北京航空航天大學
BEIHANG UNIVERSITY

智能网联汽车AI安全与标准研究

Research on AI Safety & Security and Standards for Intelligent Connected Vehicles

杨世春 二级教授

Professor Yang Shichun

北京航空航天大学 交通科学与工程学院

School of Transportation Science and Engineering，Beihang University

联系方式/Tel：13522187088

邮箱/Email：yangshichun@buaa.edu.cn

2026.9.7

一、智能网联汽车AI安全问题分析

Analysis of AI Safety & Security Issues for Intelligent Connected Vehicles

二、智能网联汽车AI安全标准研究

三、智能网联汽车AI安全开发流程

四、智能网联汽车AI安全监测防护

国家政策推动：“人工智能+”和“具身智能”
National policy promotion: "Artificial Intelligence+" and "Embodied Intelligence"

“人工智能+”战略
"Artificial Intelligence+" Strategy

2025年8月26日
《关于深入实施“人工智能+”行动的意见》
"Opinions on Deeply Implementing the 'Artificial Intelligence+' Initiative"



推动智能终端“万物智联”，培育智能产品生态，大力发展**智能网联汽车**等**新一代智能终端**
Promote "intelligent terminal" "universal intelligent connection", cultivate the intelligent product ecosystem, and vigorously develop new-generation intelligent terminals such as **intelligent connected vehicles**

“十五五”规划
the “15th Five-Year” Plan

2026年3月13日
《“十五五”规划纲要》
"The Outline of the 15th Five-Year Plan"



构建未来产业全链条培育体系，推动量子科技、……、**具身智能**、第六代移动通信等成为**新的经济增长点**
Establish a complete industrial chain cultivation system for the future, and promote quantum technology, …, **embodied intelligence**, and the sixth-generation mobile communication to become **new growth points**

“人工智能”和“具身智能”已成为国家发展战略方向
"Artificial Intelligence" and "embodied intelligence" have become the strategic direction of national development.

产业发展驱动：人工智能+汽车
Industry development driven: AI + Automobile

Driving – Full coverage

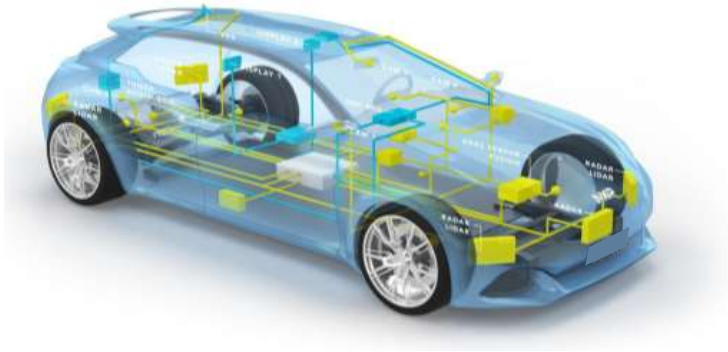


- From Modular to End-to-end
- Application of VLA models

Control – Partial coverage



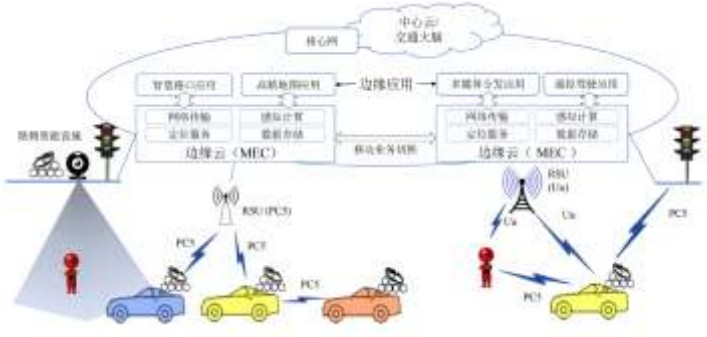
- Intelligent Chassis Control
- Intelligent Vehicle Control



Intelligent Connected Vehicles

+

Vehicle-Road-Cloud System



Cockpit – implementing



- Interactive Dialogue Applications
- Personalized Recommendations and Services

Cloud Service – widely covered



- Big-data Operation Analysis and Services
- Algorithm Iteration and OTA Updates

AI在智能网联汽车以及车-路-云系统中广泛应用，且覆盖范围快速提升

AI is widely applied in intelligent connected vehicles (ICVs) and vehicle-road-cloud systems, with its coverage expanding rapidly

汽车安全发展历程
The history of vehicle safety&security development

传统汽车安全边界
Traditional vehicle safety boundaries

智能网联汽车安全外延
Intelligent Connected Vehicle Safety&Security Extension

被动安全

~1900s

Passive Safety

事故发生后降低伤害后果

Reducing the severity of the injury after the accident

主动安全

~1950s

Active Safety

事故发生前主动识别并预防

Preventive measures were taken to identify and prevent the accident before it occurred.

功能安全

2006

Functional Safety

保障系统故障时仍可控

Ensure that the system remains controllable even in the event of a failure.

预期功能安全

2016

Safety Of The Intended Functionality, SOTIF

应对复杂场景下的误判风险

Deal with the risk of misjudgment in complex scenarios

网络安全

2016

Cyber-security

防范外部攻击与非法入侵

Preventing external attacks and illegal intrusions

数据安全

2018

Data Security

保护数据不被泄露和滥用

Protecting data from being leaked and misused

安全内涵从“机械与控制”扩展到“功能、场景、网络与数据”

The connotation of security has expanded from "mechanics and control" to "functions, scenarios, networks and data".

从传统的主被动防护，发展到智能网联时代面向功能、场景、网络与数据的系统性治理

From the traditional active-passive protection methods, to the systematic governance of functions, scenarios, networks and data in the era of intelligent connectivity

AI驱动汽车变革：从“交通工具”到“具身智能”

AI-Driven Automotive Transformation: From "Means of Transportation" to "Embodied Intelligence"

- 在AI的驱动下，汽车形态正快速从“交通工具”发展为“新一代智能终端”，并成为“具身智能”规模最大、商业化最成熟、产业链最完整的“第一落地场景”

Driven by AI, the form of automobiles is rapidly evolving from "transportation tools" to "new-generation intelligent terminals", and has become the "first practical application scenario" with the largest scale of "embodied intelligence", the most mature commercialization, and the most complete industrial chain.

新一代智能终端
The new generation of intelligent terminals



有AI大脑的“智能空间”

"Intelligent Space" with an AI brain

”人工智能+汽车“
"Artificial Intelligence + Automobiles"



具身智能
embodied artificial intelligence



有身体、能行动的“智能体”

"Intelligent entities" with a physical form

AI正在彻底重塑汽车产业，“含模量”成为衡量汽车智能化水平的新标准

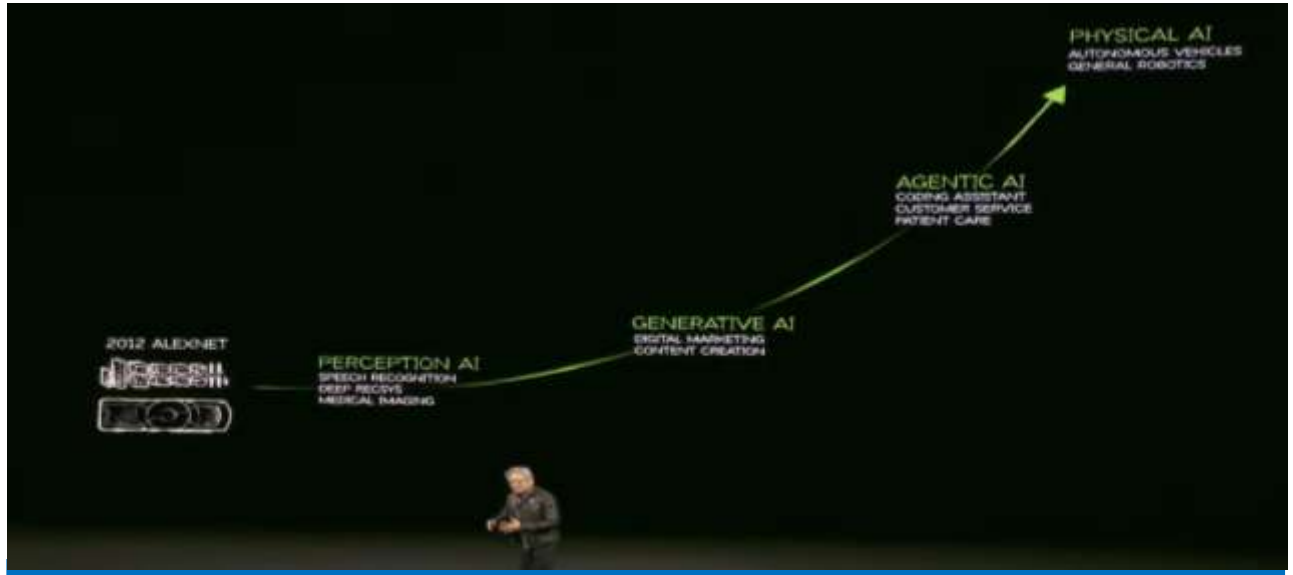
AI is completely reshaping the automotive industry, and "AI Model Ratio" has become a new standard for measuring the level of automotive intelligence.

汽车促进AI进化：“数字AI”发展到“物理AI”

Cars drive the evolution of AI from Digital AI to Physical AI, serving as the core carrier for this transition.

□ AI进化新纪元：从虚拟空间的逻辑推理到真实世界的具身交互

The New Era of AI Evolution: From Logical Reasoning in Virtual Space to Embodied Interaction in the Real World



“物理AI是AI的下一波浪潮。它们是能理解、感知物理定律，并能预测未来状态的系统，通常以机器人和自动驾驶汽车为载体。”

—— 黄仁勋 (Jensen Huang), NVIDIA CEO

"Physical AI represents the next wave of AI. These are systems that can understand and perceive physical laws, and can predict future states. They are typically implemented in the form of robots and self-driving cars."

➢ AI发展的范式转移：

The paradigm shift in the development of AI

数字人工智能	→	物理人工智能
Digital artificial intelligence		Physical Artificial Intelligence
形态：赛博空间 (Cyber)		形态：物理世界 (Physical)
核心：文本、代码、逻辑		核心：物理规律
能力：预测下一个Token		能力：预测下一秒物理状态
Form: Cyber Space (Cyber)		Form: Physical World (Physical)
Core: Text, Code, Logic		Core: Physical Laws
Ability: Predict the Next Token		Ability: Predict the next physical state

➢ 为什么汽车是核心载体？

Why are automobiles the core carriers?

- ✓ **高动态环境：** 必须实时应对复杂的交通流与物理边界；
- ✓ **硬科技集成：** 融合了感知、规划、控制的全栈能力；
- ✓ **规模化部署：** 通过千万级装车实现数据闭环，推动物理规律学习

High dynamic environment: Respond in real time to complex traffic flows;
Hard technology integration: Integrates perception, planning, and control capabilities;
Large-scale deployment: Tens of millions of automobiles on road.

汽车成为促进人工智能从“数字AI”进化到“物理AI”的核心载体

Vehicles serve as the core carrier driving the evolution of artificial intelligence from "digital AI" to "physical AI"

AI特性与安全风险
AI features and safety&security risks

“黑箱”特性
"Black box" characteristic



➢ “黑箱”特性，决策过程难以完全追踪、解释和验证

The "black box" characteristic means that the decision-making process is difficult to fully trace, explain and verify.

数据依赖性
Data dependency



➢ 模型性能受训练数据质量、规模、分布高度影响

The performance of the model is highly influenced by the quality, scale and distribution of the training data.

输出不确定性
Output uncertainty



➢ 输出可能存在幻觉、偏差、误判，带来安全风险

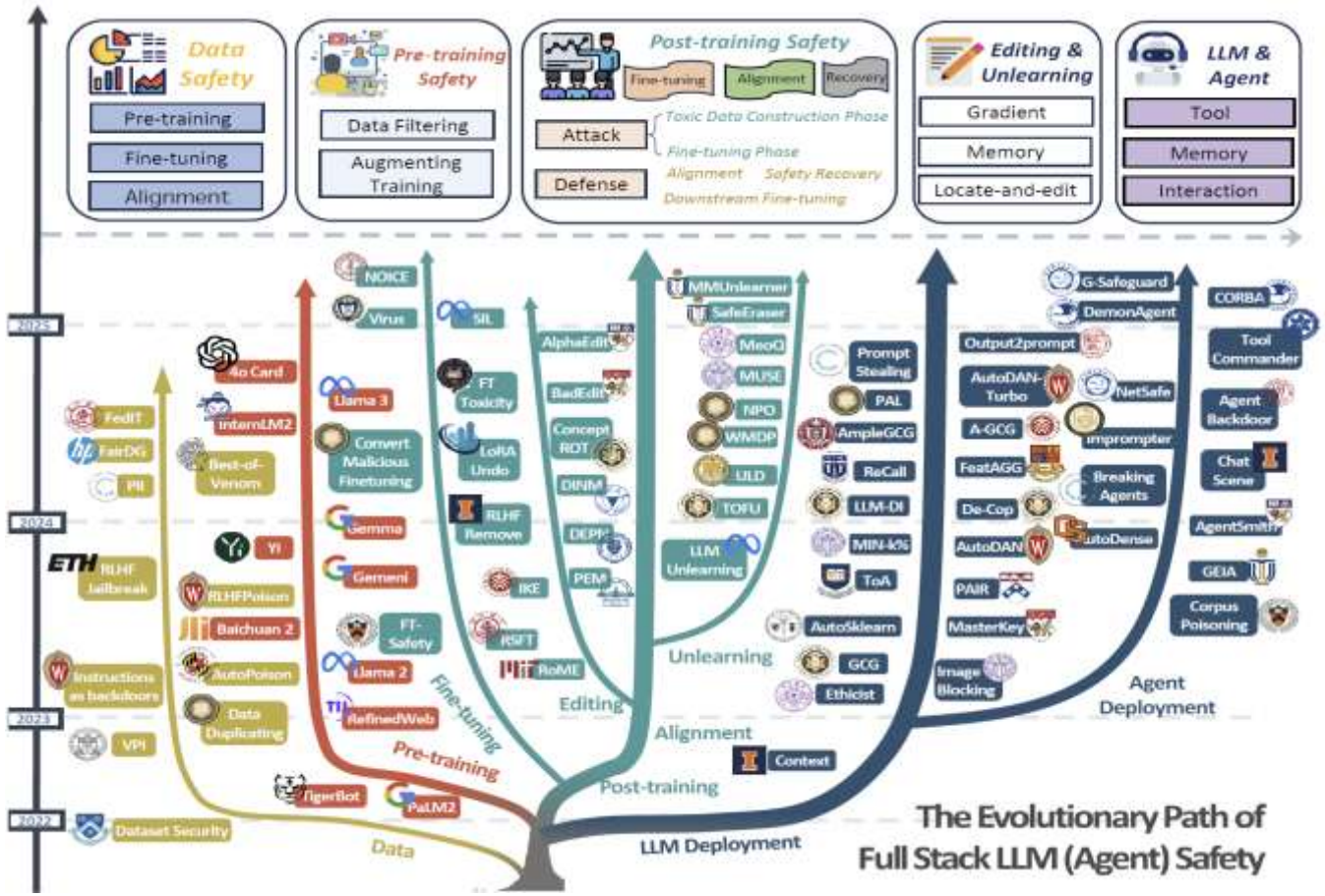
The output may contain illusions, deviations and misjudgments, thereby posing safety risks.

AI的“黑箱”特性、数据依赖性与输出不确定性，共同构成了安全治理的基础挑战

The "black box" nature of AI, its data dependence, and the uncertainty of its outputs all jointly constitute the fundamental challenges in safety&security governance.

AI特性与安全风险
AI features and safety&security risks

AI/大模型全链路安全演进路线
AI/ Large Model Full-Chain Safety&Security Evolution Roadmap



Source： https://arxiv.org/abs/2504.15585A

AI遭受外部攻击的风险
The security risks of AI

	攻击面 Attack surface	防御面 Defensive surface
数据构建 Data construction	数据投毒 Data poisoning 隐私泄露 privacy disclosure ……	数据净化 Data purification 隐私加固 Privacy Enhancement ……
模型训练 model training	后门攻击 Backdoor attack 有害微调攻击 Harmful fine-tuning attack 奖励机制操控 Reward mechanism manipulation ……	分布式防御 Distributed defense 对齐 Align 安全恢复 Security recovery ……
部署应用 Deploy the application	越狱攻击 Escape attack 对抗攻击 Adversarial attack 成员推理 Member inference ……	异常检测 Anomaly detection 对抗训练 Adversarial training 规则约束 Rule constraints 自修正系统 Self-correction system

AI应用全链路（数据、模型、部署）面临外部攻击风险
The full chain of AI application (data, model, deployment) faces external attack risks.

“AI+汽车”的安全新挑战

The safety&security challenges brought by "AI + automobiles"

□ 汽车逐渐从“AI+汽车”转为“[AI]X[汽车：机械+电子+通信]”的深度融合渗透

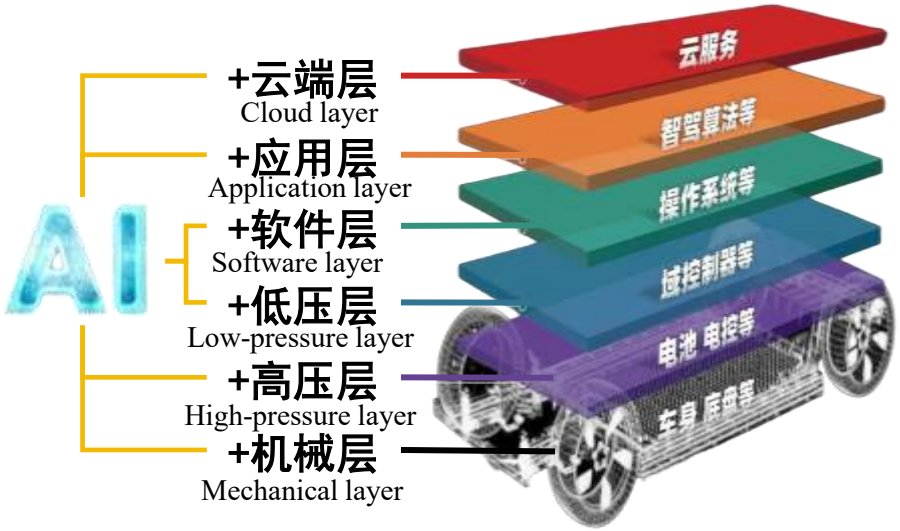
Cars are gradually shifting from the "AI + automobiles" model to a more integrated and profound penetration of "[AI] X [automobile: mechanical + electronic + communication]".

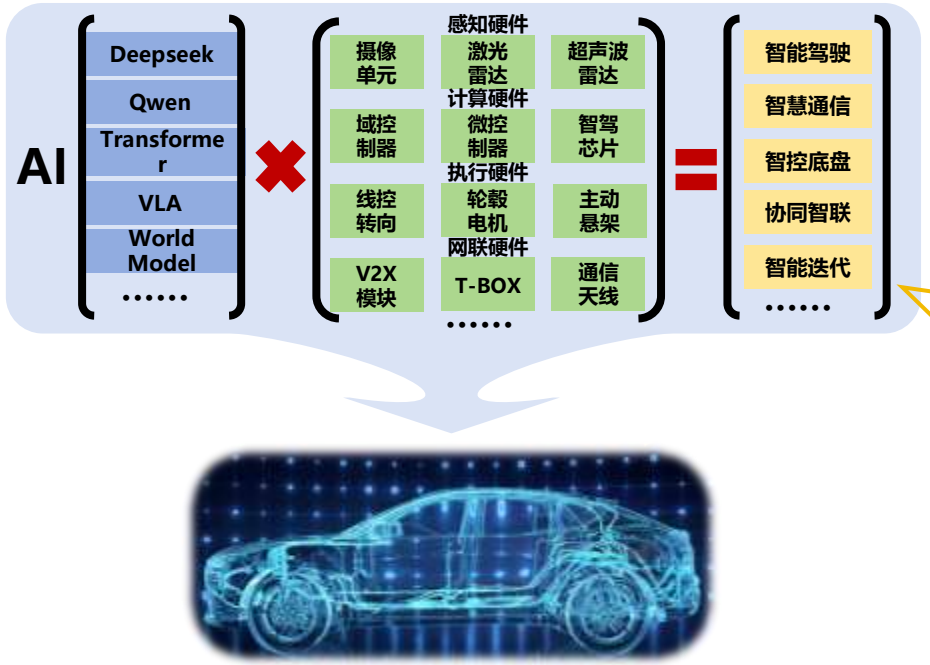
AI赋能汽车

AI-powered automobiles

AI渗透汽车

AI infiltration of automobiles







风险物理化

Risk physicalization

对抗攻击 Adv. Attack



风险跨域化

Risk Diversification



安全风险呈现“物理化、跨域化”新特征

The safety&security risks have taken on new characteristics of "physicalization and cross-domainization"

“AI+汽车”的安全新挑战

The safety&security challenges brought by "AI + automobiles"

□ AI引入后，汽车安全面临“多维度、高风险、全生命周期”新挑战

After the introduction of AI, automotive safety&security now faces new challenges that are "multi-dimensional, high-risk and across the entire lifecycle".

风险来源多样

The sources of risks are diverse.



数字世界+物理世界

Digital world + Physical world

物理安全

physical safety



直接影响行车、乘员与道路安全

Directly affecting driving, passengers' safety and road safety

开发—运行全流程

The entire process of development and operation



数据 训练 测试 部署 运行 OTA

Data Training Testing Deployment Operation OTA

多维度安全

Multidimensional safety&security



不再是单一安全问题

It is no longer a single security issue

高风险

high-risk



失效后果更直接、更严重

The consequences of failure are more direct and more severe.

全生命周期

full life circle



设计、开发、验证、运营持续管理

Design, development, verification, and continuous operation management

国内外加强“AI+汽车”安全标准制定
Global efforts on "AI + automobiles" safety&security standards

□ “AI+汽车”安全引发国内外广泛关注，国际标准已发布，国内正在加快推进标准制定工作

The "AI + automobiles" safety issue has attracted global widespread attention. International standards have been released, and China is accelerating the process of standards formulation.

全球首个汽车AI安全标准
The world's first automotive AI safety standard



ISO/PAS 8800:2024
《道路车辆-安全和人工智能》

2024年12月正式发布

ISO/PAS 8800:2024 "Road Vehicles - Safety and Artificial Intelligence" was officially released on December 2024.

汽车AI安全相关国标
China National Standard on AI Safety & Security



汽车AI安全系列国标正在制定中

China national standard for the automotive AI safety series is currently under development.

车用人工智能标准化促进中心
Automotive Artificial Intelligence Standardization Promotion Center







2025年全国汽标委发起成立**车用人工智能标准化促进中心**，从**车用AI安全管理体系、风险分级、数据安全、信息安全**等角度开展标准研究与制定工作

The National Automotive Standardization Committee has initiated the establishment of the Vehicle Artificial Intelligence Standardization Promotion Center. It will conduct standard research and formulation work from perspectives such as the vehicle AI safety management system, risk classification, data security, information security, and AI safety assessment.

一、智能网联汽车AI安全问题分析

二、智能网联汽车AI安全标准研究

AI Safety & Security Standards for Intelligent Connected Vehicles

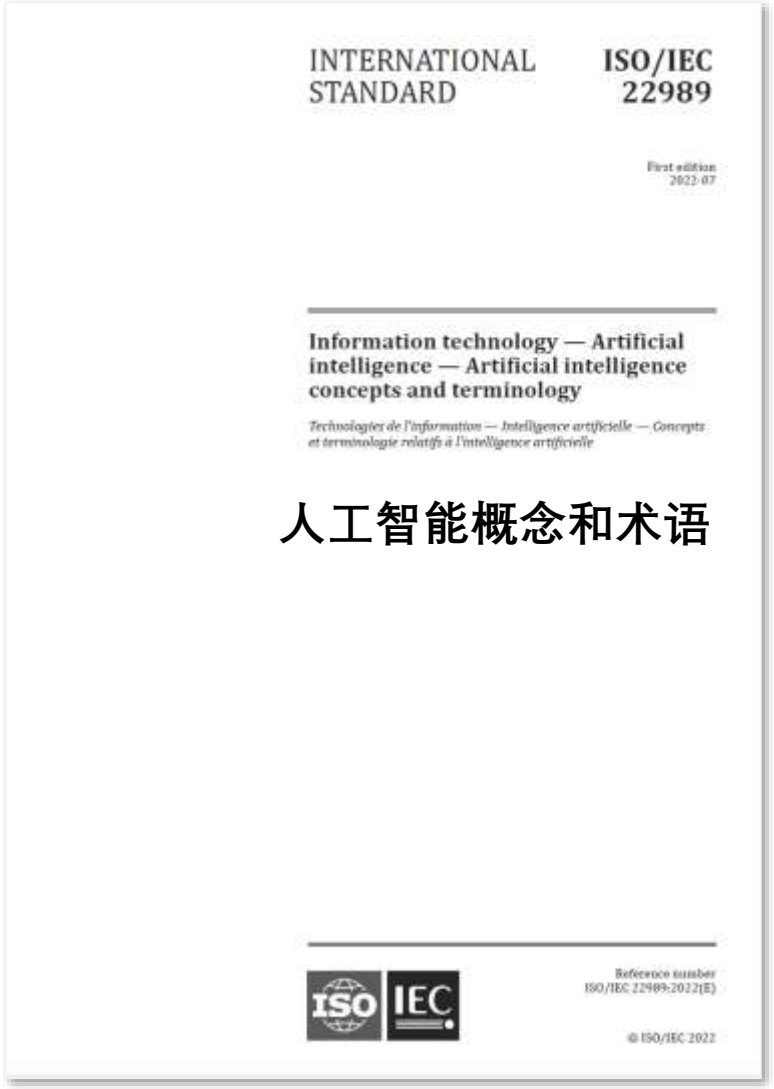
三、智能网联汽车AI安全开发流程

四、智能网联汽车AI安全监测防护

相关国际标准 - ISO/IEC 22989

Relevant international standard - ISO/IEC 22989

ISO/IEC 22989:2022 AI concept and terminology

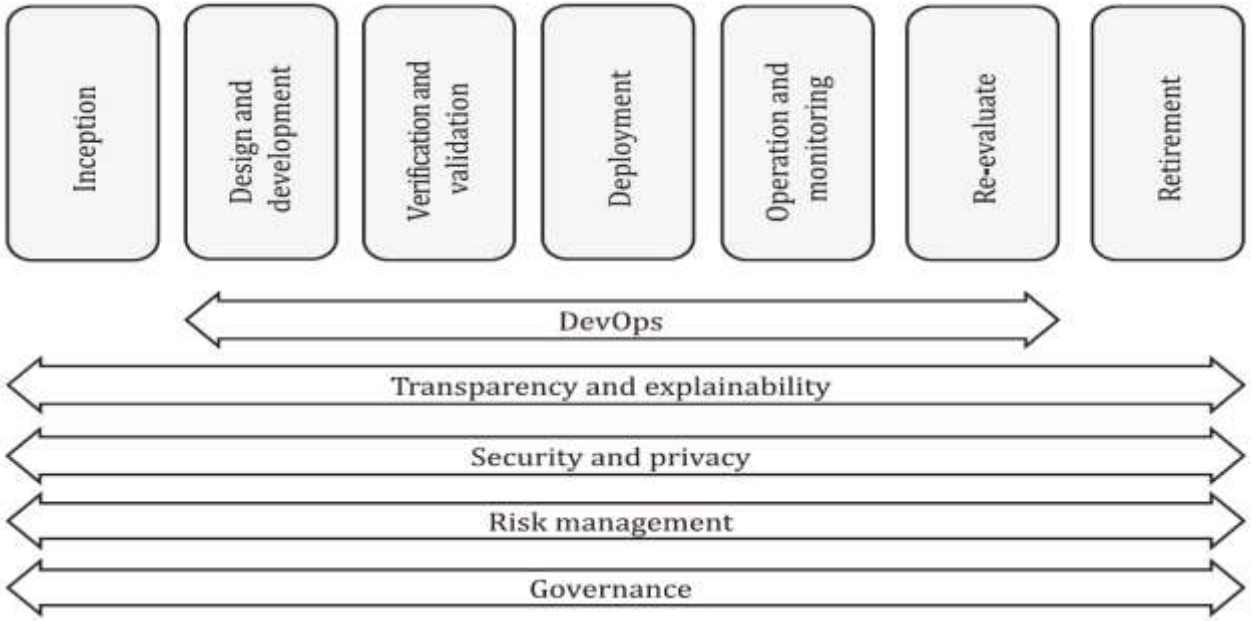


- 人工智能领域的基础性标准“总纲”，是构建整个AI治理框架的基石。

  ……

- 定义了贯穿AI领域的**核心术语**，明确了AI相关的**属性**（如鲁棒性、可解释性等）和**生命周期概念**

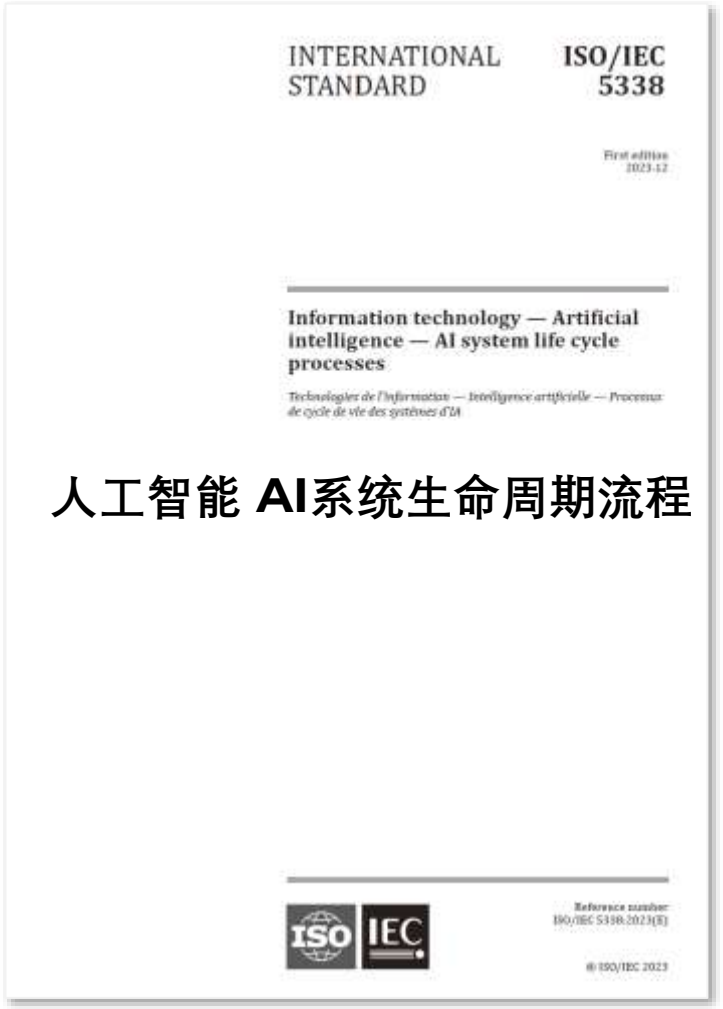
  Defined the core terms that run through the entire field of AI, clarified the attributes related to AI (such as robustness, interpretability, etc.) and the concepts of the AI life cycle



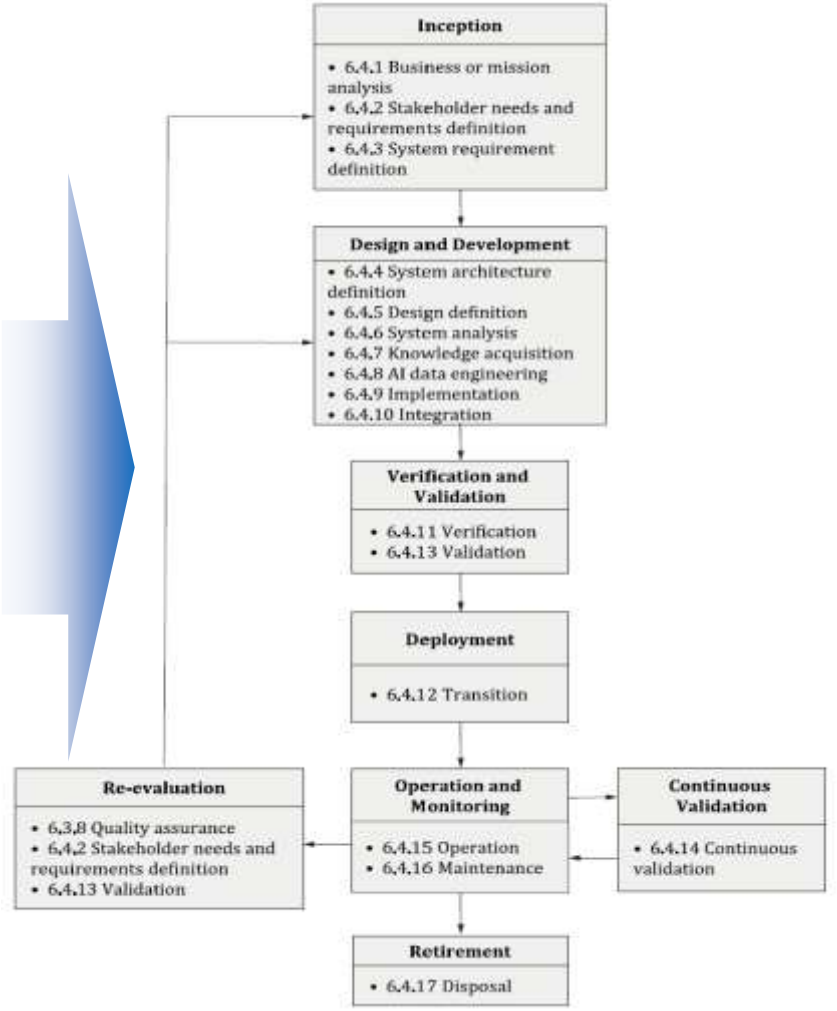
相关国际标准 - ISO/IEC 5338

Relevant international standard - ISO/IEC 5338

ISO/IEC 5338:2023 Information technology — Artificial intelligence — AI system life cycle processes



人工智能 AI系统生命周期流程



- ◆ 指导组织如何规范、可控地开发AI系统的国际通用“操作手册”。

……

- ◆ 定义了通用的AI系统开发与管理过程

Defined a universal process for the development and management of AI systems

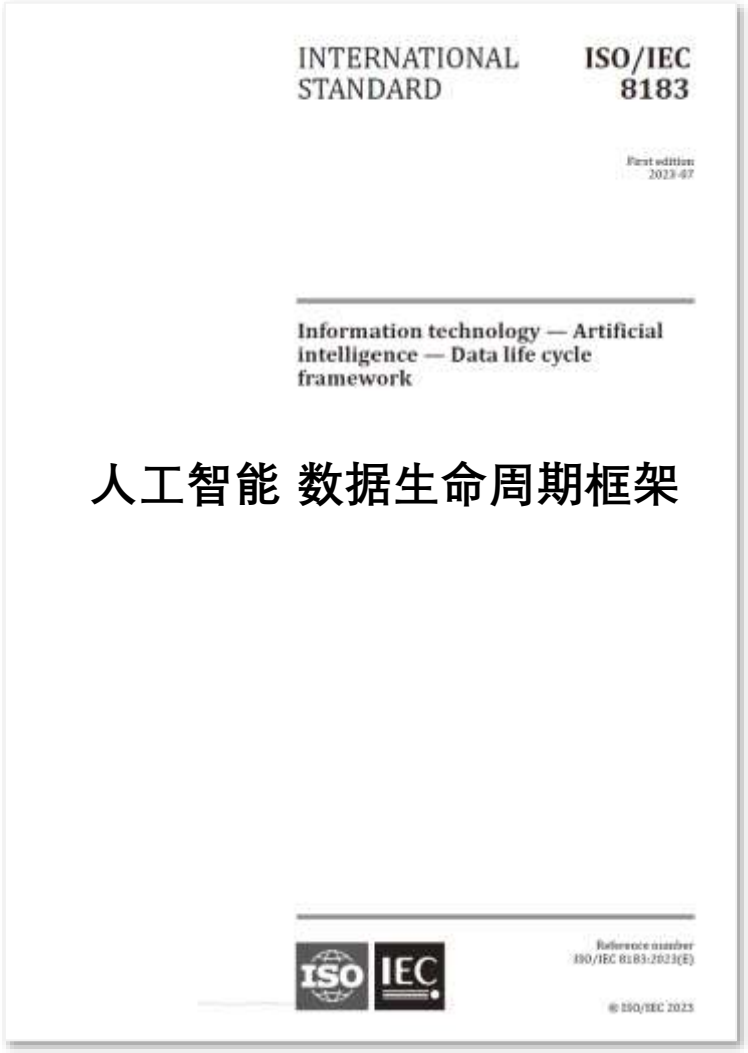
- ◆ 将AI系统开发从概念设计、工程实现、部署运行到持续维护和退役的全流程进行规范化管理

Standardize the entire process of AI system development, including concept design, engineering implementation, deployment and operation, as well as continuous maintenance and decommissioning

相关国际标准 - ISO/IEC 8183

Relevant international standard - ISO/IEC 8183

ISO/IEC 8183:2023 Information technology — Artificial intelligence — Data life cycle framework



◆ 首个为AI系统建立完整数据生命周期管理框架的国际标准，AI数据治理的“基石”

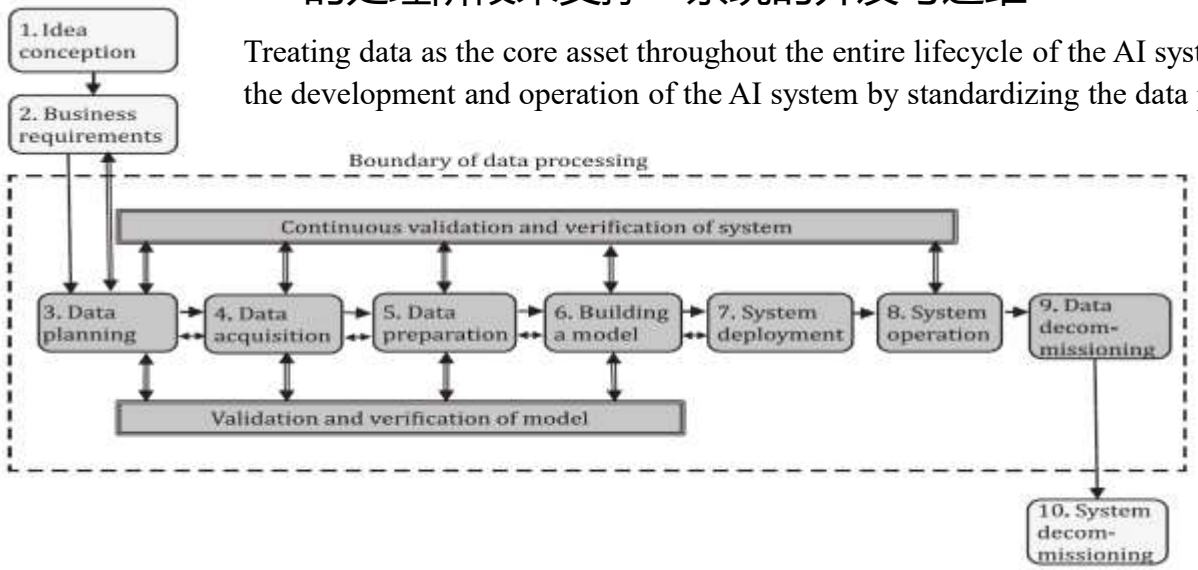
The first international standard to establish a complete data lifecycle management framework for AI systems, serving as the cornerstone of AI data governance.

◆ 提供了**数据生命周期框架**，涵盖了从数据获取、创建、开发、部署、维护到最终退役的全部阶段及相关操作

It provides a data lifecycle framework, covering all stages from data acquisition, creation, development, deployment, maintenance to eventual retirement, as well as related operations.

◆ 将数据视为贯穿AI系统全生命周期的核心资产，通过规范数据的处理阶段来支撑AI系统的开发与运维

Treating data as the core asset throughout the entire lifecycle of the AI system, and supports the development and operation of the AI system by standardizing the data processing stages.



相关国际标准 - ISO/PAS 8800

Relevant international standard - ISO/PAS 8800

ISO/PAS 8800:2024 Road vehicles — Safety and artificial intelligence



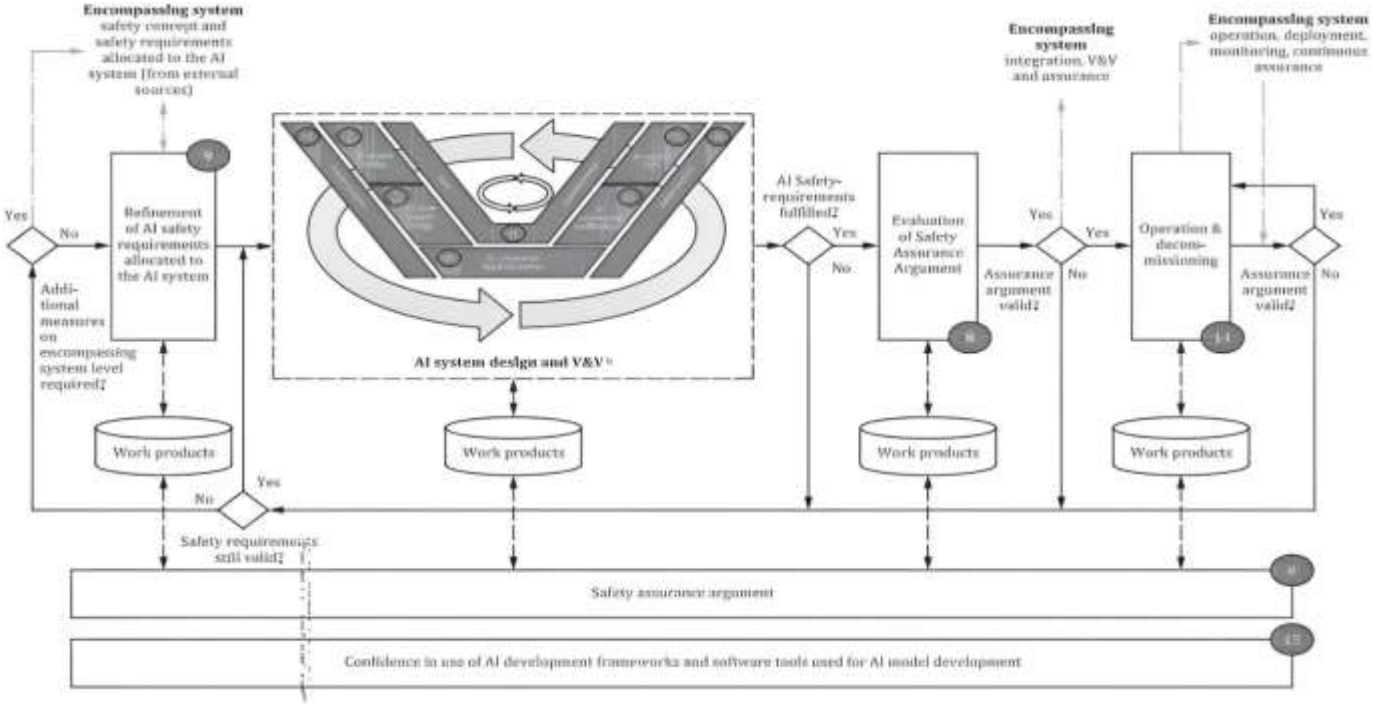
道路车辆 安全和人工智能

◆ **全球首个针对汽车领域人工智能安全的权威标准**

The world's first authoritative standard for artificial intelligence safety in the automotive domain.

◆ 定义了道路车辆**AI安全生命周期**，并围绕**安全管理、安全需求推导、安全分析、验证确认**等关键流程，提出了具体要求

The AI safety life cycle of road vehicles has been defined, and specific requirements have been proposed based on key processes such as safety management, derivation of safety requirements, safety analysis, and safety V&V.



相关国内标准 - GB 44721—2026

Relevant domestic standard - GB 44721—2026

GB 44721—2026 智能网联汽车　自动驾驶系统安全要求

Intelligent and connected vehicle—Safety requirements for automated driving system


ICS 43.020
CCS T 40

GB

中华人民共和国国家标准

GB 44721—2026

代替 GB/T 44721—2024

智能网联汽车　自动驾驶系统安全要求

Intelligent and connected vehicle—Safety requirements for automated driving system

2026-07-30 发布　　2027-07-01 实施

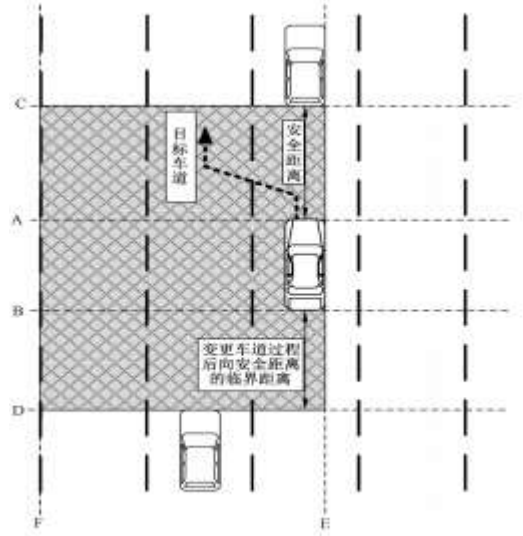
国家市场监督管理总局
国家标准化管理委员会　发布

- **强制性国家标准，2026-07-30日发布，2027-07-01实施**

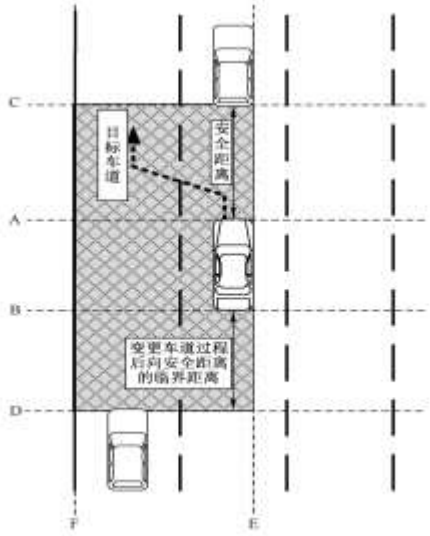
Mandatory national standard, released on July 30, 2026, implemented on July 1, 2027

- 针对 L3/L4 自动驾驶车辆提出**全生命周期安全保障要求**，规范**动态驾驶任务、最小风险策略、故障处置、安全档案及多手段验证试验**，对自动驾驶系统**风险评估、失效分析、仿真验证**提出强制约束。为 L3/L4 自动驾驶产品市场准入**划定安全底线**，但针对车用人工智能系统，仍**缺少体系化的安全开发流程相关规范**

It puts forward full-life-cycle security assurance requirements for L3/L4 automated-driving vehicles, regulates dynamic driving tasks, minimum risk maneuvers, fault handling, safety files and multi-approach verification tests, and imposes mandatory constraints on risk assessment, failure analysis and simulation verification of automated driving systems. It sets the safety baseline for market access of L3/L4 automated-driving products, yet systematic specifications for the safety development process of automotive AI systems are still lacking.



a）　目标车道外侧有车道的场景



b）　目标车道外侧无车道的场景

一、智能网联汽车AI安全问题分析

二、智能网联汽车AI安全标准研究

三、智能网联汽车AI安全开发流程

AI Safety&Security Development Process for Intelligent Connected Vehicles

四、智能网联汽车AI安全监测防护

智能网联汽车AI安全开发流程

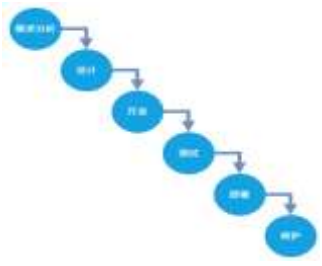
AI Safety&Security Development Process for Intelligent Connected Vehicles

□ 开发流程是保障汽车电子电气系统安全的关键

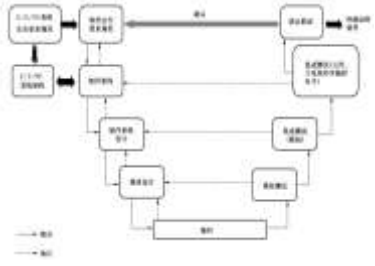
The development process is the key to ensuring the safety&security of automotive electrical and electronic systems.

□ “V型”开发流程已成为汽车电子电气系统安全开发最为广泛应用的流程

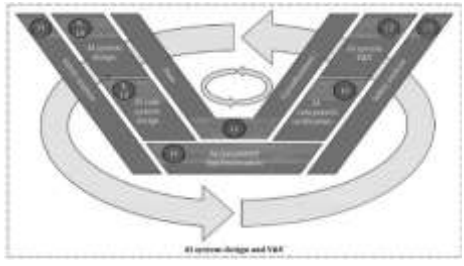
The "V-model" development process has become the most widely used process for the safety development of automotive E/E systems.











1970s
瀑布模型
Waterfall Model

- ◆ 1970年由温斯顿•罗伊斯提出
  Proposed by Winston Royce in 1970
- ◆ 将工程化思想引入软件开发，为无序的开发活动建立结构化流程，便于管理、分工和质量控制
  Introduced engineering thinking into software development, establish-ing structured processes for disorder-ly development activities, facilitating management, division of labor, and quality control
- ◆ 缺点：误差传导、难以适应需求变化
  Disadvantages: error propagation, difficulty adapting to requirement changes

1980s
V模型
V Model

- ◆ 1980年由保罗•洛克首次提出
  First proposed by Paul Rook in 1980
- ◆ 将测试提升至与开发同等重要的地位，测试阶段与开发阶段一一对应
  Elevated testing to the same level of importance as develop-ment, with testing phases cor-responding one-to-one with development phases
- ◆ 军工、航空航天率先采用，逐步应用到汽车嵌入式软件开发
  First adopted in military and aerospace industries, then gradually applied to automotive embedded software development

2000
IEC61508 功能安全
Functional Safety

- ◆ 明确引入了 V 模型作为安全相关软件的开发生命周期模型
  Explicitly introduced the V-Model as the development lifecycle model for safety-related software
- ◆ IEC 61508成为工业功能安全的“基石”和“母标准”
  IEC 61508 became the "cornerstone" and "mother standard" for industrial function-al safety
- ◆ 扩展应用到航空、核电、汽车、机械等领域
  Extended and applied to fields such as aviation, nuclear power, automotive, and machinery

2011
ISO 26262 汽车功能安全
Automotive Functional Safety

- ◆ 由IEC 61508派生而来，将V模型贯穿到汽车电子电气系统开发全生命周期，拥有核心结构地位
  Derived from IEC 61508, the V-model is applied throughout the full lifecycle of automotive electrical and electronic system development, holding a core structural position.
- ◆ 第三版ISO 26262标准正在修订中，其中一项重要更新就是加入对人工智能应用的安全考虑
  The third edition of the ISO 26262 standard is currently under revision, and one of its important updates is the inclusion of safety considerations for artificial intelligence applications.

2024
ISO/PAS 8800
道路车辆—安全与人工智能
Road vehicles — Safety and AI

- ◆ 全球首个专为道路车辆AI安全制定的标准，定义了道路车辆AI安全生命周期
  The world's first standard specifically developed for road vehicle AI safety, defining the AI safety lifecycle for road vehicles.
- ◆ 局限性：PAS仅为公开可用规范，未给出明确安全要求
  Limitation: As a Publicly Available Specifica-tion,it only provides a publicly available specification without giving clear safety requirements.
- ◆ 正式标准ISO 8800正在制定中，预计2028年发布
  The formal standard ISO 8800 is currently under development, with publication expected in 2028.

智能网联汽车AI安全开发流程
AI Safety&Security Development Process for Intelligent Connected Vehicles

□ “V模型”开发流程 VS 车用AI“数据闭环”开发流程
V-model Development Process VS Automotive AI Data Closed-Loop Development Process





对比维度 Comparison Dimension	传统“V模型”开发 Traditional "V-Model" Development	基于“数据闭环”的开发 Data Closed-Loop Based Development
核心驱动 Core Driver	明确、固定的需求驱动 Clear, fixed requirements driven	海量数据驱动，通过数据流自动发现与解决未知问题 Massive data driven, automatically discovering and solving unknown problems through data flow
开发流程 Development Process	线性、单向，由设计到验证依次推进 Linear, one-way, proceeding sequentially from design to verification	循环、迭代，形成“数据采集→模型训练→部署→再采集”的飞轮效应 Cyclic, iterative, flywheel effect of "data collection → model training → deployment → re-collection"
设计起点 Design Starting Point	从顶层的需求分析和系统架构出发 Starting from top-level requirements analysis and system architecture	从底层的场景数据出发，通过模型训练不断定义和完善系统能力 Starting from scenario data, improving system capabilities through model training
V&V Verification & Validation	多阶段在环测试(MIL/SIL/HIL)，专注于验证设计是否符合需求 Multi-stage in-the-loop testing (MIL/SIL/HIL)	以高保真仿真为核心的持续在线验证，同时兼顾真实与合成数据 Continuous online verification centered on high-fidelity simulation
生命周期 Lifecycle	有终点：版本发布是阶段性终点 Has an endpoint: version release is a milestone endpoint	无终点：部署是新一轮迭代的开始，系统通过OTA持续自我进化 No endpoint: deployment is the beginning of the next iteration; the system continuously evolves itself via OTA

智能网联汽车AI安全开发流程

AI Safety&Security Development Process for Intelligent Connected Vehicles

车用AI开发对“V模型”的挑战

Challenges to the V-Model Posed by Automotive AI Development

- **线性流程的失效**：V模型严格的自顶向下流程，无法兼容AI系统所需的数据采集、模型训练、部署验证的快速迭代

Failure of linear process: The V-model's strict top-down process cannot accommodate the rapid iteration of data collection, model training, and deployment validation required by AI systems.

- **需求的不确定性**：V模型的需求明确且固定，与AI系统通过数据持续学习、能力动态演化的特性相悖

Uncertainty of requirements: The V-model requires clear and fixed requirements, which contradicts the characteristics of AI systems that continuously learn from data and dynamically evolve their capabilities.

- **验证与确认 (V&V) 的范式困境**：传统验证方法难以证明数据驱动的“黑盒”AI模型在所有场景下都安全可靠

Paradigm dilemma of Verification and Validation (V&V): Traditional verification methods struggle to prove that data-driven "black-box" AI models are safe and reliable in all scenarios.

国际标准加紧制定

International Standards

- **第三版ISO 26262标准正在修订中，其中一项重要更新就是加入对人工智能应用的安全考虑，预计2027年发布**

The third edition of the ISO 26262 standard is currently under revision. One of its important updates is the inclusion of safety considerations for artificial intelligence applications, with publication expected in 2027.

- **正式标准ISO 8800 于2024年底发布**

The formal standard ISO 8800 has published at the end of 2024.

构建适用于车用AI系统安全开发的新型流程体系

Establish a new process system suitable for the safe development of automotive AI systems

为行业开展车用AI安全开发提供指导

Provide guidance for the industry in conducting safe development of automotive AI

抢占先机，走向国际，实现标准引领

Standards Go Global

车用人工智能安全开发X+模型

X+ Model for Automotive Artificial Intelligence Safe Development

□ 针对传统V型流程难以适配车用AI系统数据驱动、持续演进的安全特性，提出车用人工智能系统安全开发X+流程，以双V嵌套开发架构耦合运行可信迭代闭环，构建全生命周期系统性安全开发范式

To address the limitation that the traditional V-model fails to adapt to the data-driven and evolving safety features of automotive AI systems, the X+ safety development process is proposed. It couples a dual-V nested architecture with an operational trustworthy iteration loop to form a systematic full-lifecycle safety development paradigm.



车用AI系统安全开发流程标准化研究组

Research Group on Standardization of Safe Development Process for Automotive AI Systems

- **2026年5月17日，车用人工智能标准化促进中心车用AI系统安全开发流程标准化研究组（TG15）在北京正式成立**

On May 17, 2026, the Research Group on Standardization of Safety Development Process for Automotive AI Systems (TG15), under the Automotive AI Standardization Promotion Center, was officially established in Beijing.

- **标志着中国在车用AI系统安全开发流程方向的标准化研究工作正式启动**

This marks the official launch of standardization research in China on safety development processes for automotive AI systems.



车用AI系统安全开发流程标准化研究组（TG15）启动会

Kick-off Meeting of the Research Group on Standardization of Safe Development Process for Automotive AI Systems (TG15), under the Automotive Artificial Intelligence Standardization Promotion Center

序号	单位	单位角色
1	北京航空航天大学（Beihang University）	组长单位
2	中国第一汽车股份有限公司	副组长单位
3	长城汽车股份有限公司	副组长单位
4	中国汽车技术研究中心有限公司	参与单位
5	北汽福田汽车股份有限公司	参与单位
6	引望智能技术有限公司	参与单位
7	中汽智能科技（天津）有限公司	参与单位
8	比亚迪汽车工业有限公司	参与单位
9	上海天壹网安科技有限公司	参与单位
10	斑马智能信息技术股份有限公司	参与单位
11	小米汽车科技有限公司	参与单位
12	大连东软智行科技有限公司	参与单位
13	北京汽车研究总院有限公司	参与单位
14	国汽（北京）智能网联汽车研究院有限公司	参与单位
15	吉利汽车研究院（宁波）有限公司	参与单位
16	东软集团股份有限公司	参与单位
17	上海机动车检测认证技术研究中心有限公司	参与单位
18	赛力斯汽车有限公司	参与单位
19	地平线征程（上海）科技有限公司	参与单位
20	中国汽车工程研究院股份有限公司	参与单位
21	中汽研汽车检验中心（天津）有限公司	参与单位
22	惠州市德赛西威汽车电子股份有限公司	参与单位
23	中国重型汽车集团有限公司	参与单位
24	浙江远程新能源商用车集团有限公司	参与单位
25	中汽研华诚认证（天津）有限公司	参与单位
26	上海蔚来汽车有限公司	参与单位

车用AI系统安全开发流程标准化研究组

Research Group on Standardization of Safe Development Process for Automotive AI Systems

研究组工作方向
Research Group Work Direction

◆ 主要研究车用AI系统全生命周期安全开发流程，明确覆盖需求分析、设计开发、测试验证、运行安全、迭代升级全环节的安全管控要求，制定标准化开发规范与实施指南，全流程保障车用 AI 系统开发安全合规、可控、可追溯。

The research primarily focuses on the full lifecycle secure development process of automotive AI systems, clearly defining the safety control requirements covering all stages—requirements analysis, design and development, testing and validation, operational safety, and iterative upgrades. It aims to establish standardized develop-ment specifications and implementation guidelines, ensuring that the development of automotive AI systems is safe, compliant, controllable, and traceable throughout the entire process.

X∞

“1+N”系列标准
"1+N" Series of Standards

“1”

汽车人工智能 系统安全开发流程规范

Specification for System Safety Development Process of Automotive Artificial Intelligence

+

“N”

- 汽车人工智能 系统安全开发流程规范 第1部分：总则
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 1: General Principles
- 汽车人工智能 系统安全开发流程规范 第2部分：系统架构设计
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 2: System Architecture Design
- 汽车人工智能 系统安全开发流程规范 第3部分：安全分析
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 3: Safety&Security Analysis
- 汽车人工智能 系统安全开发流程规范 第4部分：数据生命周期过程
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 4: Data Lifecycle Process
- 汽车人工智能 系统安全开发流程规范 第5部分：人工智能模型开发
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 5: AI Model Development
- 汽车人工智能 系统安全开发流程规范 第6部分：安全验证与确认
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 6: Safety&Security Verification and Validation
- 汽车人工智能 系统安全开发流程规范 第7部分：运行监测
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 7: Operational Monitoring
- 汽车人工智能 系统安全开发流程规范 第8部分：系统变更
  Specification for System Safety Development Process of Automotive Artificial Intelligence – Part 8: System Change

标准研究：《汽车人工智能 系统安全开发流程规范》

Standard Research: 《Specification for System Safety Development Process of Automotive Artificial Intelligence》

□ 北航牵头开展标准《汽车人工智能 系统安全开发流程规范》研究与编制工作

Leading the research of standard 《Specification for System Safety Development Process of Automotive Artificial Intelligence》

适用范围range of application

- **适用于搭载人工智能系统的M类、N类道路车辆。**
- Applicable to M-class and N-class road vehicles equipped with artificial intelligence systems.
- **适用于车用人工智能系统从概念设计到退役的全生命周期安全开发活动，包括系统架构设计、安全分析、数据管理、模型开发、验证确认、运行监测及系统变更。**
- Applicable to the full lifecycle safety development activities of automotive artificial intelligence systems, from concept design to decommissioning, including system architecture design, safety analysis, data management, model development, verification and validation, operational monitoring, and system change.
- **规定了以“X+”安全开发流程为核心，涵盖车用人工智能系统开发、数据闭环以及运行监测与演进闭环，并将人工智能模型开发贯穿其中。**
- Specifies the development process centered on the X+ model, covering automotive artificial intelligence system development, data closed-loop, and operational monitoring and evolution closed-loop, with AI model development running throughout.

标准定位standard setting

- **在道路车辆功能安全、预期功能安全及人工智能生命周期标准基础上，建立以X+模型为核心的开发流程框架，为整车制造企业、系统供应商及第三方评估机构提供安全开发的活动准则和交付物要求。**
- Based on functional safety, safety of the intended functionality, and AI lifecycle standards, this document establishes a development process framework centered on the X+ model, providing activity guidelines and deliverable requirements for vehicle manufacturers, system suppliers, and third-party assessment organizations.
- **与面向运行阶段的安全标准共同构成车用人工智能全生命周期安全设计、开发、应用与持续改进的完整体系。**
- Together with safety standards for the operational stage, it constitutes a complete system for full-lifecycle safety design, development, application, and continuous improvement of automotive artificial intelligence.

标准研究：《汽车人工智能 系统安全开发流程规范》

Standard Research: 《Specification for System Safety Development Process of Automotive Artificial Intelligence》

□ 当前进展：第1部分 总则 已完成标准立项

Current progress: The standard project for Part 1 General Principles has been approved for initiation.

2026年8月25日-26日，全国汽标委智能网联汽车分技术委员会2026年第四次标准审查会，审查并通过了《汽车人工智能 系统安全开发流程规范 第1部分：总则》的立项申请，将陆续启动后续部分系列标准研制工作。





ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

GB

中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

汽车人工智能 系统安全开发流程规范
第 1 部分：总则

Automotive Artificial Intelligence — Specification for System Safety Development Process — Part 1: General Principles

（点击此处添加与国际标准一致性程度的标识）

草案版次选择

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

一、智能网联汽车AI安全问题分析

二、智能网联汽车AI安全标准研究

三、智能网联汽车AI安全开发流程

四、智能网联汽车AI运行安全防护

AI Operational Safety&Security for Intelligent and Connected Vehicles

基于模型的安全在线风险分析与评估方法

Model-based Online Safety&Security Risk Analysis and Assessment

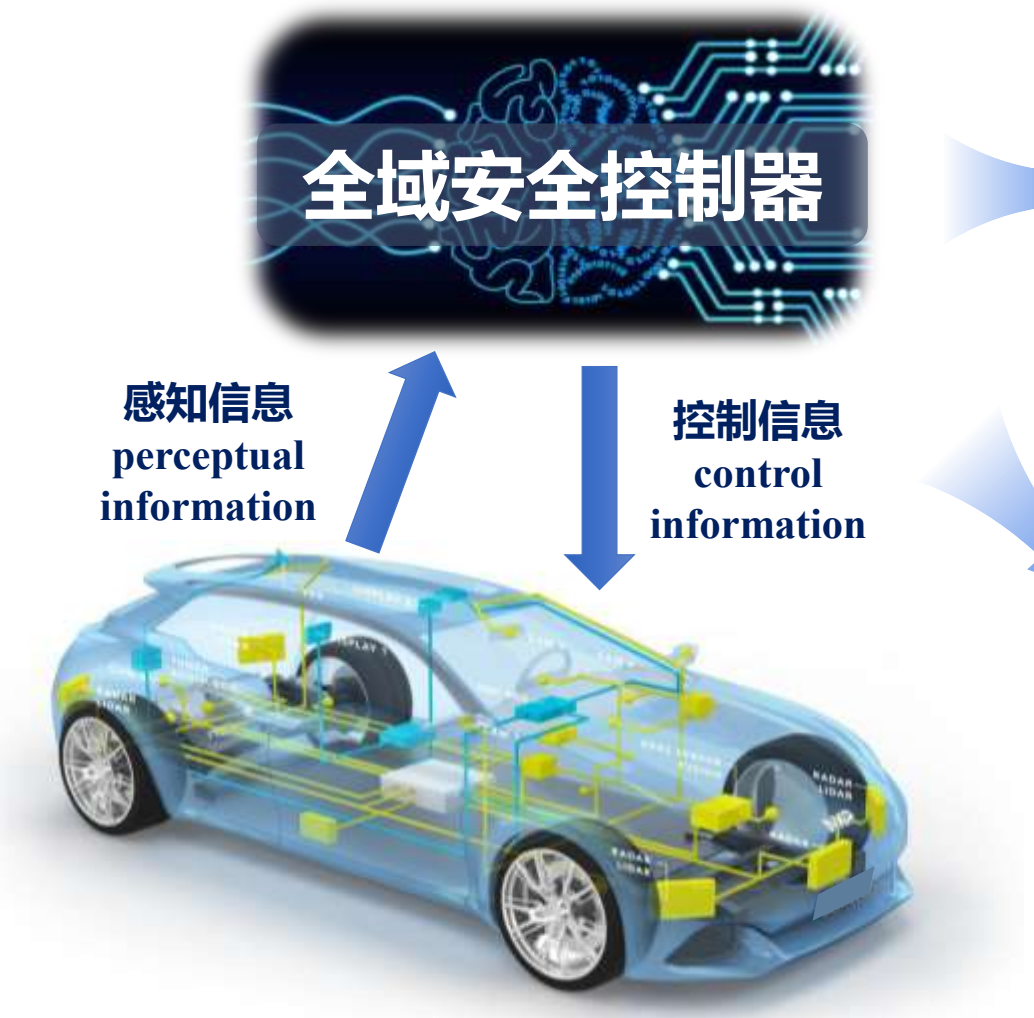
- 提出以**基于模型的安全在线风险分析与评估**（Model-based Online Safety&Security Risk Analysis and Assessment，MOSA）为贯穿全系统的核心方法论，构建"中央安全大脑+域级安全节点"的**全域安全控制器**，实现功能安全、预期功能安全、网络安全、数据安全的四链融合

多域耦合系统数字孪生模型	建立覆盖智驾、座舱、动力、底盘、数据五域的信息物理融合模型，包括车辆动力学模型、执行器故障模型、驾驶员状态模型、AI推理模型、网络攻击模型，作为离线设计与在线评估的统一基准
在线状态估计与故障诊断	基于状态观测器、粒子滤波、动态贝叶斯网络等方法，利用车载传感器与总线信号实时估计系统隐状态，在线检测、隔离、辨识故障与攻击
SECPT动态风险量化评估	构建以"**严重度(S)-暴露度(E)-可控性(C)-传播性(P)-紧迫性(T)**"为维度的在线风险向量，结合可达集分析与安全包络计算，实时输出当前风险等级与未来短时风险演化趋势
风险驱动的MRM在线决策	以风险评估结果为输入，通过模型预测控制与有限状态机混合决策架构，在线生成适应具体故障、具体场景、具体剩余能力的最小风险策略，并由ASIL-D级确定性执行层保障落地

传统 离线分析+规则兜底 → **模型驱动+在线评估+风险自适应**

智能网联汽车“全域安全控制器”

"Safety&Security Controller" for Intelligent Connected Vehicles



安全合规监测 Compliance Monitoring

实时监测汽车AI系统是否符合安全标准和法规

Real-time monitoring of whether the automotive AI system complies with safety standards and regulations

- GB《智能网联汽车 自动驾驶系统安全要求》
  GB《Requirements for Safety of Autonomous Driving Systems in Intelligent Connected Vehicles》
- GB《智能网联汽车 组合驾驶辅助系统安全要求》
  GB《Intelligent Connected Vehicle - Safety Requirements for Integrated Driving Assistance Systems》
- GB 44495《汽车整车信息安全技术要求》
  GB 44495《Technical Requirements for Cybersecurity of Complete Vehicles》
- GB 44496《汽车软件升级通用技术要求》
  GB 44496《General technical requirements for automotive software upgrades》
- ISO/PAS 8800《道路车辆 安全和人工智能》
  ISO/PAS 8800《Road vehicles, safety and artificial intelligence》

运行安全保障 Real-time safety&security guarantee

- **监测**：威胁感知、风险识别
  Monitoring: Threat perception, risk identification
- **评估**：多维分析、量化评估
  Evaluation: Multidimensional analysis, quantitative assessment
- **防控**：策略生成、综合防护
  Prevention and Control: Strategy Generation, Comprehensive Protection

全域安全控制器：汽车AI系统安全合规监测与实时安全保障解决方案

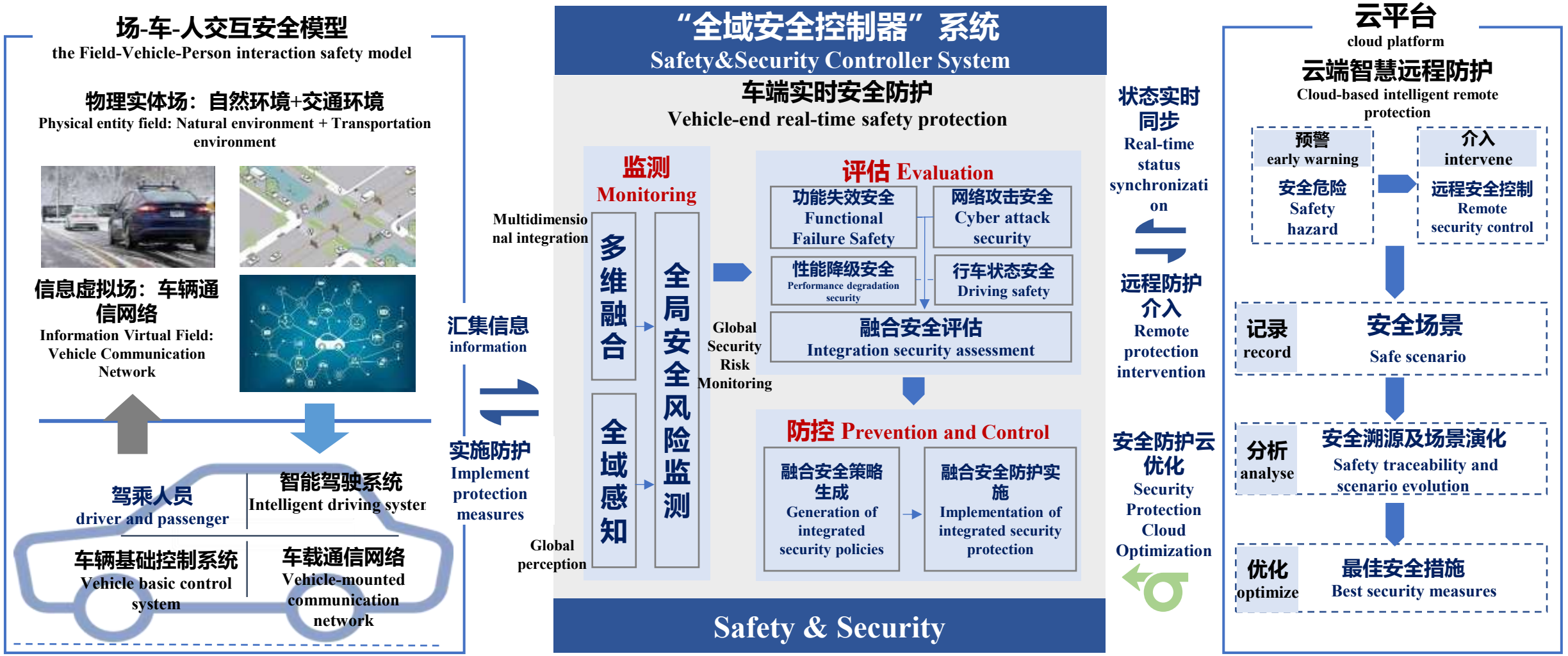
Safety&Security Controller: A Solution for AI System Safety&Security Compliance Monitoring and Real-Time Safety Assurance in Automotive Applications

智能网联汽车“全域安全控制器”系统架构

The "Safety&Security Controller" System Architecture of ICVs

□ 全域安全控制器：基于场-车-人交互安全模型，端云协同保障汽车AI系统安全

Safe&Security Controller: Based on the Field-Vehicle-Person interaction safety model, end-cloud collaboration ensures the security of automotive AI systems.



智能网联汽车AI安全监测与防护

AI Operational Safety&Security for Intelligent and Connected Vehicles

□ 基于多传感器协同的AI对抗攻击监测与防护

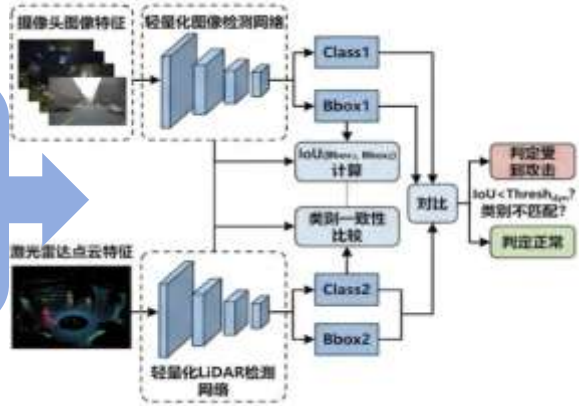
AI-based monitoring and protection against adversarial attacks using multi-sensor collaboration

BEVFusion 被攻击模型
The attacked model

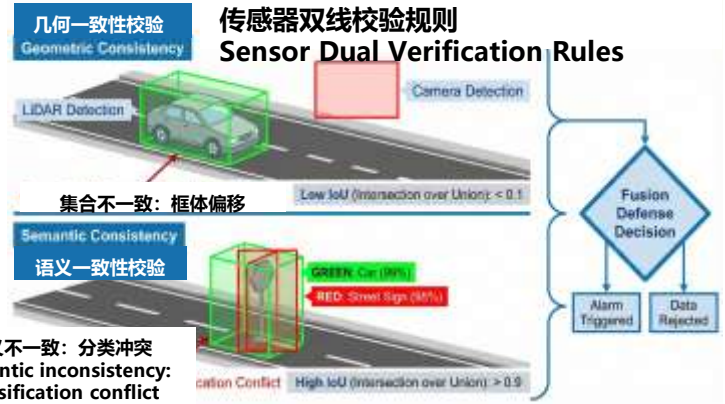


持续监测
攻击触发
Continuous monitoring
Attack trigger

攻击防御模型
Attack-defense model

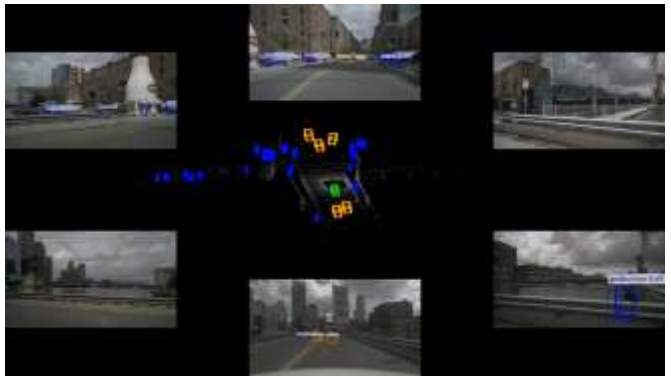


防御规则
Defense rules



实车测试
field test





场景泛化
Scene generalization

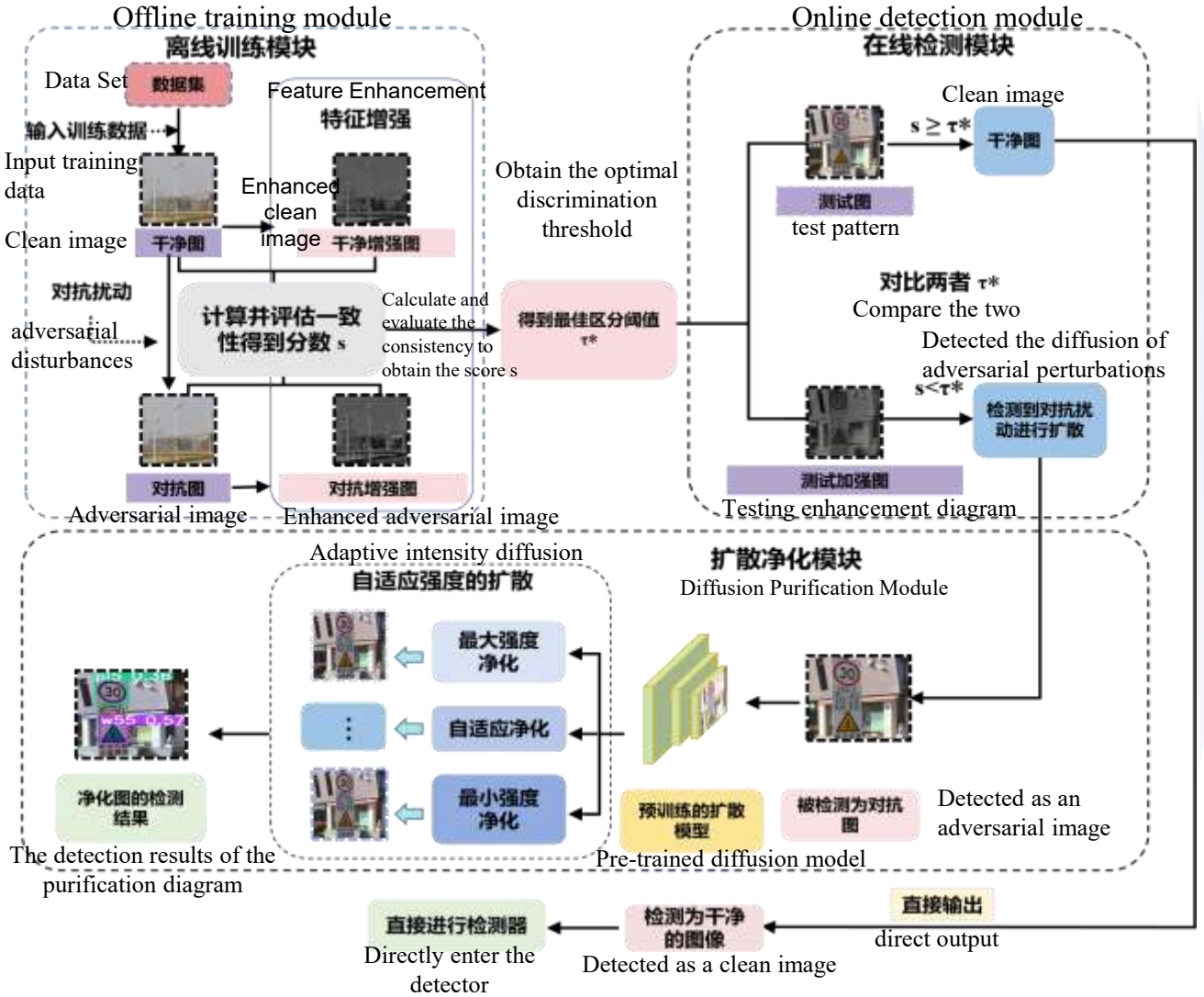


智能网联汽车AI安全监测与防护

AI Operational Safety&Security for Intelligent and Connected Vehicles

□ 基于扩散模型的AI对抗攻击监测与防护

AI Anti-attack Monitoring and Protection Based on Diffusion Models

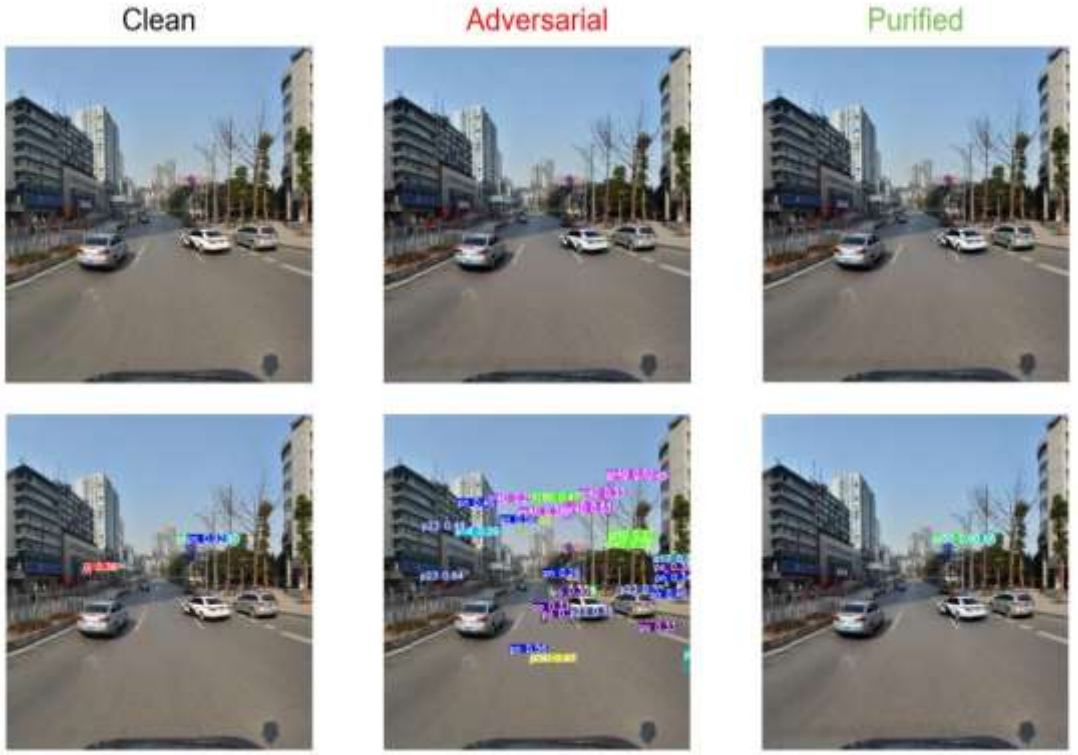


◆ 通过学习干净样本和对抗样本差异阈值，在线识别异常输入

……

◆ 自适应强度调用扩散净化模型，实现对对抗输入的净化处理

……



完成对抗攻击在线检测后并净化

Completing the online detection of counter-attacks and purifying


让安全更可靠，让智能更可信，让出行更美好
Safer, Smarter, Trustworthy – For a Better Mobility

谢谢！
THANKS！

杨世春 二级教授

国家级领军人才、国家级创新团队负责人

北京航空航天大学 交通科学与工程学院

联系方式/Tel：13522187088

邮箱/Email：yangshichun@buaa.edu.cn