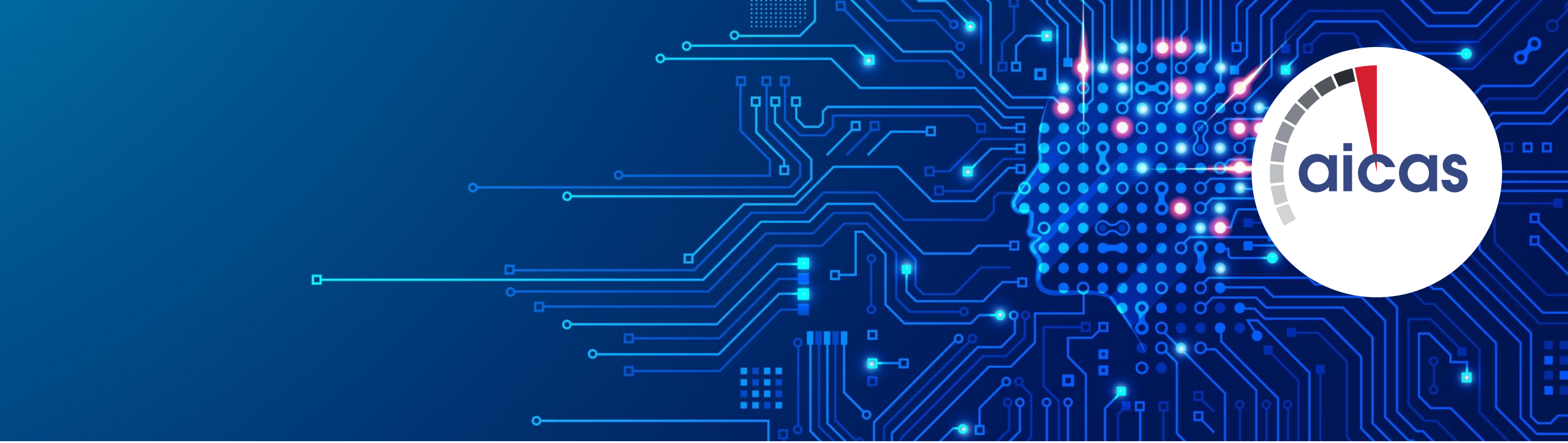


AI for Automotive

Where the Rubber Hits the Road

July 9, 2026

AI Accelerates Everything

Edge AI drives immense gains in operational efficiency

- Cutting operating costs by up to 70%[1]
- Doubling system reliability and uptime[2]

However, enthusiasm hits operational realities!

- **Edge AI must be integrated in edge systems.**
  Time-to-production must be faster; update cycle shorter
- **High quality data is foundational for model training and AI success.** [3]
  GiGo: Garbage in Garbage out! Lack of getting the right data.
- **Latency challenges in deployed models.**
  Cloud AI faces latency and edge AI hardware constraints, both have inferencing latencies
- **Prohibitive Cost**
  Cost of Data transmission and storage can exceed benefits

General performance benefits of edge AI over cloud AI to share operational improvements:
1 arXiv – Quantifying Energy and Cost Benefit of Hybrid Edge Cloud
2 IBM – Edge vs. Cloud AI, Edge's ability to work offline or with intermittent connectivity
3 Nist Study: https://strategyofthings.io/nist

Applications of AI in Vehicles

- **Advanced Driver Assistance Systems (ADAS)**
  - Object detection and recognition
  - Driver assistance
  - Driver monitoring
- **Autonomous Driving**
  - Perception (sensor fusion)
  - Path planning
  - Vehicle command and control
  - Safety monitoring
- **Predictive Maintenance**
  - Realtime vehicle data analysis
  - Recognize failure relevant deviations
  - Optimize service content and intervals
- **Vehicle User Interface**
  - Speech recognition and response
  - Personalization
  - Driver emotion monitoring & intervention
- **Cybersecurity**
  - Detect anomalies in vehicle network traffic
  - Realtime cyberattack identification
  - Realtime intrusion defense
- **Energy Management**
  - Range prediction
  - Battery usage optimization

Roles of AI in Vehicles

- **Data processing**
  - Object Recognition, Perception
  - Path Planning
  - Driver Monitoring Systems (DMS)
  - Occupant Detection
  - Shadow Mode
  - Synthetic Data
- **Control**
  - Automatic Emergency Braking (AEB)
  - EV Battery Management
  - Voice activated systems
  - Autonomous driving

- **Externally**
  - like any other in-vehicle processing
  - inputs -> processing -> outputs
- **Internally**
  - No detailed requirements tracing
  - Challenging for latency determination
  - Challenging for testing
  - Unclear certification path

Challenges of AI in Vehicles

- **Safety and Reliability**
  - Unexpected behavior
  - Overfitting
  - Hallucinations
  - Black-box nature
- **Data Privacy**
  - Risk of data leaks
  - Risk of misuse
- **Security Vulnerabilities**
  - Added complexity
  - Unexpected Behavior
  - Spoofing
  - Prompt Injection
- **Legal and Ethical Issues**
  - Liability
  - Ethical dilemmas in decision-making
  - Deception
  - Regulation change
- **Creation & Maintenance**
  - Proper training data
  - Proper data labeling
  - Model degradation (drifting)
  - API and version compatibility
- **Higher Resource Requirements**
  - Heat and power

Challenges for Model Training

- **Advanced Driver Assistance Systems (ADAS)**
  - Is recognition correct
  - When does the system deactivate itself
  - Driver recognized state vs performance
- **Autonomous Driving**
  - Is the fused world view correct?
  - Actual route vs best route
  - Driver interventions
  - Safety violations
  - Precrash Data
- **Predictive Maintenance**
  - Data around unexpected failures
- **Vehicle User Interface**
  - User feedback
- **Cybersecurity**
  - False positives
  - False responses
- **Energy Management**
  - Deviation between prediction and actual use
  - Ineffectiveness of operations

Model Updates Change the Signal Profile!

Challenge for Software Management

- **Updatability and Traceability**
  - Robust Application Over-the-Air Update
  - Incremental (modular)
  - Self-aware in-vehicle software framework
  - Version tracing and compatibility
- **Dynamic Data Acquisition**
  - Distinction between signal catalogue and data for transmission
  - Data handling updatable during operation
  - Triggers for capturing data for retraining
  - Unit Carrying Signals
- **Safety**
  - Model observability and confidence
  - Model Override
  - Staged testing and deployment

"A few race to build the future,
a few more reflect on what they are building,
and most people are watching and waiting —
observing from afar and merely hoping for the best"

— Pope Leo XIV

Beyond the Technical Challenge

More than just Data

Challenges of Regulatory Guidelines (CRA)

- **Security by design**
  - Safety guidelines are difficult to apply
  - Difficult to specify the functionality
  - Unclear relationship between inputs and outputs
  - Testing is laborious
- **Mandatory life-cycle support**
  - Requires robust OTA (FOTA vs AOTA)
- **Vulnerability reporting**
- **User transparency**
  - Collected data available to user
  - Third party interface
- **Software BOM**
  - Implicit assumption that software update is global: one number for everything
  - Does not consider in-vehicle version tracking: self-awareness
  - Does not address modular update
  - If not handled correctly, this could be the death of the software defined vehicle
- **Risk-Based Classification**
  - Four levels: default, class I, class II, and critical
  - Require increasingly invasive auditing.

EU AI Act

- **Prohibition of Certain Uses**
  The Act outright bans AI systems deemed to pose unacceptable risks.
- **Obligations for High-Risk AI**
  Providers of high-risk AI systems must comply with specific requirements, including risk assessments and transparency measures.
- **General-Purpose AI**
  Providers of general-purpose AI models must publish summaries of training data and comply with copyright laws, especially if their models pose systemic risks.
- **Extraterritorial Application**
  The Act applies to AI providers outside the EU if their systems are used within the EU, requiring them to designate authorized representatives in the EU.

Risk Level	Description
Unacceptable	AI systems that pose a significant risk to fundamental rights and public safety, such as social scoring systems.
High	AI systems that require strict compliance with legal obligations due to their potential impact, such as CV-scanning tools.
Limited	AI systems subject to lighter transparency obligations, where users must be informed they are interacting with AI (e.g., chatbots).
Minimal	AI applications that are largely unregulated, including many current AI applications like video games and spam filters.

Tracing Software Providence

UN Global Regulations

Cyber Security and Software Updating

- UNECE r155—vehicle cybersecurity and cybersecurity management systems
- UNECE r156—vehicle software updates and software update management systems

ISO Guidance and Best Practice

Road Vehicles

- ISO/SAE 21434:2021
  Cybersecurity engineering
- ISO 24089:2023
  Software update engineering

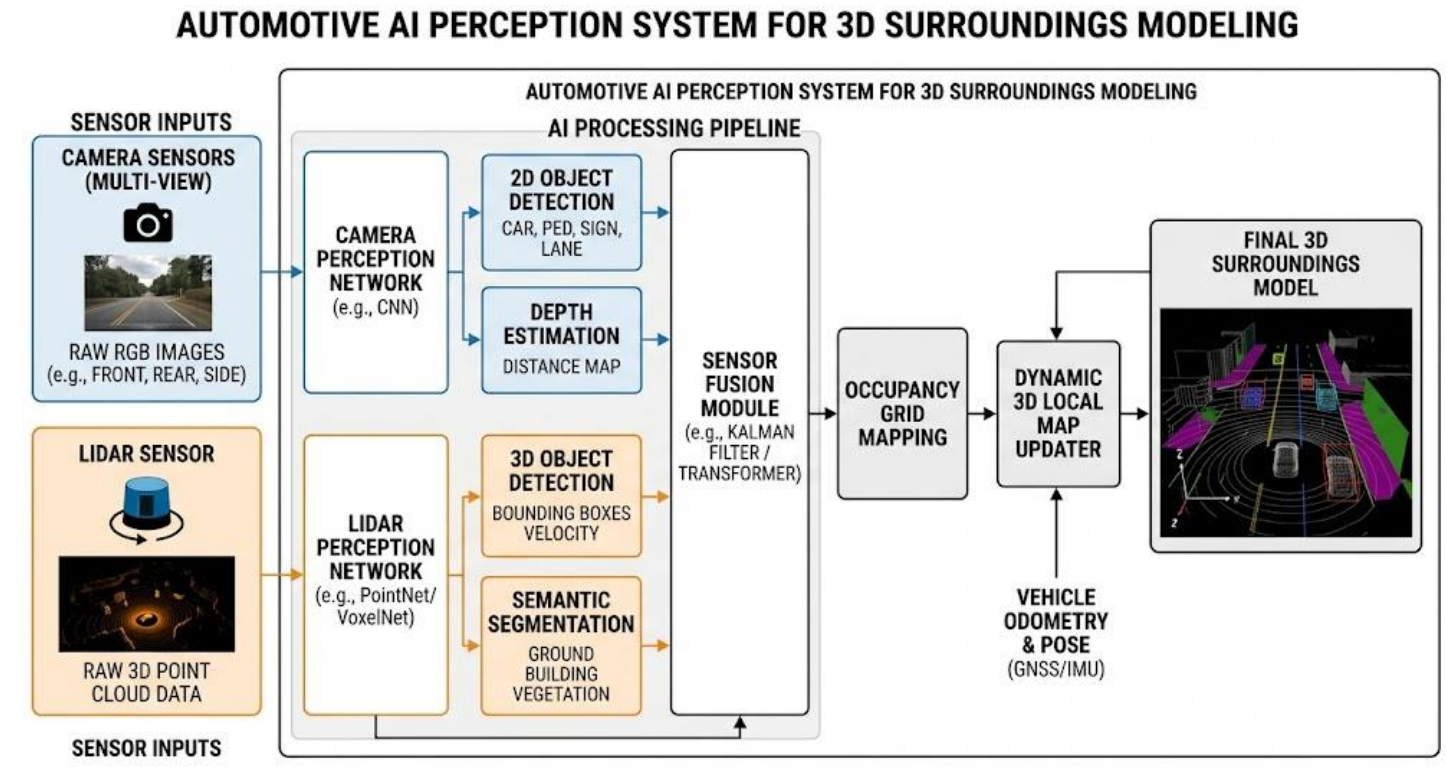
US Government: EO 14028—SECURING THE SOFTWARE SUPPLY CHAIN

A Way forward

Ensuring Robust User-Centered results

AI Automotive Data Consumption

- Simple Data
  - Signals (AUTOSAR, CAN, etc.)
  - Log data
- Complex Data
  - Video
  - Lidar
  - Audio
- Multiple interacting models
- Local consumption
  - Latency advantage
  - Cost advantage
  - Needs local subscription and routing



Data Management Process

Conversion

- Convert native data to vehicle independent signals
- Produce unified format
- No filtering
  Only CAN & AUTOSAR signals.

Signal Conversion Manifest

Preprocessing

- Compose signals not present natively.
- Compress data
- Store data
- React to triggers
- Subsystem modeling
- Interact w/ AI Model

Software Bundles
AI Models

Selection

- Decide what signals to send when
- Uses both converted signals and preprocessed data
- Describable as a network

Data Acquisition Plan
AI Assisted

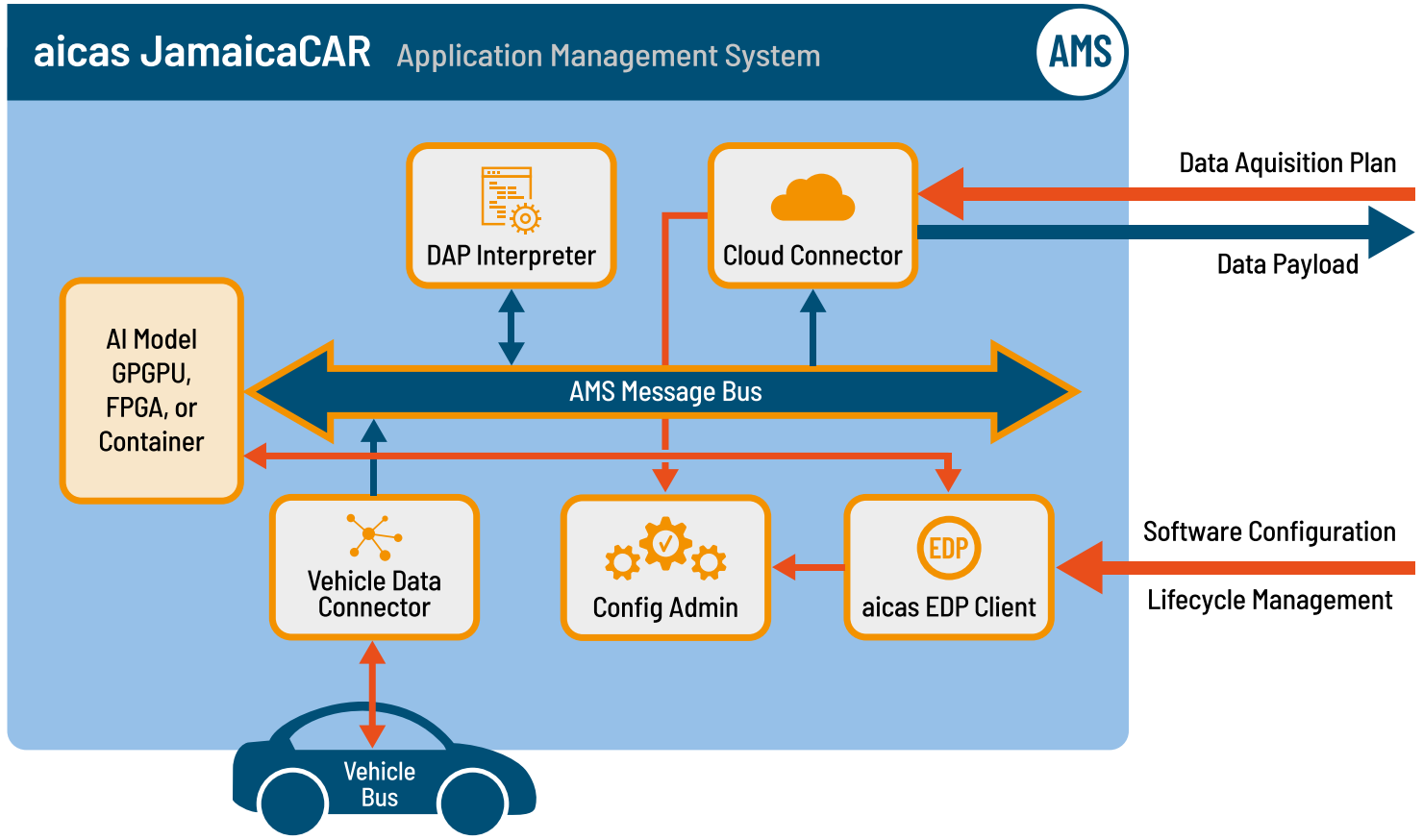
Transmission

- Connect to server
- Transmit requested data
- Handle all failure modes such as network disconnect and server failure

Sparkplug

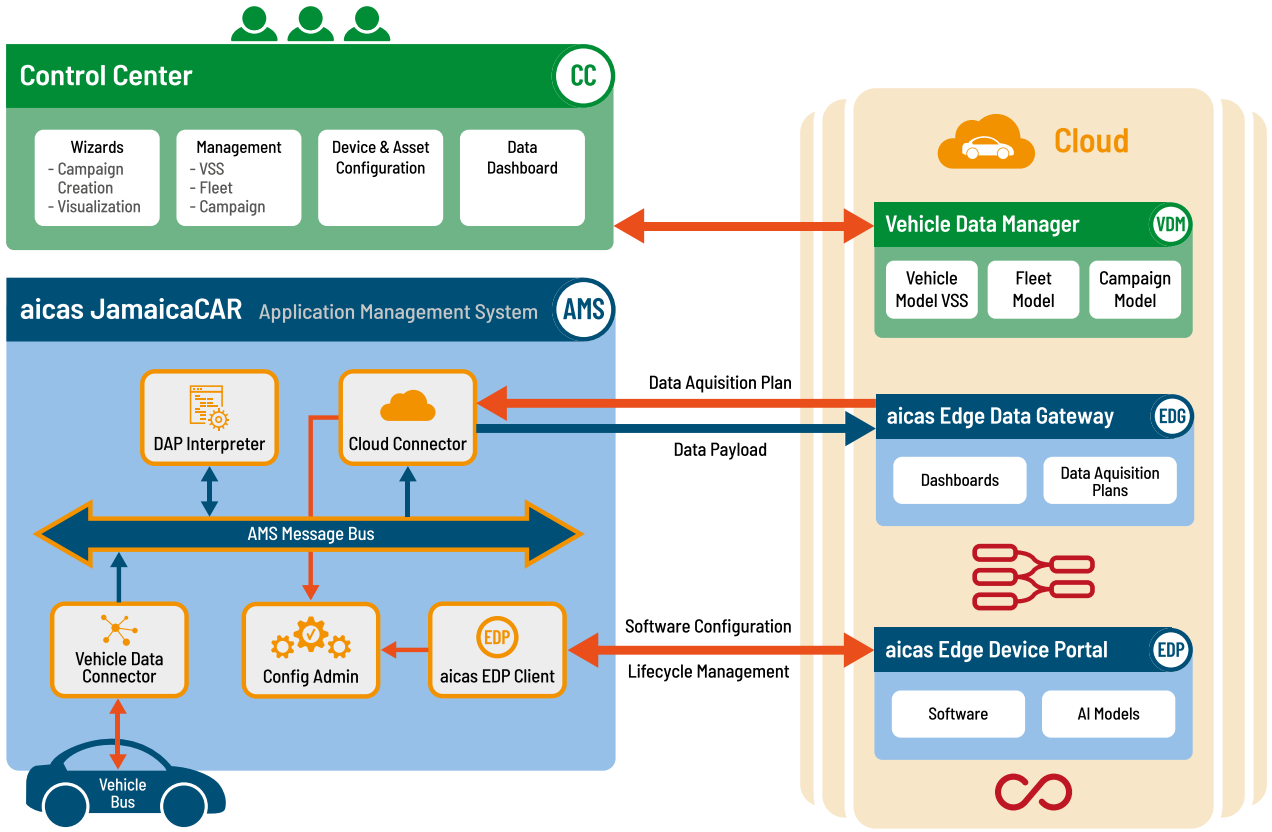
In Vehicle Support

1. OTA w/ signed code & decryption on use for AI Models
2. Full version and compatibility management for all software
3. Data Acquisition Plan for flexible data collection
4. Support for remote command and control
5. Standards-based field-tested technology



Vehicle Support Architecture

- **RT intelligence: more than just AI at the Edge**
- Robustness is paramount
  - Memory Safety
  - Modular updatability
  - Well-defined unit carrying data (signals)
  - Dynamic, synthetic signals
  - Seamless integration w/ and between AI models
  - Self-aware framework (software, versions, compatibility)
- So is the Process
  - Role-based access w/ change review & testing process
  - Well documented change history
- **Static Systems increase liability**



ML Ops: Managing AI Model Life-Cycle

Using AI in embedded systems is a **Continuous Improvement Process**.

Plan

Describe desired functionality

Design

Translate into software and ML design

Prepare data

Build

Develop software

Train ML model

Test

Validate functionality

Release

Release the application

Deploy

Distribute the application onto target systems

Operate

Execute the application

Use ML model for inference

Observe

Collect operational data

Transmit operational data

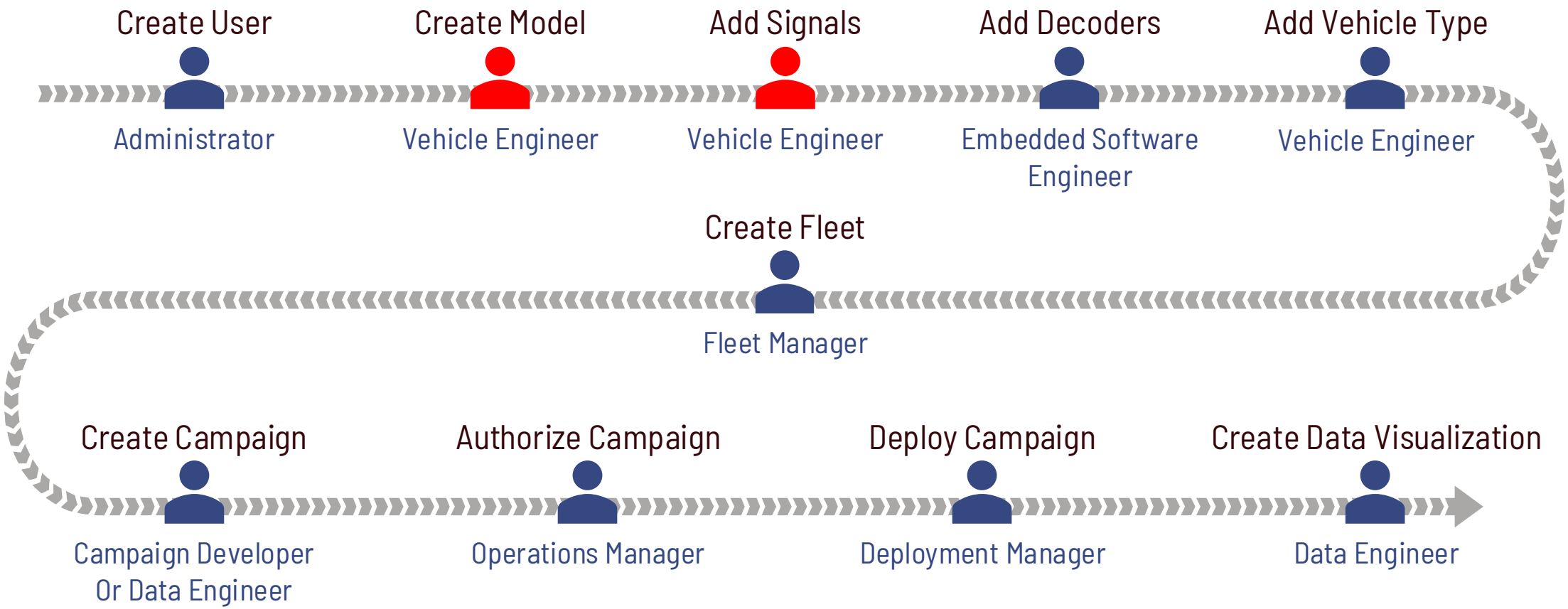
Plan anew

Derive insights of field operations

from the collected data

to improve the system's performance

Role-Based Management



Example Roles

Acquisition Element	Create	Read	Use	Authorize	Update	Delete
Vehicle connector	ESW Eng	ESW Eng SW Eng	ESW Eng SW Eng	QA	ESW Eng	ESW Eng Ops Mgr
Enterprise VSS catalog	Vehicle Mgr	Vehicle Mgr SW Eng	Vehicle Mgr SW Eng	QA	Vehicle Mgr	Ops Mgr
DB Schema	IT Eng	IT Eng SW Eng	IT Eng SW Eng	QA	IT Eng	Ops Mgr
Vehicle Data	Vehicle Eng	Vehicle Eng Data User	Vehicle Eng Data User	Vehicle Mgr	Vehicle Eng	Vehicle Mgr Ops Mgr
Vehicle Definition (VSS)	Vehicle Eng	Vehicle Eng Data User	Vehicle Eng Data User	Vehicle Mgr	Vehicle Eng	Vehicle Mgr
Fleet	Fleet Mgr	Fleet Mgr Data User	Fleet Mgr	Deploy Mgr	Fleet Mgr	Fleet Mgr
Data Acquisition Plan	Data User	Data User	Data User	Deploy Mgr	Data User	Data User
Campaign	Data User	Data User	Data User	Ops Mgr	Data User	Data User
Visualization Template	UI Design	UI Design Data User	UI Design Data User	Data Mgr	UI Design	UI Design

Importance of Memory Safety

Why is it important?

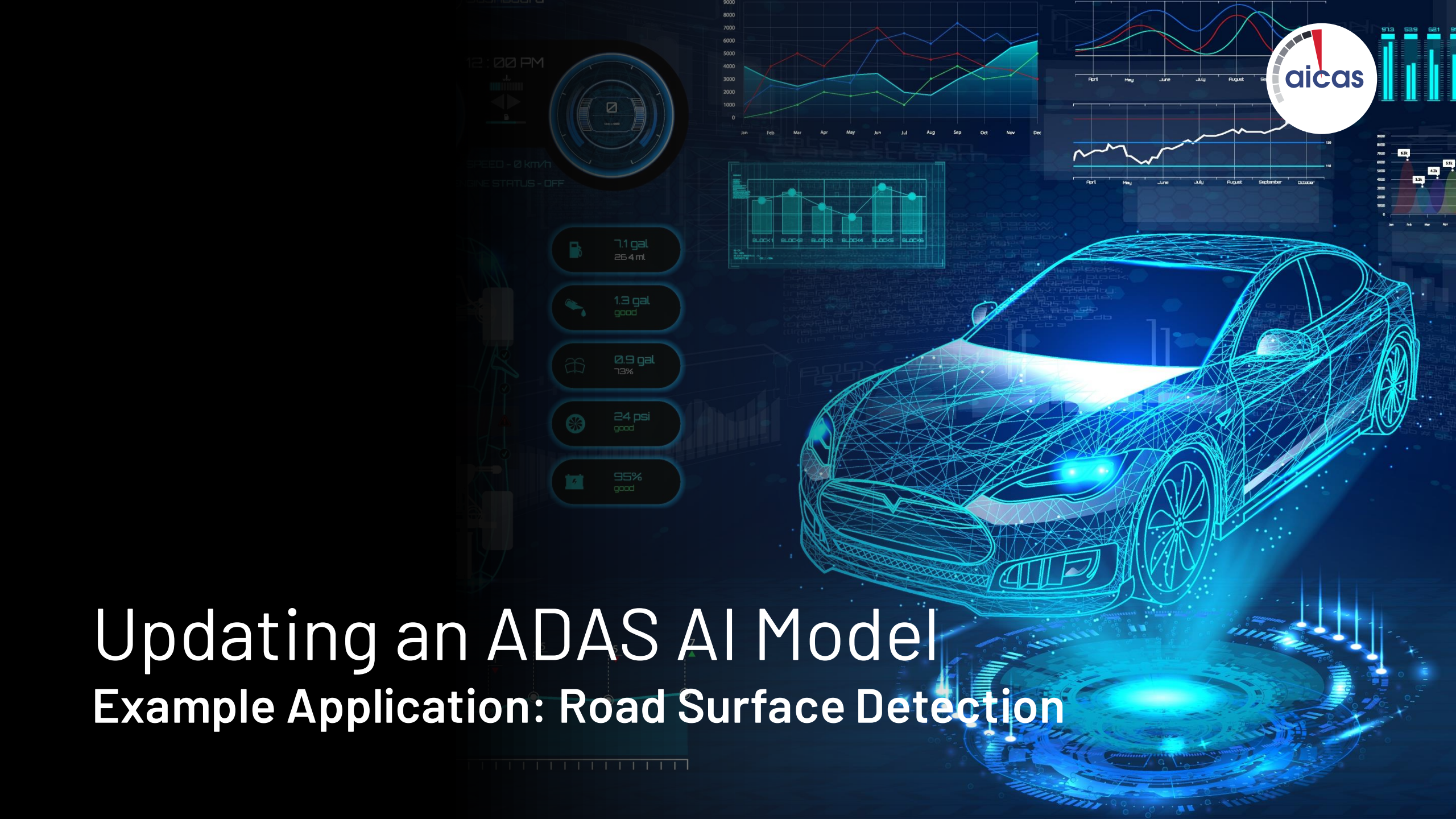
- ~70% of Security vulnerabilities are due to lack of memory safety.
- Found in iOS, Android, and Microsoft Products

What can go wrong?

- Buffer overrun or out of bounds array reference
- Reference object with wrong type
- Use number as pointer
- Reference object that has been freed

References

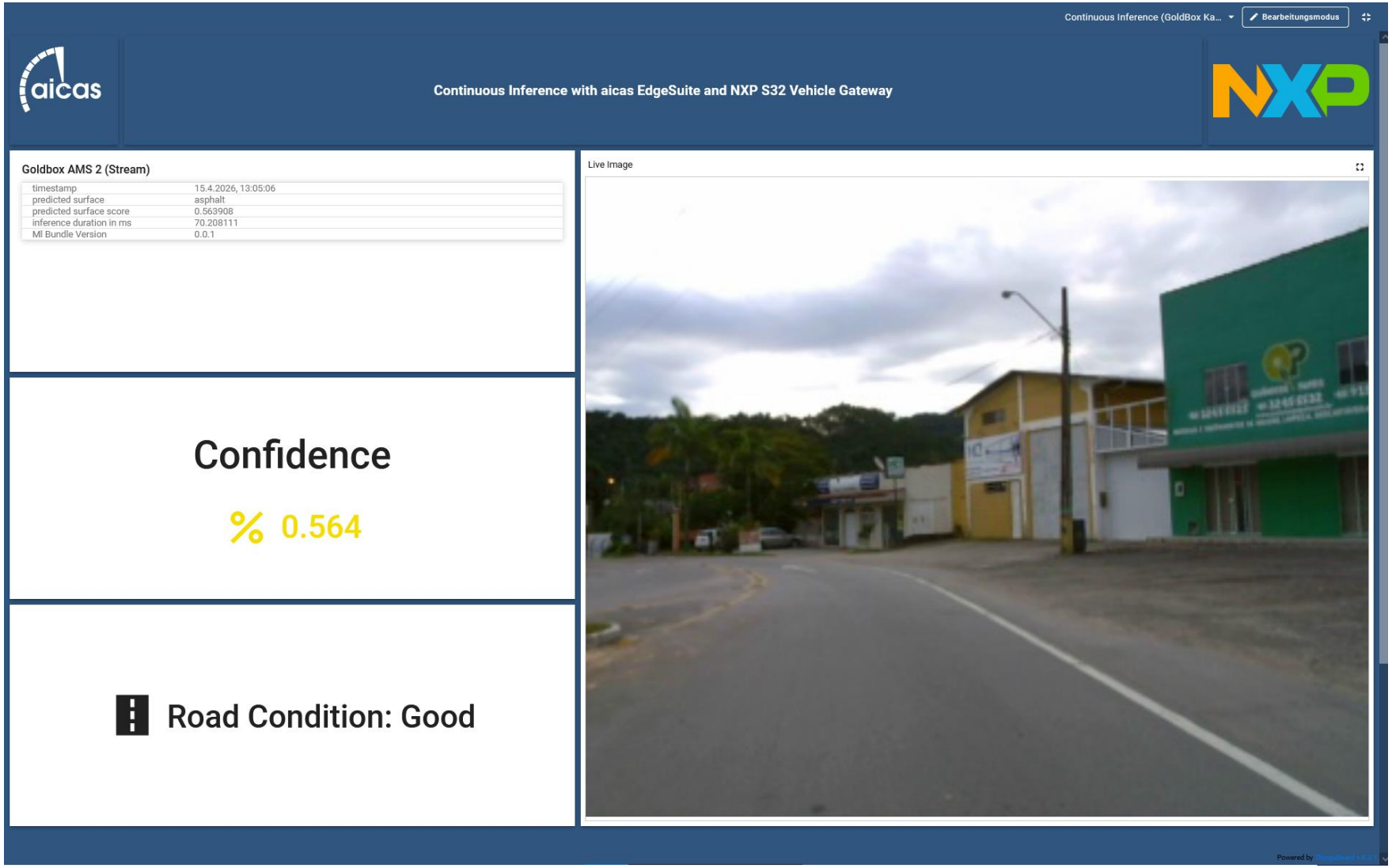
- https://www.memorysafety.org/docs/memorysafety/
- https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF
- https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf
- https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/
- https://www.chromium.org/Home/chromium-security/memory-safety/



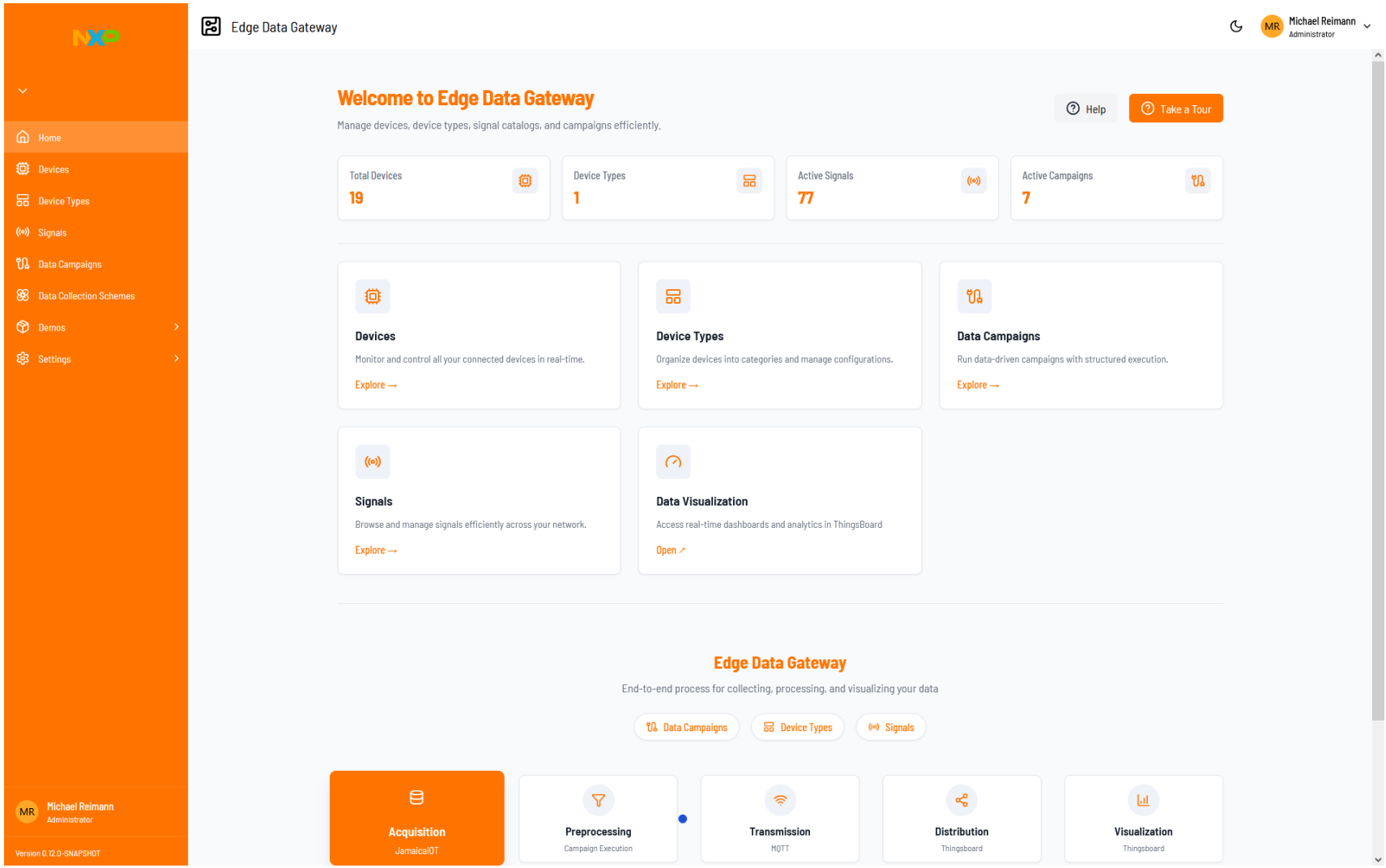
Updating an ADAS AI Model

Example Application: Road Surface Detection

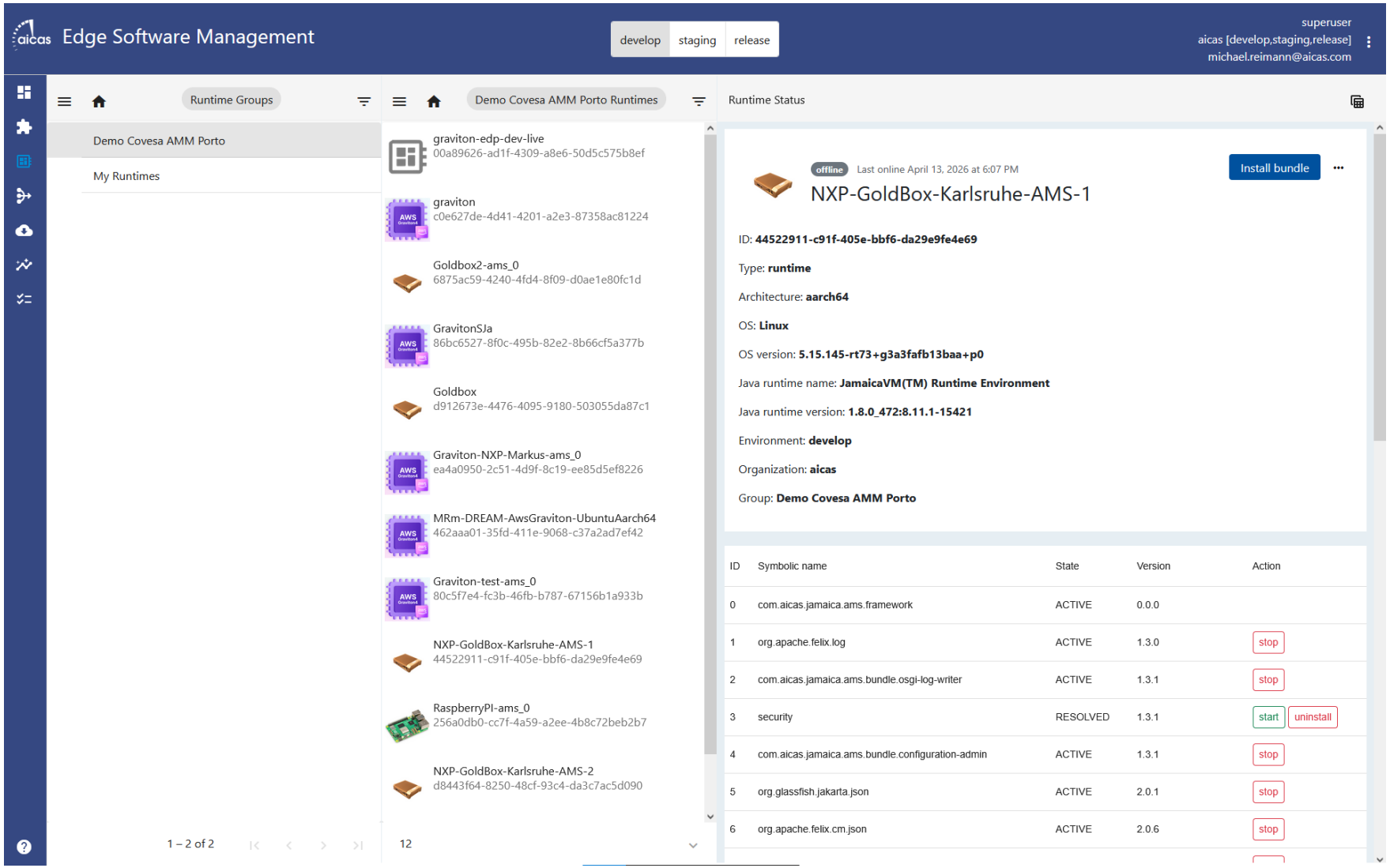
Live Perception and Performance Observation



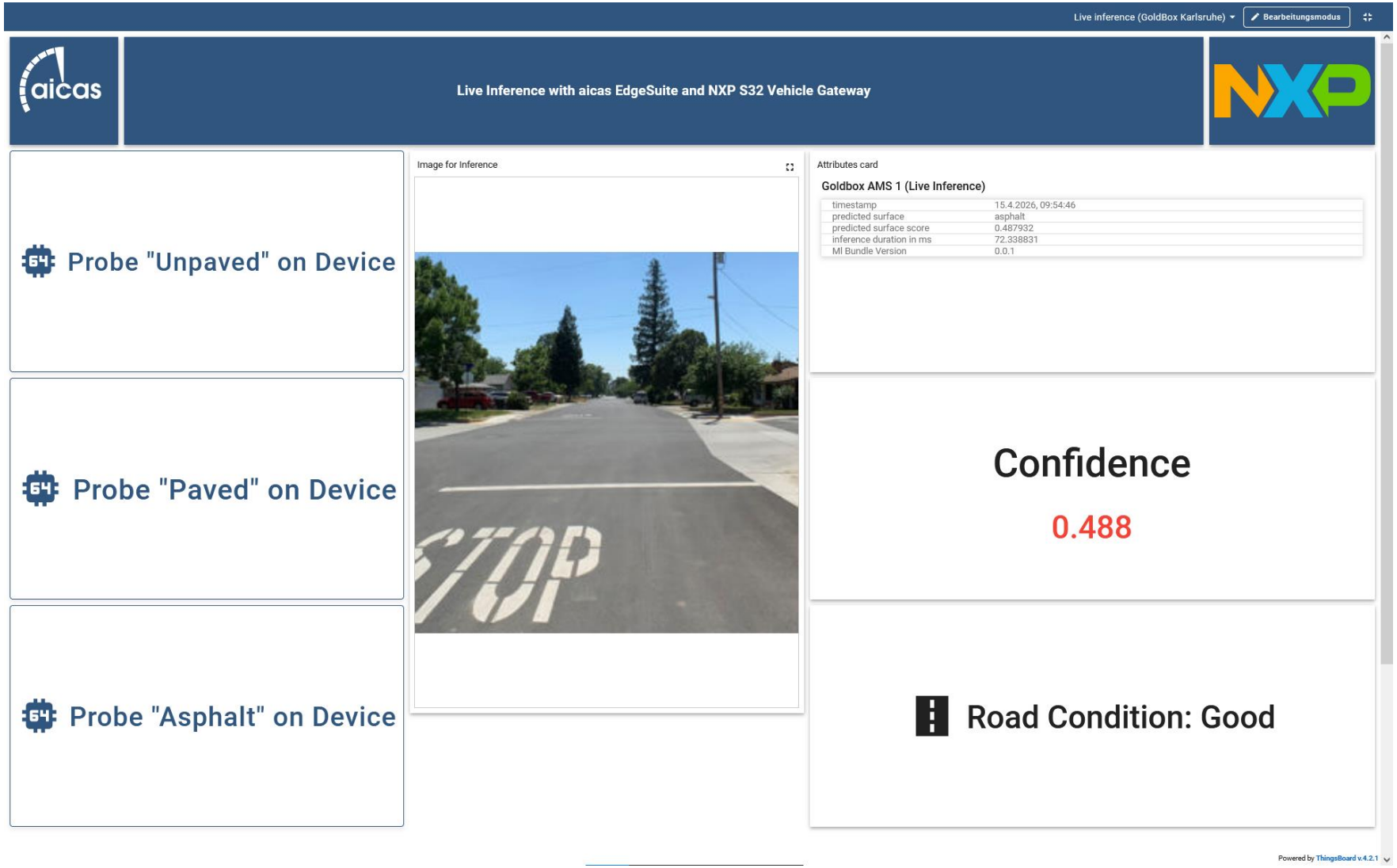
Perception Data Configuration



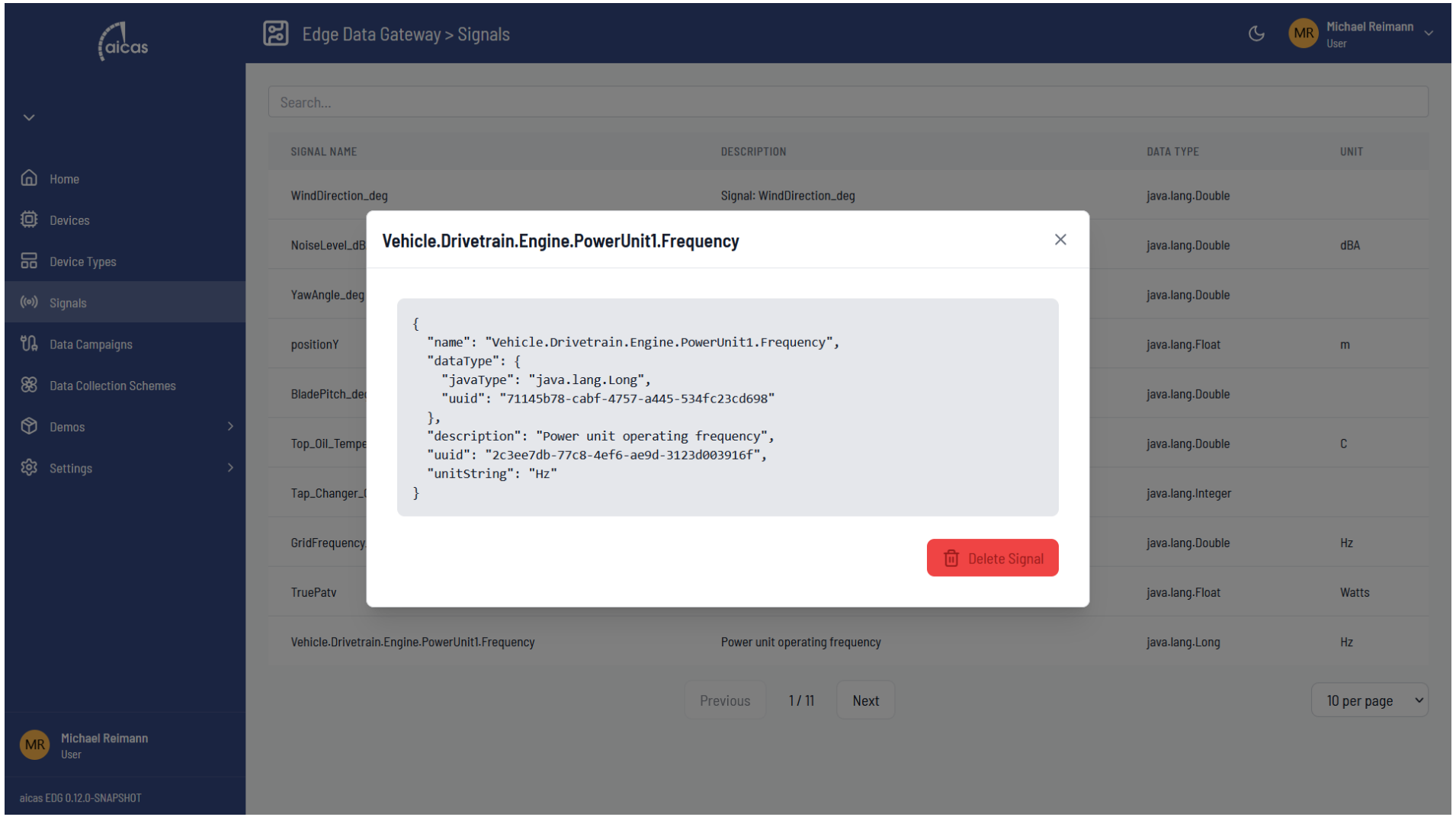
Device Management



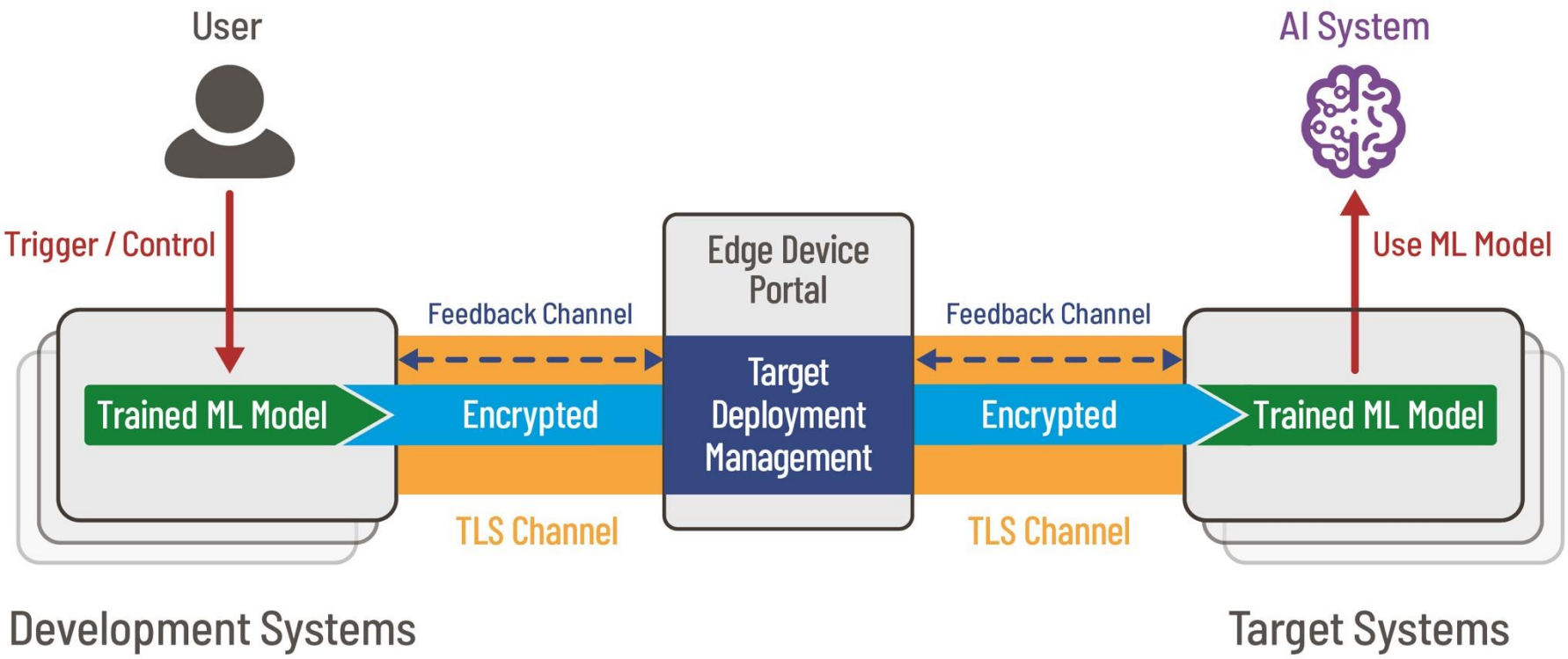
Live Inference while Training



Vehicle Signal Specification in Use



Model Deployment Security



Smarter with AI on the Edge

- The technical challenges are still the same.
  - Field updatability is a must.
  - Memory safety errors can be catastrophic.
  - How can systems be validated and certified?
  - "Garbage in, Garbage out" applies more than ever.
- AI compounds these challenges.
- Ethical, Legal, and safety issues are paramount.
  - OEM is responsible for safety, security, and functionality.
  - Updatable version aware software systems are needed.
  - Robustness through modularization and memory safety.

Thank You!

Contact Us: info@aicas.com
Visit Us: www.aicas.com

AI for Automotive: Where the Rubber Hits the Road

Dr. James J. Hunt
CEO & CTO - aicas GmbH

Artificial Intelligence (AI) changes the way systems are built. The role of data and verification have become even more important to success, not only in the design process, but also in the field. The danger of GIGO (garbage in, garbage out) affects the very foundation of AI Models. If training, and retraining data is not clean or not rich enough, it can have unforetold consequences. Care must be taken not only for how models are built, but also where they are used.

AI changes not only the way data is gathered, but also the way data is processed in a vehicle: AI does not only consume data, it also continuously generates new, derived or synthetic data whose availability and semantics depend on the resultant model itself. Dynamic data preprocessing already challenges the notion of a static data catalogue for an automotive telematics system. AI further challenges this notion: changing an AI model can directly influence which data exists and can be collected. Due to their opaque and indeterminate nature, AI models make the task of describing how derivation takes place nearly impossible. Add in the need for more complex data such as pictures, video streams, and lidar data, and it becomes clear that not all data can be transmitted all the time. The question is what data is needed for detecting anomalies and supporting retraining.

This talk will discuss these challenges and present use cases that motivate them. Using concrete use cases, it demonstrates why purpose-driven data collection is essential. Building and maintaining AI models require vast amount of data, both for accomplishing its tasks, as well as for retraining. However, training, inference, validation, and retraining have fundamentally different data requirements. Determining what data is needed where and how often is essential to success. It is also key to a real Software Defined Vehicle.

Takeaways

- Where AI is applicable.
- Challenges of data collection in conjunction with AI.
- Why selective data collection is an essential element of any software defined vehicle.
- How collecting data selectively can improve support for model maintenance and scalability.

Additional Material