

ICS **

CCS **

团体标准

T/ITS ****-2025

代替**-**

港口无人集装箱转运车预期功能安全场景 构建分析及测试评价规范

Specification for Constructing, Analyzing, and Evaluating SOTIF Scenarios of
Autonomous Container Transport Vehicles in Ports.

(征求意见稿)

在提交反馈意见时，请将您知道的该标准所涉必要专利信息连同支持性文件一并附上。

2025-XX-XX 发布

2025-XX-XX 实施

中国智能交通产业联盟 发布

中国智能交通产业联盟

目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 功能定义与危害分析	4
4.1 系统及功能定义	4
4.1.1 本节目的	4
4.1.2 本节输入	4
4.1.3 系统定义	4
4.1.4 功能规范	4
4.2 运行设计条件（ODC）定义	5
4.3 系统架构	7
4.4 危害分析与风险评估	8
4.5 安全接受准则	9
4.5.1 本节目的	9
4.5.2 总则	9
4.5.3 风险准则	9
5 港口经典场景选取及定义（产品的通用场景元素库）	10
5.1 典型场景选取	10
5.2 场景要素选取	10
5.2.1 场景要素分类	10
5.2.2 场景要素选取	13
5.3 场景格式要求	13
5.3.1 场景基本信息	13
5.3.2 场景环境	13
5.3.3 传感器与通信	13
5.3.4 场景参与者	13
5.3.5 场景动态参与者状态	14
5.4 场景数据参数化	14
5.4.1 场景参数化对象	14
5.4.2 参数化方法	14

5.5 逻辑场景生成	14
6 安全风险场景分析	15
6.1 性能局限分析	15
6.1.1 性能局限概述	15
6.1.2 本节输入	15
6.1.3 性能局限分析方法	15
6.1.4 本节输出	16
6.2 触发条件识别	16
6.2.1 触发条件概述	16
6.2.2 本条输入	16
6.2.4 本条输出	17
6.3 安全评估准则	18
6.3.1 安全评估概述	18
6.3.2 评估准则	18
6.3.3 评估方法	18
7 测试及评价规范	19
7.1 测试场景要求	19
7.1.1 场景定义	19
7.1.2 测试场景设计要求	20
7.2 量化评价要求	21
7.2.1 评价原则	21
7.2.2 量化评价体系	21
7.3 仿真测试环境(包含仿真测试环境以及对应的测试和评价条件)	23
7.3.1 仿真测试要求	23
7.3.2 仿真结果要求	23
7.4 封闭测试环境(港口的封闭真实环境)	24
7.4.1 港口环境特点	24
7.4.2 测试和评价条件	24
7.4.3 测试内容	25

前 言

本文件按照 GB/T1.1-2020《标准化工作导则第1部分:标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利,本文件的发布机构不承担识别这些专利的责任。

本文件由中国智能交通产业联盟提出。

本文件主要起草单位:上海友道智途科技有限公司、吉林大学、北京主线科技有限公司、同济大学、交通运输部公路科学研究院、中远海运港口有限公司、东风商用车有限公司、北京斯年智驾科技有限公司。

本文件主要起草人:

中国智能交通产业联盟

中国智能交通产业联盟

港口无人集装箱转运车预期功能安全场景构建分析及测试评价规范

1 范围

本标准规定了搭载自动驾驶系统的港口无人集装箱转运车的预期功能安全场景构建分析及测试评价的相关要求。

本标准适用于港口无人集装箱转运车的自动驾驶系统功能开发过程中的预期功能安全主要工作，包括典型功能定义、危害分析和风险辨识、典型场景选取及定义、安全风险场景分析、测试及评价等，测试评估结果将为功能的后续改进提供依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 40429-2021 汽车驾驶自动化分级

GB/T 43267-2023 道路车辆 预期功能安全

ISO 21448 道路车辆 预期功能安全（Road vehicles- Safety of the intended functionality）

ISO 34501 道路车辆 自动驾驶系统测试场景术语与定义（Road Vehicles - Terms and Definitions of Test Scenarios for Automated Driving Systems）

ISO 34502 道路车辆 自动驾驶系统测试场景 基于场景的安全评估框架（Road vehicles - Test scenarios for automated driving systems— Scenario based safety evaluation framework）

ISO 34503 道路车辆 自动驾驶系统运行设计范围分类（Road Vehicles - Taxonomy for Operational Design Domain for Automated Driving Systems）

ISO 34504 道路车辆 场景属性和分类（Road Vehicles - Scenario Attributes and Categorization）

GB 5768.3-2009 道路交通标志和标线 第3部分：道路交通标线

3 术语和定义

下列术语和定义适用于本文件。

3.1

港口无人集装箱转运车 Autonomous Container Transport Vehicle for Ports

港口无人集装箱转运车是一个集环境感知、决策规划等功能于一体的智能综合体。其核心为自动驾驶系统，在设计运行条件（ODC）内，无需人为干预，在接收到港口调度任务后，能够自主完成动态驾驶任务（DDT），包括路径规划、交通环境感知、驾驶决策及车辆控制等功能，实现港口内的无人化运营作业。

3.2

预期功能安全 Safety of the intended functionality

不存在因设计不足或性能局限引起的危害而导致不合理的风险，或者将设计不足、性能局限导致的风险控制在合理可接受的范围内。

3.3

场景 Scenario

一段时间内，按照一定序列或逻辑发展或发生的事件。

3.4

事件 Event

发生在某个时间点或时间段的某件事情

3.5

环境 Environment

智能网联汽车所处的空间及其中可以直接或间接影响智能网联汽车状态的各种因素。

3.6

天气 Weather

某一个地区距离地表较近的大气层在短时间内的具体状态。

3.7

交通参与者 Traffic participant

道路上的机动车、非机动车、行人等交通实体。

3.8

信息 Message

为驾驶决策等提供的有效的数据。

3.9

交通状态 Traffic state

交通流运行的态势，以及宏观层面的交通拥堵的状态。

3.10

环境感知 Environment sensing

车辆对所处交通环境中的路面、静态物体和动态物体等的检测识别、追踪和认知，以及目标危险行为预判和轨迹预测。

3.11

交通行为决策 Traffic behavior decision

交通参与者根据感知到的交通状态信息，合理判断、选择、确定其下一步所需要执行的交通行为的动

作或活动。

3. 12

运动控制 Motion control

根据决策规划的指令控制车辆响应，保证控制精度，对目标车速、路径等进行跟踪控制。

3. 13

感知系统 Perception system

通过利用多传感器目标检测与融合等技术，获取周围环境态势，从而为系统其他部分提供周围环境的关键信息。

3. 14

决策系统 Decision-making system

综合环境及主车信息，使无人车产生安全、合理的驾驶行为，指导运动控制系统对车辆进行控制。

3. 15

执行系统 Actuate system

接受系统的操作指令并响应指令，按照操作指令控制车辆的运动。

3. 16

人员状态 Human status

车内人员的驾驶状态，以及车外人员的运动、动作等状态。

3. 17

驾驶操作 Driving operation

执行智能网联汽车相关指令，通过对系统的开启、关闭，以及对车辆的横向、纵向控制操作，完成动态驾驶任务。

3. 18

人机交互 Human-machine interaction

人与智能网联汽车之间使用某种对话语言，以一定的交互方式，为完成确定任务的人与智能网联汽车之间的信息交换过程。

3. 19

人员误用 Human misuse

车内人员和车外人员或车辆，对智能网联汽车的故意、非故意地错误操作与使用，以及无法操作。

3. 20

功能不足 Functional Insufficiencies

因为算法、环境等导致的智能驾驶相关技术无法实现其应有的功能。

3. 21

设计运行条件 Operational Design Condition

智能网联汽车安全启动和运行的内、外部环境条件，驾乘人员状态，车辆状态的总称。

3. 22

设计运行域 Operational Design Domain

智能网联汽车安全启动和运行的内、外部环境条件。

4 功能定义与危害分析

4. 1 系统及功能定义

4. 1. 1 本节目的

本章的目的是实现以下目标：

- a) 提供支撑功能安全和预期功能安全开发的有条件自动驾驶系统与功能的规范定义；
- b) 在相关活动每次迭代后，应根据要求对规范定义和设计进行更新。

4. 1. 2 本节输入

本节输入包含：

任何与该自动驾驶系统有关的已有信息，应包括但不限于场景调研报告、系统架构、功能清单、产品定义、项目信息、测试报告、与自驾控制系统的外部系统交互规范、已识别出的或已实施的安全措施等各类设计文件与信息。

4. 1. 3 系统定义

港口无人集装箱转运车自动驾驶系统旨在实现港口内货物运输的自动化和智能化。系统在设计运行条件（ODC）内，无需人为干预，能够自主完成动态驾驶任务（DDT），包括路径规划、交通环境感知、驾驶决策及车辆控制等功能。

4. 1. 4 功能规范

根据 GB/T 40429-2021《汽车驾驶自动化分级》中的定义，高度自动驾驶是指驾驶自动化系统在其设计运行范围内持续地执行全部动态驾驶任务和执行动态驾驶任务接管。

在功能规范中应描述该高度自动驾驶系统功能相关的定义和约束，该部分应包括：

- a) 功能清单与功能定义，描述系统预期的功能，支持子系统和组件的功能；
- b) 设计运行条件（ODC）；

c) 高度自动驾驶功能控制车辆动态任务的权限级别和细节如表 1 所示：

表 1 高度自动驾驶功能权限划分

驾驶自动化等级	用户	驾驶自动化系统的角色 (驾驶自动化系统激活)
4 级 高度自动驾驶	1. 港口操作员（驾驶自动化系统未激活）： a) 驾驶自动化系统激活前，确认装备驾驶自动化系统的车辆状态是否可以使用； b) 决定何时开启驾驶自动化系统，参与运营； c) 在驾驶自动化系统激活后，车辆运营作业时发生异常，参与必要的作业干预或救援指挥。 远程监控员（驾驶自动化系统激活）： a) 监控系统状态，通过远程监控系统实时查看 2. 港口无人集装箱转运车的运行情况： b) 在收到系统介入请求时，及时进行远程接管操作； c) 发生车辆其他系统失效时，通过远程控制进行必要的干预； d) 监控港口无人集装箱转运车在运行过程中的动态驾驶任务完成情况； e) 在发生紧急情况时，决定是否以及如何实现最小风险状态，并判断是否达到最小风险状态； f) 在系统请求退出自动驾驶模式时，决定是否确认退出，并进行必要的手动干预。	高度自动驾驶系统（驾驶自动化系统激活）： a) 仅允许在其设计运行条件下激活； b) 激活后在其设计运行条件下执行全部动态驾驶任务； c) 识别是否即将不满足设计运行范围，并在即将不满足设计运行范围时，及时向远程监控员发出介入请求； d) 识别驾驶自动化系统失效，并在发生驾驶自动化系统失效时，及时向远程监控员发出介入请求； e) 识别远程监控员的接管能力，并在监控员的接管能力即将不满足要求时，发出介入请求； f) 在发出介入请求后，继续执行动态驾驶任务一定的时间供远程监控员接管； g) 在发出介入请求后，如果远程监控员未响应，适时采取减缓车辆风险的措施； h) 当用户请求驾驶自动化系统退出时，立即解除系统控制权； i) 在无远程监控员介入的情况下，能够自主决定并实现最小风险状态。

d) 感知系统的输入、输出、工作范围以及对自动驾驶系统的影响；

e) 不同功能中的行为决策逻辑，路径规划方案以及对车辆控制的描述；

f) 运行过程中的数据收集与系统运行情况；

g) 法律法规要求，国家与国际标准；

h) 自动驾驶系统状态转换定义。

4.2 运行设计条件（ODC）定义

港口无人集装箱转运车的 ODC 如表 2-表 3 所示。

表 2 港口无人集装箱转运车 ODC—ODD

ODC 元素名称				元素要求		备注
第二层级	第三层级	第四层级	第五层级			
道路	道路类型	集装箱码头 道路		允许		
		区域		不允许	地理围栏之外的区域	

表 2（续）

ODC 元素名称				元素要求		备注
第二层级	第三层级	第四层级	第五层级			
道路	道路表面	道路表面 覆盖物		允许	支持覆盖少量的未清理积雪或结冰	
	道路几何	平面	直道	允许		
			弯道	允许	曲率半径 $\geq 20\text{ m}$	
		纵断面	水平	允许		
			上坡	允许	坡度 $\leq 1\%$	
			下坡	允许	坡度 $\leq 1\%$	
	车道特征	道路交通 标线	标线质量	允许	支持部分污损、部分被树叶或油污覆盖	
			无道路交 通标线	不允许	会抑制 ADS 功能和导致 ADS 退出	
			标线颜色	允许	颜色符合 GB 5768.3	
			标线类型	允许	类型符合 GB 5768.3	
		车道宽度		允许	3.5 m~4.2 m（异型车道除外）	
道路设施	交通控制 设施	道路交通 标志		允许		
		交通信号灯		允许		
	特殊设施	隔离栏		允许		
		起重机		允许	支持在岸桥和场桥下行驶和停车	
		锁站			支持通过锁站和在锁站停车	
目标物	机动车/ 移动设备			允许	-有人集卡、其他有人特种作业车辆等 -堆高机、RTG 等港口常见移动设备	
	非机动车			允许	自行车	
	行人			允许	无遮挡下进入道路的行人	
	障碍物			允许	港口常见的障碍物	
天气环境	风速			允许	0~6 级	
	降雨			允许	大雨	
	雪	降雪		允许	中雪	
		积雪		不允许		
	能见度			允许	大于 50 m	
	光照	自然光源		允许		

		人工光源	路灯	允许		
			车灯	允许		
	气温			允许	-20 ~ 45℃	
数字信息	位置信号	全球卫星导航系统		允许	定位丢失或者定位误差大于 1 米	
	无线通信			允许	通信故障	

表 3 港口无人集装箱转运车 ODC—车辆状态

ODC 元素名称				元素要求		备注
第二层级	第三层级	第四层级	第五层级			
车辆运动状态	速度	运行速度		允许	0 km/h~35 km/h	
		激活速度		允许	0 km/h	
	加速度	运行加速度		允许	-2 m/s ² ~ 2m/s ²	
		激活加速度		允许	0 m/s ²	
自动驾驶系统状态				允许	自动驾驶系统软硬件无影响自动驾驶安全作业的故障	
车辆其他系统状态				允许	没有影响自动驾驶系统运行的故障	

4.3 系统架构

应描述本高度自动驾驶系统的范围，明确属于该系统的子系统和要素，并识别与其存在交互关系的外部系统或要素，包括但不限于：

a) 定义本高阶自动驾驶系统的范围，明确属于该系统中的子系统和要素及其设计，包括感知系统、决策系统、控制系统、外部接口及其性能目标（例如：感知系统对于港口道路中装卸设施、工作人员等关键目标的感知和响应要求）；

b) 识别并定义与该系统存在交互关系的外部系统和/或要素，例如闸机、红绿灯、龙门吊等；

c) 系统架构图，包括系统和整车架构，说明该高级自动驾驶系统及其要素构成、外部相关系统及零部件及其内外部接口；

d) 完成该高级自动驾驶系统的组件清单（包括硬件和软件），应明确软件和软件的版本，并确保其与后续设计的一致性，如后续开发设计过程中版本发生变化应做相应更新；

e) 感知系统组件的安装说明，说明感知系统中单个组件的安装信息，包括但不限于：

1) 部件在车辆上的位置；

2) 部件外表面材料；

3) 部件外表面的尺寸和形状；

4) 部件外表面的光洁度。

4.4 危害分析与风险评估

a) 宜采用 HAZOP 或者 STPA 方法归纳出由于系统功能不足、超出 ODC 以及人员误操作可能引起的整车危害。针对本标准规定的港口无人集装箱转运车的功能定义、远程人员操作功能定义和 ODC，采用 HAZOP 方法归纳出的典型危害列表可参见表 4；

b) 应在给定场景的前提下，对所归纳出的危害进行风险评估，给出危害严重度和可控度的定性或者定量评分。典型危害的定性风险评估结果可参见表 4。

表 4 危害分析与风险评估

危害 ID	危害描述	潜在后果	S 严重度评分	C 可控度评分	风险是否可接受 (Y/N)
H001	车道内行驶时不恰当的横向控制	偏离出车道，与相邻车道车辆发生碰撞	S>0	C>0	N
H002	本车自主换道时机不恰当	与目标车道的车辆发生碰撞	S>0	C>0	N
H003	过度加速	与前车碰撞	S>0	C>0	N
H004	过度减速	被后车追尾	S>0	C>0	N
H005	无信号灯路口直行、转弯	与其他方向行驶车辆碰撞、与进入路口的行人、非机动车发生碰撞	S>0	C>0	N
H006	雨、雪、雾天气下作业	环境因素变化，超出 ODC，与其他车辆、港口设备、行人、非机动车等发生碰撞	S>0	C>0	N
H007	行驶前方出现不常见的车辆或机动车	没有识别出目标，与目标（车辆、非机动车）发生碰撞	S>0	C>0	N
H008	进入锁站时车辆位姿不正	与锁站发生碰撞，可能波及锁站工作人员	S>0	C>0	N
H009	行驶前方有悬空集装箱移动	没有识别出悬空目标，与集装箱发生碰撞	S>0	C>0	N
H010	抓、放箱作业，箱体调离误判完成	拉扯损坏吊具，集装箱摆幅较大时波及周围作业车	S>0	C>0	N

		辆			
H011	远程系统命令换道时机不恰当	与目标车道的车辆发生碰撞	$S>0$	$C>0$	N
H012	车辆被遥控时，出现不恰当的转向和加速	与遥控人员或周围车辆、行人、非机动车发生碰撞	$S>0$	$C>0$	N

4.5 安全接受准则

4.5.1 本节目的

a) 根据 4.4 中危害事件分析结果，制定防止危害事件发生或减轻危害程度的安全目标，以避免不合理的风险；

b) 定义相应的接受准则，包括危害行为接受准则和残余风险接受准则。

4.5.2 总则

a) 针对 4.4 中危害事件与风险评估结果，制定安全目标，并选取、定义可度量的参数进行描述，标识可以接受的风险程度；

b) 当系统受限于各种条件无法直接对风险进行有效控制时，需要做好风险管理，即用安全措施来应对风险，对于采用管理与控制措施不能完全消除风险的危害行为事件，应评估其采用安全措施后的残余风险，并制定相应的残余风险接受准则，明确残余风险的接受标准和要求。

4.5.3 风险接受准则

对于高度自动驾驶系统，通过准则包括一般通过准则与残余风险接受准则。

a) 第一接受准则：第一层接受准则是针对特定危险行为事件所设定的具体、安全、可量化的参数或标准，以确保高度自动驾驶系统在正常操作中的安全性。例如对于特定的风险场景，设计最大减速度、最大制动响应时间，最大安全距离等相应的评价指标；

b) 残余风险接受准则：残余风险接受准则是在高度自动驾驶系统无法完全满足第一层接受准则的情况下，用来评估和管理剩余风险的标准。残余风险接受准则确保即使在复杂和紧急情况下，系统的风险水平仍然在可接受范围内，不高于人类驾驶的风险水平。

常用的风险接受原则包括：GAMAB 原则、正向风险平衡原则、ALARP 原则、MEM 原则等。对于有条件自动驾驶系统的残余风险接受准则，等效后应低于 10^{-4} /小时一次严重碰撞事故，即装备有条件自动驾驶系统的车辆累积运行 10000 小时，产生的伤人/严重物损的碰撞事故应低于 1 次。

5 港口典型场景选取及定义

5.1 典型场景选取

本节目的在于识别并定义适用于港口无人集装箱转运车预期功能安全评估的典型场景。选取的场景应覆盖港口无人集装箱转运车运营中的关键操作，以便进行全面的风险评估和功能验证。

在进行典型场景选取时基于以下原则：

- a) 代表性，即选取的场景必须代表港口内港口无人集装箱转运车的典型运营环境和任务；
- b) 关键性，即场景中包含的操作应涉及港口无人集装箱转运车安全性的关键要素；
- c) 复现性，即场景应在安全测试中可重复，以验证港口无人集装箱转运车的响应和性能。

根据以上原则，选取典型场景。例如：

1. 港口通行工况

a) 港区直道变道通行

场景描述：路面状态正常，自车向右变道，后方有车辆通行。

b) 港口弯道通行

场景描述：路面状态正常，自车通过大曲率路段，右侧邻近车辆高速切入。

2. 泊车工况

a) 泊入时行人在库位横穿

场景描述：路面状态正常，泊车过程，库位角落有行人横穿通过。

b) 泊出时车辆前方通行

场景描述：路面状态正常，泊车出库过程，前方车辆低速横向通行。

5.2 场景要素选取

5.2.1 场景要素分类

根据 SOTIF 需求，场景要素将以七层场景架构分类给出，分别为：道路结构、交通基础设施、道路和设施的临时改变、交通参与者、自然环境、通信信息以及自车状态。港口运行的典型场景要素可以定义为如表 5 所示。

表 5 港口运行的典型场景要素

场景要素	要素主要属性	属性类型
道路结构	道路拓扑信息	车道数量
		车道宽度

场景要素	要素主要属性	属性类型
		车道方向
		车道曲率
		...
	道路路面状态	路面材质
		路面覆盖物
		路面反光
		...
	道路附属物	中央分隔带
		减速带
		路面反光标识
		...

表 5（续）

场景要素	要素主要属性	属性类型
交通基础设施	交通信号灯	机动车信号灯
		人行横道信号灯
		...
	交通标志	减速标识牌
		...
		...
	交通标线	白实线
		黄实线
		人行横道
		泊车库位线
		...
道路和设施的临时改变	车道占据障碍物	施工牌
		桩桶
		轮胎

场景要素	要素主要属性	属性类型
		栏杆
		...
	气象/光照条件变化	气象条件变更属性
		...
交通参与者	车辆/移动设备信息	乘用车
		大货车
		工程车
		堆高机
		...
	VRU 信息	行人
		电动车
		动物
		...

表 5（续）

场景要素	要素主要属性	属性类型
自然环境	天气	晴天
		雨天
		雪天
		雾天
		...
	光照信息	光源类型
		光照强度
		...
通信信息	通信状态	有无额外通信设备
		通信状态
		...
自车状态	车辆静态要素	车辆尺寸
		自动驾驶功能状态
		...

场景要素	要素主要属性	属性类型
	车辆动态要素	车辆速度
		车辆位置
		车辆行为决策
		...

5.2.2 场景要素选取

场景要素选取应结合实际情况，考虑测试条件限制，删除无法复现的场景要素；并根据典型功能场景的描述选择要素。

5.3 场景格式要求

5.3.1 场景基本信息

场景的基本信息应包括：

- 场景名称：简洁明确地命名场景；
- 场景编号：唯一标识符，便于管理和引用；
- 场景描述：简要描述场景的背景、目的及涉及的主要活动。

5.3.2 场景环境

场景的环境信息应包括：

- 地理位置：详细描述港口内场景的具体位置，可以包括地图或位置示意图；
- 道路特征：场景内的地面材质、道路宽度、曲率等 5.2 中描述的道路结构要素；
- 交通基础设施：场景内存在的限速、交通标志及信号灯等 5.2 中描述的交通基础设施要素；
- 天气条件：包括晴天、雨天、雾天、沙尘等可能影响无人车操作的天气状况。

5.3.3 传感器与通信

场景的传感器与通信信息应包括：

- 传感器配置：在该场景中使用的传感器类型及其安装位置，如摄像头、雷达、激光雷达等；
- 通信要求：场景内通信设施及网络要求，包括信号覆盖、数据传输速度等。

5.3.4 场景参与者

场景的参与者信息应包括：

- 静态参与者：固定设施如集装箱、货物堆放区、建筑物、施工牌等；
- 动态参与者：无人车、工程车、堆高机、行人等 5.2 中描述的交通参与者要素。

5.3.5 场景动态参与者状态

场景的动态参与者状态信息应包括：

- a) 速度：描述动态参与者的速度；
- b) 位置：描述动态参与者的位置；
- c) 行为：描述动态参与者的行为，如直行、换道、倒库等。

5.4 场景数据参数化

5.4.1 场景参数化对象

场景的参数化对象为动态参与者的状态参数，如速度、位置等要素。

5.4.2 参数化方法

场景参数化步骤为：

- a) 描述动态，确定动态参与者行为；
- b) 确定冲突点；
- c) 反推起点，反向推导出参与者的初始状态范围。

5.5 逻辑场景生成

逻辑场景生成步骤为：

- a) 输入数据：描述生成逻辑场景所需的输入数据，包括功能场景描述、场景要素；
- b) 场景生成：配置不同的场景要素组合，生成多样化的逻辑场景，并检查场景的合理性。

以港区弯道通行为例，一个逻辑场景的生成步骤如下：

- 1) 场景描述：大雨傍晚，路面状态正常，自车通过大曲率路段，右侧邻近车辆高速切入；
- 2) 场景要素选取与组合：大曲率弯道+白实线+正常状态+无路缘+无标识+能见度<500m+光强<50lux+

降雨>50mm+卡车+高速 cut-in（可行组合之一）。

- 3) 确定冲突点，如图 1 所示。



图 1 冲突点的确定

- 4) 反推逻辑场景起点：

自车状态：速度（30-40 km/h），位置（距离碰撞点 15-25 m）

卡车状态：速度（30-40 km/h），位置（距离碰撞点 25-35 m）

6 安全风险场景分析

6.1 性能局限分析

6.1.1 性能局限概述

性能局限指自动驾驶系统在特定条件下的技术和操作限制，如感知能力、反应速度和环境适应性等。这些局限会影响系统的安全性和可靠性。

6.1.2 本节输入

本节的输入包含：

- a) 危害分析与风险评估结果，即已确定存在与 SOTIF 相关风险的危害事件、合理可见的人员误用；
- b) 系统描述（包括系统的结构、功能、组成部分、交互关系等）与系统需求（系统设计或运行的要求、限制等）；
- c) 已知的软件、硬件的性能局限。

6.1.3 性能局限分析方法

对系统的性能局限进行分析目的主要包含识别潜在问题，指导系统的设计与优化，提高系统的稳定性与可靠性，同时性能局限分析结果也为决策与规划提供了依据。归纳分析、演绎分析、探索性分析、探索性模拟（采用先进的组合技术）和探索性驾驶（采用适当的安全措施）。

分析性能局限应至少采用 2 种及以上的分析方法，常用的方法有 STPA、CTA 等，以提高分析的全面性。通过采用的分析方法，识别和评估系统中的潜在安全风险和危险事件，以及这些事件可能导致的安全问题，找到相应的触发条件。下面是推荐采用的分析方法简介：

a) 归纳分析法：归纳分析法是一种从具体实例出发，通过观察和总结，得出一般性结论的分析方法。在性能局限分析中，归纳分析法通过收集系统运行过程中的数据和实际案例，识别出系统可能存在的性能局限。通过这种方法，可以发现系统在实际运行中的具体问题，并为系统优化提供依据；

b) STPA（系统性理论过程分析）：STPA 是一种基于系统理论的安全分析方法，旨在通过系统性地识别和分析潜在的危险事件及其原因，以便制定相应的安全措施。STPA 通过识别系统的控制结构、找出可能导致不安全状态的控制动作、分析失效路径以及制定安全措施，全面、系统地分析性能局限和潜在风险，从而提高系统的安全性和可靠性；

c) CTA：CTA 通过任务分解、认知需求分析、识别性能局限和制定改进措施，识别由于人机交互复杂性导致的性能局限。它帮助优化系统设计，提升系统的可操作性和安全性。通过归纳分析法、STPA 和 CTA

等方法的综合运用，我们可以全面识别和评估自动驾驶系统在港口环境中的性能局限，为系统的优化和提升提供科学依据和指导。

6.1.4 本节输出

本条目的输出包含：感知、控制、执行各系统的性能局限。

以定位中激光雷达的性能局限为例，分析泊车-换道功能中的性能局限，如表 6 所示。

表 6 激光雷达中的泊车-换道功能的性能局限

ID	系统架构功能	分配至系统或软硬件要素	SOTIF 相关交互或要素	SOTIF 相关设计缺陷
1	泊车-换道	感知 HW-激光雷达	点云结果	雨雾扬尘等天气，导致激光原始点云噪声大
				激光束飘移
				路面扬尘/不明物体遮挡/扫描平台限制，导致扫描视角受到限制
				多路径效应导致反射不准确
				激光雷达对其他物体遮挡目标的处理不足
.....				

6.2 触发条件识别

6.2.1 触发条件概述

触发条件是指引发自动驾驶系统安全风险或异常行为的具体情境或事件，如突发障碍物、复杂交通状况和恶劣天气等。这些条件需要被识别和管理以确保安全。

6.2.2 本条输入

触发条件分析的输入包含：

- a) 系统输入与设计运行规范，这些信息有助于理解系统的运行机制和可能涉及的各种事件，系统的设计要求、约束条件和操作流程；
- b) 专家经验与事件数据，用于识别潜在的触发条件和分析事件的可能性；
- c) 环境条件、系统运行数据。

6.2.3 触发条件分析规范

在进行触发条件分析时，通常可以采用以下格式来记录和描述触发条件：

- a) 描述导致事件发生的触发条件，即事件发生的先决条件或导致因素，触发条件应该是具体、清晰的条件，可以是单一条件或多个条件的组合；

- b) 对于每个触发条件，可以描述其发生的背景、引起的原因、以及可能的影响；
- c) 可以使用定量或定性的方法对触发条件进行评估和分类，以便确定应对策略和措施的优先级；
- d) 可以根据需要记录其他与触发条件相关的信息，如触发条件的时间、地点等。

6.2.4 本条输出

以泊车-换道场景为例，针对感知 HW-激光雷达的性能局限所得到的触发条件如表 7 所示。

表 7 感知 HW-激光雷达的性能局限所得到的触发条件

SOTIF 相关设计缺陷 SOTIF-related design weaknesses	触发条件 Triggering conditions		
	场景特性 Scene characteristics	驾驶场景 Driving scenario	其他交通参与者行为 Behaviour of other drivers road users
雨雾扬尘等天气，导致激光原始点云噪声大	雨雾扬尘等天气，车辆不能从行车道离开换道至倒车道，不能完全离开行车道，阻碍后方跟随的卡车进行泊车	以 15KM/H 速度行驶在行车道	后方车辆跟随本车辆行驶
	雨雾扬尘等天气，车辆换道过度，越过倒车道外边界与边界外工作人员/静态障碍物发生碰撞	以 15KM/H 速度行驶在行车道	倒车道边界外有工作人员
	雨雾扬尘等天气，车辆不满足换道条件时，非预期地执行了换道，与倒车道上正在寻库/泊入的车辆发生碰撞	以 15KM/H 速度行驶在行车道	倒车道上有车辆正在寻库/泊入
多路径效应导致反射不准确	路面积水较多，车辆不能从行车道离开换道至倒车道，不能完全离开行车道，阻碍后方跟随的卡车进行泊车	以 15KM/H 速度行驶在行车道	后方车辆跟随本车辆行驶
	路面积水较多，车辆换道过度，越过倒车道外边界与边界外工作人员/静态障碍物发生碰撞	以 15KM/H 速度行驶在行车道	倒车道边界外有工作人员
	路面积水较多，车辆不满足换道条件时，非预期地执行了换道，与倒车道上正在寻库/泊入的车辆发生碰撞	以 15KM/H 速度行驶在行车道	倒车道上有车辆正在寻库/泊入
.....			

对于支持泊车和行车功能的港口无人自动驾驶系统，性能局限与触发条件的分析要求覆盖泊车和行车中的典型场景，如表 8-表 9 所示。

表 8 港口无人集装箱转运车行车典型场景

序号	典型场景
1	前车紧急切入
2	通过红绿灯
3	通过无保护（无红绿灯）路口
4	通过闸机
5	通过锁站
6	高速路汇入/汇出
7	通过施工路段
8	雨雪扬尘环境变化
9	隧道
10	U 型弯道
11	路口会车
.....	

表 9 港口无人集装箱转运车泊车典型场景

序号	典型场景
1	库位上摆放锥桶
2	多车辆同时寻库
3	泊入/泊出
4	泊出时存在车辆泊入/寻库
5	无空余库位
6	

6.3 安全评估准则

6.3.1 安全评估概述

基于 6.2 与 6.1 中的性能局限与触发条件分析和 4.4 中危害分析与风险评估中的结果，组合成一些有现实意义的对港口无人驾驶有挑战性的风险场景，需要对其进行相关验证工作。验证单一风险场景的通过原则。

6.3.2 评估准则

接受指标可以参考 UN ECE R157 里的驾驶员模型，以避免碰撞为准则。有条件自动驾驶（L3）系统的要求表现要超过人类的一般驾驶水平。港口无人集装箱转运车搭载高度自动驾驶系统，就要求在需要人类接管的场景中，车辆表现也要超过人类驾驶水平。

接受指标可以是时间型指标，例如 TTC、THW 等；也可以是距离型指标，例如最小空间距离等；可以是加速度型指标，例如纵向加减速度、横向加速度等；也可以是综合型指标，例如势场、风险场等。

6.3.3 评估方法

对于每个组合而成的风险场景，应从验证的效率、成本和充分性来选择实车测试、封闭环境测试、仿

真模拟测试三种验证方式的一种或组合。

a) 实车测试是指在真实道路环境中进行的测试，旨在评估系统在实际操作中的性能和行为。测试环境选择具有代表性的港口道路环境，包括不同的道路类型、交通情况和天气条件。要配备多种传感器和数据记录设备，全面采集车辆的行为数据、环境数据和系统运行数据以便全面评估；

b) 仿真模拟测试：仿真模拟测试是利用计算机仿真技术，在虚拟环境中模拟真实世界中的测试场景，评估系统在不同情况下的性能和反应。仿真测试要选择高精度、高可靠性的仿真平台，能够尽可能地还原模拟港口内的道路、交通和环境，要通过创建多种典型和极端场景，包括不同的天气、光照和交通情况进行测试。确保将港口无人集装箱转运车的自动驾驶系统集成到仿真平台中，确保系统能够在虚拟环境中正常运行。后续要反复测试，在不同条件下进行多次测试，以验证系统的一致性和稳定性；对于危险度高、复杂度高，不易在真实环境中测试的场景，应优先采用仿真的手段进行验证。

c) 封闭环境测试，封闭环境测试是在控制的封闭场地内进行的测试，旨在模拟真实港口环境中的各种场景，以验证系统的性能和安全性。测试场地要有代表性，选择专门的测试场地，模拟港口内的各种道路和设施，包括交叉口、弯道、坡道等。依据预设的评估标准，对测试结果进行分析和评价，确认系统在封闭环境中的表现是否达到预期。

对于整车级难以实现的场景，可以在组件级上进行测试，并且需要对其结果的整车代表性及合理性进行必要的说明。

若采用仿真，应基于不同验证目的选择 SIL 软件在环、HIL 硬件在环、VIL 整车在环、DIL 驾驶员在环等不同环境。

7 测试及评价要求

7.1 测试场景要求

7.1.1 场景定义

在测试场景的定义中将明确定义用于测试的各种场景，以确保对港口无人集装箱转运车的全面评估和验证。测试场景的设计是系统测试的关键环节，它直接影响到测试结果的真实性和可靠性。完整地描述一个场景，需要但不限于有如表 10 中的内容。

表 10 场景元素及其说明

场景元素	说明
天气环境条件	描述当前的天气状况，包括晴天、雨天、雪天、雾天等不同的天气情况，以及气温、湿度、风力等相关因素
交通参与者	指路上的各种交通参与者，包括港口特种车辆、卡车、乘用车、自行车、行人等，描述其数量、行驶速度、行驶方向等信息
道路类型	描述行驶道路的特征和分类，包括港口内部作业道、岸桥、泊车专用道、高速路等不同类型的道路情况
光照条件	指光线和能见度的情况，包括白天、夜晚、日出日落时分等不同的照明情况，以及路灯、车灯等的亮度和影响范围
地理环境	描述所处地理位置的特点，包括城市、郊区、乡村、高海拔地区等地理环境的特征和地形地貌
道路设施	指道路上的各种设施和标志，包括交通信号灯、路牌、路障、标线等，以及路面的平整程度、坡度、弯道情况等
...	...

7.1.2 测试场景设计要求

测试场景的设计原则是确保测试覆盖全面、具有代表性和可重复性的关键指导方针。要充分结合安全分析中所得出的性能局限与触发条件，测试场景有以下要求：

- a) 系统特点考量：首先，需要全面理解系统的特点，包括其功能、性能、安全性等方面。根据系统的特点，确定适用于该系统的测试场景设计原则，以确保测试覆盖到系统的关键功能和特性；
- b) 测试目的明确：明确测试的目的和目标，确定测试的重点和重点关注区域。测试场景设计应围绕测试目的展开，确保测试场景能够有效地评估系统的性能和功能；
- c) 多样性和代表性：测试场景应具有多样性和代表性，涵盖不同类型的道路、交通情况、天气条件等因素。这有助于评估系统在各种情况下的性能和稳定性；
- d) 边界条件考虑：考虑系统性能的边界情况和极端情况，确保测试覆盖到系统的极限情况。这有助于评估系统在极端条件下的应对能力和安全性能；
- e) 实用性和可行性：测试场景设计应具有实用性和可行性，符合实际使用需求和操作场景，能够为系统的实际应用提供有效的参考和指导。

7.2 量化评价要求

7.2.1 评价原则

评价原则是评价过程中的指导方针，它们指导着我们如何进行评价，确保评价的准确性和有效性。在评价港口无人集装箱转运车在测试场景中的表现时要考虑下面各项原则：

- a) **交规符合性**：港口无人集装箱转运车在运行过程中是否遵守交通规则，如道路限速、弯道限速、不在弯道超车、右侧不超车，除紧急情况不在应急车道行驶；
- b) **无人作业能力**：驾驶任务完成情况，评价港口无人集装箱转运车完成驾驶任务的情况，包括导航到目的地、避免障碍物、正确执行车辆控制指令等；
- c) **行驶平顺性**：评价港口无人集装箱转运车的直道行驶平稳性、转弯平稳度、加减速平稳度等；
- d) **安全性**：港口无人集装箱转运车执行任务时的安全性，评价港口无人集装箱转运车执行任务时的安全性，包括避免与其他车辆和障碍物碰撞，故障降级处理合理性等。

7.2.2 量化评价框架

量化评价体系可以参考 ISO-34502 中的四阶段评价框架。

- a) **第一阶段安全状态评估**：在测试用例中，若主车始终处于安全状态则判定测试通过，并结束评价流程；若存在潜在风险，则需判断港口无人集装箱转运车是否会主动采取危险规避行为来降低潜在风险，并进入阶段 2；
- b) **第二阶段碰撞检测评估**：判断主车是否发生碰撞，若未发生碰撞则测试用例通过（需考虑必要的安全设计裕量，如刹停后自车与障碍物的剩余距离 >1 米，否则判定为未通过，具体判定指标需根据不同测试场景和车型等条件设定），并结束评价流程；反之测试未通过，并进入阶段 3；
- c) **第三阶段可控性评估**：系统不对不可避免碰撞事故负责，若港口无人集装箱转运车驾驶系统合理响应测试触发条件、其他车辆的风险行为能避免碰撞事故的发生，但却没有合理响应。则可控性评估失败；若事故碰撞无法避免则不可控，可控性评估通过；无论测试用例是否通过都进入阶段 4；
- d) **第四阶段碰撞缓解评估**，首先评估港口无人集装箱转运车驾驶系统是否提供适当控制行为减缓主车与目标车碰撞时的相对速度，若未有明显减缓碰撞时的相对车速则判定为测试未通过，结束评价流程；若减缓碰撞时的相对速度，则继续判断是否降低驾乘人员受到伤害的概率，若显著降低，测试用例通过，反之测试用例失败，结束评价流程。

以泊车-换道为例，生成具体场景、确定单一风险场景接受准则如表 11 所示。

表 11 泊车-换道生成的具体场景及其接受准则

序号	典型场景要求触发条件	典型功能场景	具体交通场景	接受准则
1	后车跟随	自车在行车道上准备执行泊车-换道功能, 后方存在其他卡车跟随本车辆行驶	白天, 晴天, 直道, 车道线清晰, 自车在自动驾驶功能激活状态下匀速行驶, 车速(大于15kph), 准备从行车道换道至倒车道, 后方存在其他卡车以相近车速(15kph)跟随本车辆行驶, 距离(5m)	1. 车辆不发生碰撞, 且换道过程无急刹等情况, 与后车保持安全距离; 2. 车辆换道成功; 3. 判断客观数据是否满足相应的整车安全接受准则
	倒车道占用	自车在行车道上准备执行泊车-换道功能, 倒车道上有车辆正在寻库/泊入	白天, 晴天, 直道, 车道线清晰, 自车在自动驾驶功能激活状态下匀速行驶, 车速(大于15kph), 准备从行车道换道至倒车道, 倒车道内有车辆(卡车)正在寻库, 车速(10kph)	1. 车辆不发生碰撞, 且换道过程主动限制车速, 与前车保持安全距离; 2. 车辆换道成功; 3. 判断客观数据是否满足相应的整车安全接受准则
			白天, 晴天, 直道, 车道线清晰, 自车在自动驾驶功能激活状态下匀速行驶, 车速(大于15kph), 准备从行车道换道至倒车道, 倒车道内有车辆(卡车)正在泊入, 车速(5kph)	1. 车辆不发生碰撞, 必要时停车, 并能与泊入车辆保持安全距离; 2. 车辆换道完成; 3. 判断客观数据是否满足相应的整车安全接受准则
	车道边界外有人	自车在行车道上准备执行泊车-换道功能, 倒车道边界外有工作人员	白天, 晴天, 直道, 车道线清晰, 自车在自动驾驶功能激活状态下匀速行驶, 车速(大于15kph), 准备从行车道换道至倒车道, 倒车道边界处有工作人员	1. 车辆换道及经过工作人员时, 始终保持横向安全距离; 2. 判断客观数据是否满足相应的整车安全接受准则
2	雨雾天气, 路面积水	雨雾天气, 自车在自动驾驶功能激活状态下跟车行驶, 前车紧急制动	雨天、光线不足, 车道线不清晰, 直道, 自车在自动驾驶功能激活状态下跟车行驶, 车速60kph, 跟车时距THW=2.0s, 遇大雨天气, 前车紧急制动, 减速度0.4g, 持续时间2s	1. 车辆不发生碰撞; 2. 判断客观数据是否满足相应的整车安全接受准则
.....				

7.3 仿真测试要求

7.3.1 仿真环境要求

港口无人集装箱转运车驾驶系统的仿真测试平台应当满足以下要求：

- a) 虚拟道路网络模拟：模拟真实道路网络的虚拟环境，包括城市道路、高速公路、港口内部道路、泊车区道路等。这些道路网络应该能够反映真实道路的各种特征，如道路宽度、弯道曲率、路面状况等；
- b) 交通情况模拟：模拟各种交通情况，包括车辆行驶、停车、变道等行为。仿真测试环境应该能够模拟多辆车同时行驶的场景，并考虑到不同车辆之间的相互影响和交互作用；
- c) 天气条件模拟：模拟各种天气条件，包括晴天、雨天、雪天等，以评估系统在不同天气条件下的性能表现。仿真测试环境应该能够根据不同的天气情况改变道路湿滑程度、能见度等参数，以模拟真实天气条件下的驾驶环境；
- d) 车辆传感器模拟：模拟港口无人集装箱转运车搭载的传感器设备，如摄像头、雷达、激光雷达等。这些传感器应该能够在仿真测试环境中产生与真实场景相符的数据，以提供给港口无人集装箱转运车驾驶系统进行感知和决策；
- e) 远程控制模拟：港口无人集装箱转运车，不再配有驾驶员。仿真平台应能够当模拟运营人员远程控制港口无人集装箱转运车，模拟命令信号输入以及可预见的误用行为；
- f) 动力学仿真：仿真测试平台应具备车辆动力学仿真建模能力，支持外部车辆动力学模型设置和导入等，至少要覆盖现实场景中所能遇到的所有车型；
- g) 地图导入：仿真测试平台应支持多种不同的高精地图格式导入。

7.3.2 仿真能力的要求

港口无人集装箱转运车驾驶系统的仿真测试应当满足以下要求，以确保测试结果的准确性、全面性和可靠性：

- a) 准确性要求：仿真测试结果应当尽可能接近真实场景，确保对系统性能的评估具有准确性和可信度。这包括对道路网络、交通情况、天气条件等多个方面的准确模拟和反映，仿真环境应准确模拟各种道路情况，包括道路类型、路面状况、交通标志和信号等，以确保测试结果与实际驾驶场景相符；
- b) 覆盖率要求：仿真测试应覆盖多种不同情况和场景，包括不同的道路类型（园区道路、高速道路、泊车区域、闸机通行等）、交通情况（拥堵、车流稀少、交叉路口、施工路段等）和天气条件（晴天、雨天等）；
- c) 实时性要求：仿真测试应具有一定的实时性，能够在测试过程中实时反馈系统的性能和行为。这包括对车辆动态、交通情况和道路状态等实时变化的及时响应。系统应能够模拟真实驾驶环境中的各种实时

因素，如车辆的突然变道、突然停车等，以提高测试的真实性和可靠性；

d) 可重复性要求：仿真测试应具有可重复性，能够在不同时间、不同条件下进行多次重复测试，以验证测试结果的稳定性和一致性。这有助于发现系统性能的变化趋势和稳定性水平。通过多次重复测试，可以评估系统在不同情况下的稳定性和一致性，为系统的优化和改进提供可靠的数据支持，并确保系统的可靠性和稳定性；

e) 安全性要求：仿真测试应注重系统的安全性评估，在测试过程中确保系统对潜在危险情况的正确响应。这包括对系统在紧急情况下的应急处理能力进行测试和验证。

7.4 封闭场景测试要求

7.4.1 港区环境特点

7.4.1.1 港区运营环境

港口无人集装箱转运车的典型实际运行环境有：

港口内部道路：主要包括码头、岸桥、堆箱区、匝道、闸机等

社会公开道路：主要有匝道、十字路口、主干路、分岔路口等。

7.4.1.2 港区交通环境

在港口无人集装箱转运车作业工程中，其交通环境特点主要有以下几个方面：

a) 港口内部与社会公开道路存在行人活动，在港口内主要为工作人员，如装卸工人、码头工人等，他们需要徒步或驾驶车辆穿梭于各个码头、仓库和停车场之间；在社会公开路段主要为行人，他们不一定有很高的安全意识，不了解港口无人集装箱转运车的运行状态；

b) 港口内与社会道路上存在园区车辆与工作车辆，主要包括轿车、各类卡车、内部物流车辆等，其中工作车辆有人工驾驶、有人智能驾驶、无人自动驾驶三种，在港口内部道路网络中快速、高效的运营作业。在工作重合区域可能出现多车混行的情况；

c) 交通流动性：由于车辆活动频繁，港口内部的交通流动性需求较高，需要保持良好的交通运行状态，以确保货物的及时运输和交付效率；

7.4.2 评估条件

在封闭测试环境中，验证符合港口作业环境的无人转运能的安全性，需明确系统性能评估的条件，应至少包含以下内容：

a) 场景覆盖率评估：测试覆盖港口内各种道路类型、交通情况和地形特点，确保系统在不同场景下的表现得到充分评估；

b) 行为一致性评估：确保系统在封闭测试环境中的行为与真实场景一致，测试结果准确可信；如果存

在偏差，应做好记录及偏差内容，作为后续申请真实运营环境测试验证的测试项。

c) 安全性评估：评估系统在港口环境中的安全性表现，包括遵守交通规则、与其他车辆和行人的互动等方面。

7.4.3 测试内容

测试应至少包含以下内容：

a) 路径规划测试：设计港口典型无人运营作业路线，评估无人转运车的基本路径规划能力；

b) 交通协同测试：设计多车混行、装卸箱作业任务交互的测试场景，评估在混行作业、车云系统交互的协同应对能力，包括避让行人、避让装卸车辆、路口顶牛博弈等；

c) 安全性能测试：测试系统在港口环境中的安全性能，包括遵守交通规则、在拥有路权情况下的避撞能力和应急处理能力等。



中国智能交通产业联盟

标准

港口无人集装箱转运车预期功能安全场景

构建分析及测试评价规范

T/ITS XXXX-2025

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：<http://www.c-its.org.cn>

2025 年 X 月第一版 2025 年 X 月第一次印刷