概念阶段安全目标的量化评估方法

赵令国　宁甲奎　唐文强　刘阳　秦加合

（中国第一汽车股份有限公司研发总院，长春 130011）

【欢迎引用】赵令国，宁甲奎，唐文强，等．概念阶段安全目标的量化评估方法[J]．汽车文摘，2026(9)：50-57.

【Cite this paper】ZHAO L G, NING J Q, TANG W Q, et al. Quantitative Evaluation Method of Safety Goal During Concept Phase[J]. Automotive Digest (Chinese), 2026(9): 50-57.

【摘要】针对概念阶段功能安全量化数据缺失的问题，基于ISO 26262标准，提出一种安全目标量化评估方法。通过构建故障场景动力学与人身伤害特征的映射模型，利用仿真实现严重度（S）、可控性（C）及故障容错时间间隔（FTTI）的定量计算。结果表明：FTTI随车头时距增大而增加，随驾驶员反应时间延长而缩短，高速工况对上述参数变化更为敏感。该方法仅通过参数配置高效输出量化指标，为概念阶段安全目标的精准制定提供支撑。

关键词：功能安全；危害分析与风险评估；安全目标；安全状态

中图分类号：X951　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20240315

Quantitative Evaluation Method of Safety Goal During Concept Phase

Zhao Lingguo, Ning Jiakui, Tang Wenqiang, Liu Yang, Qin Jiahe

(Global R&D Center, China FAW Corporation Limited, Changchun 130013)

【Abstract】To address the issue of quantitative data during the concept phase, this paper proposes a quantitative safety goal assessment method based on the ISO 26262 standard. By establishing a mapping model between fault scenario dynamics and injury characteristics, simulations were conducted to quantitatively determine the Severity (S), Controllability (C), and Fault Tolerant Time Interval (FTTI). The results indicate that the FTTI increases with rising time headway but decreases as driver reaction time extends; moreover, high-speed conditions exhibit higher sensitivity to variations in these parameters. Without requiring physical prototypes, this method efficiently generates quantitative metrics through parameter configuration, thereby supporting the precise definition of safety goals in the concept phase.

Key words: Function safety, Hazard analysis and risk assessment, Safety goal, Safety state

0　引言

随着汽车电动化、智能化、网联化进程加速，整车电子电气架构及软件算法的复杂度显著提升，由电子电气系统性失效、随机硬件失效带来的整车安全风险日益受到行业关注。ISO 26262功能安全标准旨在通过全生命周期的安全管理，规避因电子电气系统故障导致的不合理风险。危害分析与风险评估（Hazard Analysis and Risk Assessment, HARA）作为功能安全开发的起始环节，其核心任务是识别潜在危害事件，确定汽车安全完整性等级（Automotive Safety Integrity Level, ASIL），并导出整车级安全目标，以指导后续开发活动。

根据ISO 26262标准[1]，HARA需针对特定运行场景，评估系统功能异常行为可能导致的整车危害及其对车内乘员与周边交通参与者的伤害风险。安全目标需根据评估的严重度等级（Severity，S）、暴露概率等级（Exposure，E）、可控性等级（Controllability，C）确定汽车安全完整性等级（Automotive Safety Integrity Level，ASIL）。其中，暴露概率仅取决于运行场景与工作模式，与系统失效无关。而严重度等级、可控性等级不仅与运行场景与工作模式相关，还与系统功能失效导致的整车危害相关。为降低后续技术安全开发的复杂度，需要在HARA分析过程中将原理类似的危害进行归类分析，并提出统一的安全目标。除定义安全状态外，安全目标还需明确ASIL等级、安全状态、故障容错时间间隔（Fault Tolerant Time Interval，FTTI）。其中，FTTI[2]定义为从相关项发生故障到潜在危害事件发生

所允许的最短时间窗口，即安全机制需在此时限内激活，以确保车辆在规定时间内进入规定的安全状态。

目前，HARA分析方法主要包括定性、仿真和实车试验3种。在定性分析方面，文献[3-7]对线控制动等车辆关键安全系统进行了HARA分析。Chen等[8]提出了融合系统理论过程分析（Systems Theoretic Process Analysis, STPA）与失效模式及影响分析（Failure Mode and Effects Analysis, FMEA）的综合评估方法。为提高评估结果的可信度，文献[9-10]提出基于规则集与专家评审的机制，以降低因评估者主观认知差异导致的偏差。在行业标准方面，SAE J2980提供了HARA分析的指导流程，但没有提及如何进行相关安全量化参数的计算方法[11]。德国汽车工业协会标准VDA 702[12]虽针对特定场景细化了暴露概率等级，但在严重度与可控性的量化判定上仍存在不足。在量化评估技术方面，Sini等[13]利用整车仿真平台构建了虚拟测试环境，实现了对碰撞相对速度与时间等参数的计算。Kwon等[14]通过实车故障注入试验确定了非预期转向助力失效的FTTI指标。然而，上述量化方法高度依赖成熟的物理验证平台或固化的系统定义，在产品开发的概念阶段，受限于功能定义尚未锁定及硬件原型缺失，难以有效实施。

基于模型的仿真技术通过构建物理系统虚拟原型，支持开发前期的快速迭代与可重复验证，有效提升研发效率与精度[15]。为避免后期设计变更导致的周期延长与成本增加，本文提出了一种概念阶段安全目标的量化评估方法。该方法首先解析车辆非预期失效引发的功能异常行为及人员干预的交互机制，构建故障场景动力学与人员伤害特征间的映射关系及关联数学模型；然后，将模型嵌入系统仿真平台，通过输出关键场景量化参数，实现对严重度（S）与可控性（C）等级的定量评估，并推导具体的FTTI指标。本文详细阐述该方法的实施流程，以前车非预期制动危害为例进行了实例验证，输出量化的安全目标，旨在为概念阶段功能安全开发提供数据支撑。

1　量化评估方法流程

为明确评估边界与物理含义，首先对关键术语定义如下：

（1）安全量化参数：用于量化评估严重度等级、可控性等级和确定FTTI的相关物理参数。

（2）碰撞相对速度：车辆与其他车辆、物体、行人碰撞时的相对速度。

（3）驾驶员反应时间：从车辆故障导致的功能异常表现开始，到本车或其他车辆驾驶员为避免导致人身伤害的碰撞事故发生而采取有效操作所经历的时间间隔。

安全量化指标计算流程如图1所示，以下对每个环节分别进行阐述。

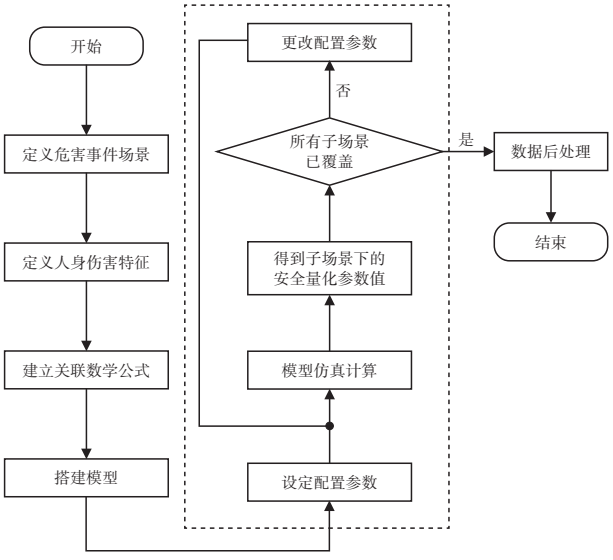


图1　安全量化指标计算流程

（1）危害事件场景定义：危害事件场景需要定义在特定的运行场景及工作模式下，由系统功能异常至人身伤害产生的具体过程。场景要素涵盖功能异常表现、工作模式、运行环境及目标安全项。其中，在评估严重度等级和确定FTTI时，危害事件场景不考虑安全机制作用，但可以考虑驾驶员按照C0可控性等级进行的安全操作。而在进行可控性等级量化指标计算时，无需考虑安全机制的作用但需考虑驾驶员操作的影响，使最终危害事件的严重度等级为S0。针对相同失效模式的危害场景，可进行聚类分析，并通过调整配置参数形成差异化的子场景，以支撑后续安全量化参数的仿真计算。

（2）人身伤害特征定义：人身伤害特征是指判定车辆危害事件是否导致驾乘人员出现人身伤害的判断准则。该特征需依据车辆配置、运行场景等变量进行具体设定。人身伤害特征举例如表1所示。

（3）关联数学公式建立：通过分析危害事件场景的发生过程与人身伤害特征之间的关系，建立关联数学公式。在进行可控性等级量化参数计算时，计算得到的驾驶员反应时间确保满足人身伤害特征。进行严重度等级和FTTI的量化参数计算时，需要考虑驾驶员按照C0可控性等级对应的反应时间，模拟驾驶员在标准生理极限下的避险操作。

表1　人身伤害特征举例

整车危害	运行场景	人身伤害特征
车辆非预期移动	车辆周围2 m存在行人	车辆不允许与行人碰撞
车辆非预期反向移动		
坡路无法驻车		
车轮非预期抱死失去转弯能力	车辆在弯道行驶，且路边存在固定物	车辆与路边固定物碰撞时，相对速度需≤2.5 km/h
	车辆在弯道行驶，且路边存在行人	车辆不允许与行人碰撞
前车非预期制动	两车在同一车道以相同速度行驶	车辆追尾碰撞时，相对速度需≤7 km/h

通过按照一定步长改变规定的时间变量，依据关联数学公式计算得到车辆碰撞对应的时间点，继而计算得到该碰撞时间点对应的安全量化参数值。此外，也需设置车速、时间等物理量不能小于零的物理限制。针对不同的细分子场景，则通过条件关系式来加以区分。

(4)仿真模型搭建：根据关联数学公式、物理限制及条件关系式搭建模型。模型主要包括时间变量步进设定、初始车距计算、时间计算、车速计算、行驶距离计算、碰撞判断模块。其中，针对车辆的初始车速、初始车距、前车加速度、后车加速度、C0可控性等级对应的驾驶员反应时间等配置参数需要根据细分子场景的具体情况进行设定。

(5)仿真计算执行：根据子场景设定配置参数，进行模型仿真计算，得到当前子场景下的安全量化参数值。重复以上过程，直到所有同类型的子场景均已被覆盖，即得到所有配置参数组合的仿真计算结果。

(6)数据后处理：针对严重度等级和可控性等级的判断，需要结合相关评判准则得到子场景的严重度等级与可控性等级。以前车非预期制动举例，严重度等级评判参考SAE J2980标准中的B1表格，以表2规定的碰撞相对速度作为评判指标。可控性等级评判方面，因后车驾驶员能直接观察到前车的非预期减速行为，根据驾驶员反应时间作为可控性等级的评判标准(表3)，计算得到的驾驶员反应时间越短，代表对后车驾驶员制动反应速度要求越高，因而可控性等级越高。

准确的评判准则由车型结构、车辆安全辅助配置、乘员状态与健康情况、避险能力等因素决定，可通过专家判断、历史事故分析、模拟仿真、实车试验进行确定[11]。在得到所有子场景的严重度等级与可控性等级后，结合对应子场景的暴露概率等级，可以得到不同子场景的ASIL等级。其中，最高的ASIL等级将被用于安全目标的制定。而针对FTTI，对所有不为QM ASIL等级对应的FTTI进行比较，选取最小值作为最终的FTTI。

表2　严重度等级评判准则举例

严重度等级	碰撞时相对速度 V_d/km·h^{-1}
S0	$V_d \leqslant 7$
S1	$7 < V_d \leqslant 35$
S2	$35 < V_d \leqslant 50$
S3	$V_d > 50$

表3　可控性等级评判准则举例

可控性等级	驾驶员反应时间 T_r/s
C0	$T_r \geqslant 2$
C1	$1.3 \leqslant T_r < 2.0$
C2	$0.95 \leqslant T_r < 1.30$
C3	$T_r < 0.95$

2　量化评估方法的典型应用

在前车非预期制动导致后车追尾碰撞的危害事件中应用本方法，以完成严重度等级与可控性等级的量化评估，并得到FTTI指标。

2.1　可控性等级的量化评估

2.1.1　定义危害事件场景

车辆非预期制动属于常见的电控系统故障导致的车辆危害现象。本危害事件场景定义为前、后两车以相同车速在同一车道行驶，行驶速度范围为10~130 km/h，两车初始距离为S_0。按时间顺序对车辆行为进行描述，如图2所示。

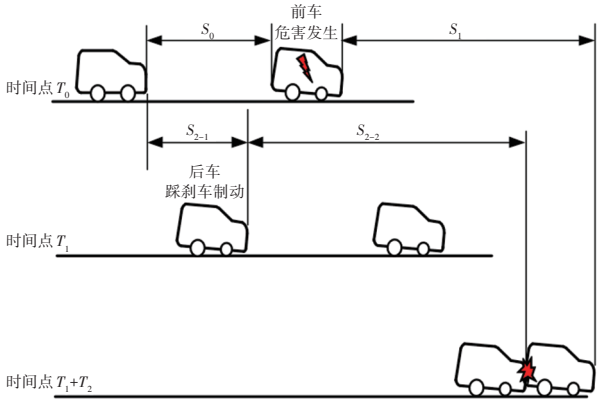


图2　用于评估可控性等级的危害事件场景

时间点T_0：两车以相同速度在同一车道同向行驶，两车初始间距为S_0。前车在行驶过程中由于电控系统故障导致非预期制动危害事件的发生，前车减速

度为A_f。

时间点T_1：前车非预期制动后经过时间点T_1，后车驾驶员进行制动以避免与前车发生追尾碰撞，后车减速度为A_b。

时间点T_1+T_2：后车制动后经过T_2时两车发生追尾碰撞。

2.1.2 定义人身伤害特征

针对前后车追尾碰撞场景，依据行业相关法规及人体耐受损伤阈值，设定碰撞相对速度V_{S0}≤7 km/h时，车内乘员不存在人身伤害风险。因此，定义车辆安全碰撞相对速度V_{S0}=7 km/h，作为后续严重度等级判定的物理依据。

2.1.3 建立数学公式

对危害事件场景进行分析后，通过建立危害事件场景与人身伤害特征之间的关系可得到如下关联数学公式。

车辆初始间距S_0由车辆初始车速V_0与车头时距T_{head}确定。其中，车头时距定义为前、后两辆车的车头通过同一地点的时间差[15]。

$$S_0 = V_0 \times T_{head} \tag{1}$$

式中：S_0为初始间距，V_0为初始车速，T_{head}为车头时距。

设后车驾驶员反应时间为T_1，为满足碰撞相对速度V_{S0}的要求，需计算后车所需减速时间T_2。前车从初速V_0匀减速至静止所需时间为T_{Spd0}。

$$T_{Spd0} = \frac{V_0}{A_f} \tag{2}$$

为保证两车碰撞时严重度等级为S0，碰撞相对速度须控制在V_{S0}。假设碰撞时前车未减速到静止，则后车减速时间为：

$$T_{2-1} = \frac{(A_f \times T_1 - V_{S0})}{A_b - A_f} \tag{3}$$

当$T_1+T_{2-1}<T_{Spd0}$，说明碰撞时前车未减速到静止，此时后车减速时间$T_2=T_{2-1}$。

当$T_1+T_{2-1}\geqslant T_{Spd0}$，说明碰撞时前车已减速到静止，则后车减速时间$T_2=T_{2-2}$。

$$T_{2-2} = \frac{(V_0 - V_{S0})}{A_b} \tag{4}$$

通过计算得到的T_1与T_2结合其他参数计算前车行驶距离S_1和后车行驶距离S_2。按一定步长逐步更改T_1，并计算两车各自的行驶距离。当两车各自行驶距离相差为S_0时，则认定两车发生追尾碰撞。此时对应的T_1即为对应场景下的驾驶员反应时间。当$S_2 \geqslant S_1 + S_0$时，认定两车发生追尾碰撞。

2.1.4 模型搭建

根据上述数学公式、条件关系式及物理限制，搭建相关仿真模型。模型包括变量步进设定、时间计算、车速计算、行驶距离计算、碰撞判断以及驾驶员反应时间显示模块，部分模块介绍如下。

（1）变量步进设定模块：该模块以步长T_{step}对将变量T_1进行累加并利用上述公式计算两车的行驶距离，以判断两车是否发生碰撞（图3）。步长的设定决定了最终计算得到的驾驶员反应时间的精度。

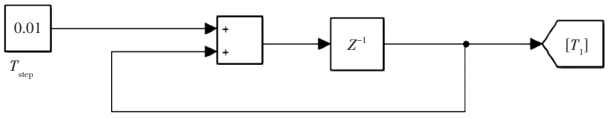


图3 变量步进设定模块

（2）后车减速时间T_2计算模块：根据式（3）、式（4）、相关条件关系式及物理限制搭建后车减速时间T_2的计算模块（图4）。该模块利用Simulink中的Switch逻辑模块，实时比较T_1+T_{2-1}与T_{Spd0}的大小关系，自动切换计算分支。若前车未停止，输出T_{2-1}；若前车已停止，则切换至T_{2-2}的计算逻辑，从而实现不同工况下的T_2动态求解。

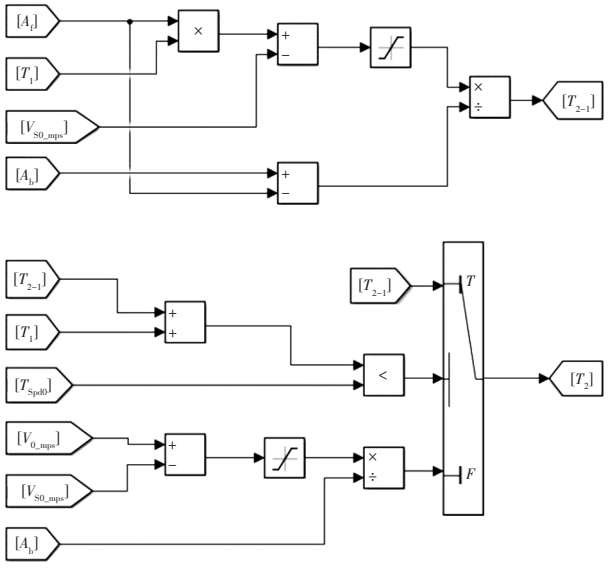


图4 后车减速时间计算模块

除上述核心模块外，车辆初始间距S_0、前车减速时间T_1、前车车速V_1、前车行驶距离S_1、后车车速V_2、后车行驶距离S_2，也均按对应的数学公式进行建模。

模型通过逻辑判断模块实时监测两车相对位置。定义碰撞标志变量P_{harm}。当后车行驶距离满足或超过前车行驶距离与初始间距之和（$S_2\geqslant S_1+S_0$）时，P_{harm}会由0变为1。当系统检测到P_{harm}的上升沿触发锁存机制时，此时T_1即为后车驾驶员反应时间T_r。以典型

工况为例进行仿真验证：设定车头时距T_{head}=1.8 s，初始车速V_0=50 km/h，前车减速度A_f=7 m/s^2，后车减速度A_b=8 m/s^2。在该组参数下，模型输出的驾驶员最小反应时间T_r为1.95 s。

2.1.5 仿真与数据处理

本模型中将车头时距T_{head}、初始车速V_0、前车减速度A_f、后车减速度A_b设定为配置参数。通过对表4配置参数设定不同的数值并进行仿真，可以得到对应子场景的驾驶员反应时间。配置参数的所有数值组合均被计算后，依据前面规定的评判准则可以确定不同子场景下的可控性等级。部分计算得到的驾驶员反应时间与对应的可控性等级如表5所示。

表4 可控性等级评估的模型配置参数

配置参数	仿真数值
T_{head}/s	1.0, 1.4 ,1.8
V_0/km·h^{-1}	10, 30, 50, 70, 90, 110, 130
A_f/m·s^{-2}	7
A_b/m·s^{-2}	8

表5 不同子场景下可控性等级评估

T_{head}/s	V_0/km·h^{-1}	T_r/s	可控性等级
1.8	10	1.91	C1
	50	1.95	C1
	90	2.04	C0
	130	2.13	C0

2.2 严重度等级的量化评估与FTTI的确定

2.2.1 定义危害事件场景

本危害事件场景针对同车道行驶的车辆发生前车非预期制动的故障模式。设定前后两车初始速度相同，取值范围为10~130 km/h，两车初始距离为S_0。按时间顺序对车辆行为进行描述，如图5、图6所示。

时间点T_0：两车以相同速度在同一车道同向行驶，两车初始间距为S_0。此时前车在行驶过程中由于电控系统故障发生非预期制动现象，前车减速度为A_f。

时间点T_{C0}：前车非预期制动后经过T_{C0}时，后车驾驶员进行制动以避免与前车发生追尾碰撞，后车减速度为A_b。其中，T_{C0}对应可控性等级为C0的驾驶员反应时间，即保证后车驾驶员可执行常规可控的制动前提下，计算两车碰撞相对速度与FTTI值。

时间点T：前车产生非预期制动开始到两车发生追尾碰撞所经历的时间为T。需要注意的是，T可能小于T_{C0}，即在后车驾驶员进行制动前两车已发生碰撞。或者T大于T_{C0}，即两车碰撞在后车驾驶员制动后发生。

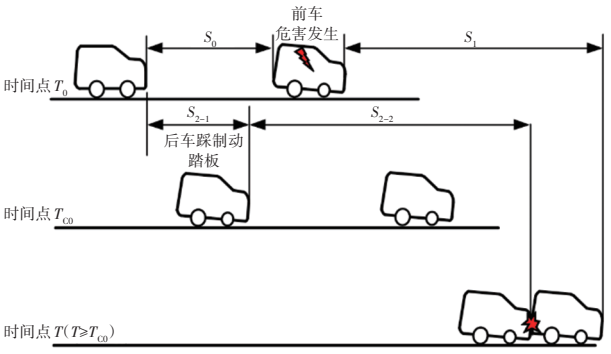


图5 用于评估严重度等级的危害事件场景（$T\geq T_{C0}$）

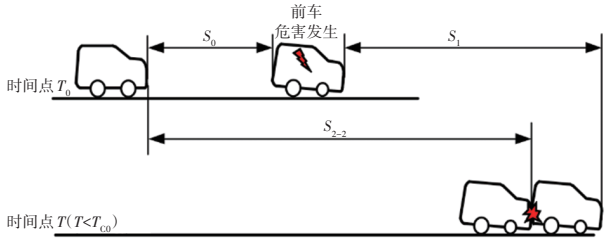


图6 用于评估严重度等级的危害事件场景（$T<T_{C0}$）

2.2.2 定义人身伤害特征

人身伤害特征定义需计算两车发生碰撞时的碰撞相对速度V_d，以进行严重度等级评估。

2.2.3 建立数学公式

车辆初始间距S_0按照式(1)进行计算，且前车的车速为V_1，前车的减速距离为S_1。

当$T\geq T_{C0}$时，使用式(5)计算后车车速V_2。当$T<T_{C0}$，使用式(6)计算后车车速V_2。

$$V_2 = V_0 - A_b \times (T - T_{C0}) \quad (5)$$

$$V_2 = V_0 \quad (6)$$

当$T\geq T_{C0}$，使用式(7)计算后车车速S_2。当$T<T_{C0}$时，使用式(8)计算后车车速S_2。

$$S_2 = V_0 \times T_{C0} + \frac{V_0^2 - V_2^2}{2 \times A_b} \quad (7)$$

$$S_2 = V_0 \times T \quad (8)$$

当$S_2\geq S_1+S_0$时，认定两车发生追尾碰撞，碰撞时两车相对速度$V_d=V_2-V_1$。

2.2.4 模型搭建

模型包括变量步进设定、车速计算、行驶距离计算、碰撞判断以及碰撞相对速度与FTTI显示模块。将变量T以一定步长进行累加并利用关联数学公式计算两车的行驶距离，以判断两车是否发生碰撞。

2.2.5 仿真与数据处理

本模型的车头时距T_{head}、初始车速V_0、前车减速度A_f、后车减速度A_b以及C0等级对应的驾驶员反应时间

T_{C0}为配置参数。通过对表6参数进行模型仿真，可以得到各个子场景的碰撞相对速度及FTTI。依据表2规定的评判准则可以确定对应场景下的严重度等级。部分计算得到的FTTI值、碰撞相对速度及对应的严重度等级如表7所示。

表6　严重度等级评估的模型配置参数

配置参数	仿真数值
T_{head}/s	1.0, 1.4 ,1.8
V_0/km·h^{-1}	10, 30, 50, 70, 90, 110, 130
A_f/m·s^{-2}	7
A_b/m·s^{-2}	8
T_{C0}/s	1.5, 2, 2.5

表7　不同子场景下严重度等级（T_{C0}=2 s）

T_{head}/s	V_0/km·h^{-1}	FTTI/s	V_d/km·h^{-1}	严重度等级
1.8	10	2.00	10	S1
	50	3.23	14.58	S1
	90	无法碰撞		S0
	130	无法碰撞		S0

上述在各个子场景的严重度等级和可控性等级确定后，结合该场景对应的暴露概率等级即可确定相应的ASIL等级，所有子场景中最高的等级即为该安全目标的ASIL等级。而针对FTTI，需选择所有不为质量管理（Quality Management, QM）等级的子场景中最小的时间值作为最终的FTTI指标，以保证在最严苛工况下系统仍能及时响应。

3　数据分析与讨论

安全量化参数的分析结果直接决定了后续安全机制的触发阈值与设计边界，是功能安全概念设计的核心输入。本节基于前文的仿真数据集，重点探讨车头时距与驾驶员反应时间对FTTI及碰撞相对速度的影响规律。

驾驶员反应时间的影响：在保持C0级基准驾驶员反应时间恒定（如T_{C0}=2 s）的前提下，仿真结果表明，随着车头时距T_{head}的增加，FTTI值呈显著上升趋势，而碰撞相对速度则逐渐降低，如图7、图8所示。这表明较大的跟车间距为系统提供了更充裕的故障响应窗口，同时有效缓解了碰撞剧烈程度，验证了增大车头时距对提升行车安全的积极作用。

驾驶员反应时间的影响：当车头时距维持不变（如T_{head}=1.4 s），且增加C0等级对应的驾驶员反应时间T_{C0}时，FTTI值呈现下降趋势，而碰撞相对速度增加，如图9、图10所示。相较于低速工况，高速工况下的FTTI与碰撞相对速度对T_{C0}的变化更为敏感。这意味着在高速场景下，驾驶员哪怕是微小的反应延迟，都将显著压缩系统的容错时间窗口，并大幅加剧潜在的碰撞严重程度。因此，在高速运行场景的安全目标设定中，应对驾驶员反应时间预留更为保守的设计裕度。

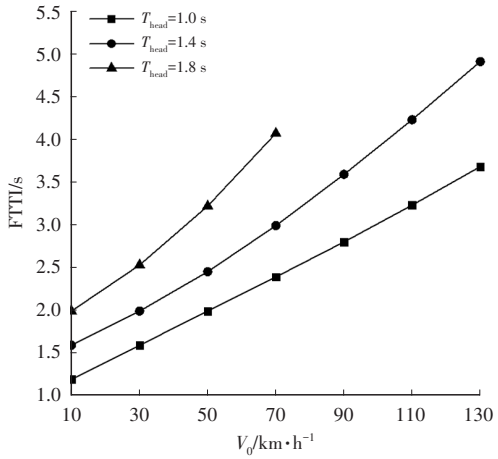


图7　不同车速下的FTTI值（T_{C0}=2 s）

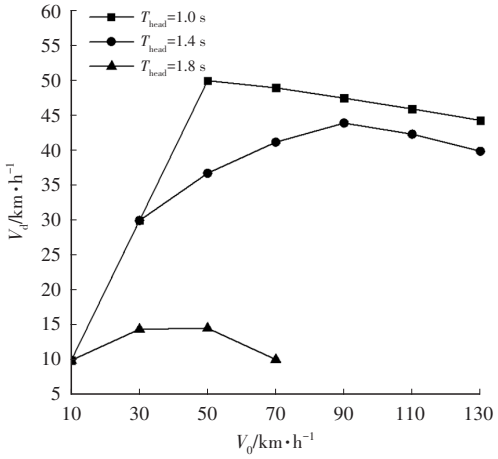


图8　不同车速下的碰撞相对速度（T_{C0}=2 s）

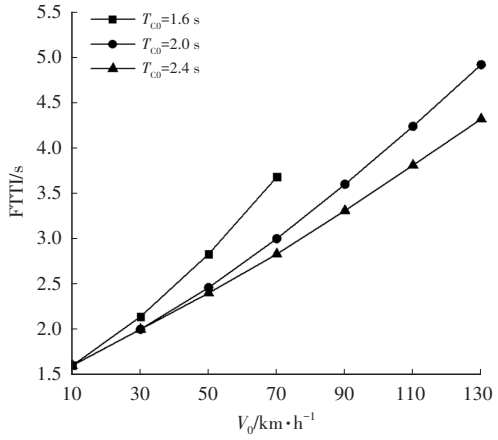


图9　不同车速下的FTTI值（T_{head}=1.4 s）

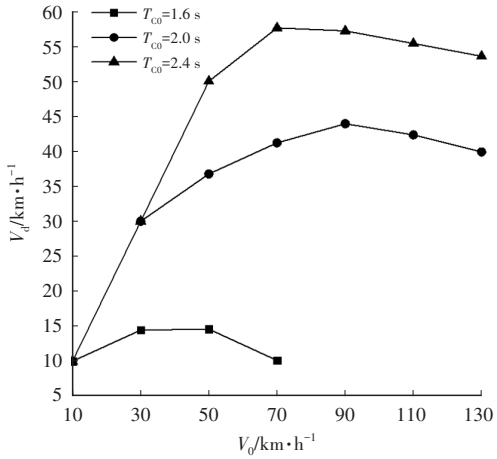


图10　不同车速下的碰撞相对速度(T_{head}=1.4 s)

综上,增加车头时距与减少后车驾驶员反应时间对于降低人身伤害风险具有重要现实意义。可以通过增加技术手段实现以上效果,如配备雷达探测驾驶车辆与前车之间距离,根据两车距离等参数计算驾驶员反应时间,当驾驶员反应时间小于阈值时进行仪表提示。对于减少驾驶员反应时间,则可以考虑在监控到能导致车辆非预期制动的故障时,车辆滑行的同时通过驱动制动灯来警示后车驾驶员,以达到提升后车驾驶员反应速度的效果。由此提出两条安全状态,如表8所示。

表8　功能安全状态

安全项	安全状态描述
安全状态1	当后车探测到与前车距离过近时(驾驶员反应时间小于阈值),则进行仪表提示
安全状态2	当监控到非预期制动故障后,车辆滑行并点亮制动灯

4　结束语

在汽车电子产品迭代周期持续缩短的背景下,尽早进行安全目标的准确定义对于后续功能安全开发具有重要的现实意义。针对当前功能安全开发中缺乏适用于概念阶段、通用性强且成本低廉的量化评估手段的问题,本文提出了一种基于模型的安全目标量化评估方法。

该方法通过解析危害事件场景与人身伤害特征之间的映射关系,构建了关联数学描述,并搭建了仿真模型。结果表明该方法在以下方面具有优势:

(1)高效性与易用性:在尚未开展详细技术设计的概念阶段,本方法仅需通过调整配置参数,即可实现对同类失效模式下多子场景安全量化参数的快速迭代计算,无需依赖昂贵的专用仿真软件或物理测试环境,显著缩短了评估周期。

(2)有效性验证:将该方法应用于车辆非预期制动危害的分析,成功量化了不同场景下的可控性(C)等级、严重度(S)等级及FTTI,验证了方法的工程实用价值。

(3)指导性与扩展性:基于仿真数据的敏感性分析,揭示了关键参数对行车安全的演变规律,为安全状态的精准定义提供了数据支撑。由此导出的安全目标可作为顶层输入,逐级分解为功能安全需求并分配至软硬件组件,从而有效指导后续的设计、分析与验证活动。

综上,本文提出的方法为概念阶段的功能安全正向开发提供了可行的技术路径,有助于提升功能安全分析的客观性与准确性。

参　考　文　献

[1] ISO. Road vehicles — Functional safety Part 3: Concept phase: ISO 26262-3: 2018[S]. Geneva: ISO, 2018.

[2] ISO. Road vehicles—Functional safety Part 1: Vocabulary: ISO 26262-1:2018[S]. Geneva: ISO, 2018.

[3] CHEON J S, KIM J, JEON J, et al. Brake by Wire Functional Safety Concept Design for ISO/DIS 26262[C]// SAE 2011 Annual Brake Colloquium And Engineering Display. Warrendale: SAE International, 2011.

[4] TAO C. Functional Safety Concept Design of Hybrid Electric Vehicle Following ISO 26262[C]// 2014 IEEE Conference and Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific). Piscataway: IEEE, 2014.

[5] 王俊明,周宏伟. 基于ISO26262的车道保持辅助的功能安全概念设计[J]. 重庆交通大学学报(自然科学版), 2019, 38(3): 135-142.

[6] STOLTE T, BAGSCHIK G, RESCHKA A, et al. Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle[C]// 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC). Piscataway: IEEE, 2017.

[7] NAG P, HARMALKAR J, GHANEKAR U. A Novel Hazard Analysis and Risk Assessment for Automotive Embedded System Development as Safety Element Out of Context[C]// 2019 IEEE Intelligent Transportation Systems Conference (ITSC). Piscataway: IEEE, 2019.

[8] CHEN L, JIAO J, ZHAO T. A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA[J]. Applied Sciences, 2020, 10(21): 7400.

[9] KHASTGIR S, BIRRELL S, DHADYALLA G, et al. Towards Increased Reliability by Objectification of Hazard

Analysis and Risk Assessment (HARA) of Automated Automotive Systems[J]. Safety Science, 2017, 99: 166-177.

[10] BECKERS K, HOLLING D, COTE I, et al. A Structured Hazard Analysis and Risk Assessment Method for Automotive Systems-A Descriptive Study[J]. Reliability Engineering & System Safety, 2016, 158:185-195.

[11] SAE International. Considerations for ISO 26262 ASIL Hazard Classification: SAE J2980_201804[S]. Warrendale: SAE International, 2018.

[12] VDA. Situation Catalogue E-parameters as Per ISO 26262-3:2018: VDA 702[S]. Berlin: VDA, 2023.

[13] SINI J, VIOLANTE M. A Simulation-Based Methodology for Aiding Advanced Driver Assistance Systems Hazard Analysis and Risk Assessment[J]. Microelectronics Reliability, 2020, 109: 113661.

[14] KWON H, ITABASHI-CAMPBELL R, MCLAUGHLIN K. ISO26262 Application to Electric Steering Development with a Focus on Hazard Analysis[C]// 2013 IEEE International Systems Conference (SysCon). Piscataway: IEEE, 2013: 655-661.

[15] 孟凡兴, 张良, 张伟. 驾驶员车头时距研究[J]. 工业工程与管理, 2013, 18(2): 131-135.

（责任编辑　**明慧**）

《汽车文摘》征文

《汽车文摘》(月刊)于1963年7月3日创刊,由国务院国有资产监督管理委员会主管、中国第一汽车集团有限公司主办,为中国汽车工程学会会刊。《汽车文摘》以“览全球汽车技术文献,指中国汽车技术之道”为使命,以打造“中国汽车前沿与创新技术传播与交流的重要平台”为愿景,致力于成为汽车领域最具影响力的综述类期刊。

《汽车文摘》深耕电动化、智能化、网联化、共享化和智能制造5大方向和10大领域,聚焦新能源、燃料电池与混合动力汽车、智能网联汽车、氨氢融合零碳和碳中性燃料、汽车安全、健康与舒适、碳达峰与碳中和、生命周期评价(LCA)与技术经济分析、智能制造、材料轻量化与一体化压铸、飞行汽车前沿与创新技术综述论文,揭示相关领域的新动态、新趋势、新技术和新进展,为广大科研和工程技术人员进一步发展这一领域提供新突破口、新出发点和新基准。

欢迎高等院校师生、研发工程技术人员、技术管理人员,充分发挥专业领域优势,深度挖掘国内外高影响力学术期刊与其它文献,形成某个技术领域前沿综述。

《汽车文摘》选题范围:

电动化:混合动力关键技术;动力电池关键技术;先进充电技术;电驱动系统及电力电子技术;智能底盘及子系统线控关键技术;燃料电池动力系统设计与优化。

智能化:新型电子电气架构;自动驾驶感知、决策与运动控制;智能新能源汽车测试评价方法与工具链;车辆智能安全技术。

网联化:智能网联云控技术;车用通信及网络技术;车路协同技术;汽车人因、人机交互与智慧座舱;信息安全与预期功能安全;车网融合(V2G)及应用。

低碳化:汽车节能与排放技术;清洁能源动力系统技术;碳达峰、碳中和;氢燃料制、储、运、加及安全管控技术;生命周期评价(LCA)、标准法规与技术经济分析;氨氢融合零碳和碳中性燃料。

轻量化:新能源汽车新材料技术;混合材料轻量化设计;一体化压铸。

共享化:区块链技术与移动出行;车辆大数据挖掘方法与应用案例。

燃料电池:电池堆、电池系统与基础设施。

智能制造:机器人与自动化控制、四大工艺、物流技术、设计-制造-服务。

颠覆式出行:飞行汽车;未来低空智能交通体系及其关键技术。

汽车安全:主被动安全与融合;智能安全;健康与舒适。

《汽车文摘》发表论文的独特优势:

《汽车文摘》是国家级刊物、中国汽车工程学会会刊、汽车领域唯一的综述期刊。《汽车文摘》不收版面费、4个月左右可发稿。

投稿要求:

1. 综述篇幅在10 000 ~ 15 000字(6~10页),图文并茂,图、表和公式非原创要求标注引用文献;

2. 请按科技论文要求撰写文章摘要,摘要中文字数约200字;

3. 文章必须附有公开发表、体现本领域最新研究成果和高影响力出版物作为参考文献,一般要求参考文献在20篇以上,一半左右为外文参考文献,且在文中标注所引用文献;

4. 来稿保密审查工作由作者单位负责,确保署名无争议,文责自负;

5. 切勿一稿多投。

《汽车文摘》投稿网址:http://www.qcwz.cbpt.cnki.net

邮箱:autodigest@faw.com.cn

《汽车文摘》编辑部