中国汽车工程研究院股份有限公司

China Automotive Engineering Research Institute Co., Ltd.

智能汽车融合安全标准协同研究与实践

Research and Practice on Collaborative Standardization of Integrated Safety for Intelligent Vehicles

中国汽研信息智能事业部 张强

The Information and Intelligence Division of CAERI，Zhang Qiang

目录
CONTENTS

1 标准与法规解析
Analysis of Standards & Regulations

2 标准协同研究
Research on Standard Collaboration

3 中国汽研实践
Practice by CAERI

目录
CONTENTS

1 标准与法规解析
Analysis of Standards & Regulations

2 标准协同研究
Research on Standard Collaboration

3 中国汽研实践
Practice by CAERI

国际与国内的关键节点
CKey Milestones, International and China

2018
ISO 26262:2018
功能安全第二版
FuSa 2nd ed.

2021
ISO/SAE 21434
UN R155 / R156
网络安全工程与型式批准
Cybersecurity & type approval

2022
ISO 21448:2022
预期功能安全
SOTIF

2024
ISO/PAS 8800
GB 44495 / 96 / 97
AI 安全；中国强标发布
Published

2025
ISO/TS 5083:2025
自动驾驶安全
Safety for ADS

2026.1/7
GB 44497
GB 44495/96
强制实施
Mandatory in China

中国市场 China
三项 GB 强标自 2026 年 1 月 1 日起实施；已获型式批准的车型自 2028 年 1 月 1 日起执行。
Effective 1 Jan 2026 for new type approvals; 1 Jan 2028 for existing approved types.

国际市场 International
UN R155 / R156 通过型式批准约束 CSMS 与 SUMS；出口车型需按目标市场分别验证。
UN R155 / R156 bind CSMS and SUMS through type approval; verify separately per market.

标准层与法规层：分工与对应

Two Layers: Technical Standards vs. Mandatory Regulations

标准层 Standards

提供方法、流程与工作产物 —— 回答「如何做到」

ISO 26262	ISO 21448	ISO/SAE 21434	ISO 24089	ISO/PAS 8800	ISO/TS 5083
2018	2022	2021	2023	2024	2025
功能安全 Functional Safety	预期功能安全 SOTIF	网络安全工程 Cybersecurity Eng.	软件升级工程 Software Update Eng.	AI 安全 Safety and AI	自动驾驶安全 Safety for ADS

法规层 Regulations

强制准入要求 —— 回答「必须做到什么」

UN R155	UN R156	GB 44495—2024	GB 44496—2024	GB 44497—2024
CSMS 网络安全管理体系 Cyber Security Mgmt System	SUMS 软件升级管理体系 Software Update Mgmt System	汽车整车信息安全技术要求 Vehicle Cybersecurity Requirements	汽车软件升级通用技术要求 Software Update Requirements	自动驾驶数据记录系统 Automated Driving Data Recorder

三项GB强制性国家标准在研制过程中与UN R155 / R156进行了协调，GB 44497于2026年1月1日起实施，GB 44495/44496于7月1日起实施。

China's three mandatory GB national standards were developed in coordination with UN R155/R156. GB 44497 took effect on 1 January 2026, while GB 44495 and GB 44496 took effect on 1 July 2026.

ISO 26262:2018 功能安全
Functional Safety — Hazards Caused by Malfunctioning Behaviour

消除 E/E 系统失效带来的不合理风险
Eliminate unreasonable risks caused by E/E system failure

ISO 26262-1:2018, 3.67

两类失效 Two failure classes

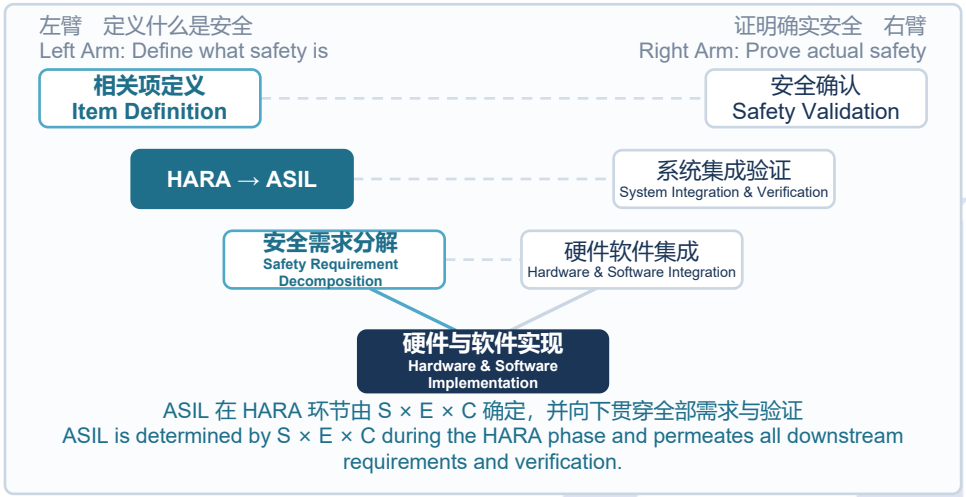
系统性失效 Systematic failure
由设计与流程引入，靠过程与方法学消除 Introduced by design and process, eliminated through methodology and processes

随机硬件失效 Random hardware failure
可用失效率量化，靠诊断覆盖率控制 Quantifiable by failure rate, controlled by diagnostic coverage

方法链条 Method chain

- 相关项定义 Item definition → HARA 危害分析与风险评估 Item definition → HARA (Hazard Analysis and Risk Assessment)
- 由 S 严重度 × E 暴露率 × C 可控性 确定 ASIL A–D ASIL A–D determined by Severity (S) × Exposure (E) × Controllability (C)
- 推导安全目标与 FTTI，分解为功能与技术安全需求 Derive safety goals and FTTI, decomposed into functional and technical safety requirements
- 落地为安全机制：诊断、冗余、监控、降级与安全状态 Implemented as safety mechanisms: diagnostics, redundancy, monitoring, degradation, and safe state

典型示例：制动控制器随机硬件失效导致助力丧失 → 安全机制须在 FTTI 内检测并进入安全状态。
Typical example: Random hardware failure of brake controller causing loss of boost → safety mechanism must detect within FTTI and enter safe state.



ASIL 在 HARA 环节由 S × E × C 确定，并向下贯穿全部需求与验证
ASIL is determined by S × E × C during the HARA phase and permeates all downstream requirements and verification.

与网络安全的接口 Interface with Cybersecurity

2018 版仅在有限范围内纳入网络安全——只覆盖“从功能安全到网络安全”的接口，不提供威胁分析方法。
The 2018 edition covers only the interface from functional safety to cybersecurity.

ISO 21448:2022 预期功能安全（SOTIF）

Safety of the Intended Functionality — Hazards Without Any Failure

不存在因功能不足或可合理预见的人为误用所导致的不合理风险

Absence of unreasonable risk due to functional insufficiencies or reasonably foreseeable misuse

ISO 21448:2022

核心概念 Key concepts

触发条件 Triggering condition

使功能不足显现为危险行为的具体场景要素 The specific scenario elements that cause a functional insufficiency to manifest as hazardous behavior

功能不足 Functional insufficiency

规格不足与性能局限，系统无故障却不够用 Insufficiencies of specification and performance limitations — the system has no faults, yet is inadequate

验证逻辑 Validation logic

- 识别并分析触发条件，建立场景库与 ODD 边界 Identify and analyze triggering conditions; establish a scenario library and ODD (Operational Design Domain) boundaries
- 以仿真、场地与实车里程支撑充分性论证 Support the sufficiency argument through simulation, closed-course testing, and real-world vehicle mileage
- 依据验收准则判定残余风险是否可接受 Determine whether residual risk is acceptable based on acceptance criteria
- 持续把“未知”场景转为“已知”并加以处置 Continuously convert "unknown" scenarios into "known" ones and address them accordingly

典型示例：逆光条件下摄像头漏检异形障碍物 → 传感器没有失效，是能力边界不够。
Typical example: Under backlight (glare) conditions, the camera fails to detect an irregularly shaped obstacle → the sensor has not malfunctioned; rather, its performance capability boundary is insufficient



与网络安全的边界 Boundary with Cybersecurity

SOTIF 在制定阶段即明确将网络安全排除在范围之外——恶意触发条件不由本标准处理。
Cybersecurity is explicitly outside the scope of SOTIF.

ISO/SAE 21434:2021 道路车辆网络安全工程

Road Vehicles — Cybersecurity Engineering

车辆的 E/E 系统、组件与功能所涉及的资产，处于免受威胁侵害的状态
Condition in which assets of road-vehicle E/E systems are sufficiently protected against threats

ISO/SAE 21434:2021

标准要求的两个层面 Two levels of requirement

组织层：CSMS 网络安全管理体系 Organizational Layer：CSMS

治理、文化、能力、分布式开发责任与持续的网络安全活动 Governance, culture, competence, distributed development responsibilities, and ongoing cybersecurity activities

项目层：概念 → 开发 → 生产 → 运维 → 退役 Project Layer：Concept → Development → Production → Operation → Decommissioning

覆盖全生命周期，运维阶段承担漏洞监测与事件响应 Covers the full lifecycle; the operation phase is responsible for vulnerability monitoring and incident response

与功能安全的显式引用 Explicit cross-reference

TARA 影响评级的四个维度中，S（安全）直接沿用 ISO 26262 的严重度分级。
In TARA impact rating (S / F / O / P), the Safety dimension reuses the ISO 26262 severity classification.

TARA 威胁分析与风险评估 Threat Analysis and Risk Assessment

1. **资产识别** *Asset identification*
2. **威胁场景识别** *Threat scenario identification*
3. **攻击路径与可行性** *Attack path & feasibility rating*
4. **影响评级 S / F / O / P** *Impact rating*
5. **风险值与风险处置** *Risk value & treatment decision*

第 4 步的 S 维度沿用 ISO 26262 严重度分级 Reuses ISO 26262 severity

S评级是三套标准之间目前最明确的一条技术接口——标准协同已经写进现有条文
Impact rating of S-dimension is the most explicit technical interface among the three frameworks today — convergence is already in the current text

目录
CONTENTS

1 标准与法规解析
Analysis of Standards & Regulations

2 标准协同性研究
Research on Standard Collaboration

3 中国汽研实践
Practice by CAERI

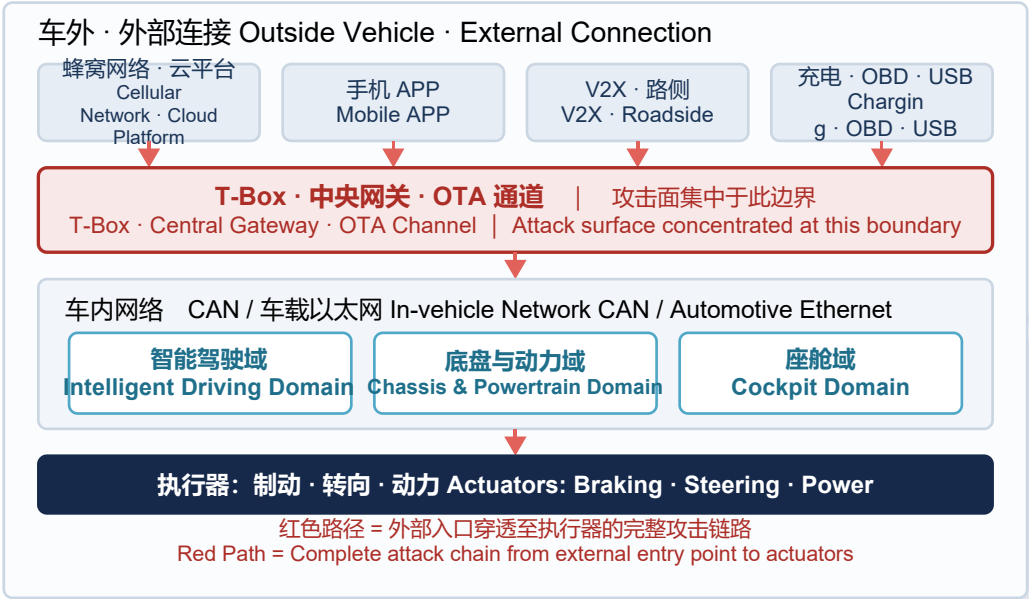
为什么标准必须协同
Why the Standards Must Collaborate

① 攻击已成为安全失效的根因
Cyberattack has become a root cause of safety failure

网络攻击不再只是数据与隐私问题——它可以直接引发功能安全失效与 SOTIF 失效，最终演变为道路交通事故。
An attack can trigger both a functional-safety failure and a SOTIF failure, ending in a real road accident.

② 三套标准分立，边界处无人覆盖
Three separate standards leave the boundaries uncovered

ISO 26262 假设失效非恶意；ISO 21448 明确将网络安全排除在范围之外；ISO/SAE 21434 分析到风险处置为止。跨域诱因落在三者之间。
ISO 26262 assumes non-malicious failure; ISO 21448 explicitly excludes cybersecurity; ISO/SAE 21434 stops at risk treatment.



外部连接 → 网关 → 车内网络 → 执行器：一条完整的攻击链路
External interface → gateway → in-vehicle network → actuator

标准协同是消除安全盲区的必要条件。
Standard collaboration is necessary to eliminate safety blind zones

法规层：UN 法规与中国强制性国家标准

Regulatory Layer: UN Regulations and China's Mandatory GB Standards

国际 UN / UNECE WP.29
International

UN R155	网络安全与 CSMS 型式批准 Cybersecurity & CSMS type approval
UN R156	软件升级与 SUMS 型式批准 Software update & SUMS type approval
ISO 24089:2023	软件升级工程，支撑 R156 落地 Software update engineering

中国 China GB（强制性）
Mandatory national standards

GB 44495—2024	汽车整车信息安全技术要求 Technical requirements for vehicle cybersecurity
GB 44496—2024	汽车软件升级通用技术要求 General technical requirements for software update of vehicles
GB 44497—2024	智能网联汽车 自动驾驶数据记录系统 Intelligent and connected vehicle—Data storage system for automated driving

UN 法规通过型式批准约束“体系 + 车辆”，GB 强标同样将管理体系要求写入强制条款，二者在研制阶段做过协调，但试验方法与判定细则仍有差异，出口车型需分别验证。
Both bind the management system and the vehicle. They were coordinated during drafting, yet test methods and criteria still differ — export models require separate verification.

标准之间已经存在的接口

Existing Cross-References Between the Standards

ISO 26262 功能安全	ISO 21448 预期功能安全	ISO/SAE 21434 网络安全

ISO 26262 ⇄ ISO/SAE 21434	26262:2018 纳入“从功能安全到网络安全”的接口；21434 的影响评级中，S 维度沿用 26262 严重度分级。 *26262 includes the interface to cybersecurity; 21434 reuses the 26262 severity scale in impact rating.*
ISO 26262 ⇄ ISO 21448	共用相关项定义、危害分析基础与安全目标概念；21448 处理 26262 范围之外的功能不足。 *Shared item definition, hazard analysis basis and safety-goal concept.*
ISO 21448 × ISO/SAE 21434	**无直接接口。SOTIF 明确将网络安全排除在范围之外，恶意构造的触发条件不由该标准处理。** **No direct interface. Cybersecurity is explicitly outside the scope of SOTIF.**

补位标准 Bridging standards

ISO/PAS 8800:2024
扩展 ISO 26262 与 ISO 21448，覆盖 AI 引入的安全问题
Extends ISO 26262 and ISO 21448 for AI

ISO/TS 5083:2025
取代 ISO/TR 4804，将网络安全考量纳入自动驾驶安全论证
Replaces ISO/TR 4804; includes cybersecurity considerations

两条跨域路径：现行标准的覆盖缺口
Two Cross-Domain Paths Left Uncovered by the Current Standards

路径一：攻击 → 失效 → 危害 Path 1: attack → failure → harm



缺口：21434 分析到风险处置为止，不推导安全目标；26262 从失效起算且假设非恶意。「攻击如何转化为具体失效模式」没有标准规定分析方法与责任归属。
21434 stops at risk treatment; 26262 starts from failure and assumes non-malicious causes.

路径二：攻击 → 功能不足 → 危害 Path 2: attack → functional insufficiency → harm



缺口更彻底：SOTIF 的充分性论证建立在触发条件随机、罕见的统计假设之上；恶意触发条件可被主动构造、精确复现，该假设不成立，而标准明确不管这一部分。
SOTIF validation assumes random, rare triggering conditions — an assumption that malicious triggering breaks.

缺口不会由某一部标准单独填平。可行的做法是在企业流程中显式指定责任方——把 TARA 的攻击路径作为强制输入，回注到 HARA 与 SOTIF 分析。
The gap will not be closed by any single standard. Make TARA attack paths a mandatory input to HARA and SOTIF analysis, with a named owner.

融合方法论：五个支柱及其标准依据
Five Pillars of Convergence, Mapped to the Standards

1 统一风险视角 *Unified risk view*
HARA / SOTIF 分析 / TARA 共用相关项定义与严重度分级
ISO 26262-3 · ISO 21448 · ISO/SAE 21434 Cl.15

2 生命周期对齐 *Aligned lifecycles*
三套 V 模型在概念、设计、验证、运行四点强制交互
ISO 26262-2 · ISO/SAE 21434 Cl.5–6

3 跨域可追溯 *Cross-domain traceability*
危害与威胁 → 目标 → 需求 → 验证证据，双向可追溯
ISO 26262-8 · ISO/SAE 21434 Cl.9

4 联合安全论证 *Integrated safety case*
一份论证覆盖三类主张，显式记录冲突与权衡
ISO/TS 5083 · ISO/PAS 8800

5 体系与合规对接 *Compliance interface*
CSMS / SUMS 与功能安全管理体系共用治理与证据
UN R155 / R156 · GB 44495 / 44496



四个强制交互点与三套标准的工作产物对照
Four Mandatory Interaction Points, Mapped to Work Products

概念阶段 *Concept*

ISO 26262
相关项定义 · HARA · 安全目标
Item Definition · HARA · Safety Goals

ISO 21448
ODD 定义 · 触发条件初步分析
ODD Definition · Preliminary Analysis of Triggering Conditions

ISO/SAE 21434
资产识别 · TARA · 网络安全目标
Asset Identification · TARA · Cybersecurity Goals

共用一份相关项定义与 ODD
Share a common item definition and ODD

设计阶段 *Design*

ISO 26262
功能与技术安全需求 · 安全机制
Functional & Technical Safety Requirements · Safety Mechanisms

ISO 21448
功能改进措施 · 性能规格
Functional Improvement Measures · Performance Specifications

ISO/SAE 21434
网络安全需求 · 架构与控制措施
Cybersecurity Requirements · Architecture & Control Measures

显式记录三类需求的冲突与权衡
Explicitly document conflicts and trade-offs among the three categories of requirements

验证阶段 *Verification*

ISO 26262
故障注入 · 集成验证 · 安全确认
Fault Injection · Integration Verification · Safety Validation

ISO 21448
场景测试 · 充分性论证
Scenario Testing · Sufficiency Argumentation

ISO/SAE 21434
渗透测试 · 网络安全验证报告
Penetration Testing · Cybersecurity Verification Report

把攻击场景纳入安全验证用例
Incorporate attack scenarios into safety verification test cases

运行阶段 *Operation*

ISO 26262
现场监控 · 安全相关变更管理
Field Monitoring · Safety-Related Change Management

ISO 21448
场景库更新 · 残余风险复评
Scenario Database Update · Residual Risk Re-evaluation

ISO/SAE 21434
漏洞监测 · 事件响应 · 安全 OTA
Vulnerability Monitoring · Incident Response · Secure OTA

任一变更触发三方联合复评
Any change triggers a joint re-evaluation by all three parties

每个交互点同时输出三类工作产物，任何一类缺失都不放行。
Each gate must deliver work products from all three frameworks — no gate passes with one missing.

目录
CONTENTS

1 标准与法规解析
Analysis of Standards & Regulations

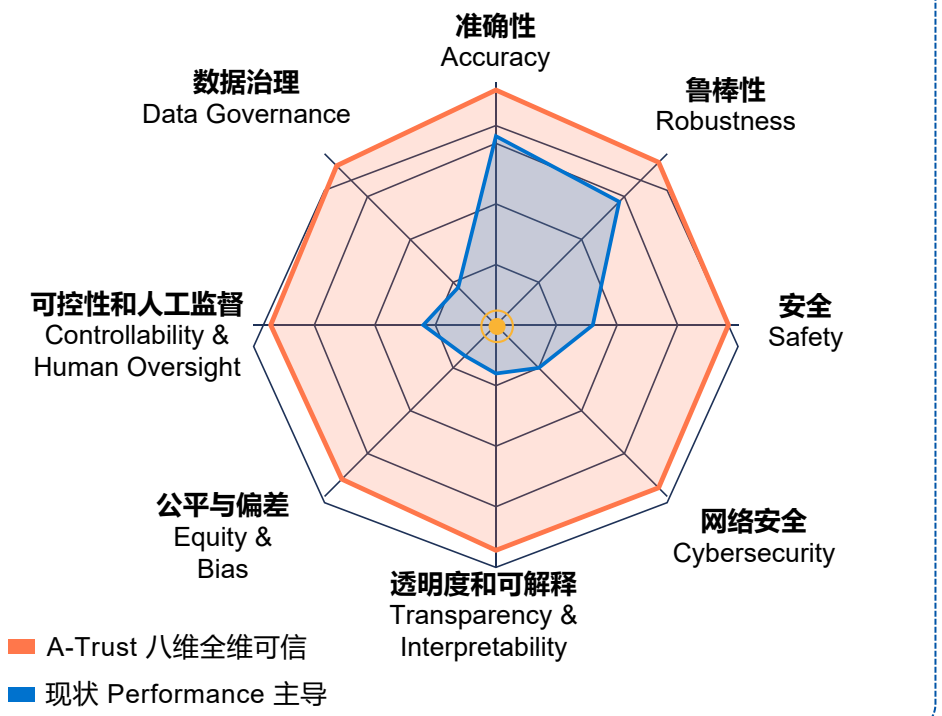
2 标准协同研究
Research on Standard Collaboration

3 中国汽研实践
Practice by CAERI

实践1：车用AI可信度能力分级体系（A-Trust）

Practice 1: Automotive AI Trustworthiness Level Testing & Assessment

A-TRUST：八维可信 · 全域通用



中国汽研、TÜV南德共建体系，2026世界人工智能大会正式发布

CAERI and TÜV SÜD jointly establish A-Trust, officially launched at the 2026 WAIC.

智能座舱 Cockpit	智能驾驶 Driving	智能车控 Control	网联车云 Cloud

驾舱融合 / 跨域协同

可信等级 L1 → L4
Trustworthiness Levels

L1	L2	L3	L4
基线可测级	场景验证级	系统可信级	持续保障级
		EU AI Act 高风险合规门槛	行业标杆

两大权威平台联合赋能，深度支撑企业智能车型AI全域可信。

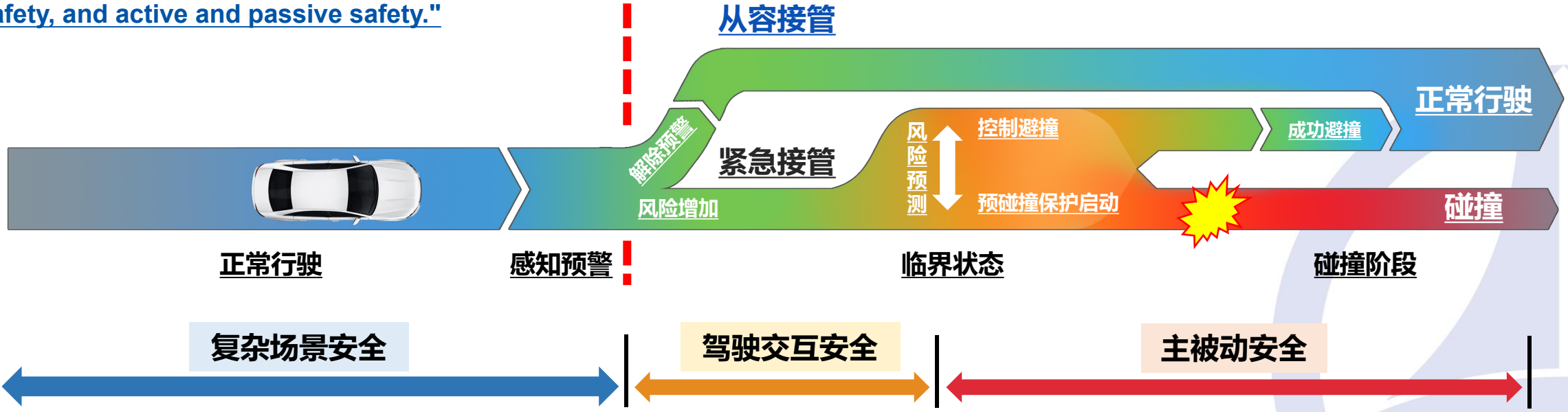
Two authoritative platforms jointly provide support and deeply guarantee the full-compliance automotive AI trustworthy.

实践2：IVISTA2026 智能安全测评
Practice 2: IVISTA 2026 Intelligent Safety Test & Assessment

综合分析车辆行驶过程中的安全风险时间链条，构建包含

“复杂场景安全、驾驶交互安全、网络隐私安全、主被动安全”四维一体的智能安全测评分指数

By comprehensively analyzing the temporal chain of safety risks during vehicle operation, a four-dimensional integrated intelligent safety evaluation sub-index is constructed, encompassing "complex scenario safety, driving interaction safety, network privacy safety, and active and passive safety."



网络与隐私安全（新增） Cybersecurity and Privacy（New）

总结：从分立合规走向标准协同
Summary: From Compliance Separation to Standard Collaboration

接口已经存在
Interfaces already exist
26262 与 21434 之间、26262 与 21448 之间的引用已写入条文，协同不是新概念。

缺口也真实存在
The gap is real too
21448 与 21434 之间没有直接接口，两条跨域路径没有标准归属。

补位靠流程与责任人
Process closes the gap
把 TARA 攻击路径作为强制输入回注，并在每个交互点指定单一责任人。

展望 Outlook

- 标准持续整合：ISO/PAS 8800 与 ISO/TS 5083 正把 AI 安全与自动驾驶安全纳入同一论证框架
- Ongoing Standards Integration: ISO/PAS 8800 and ISO/TS 5083 are incorporating AI safety and autonomous driving safety into a unified argumentation framework.
- 法规持续加严：网络安全与软件升级已成为准入前提，运行阶段的持续保障能力将成为下一个焦点
- Continuously Tightening Regulations: Cybersecurity and software updates have become prerequisites for type approval, and the capability for continuous assurance during the operational phase will be the next focal point.
- 国际协调深化：GB 强标与 UN R155 / R156 在研制中已做协调，体系与证据的互认仍在推进
- Deepening International Harmonization: Chinese mandatory GB standards have already been coordinated with UN R155/R156 during their development, while mutual recognition of systems and evidence is still being advanced.

融合安全不再是三条平行线，而是一张相互支撑的网。
Integrated Safety is no longer three parallel lines, but one mutually supporting network.



中国汽车工程研究院股份有限公司

China Automotive Engineering Research Institute Co., Ltd.

感谢聆听

Thank you

中国汽研 伴你同行

安全 · 绿色 · 体验

CAERI Care For You