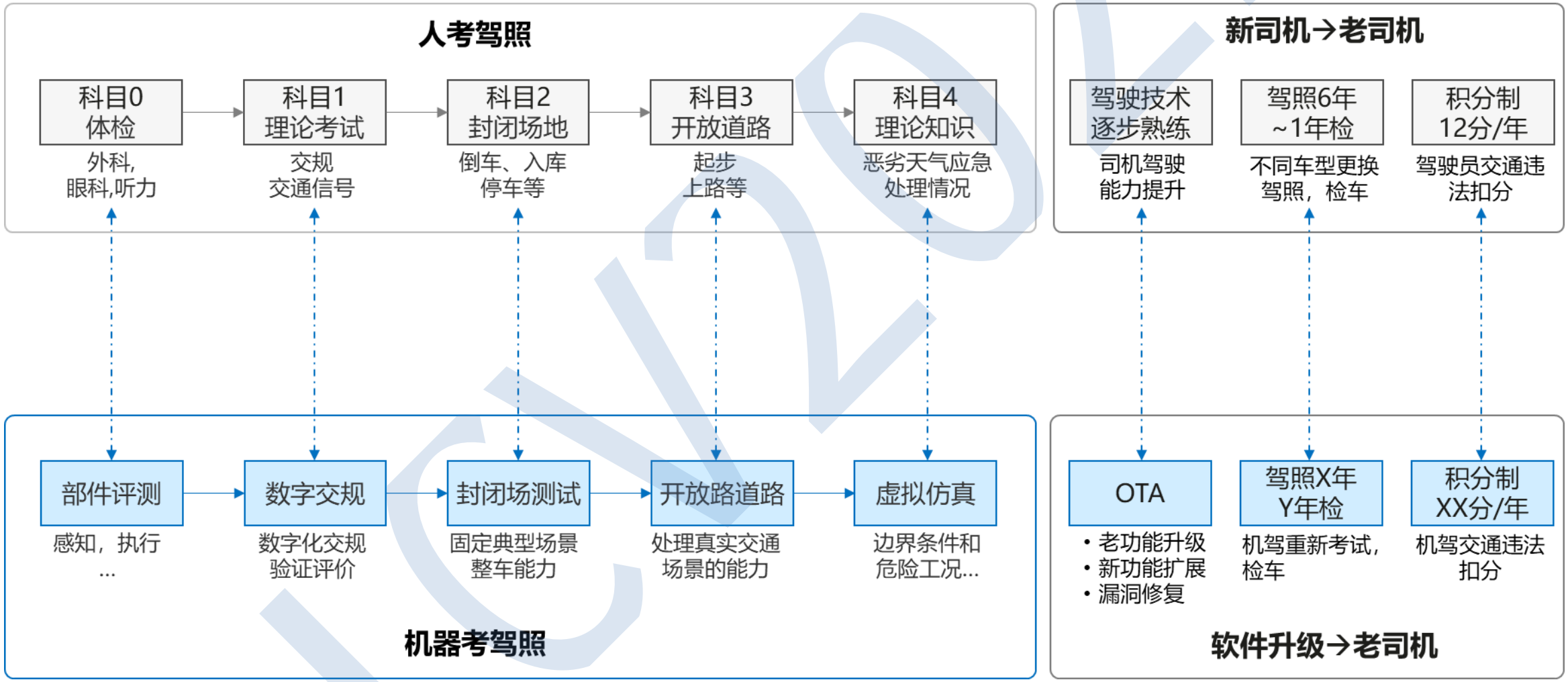
- 交通信号灯倒计时
- 提前开启转向灯

违章判断：**车辆时间域路径 & 转向灯状态** 匹配 **时间域交规事件**

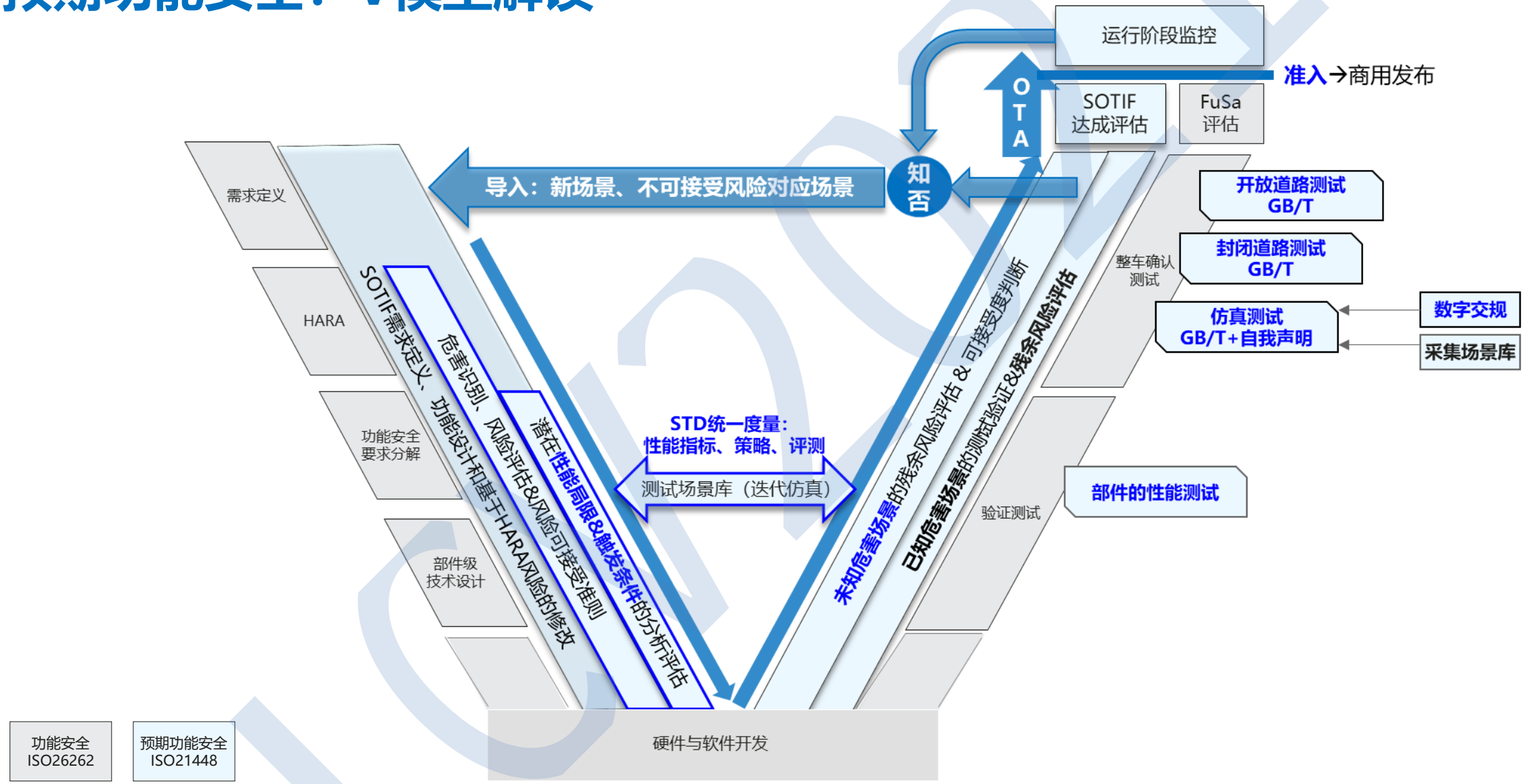


HUAWEI

自动驾驶车辆全生命周期：人机同规



预期功能安全：V模型解读



Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI