



Sharing on the Practice of Risk Governance for Automotive Artificial Intelligence

Contents

1 — **Background**

2 — **Risk Governance for Automotive Artificial Intelligence**

3 — **Challenges of Automotive Artificial Intelligence**

AI Technology Empowering Rapid Development of Global Automotive Industry

AI Transformation: Artificial intelligence is a key driver and core competitiveness in the automotive industry, cutting costs and boosting efficiency across the value chain while upgrading vehicle functions and user experience.



Application of driving automation system

- Automatic labeling of training data
- Synthetic training data and simulation testing
- Large perception models (vision/multimodal)
- End-to-end integrated perception and decision-making



Intelligent cockpit applications

- Intelligent voice assistant
- Multimodal perception and interaction
- Intelligent entertainment system
- Proactive care service



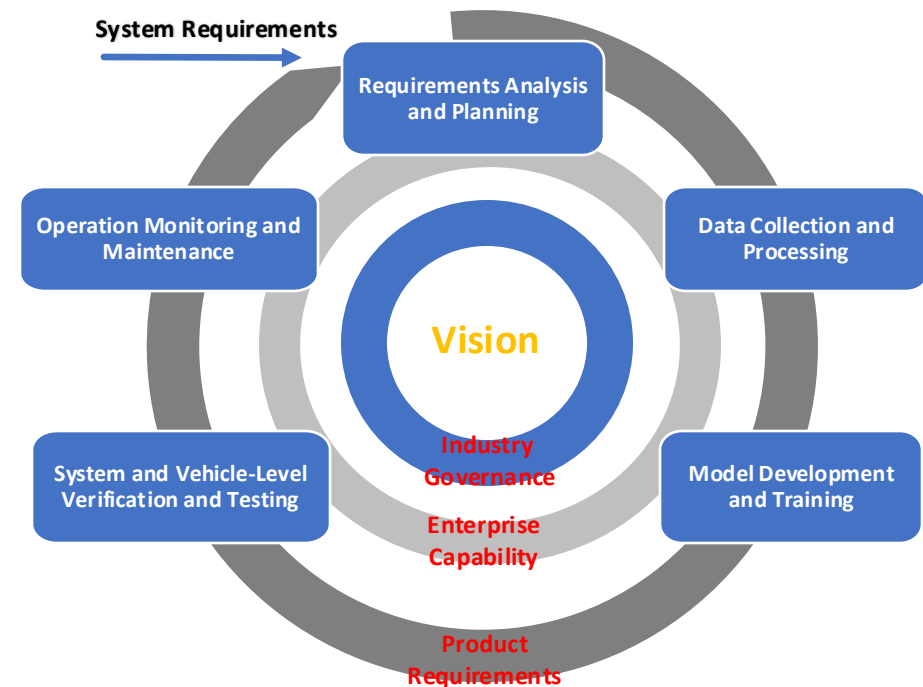
AI-related technologies provide technical support and assurance

- | | |
|------------------|---------------------|
| Machine learning | Deep learning |
| Computer vision | IoT |
| Robotics | Intelligent control |
| Trasformer | Edge computing |

Automotive AI : Delivering AI-powered automotive products AI

The Chinese SAFER AI Program has been Officially Launched

In order to better collaborate through international cooperation, unite global forces, and jointly carry out research on common technologies of artificial intelligence for vehicles, engineering verification, standard pre research, and key database construction, we propose **the Safety & Security Assessment Framework and Engineering Research on Automotive AI**.



Automotive AI Risk Governance

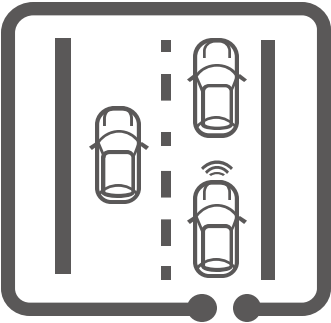
Automotive AI risk governance Based on Risk Assessment and Risk Classification:

1. Conduct risk assessment and corresponding risk classification for AI applications by clarifying risk identification dimensions based on the risk scenarios and risk types of automotive AI applications.
2. Implement risk governance for specific types of risks according to the results of AI risk assessment and classification.



Automotive AI Risk Governance

Use Case



Risk Assessment

Risk Assessment & Classification

Personal Safety Risk

- Casualties due to AI system failure/incorrect outputs

Cybersecurity Risk

- Privacy & Data Protection
- Adversarial Attack

Ethical Risk

- Fairness



Risk Classification

Governance Requirements

- Functional Requirements
- Robustness Requirements
-

- Transparency Requirements
- Cybersecurity Requirements
-

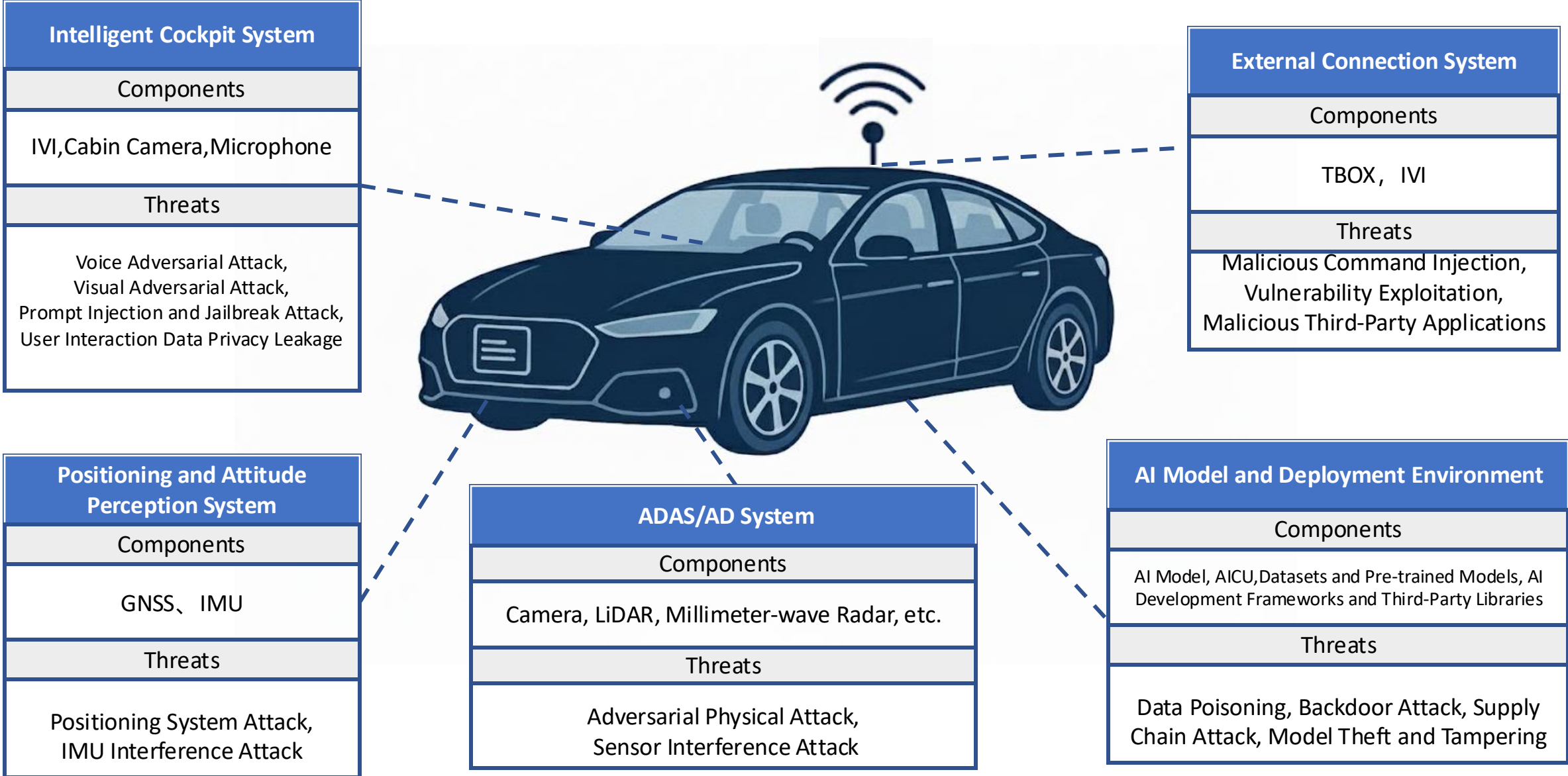
- Fairness

- Simulation Test Items & Requirements
- Closed-course Test Items & Requirements
- Open Road Test Items & Requirements
-

- Notification Function Review and Assessment
- Data Security Test Requirements and Test Items
-

- Data set integrity Requirements
-

Cybersecurity Risk



Cybersecurity Risk

Digital watermarking

Embed invisible identifiers in the vehicle-mounted data stream to achieve rapid traceability in case of leakage.

Differential Privacy

Inject noise during the model training and release stages to ensure that the statistical output does not reveal the individual vehicle behavior.

AI-driven automated auditing

Automatically and continuously verify whether the data processing behaviors at the vehicle end, communication end and cloud end strictly comply with the internal security policies.



Automotive AI Data Security

Trace (against Data Leakage)

Depend on watermarks to uniquely identify the responsible party for tracking, and construct a transparent path for data flow.

Protection (against Data Leakage)

By using differential privacy to reduce the identifiability of sensitive information, we can protect user privacy at its source.

Audit

Utilize AI to generate verifiable and compliant evidence, meeting regulatory requirements.

Ethical Risk

Regarding the ethical principles and requirements for autonomous driving, how should enterprises incorporate them into their technology and products? At present, there is a lack of an effective methodology to guide enterprises in their practices.



Principles and Requirements



GAP



Technology and Products

Thank you!

Contact:

CN: huayiding@catarc.ac.cn