智能网联汽车系列知识分享（三）：HARA 分析及 ASIL 等级评定

一、什么是 HARA 与 ASIL 等级

ISO26262 实施过程中，一个重要的基础性步骤是对系统进行**危害分析和风险评估** HARA（Hazard Analysis and Risk Assessment），我们在 HARA 过程定义和识别出系统的危害并以此确定危害的风险等级——ASIL 等级(Automotive Safety Integrity Levels，汽车安全完整性等级)。

ASIL 有五个等级，分别为 QM，A，B，C，D，其中 QM 是最低的等级，D 是最高的等级。ASIL 等级决定了对系统安全性的要求，ASIL 等级越高，也意味着对系统的安全性要求越高，系统开发过程对软硬件的安全要求也越高，开发流程和技术也会要求的越严格。

功能安全（Fusa）活动是基于 ASIL 等级的。从第四部分到第六部分，许多要求和方法均与要素的 ASIL 等级关联，见表一.

方法		ASIL 等级			
		A	B	C	D
1a	检查 [a]	+	++	++	++
1b	走查 [a]	++	+	o	o
2a	仿真 [b]	+	+	++	++
2b	系统原型和车辆测试 [b]	+	+	++	++
3	系统架构设计分析 [c]	见表 1			

引自 ISO26262-5 表 2

说明：

++ 对于指定的 ASIL 等级，高度推荐该方法

+ 对于指定的 ASIL 等级，推荐该方法

o 对于指定的 ASIL 等级，不推荐也不反对

ASIL	示例	示例评分	示例要求:诊断覆盖/特定措施	在第 4，5，6 部分中的表格标记为++的项目数量
A	巡航控制:减速失效	S1，C2，E4	无	~50
B	巡航控制:减速度超出设计限制	S1，C3，E4	90%单点故障 60%潜伏故障	~80
C	乘客安全气囊错误展开	S3， C3，E1	97%单点故障 80%潜伏故障	~130
D	电动转向错误辅助，EPB 后轮锁死，SCS 错误介入	s3， c3，E4	99%单点故障 90%潜伏故障	~150

图一：更高的 ASIL 要求更多的工作示例

二、HARA 危害分析和风险评估流程

1、HARA 应基于相关项定义来进行，并且**不考虑**相关项中计划实施或已经实施的安全机制。危害分析和风险评估由三个基本步骤构成:

1) Hazard Identification 危害识别

识别相关项可能引起危险事件的潜在非预期行为。包括:

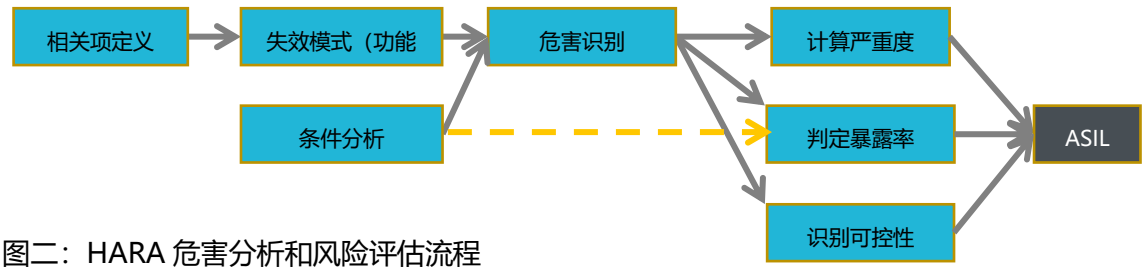
- 定义相关项可能的功能异常
- 条件分析

2) Hazard Classification 危害分级

判定与相关项危害关联的严重度（S)、暴露度（E）和可控性（C）

3) ASIL Determination ASIL 判定

判定要求的 ASIL 等级。



图二：HARA 危害分析和风险评估流程

2、危害识别

危害分析包括功能异常及运行条件分析。

危害← 功能异常 + 运行条件

功能异常 Malfunction 是指相关项在其设计目的（功能要求）方面的失效或非预期行为。特定的功能异常导致失效模式（Failure Mode)。典型的功能异常包括:

- NO function 无功能

- REVERSE function 相反的功能
- MORE/LESS function 过多/过少的功能
- PARTIAL function 部分功能
- function EARLY 功能过早
- function LATE 功能过晚
- Unexpected 非预期的功能

ID	功能名称	功能需求		MF-ID	功能异常	故障导致失效模式
IR001	按照指令展开	速度>30km/h 时发生正面碰撞(固态障碍物)时	n ms 内全面展开	IR001_MF1	无功能	不展开
				IR001_MF2	部分功能	未完全展开
				IR001_MF3	过晚功能	展开时间> n ms
				IR001_MF4	非预期功能	无正面碰撞时展开

表二：功能异常分析（安全气囊系统）示例

故障只有在特定的驾驶场景下（运行条件），才会造成真正的危害，即人身伤害。以雨刮为例，如果在恶劣的天气环境影响下，如暴雪，大雨等天气，雨刮器不工作，随着前挡风玻璃逐渐被雨雪附着，驾驶员看不清道路状况，可能会造成严重的交通事故；而此功能故障如果发生在晴朗的天气就不会产生任何安全上的影响，只是会一定程度影响用户体验。所以在进行危害分析时，需进行运行条件分析。

运行条件分析需要识别所有相关的运行条件，包括：

- 车辆使用情景，例如高速驾驶，城市驾驶，停车，越野等；
- 环境条件，如道路表面附着力，侧风等
- 合理可预期的驾驶员使用和误用；
- 与操作系统之间的交互。

3、危害分级

危害分级涉及到三个方面：

- Severity 严重度 (S)
- Exposure 暴露度(E)
- Controllability 可控性(C)

等级	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害

等级	E0	E1	E2	E3	E4

描述	不可能	非常低的概率	低概率	中等概率	高概率

等级	C0	C1	C2	C3
描述	可控	简单可控	一般可控	难以控制或不可控

表三：S/E/C 评级表　　引自 ISO26262-3 表 1/2/3

4、ASIL 等级判定

ASIL 根据三个因子——严重度（Severity）、暴露率（Exposure）和可控性（Controllability）进行风险等级的判定。

严重度等级	暴露度等级	可控性等级		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	QM	QM	QM
严重度等级	暴露度等级	可控性等级		
		C1	C2	C3
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

表四：ASIL 等级评定表　　引自 ISO26262-3 表 4