# Security Aspects of Over-The-Air (OTA) Updates

- **One of the biggest concerns with OTA updates is the potential for security breaches during data transfer.**
- **aicas addresses this challenge by providing a multi-layered approach to security.**
- **Security must encompass all software and data used in a vehicle, regardless of where it comes from and when it is activated for distribution to a vehicle.**

In this article, you will learn who benefits from over-the-air (OTA) updates, why security is incredibly important, and why the use of AI in vehicles is inseparable from OTA.

In a world where technology is rapidly evolving, ensuring seamless and secure management of connected devices is paramount. Over-the-air (OTA) updates have proven to be a game-changer in industries where timely software management is critical to efficiency, security, and a seamless user experience. Vehicles are a prime example: keeping software releases up-to-date without having to visit a service center saves time and money. Everyone benefits.

OTA updates have transformed the automotive industry by revolutionizing the way software is managed in fleets. Vehicles are no longer just losing value from the day of purchase, now they can continue to be improved over the lifetime of the vehicle with current software updates. Over-the-air software delivery allows a wide distribution of updates in a variety of fields and industries. All while reducing the cost of keeping software current and increasing the adoption rate of updates. OTA updates allow automakers to offer their current vehicle owners a range of new options and applications, thereby deepening customer relationships and creating new revenue streams for automotive companies and their partners.

"The need for over-the-air updates is being driven by the industry's digital transformation for software and artificial intelligence – both of which require solution providers to rethink the entire DevOps cycle," said Dr. James J. Hunt, founder, CEO, and CTO of aicas." A key component is bridging the gap between IT and OT, with their different requirements, practices, and mindsets. Doing so intelligently is key to product and transformation success. Think of the vehicle ecosystem as a software-enabled and extended enterprise that is always connected. This is similar to running a very large IT footprint, but with even higher requirements for security and robustness of software solutions."

Keeping the connection between the vehicle and the cloud secure is critical to the digital transformation of the automotive and transportation industries, as well as for mobility in other settings like Smart Cities and Smart Factories.

## The Security Aspects of OTA Updates Cannot be Overstated

When deploying a software update to a vehicle or edge device, it is essential to implement strict access control measures. The primary objective is to limit the update process to authorized individuals or appropriate staff. In addition, ensuring that each software update is signed and verified against known keys adds an extra layer of security and builds confidence in the authenticity and integrity of the update.

Establishing a secure connection from the edge to the back end is critical to ensure that you do not inadvertently connect to the wrong back end. No inbound connections should be allowed to minimize attack vectors. Any potential vulnerability must be addressed, as the presence of malicious software in vehicles could compromise their safety and security. Preventing unauthorized access to sensitive data is also essential to avoid potential data leakage.

Maintaining data security, validation, and privacy is an ongoing commitment. Only by maintaining the highest standards of security can we confidently ensure the seamless and reliable operation of software that keeps vehicles safe and private data secure. Having a strong and dynamic process in place is critical to respond effectively to security concerns and ensure customers' systems are kept up to date.

The World Forum for Harmonization of Vehicle Regulations (hosted by UNECE) has approved two UN Regulations (UN R155/R156) for vehicle manufacturers seeking approval for OTA updates. These standards provide a regulatory framework for OTA vehicle software updates aiming to ensure safe and secure software updates without compromising vehicle safety. This is important to keep in mind when designing a vehicle security architecture.

## In-Vehicle Use of AI Is Inseparable From OTA

The emergence of a range of powerful AI models behind autonomous driving will evolve as knowledge of the environmental impact of driving improves and as the environment, both physical and regulatory, evolves. New features can be added by the touch of a screen, using operational insights from AI-based learning. In fact, the driver may no longer configure the car in the car, but from any browser or smartphone. The customer will be able to purchase services, prepare trips, and schedule maintenance, all online. However, this will not be possible without secure, dynamic, and robust OTA solutions.

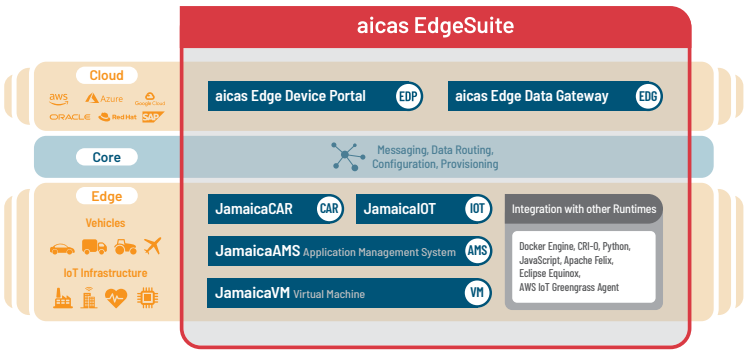

## aicas – Strategic and Technology Partner for OTA Updates

Hardware security anchors must be extended with an internal chain of trust to incorporate dynamically added software without requiring a full firmware update. Cryptographic means must be used to provide vehicle identification and software provisioning. Resource usage must be limited to prevent overcommitment. Software access must be limited to the task at hand. These and more are already supported by aicas' products.

For OEMs, software-driven transformation requires strategic and technology software partnerships. aicas has a strong foothold in the automotive industry as a partner that delivers value across the automotive software value chain. From enhancing the in-vehicle user experience to supporting the deployment and lifecycle management of third-party microservices and transportation applications, aicas provides solutions for safe mobility.

The company's products and services reduce time-to-market while maintaining uncompromised security. The company's middleware and embedded development kits for managing connected and autonomous features and services ensure security throughout the life of the application with over-the-air (OTA) software updates and maintenance. aicas' solutions protect the features and services deployed today and prepare organizations for evolving security, regulatory, and business requirements. Whether implementing new vehicle features, making critical fleet management updates, troubleshooting system failures, or defending against application intrusions, aicas' tools provide targeted and granular control.

## A Software Framework for Automotive Edge Applications




JamaicaCAR helps accelerate the development of software-defined vehicles, improving the user experience and increasing customer loyalty. It extends aicas' application management system, JamaicaAMS, with specific automotive services for vehicle communication, dynamic data collection, and information delivery. The software framework for automotive applications enables fast, targeted, and secure OTA updates. Multiple or single application services can be easily provisioned, even at run-time, to ensure continuous operation. High portability through platform independence allows easy transfer of software to new vehicle models without major customization.

## Summary

OTA updates have emerged as a game-changing solution for the automotive industry, providing manufacturers with powerful tools to efficiently and reliably improve vehicle functionality, safety, and customer experience. By adopting strong security practices, automotive companies can successfully overcome the challenges and take full advantage of OTA updates, ushering in a new era of automotive embedded software.

With these opportunities come challenges, particularly in ensuring robust security measures are in place. aicas has demonstrated a strong commitment to addressing these security concerns and making OTA updates safer and more reliable. By embracing OTA technology and complying with industry regulations, automakers can usher in a new era of secure and seamless software management and propel the industry into a brighter and safer future of mobility.

"OTA is already a key factor in making autonomous driving systems trustworthy", said Dr. James J. Hunt. "AI will greatly accelerate the need for secure, dynamic, and robust OTA solutions. At aicas, we look forward to sharing our expertise and proven OTA capabilities in this area, which will be integrated into our aicas EdgeSuite portfolio with future customers and partners."

**Get in touch with us to learn more about our solutions!**

aicas GmbH
Emmy-Noether-Str. 9
76131 Karlsruhe, Germany

**Web:** https://www.aicas.com
**Email:** info@aicas.com
**Phone:** +49 721 663 968 0