TASKING®

GAIN OTA BENEFITS WHILE REDUCING CYBERSECURITY RISKS

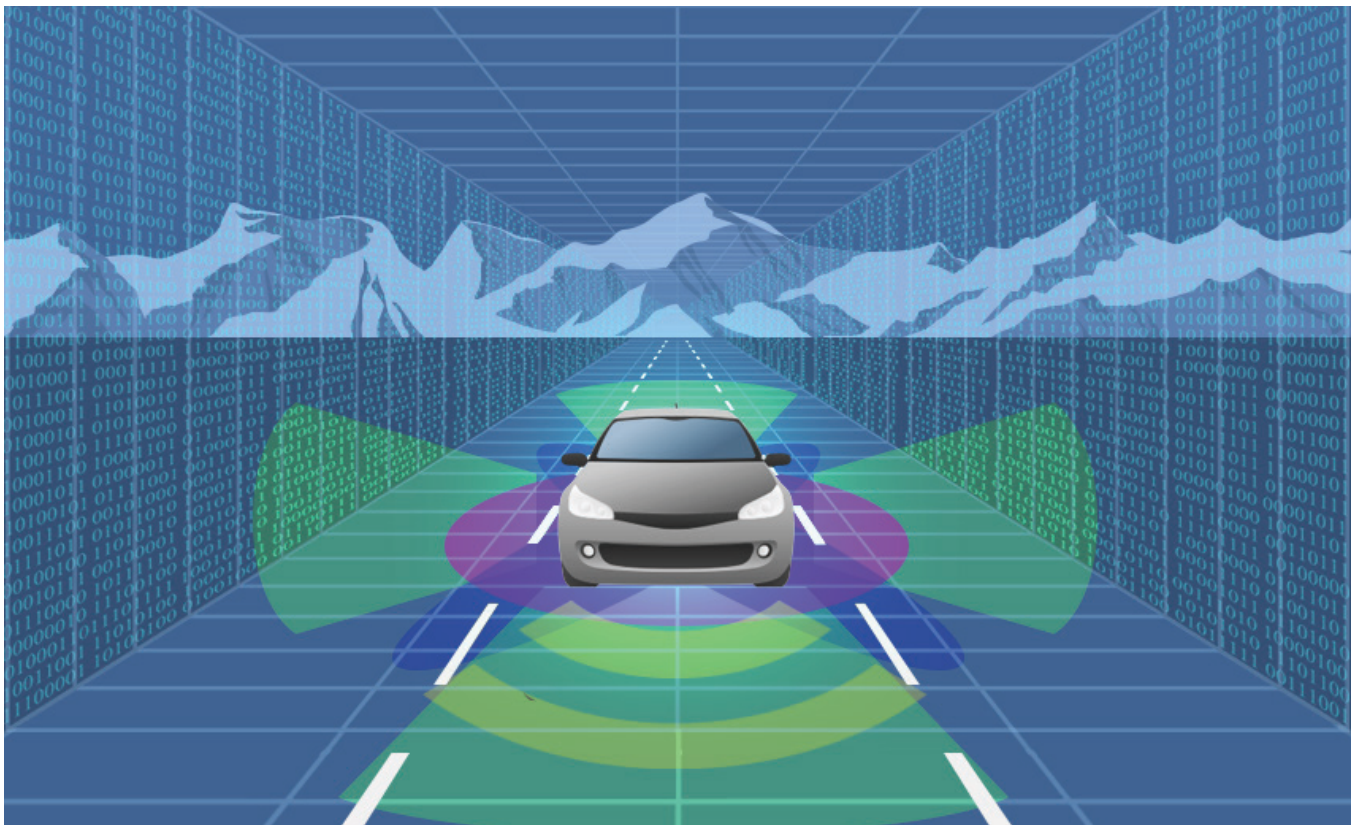
Mark Forbes
Director of Marketing Content

GAIN OTA BENEFITS WHILE REDUCING CYBERSECURITY RISKS

INTRODUCTION

Crash-avoidance features, such as lane departure warnings and adaptive cruise control as well as autonomously driven vehicles, are improving rapidly with the introduction of new software capabilities. These new features are changing the way consumers evaluate cars, putting a greater emphasis on the user experience and improved safety. But these software-reliant systems require nearly continuous updates, such as map changes, road construction information, or modifications to safety features. The ability to share previously unknown situations and solutions collected from other vehicles already on the road can also dramatically improve safety.

Over-the-air (OTA) software updates can increase safety while reducing costs by keeping driver-assistance features up to date. But OTA updates must also address the known vulnerability of cyberattacks, which can propagate across the in-vehicle network. Software architects must select a solution that meets high-performance, security, and safety standards while still enabling cost-effective OTA updates. This type of solution features hardware and software that are tightly coupled.



OTA UPDATES PROVIDE NUMEROUS ADVANTAGES

Historically, consumers perceived the hardware—or tangible aspects—of the vehicle as the most valuable. But software features, such as crash-avoidance systems, are becoming increasingly more valuable to car buyers (Figure 1). Since most vehicles will be on the road for ten years or more, OTA updates make advanced driver assistance systems (ADAS) possible. As cars learn, ADAS will improve over time.

OTA updates provide enormous advantages in keeping in-vehicle software systems up to date and maintaining consumer satisfaction (see Figure 1). ABI Research, the leader in transformative technology innovation market intelligence, forecasts nearly 203 million OTA-enabled cars will ship by 2022.(1) The benefits from OTA updates include:

- **Lower cost:** OTA updates to systems in near real time, without requiring the owner to bring the car to a dealership or mechanic, helps reduce warranty issues and recalls across potentially millions of vehicles.
- **Improved safety:** Many under-the-hood systems, such as steering, braking, and acceleration are electronically actuated. These safety-critical systems can be immediately updated using OTA technology when issues are identified.
- **Improved customer satisfaction:** Consumers are spared the inconvenience of bringing their cars to a dealership and they can receive the latest information and safety updates, often without being aware of the change.
- **Frequent updates:** Especially in situations that might otherwise require a recall, OTA updates can be transmitted to all vehicles, whether in the sales lot or on the road. OTA updates allow manufacturers to update software as frequently as necessary in near real time.
- **Increased value:** By consistently maintaining in-vehicle software systems with OTA updates, the overall value of the car increases and opens new revenue opportunities to automakers. Also, software configuration costs decrease when a single, compatible operating system (OS) can be used across multiple software solutions.

IHS Automotive, an auto-industry data consulting company, predicts that automakers will save USD 35 billion by using OTA updates in 2022, up from USD 2.7 billion in 2015.(2)

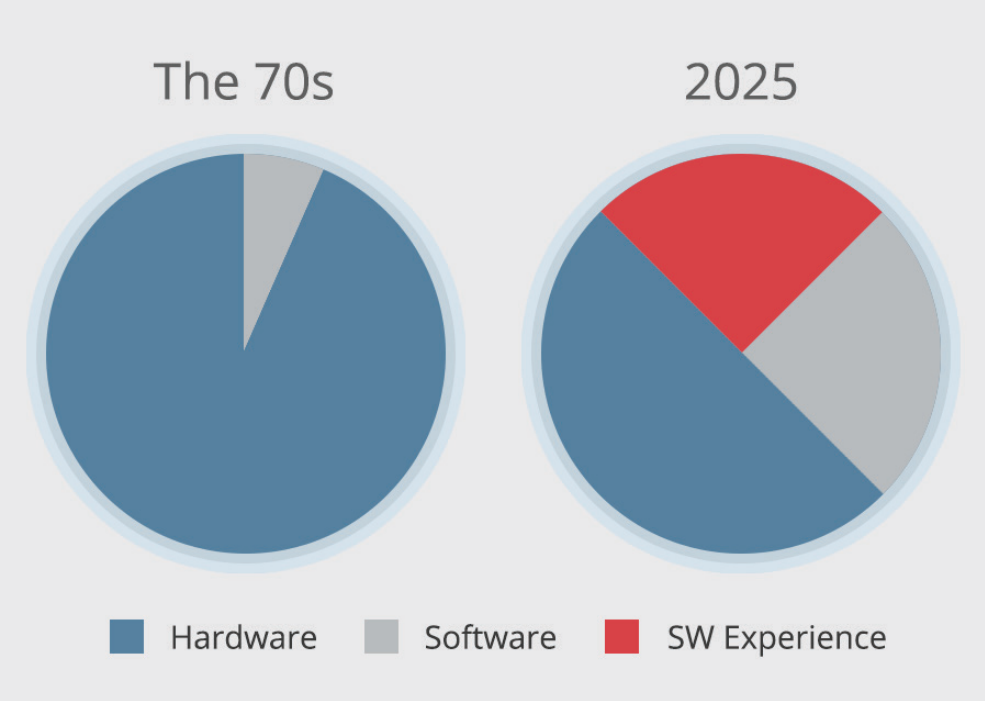


Figure 1. Today's automotive consumers value software solutions, such as assisted parking, more than hardware, making over-the-air (OTA) updates a crucial factor in automotive design and customer satisfaction. Figure courtesy of European Business Press.

OTA UPDATES ALSO POSE CHALLENGES

Automakers are looking to deliver increasingly connected systems inside and outside the vehicle. Yet many do not have the technology platform to take advantage of OTA updates, which require a carefully planned methodology to develop, deploy, and maintain. And when a vehicle's central gateway—the entry point into the software systems—is receiving and sending information, it is more vulnerable to cyberattacks.

Implementing OTA updates can present the following challenges:

- **Data integrity:** Data coming into the vehicle must meet high standards of reliability, especially in dynamic situations like moving vehicles.
- **System security:** Cyber threats are dynamic and can rapidly propagate through the in-vehicle network. The OTA update solution must be able to prevent external breaches that could expose vehicle systems and data.
- **Connectivity:** Real-time, nearly continuous OTA updates rely on robust connectivity. As IoT solutions become ubiquitous, connectivity is improving, but it varies across global markets.
- **Standardization:** A lack of industry-wide standards for all OEMs adds to the complexity of software design, interoperability, and connectivity. Handling multiple, independent components and OS configurations requires coordination across vendors and efficient, secure communication.

Automakers must have a strong understanding of the software environment to deliver the highly connected experience consumers expect. Today's cars can include over one hundred Engine Control Units (ECUs) that require carefully designed and managed software development cycles. Identifying solutions that help prevent cyberattacks is a critical step in implementing OTA updates.

EMBEDDED SECURITY PREVENTS CYBERATTACKS

The automotive industry's specific security concerns require an OTA update solution that protects the in-vehicle network from cyberattacks and addresses future autonomous decision-making capabilities. The vehicle's central gateway connects, routes, and controls access to all the vehicle's systems, including ECUs that control the powertrain, chassis, and driver-assistance features. Managing multiple OS configurations adds a layer of complexity, and position independent code (PIC) is a necessary component of any solution. The best way to protect this central gateway is to choose a highly secure microcontroller that is tightly integrated with the software compiler and linker—thus ensuring optimized security features.

The AURIX™ TC3xx microcontroller family, manufactured by Infineon, includes an embedded hardware security module (HSM) that meets the industry requirements with security levels up to that of E-safety Vehicle Intrusion ProTected Applications (EVITA) (Figure 2). The TC3xx multicore microcontroller family offers a scalable portfolio of devices with HSM, integrated with the Intrusion Detection and Prevention System (IDPS) from Argus Cyber Security Ltd., to protect the vehicle's central gateway from remote attacks.

The IDPS component provides a foundational security solution that can detect and prevent anomalous messages in real time. IDPS offers high performance, low latency, and context-aware heuristic and learning algorithms that enable optimal detection rates.

The AURIX TC3xx family with IDPS protects against cyberattacks in the following ways:

- **Support for security protocols:** In safety-related systems, AURIX microcontrollers support security protocols and required security functions in hardware.
- **Hardware protection:** The built-in HSM protects software and data communications within the vehicle at the highest security levels up to that of the EVITA project.

- The TC3xx family, with its combination of performance and powerful safety architecture, is designed for domain control and radar and sensor applications. The features include:
- **High-performance hexa-core architecture:** The advanced features for connectivity, security, and embedded safety are ideally suited to automotive applications.
- **Traditional, electric, and hybrid management:** Engine management and transmission control, as well as powertrain applications, include new systems in electrical and hybrid drives. This includes hybrid domain control, inverter control, battery management, and DC-DC converters.

Radar and camera support: The AURIX TC3xx microcontrollers are well suited for safety-critical applications ranging from airbag, braking, and power steering to sensor-based systems using radar or camera technologies.

AURIX TC3xx microcontrollers include up to six cores with memory scalability up to 16 MB Flash and connectivity up to 12 CAN-FD channels, eMMC interface, and Ethernet functionality. When combined with a remote cloud platform, AURIX microcontrollers with IDPS can also provide automakers with actionable information about the cyber-health of their fleets.

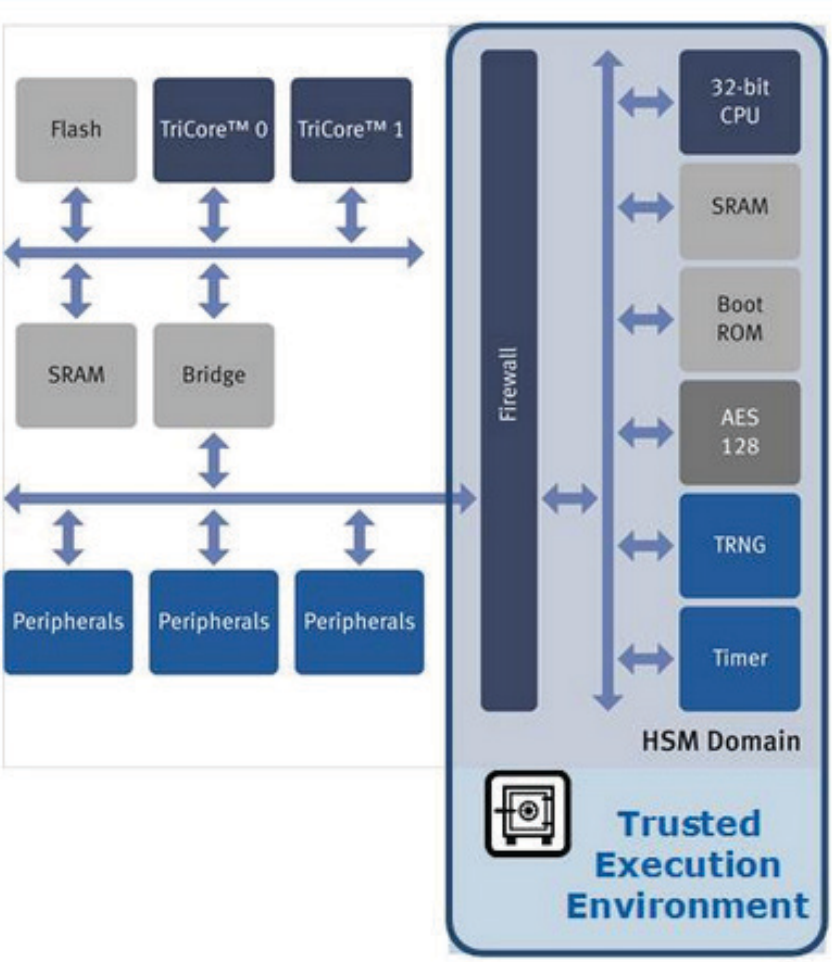


Figure 2. To better protect in-vehicle systems, the AURIX integrated hardware security module (HSM) is separated from the rest of AURIX microcontroller by a firewall. Image courtesy of Infineon Technologies.

CONCLUSION

The benefits of OTA updates are clear. Consumers are increasingly migrating toward cars that offer a wide range of driver-assistance features and that meet the highest safety standards. Automakers can also reduce costs significantly with the capability of updating their sales fleets and cars already on the road simultaneously, especially where a recall might otherwise be necessary. But this requires an OTA updates solution that protects data security and manages multiple modules and OS configurations. When designing software applications for automotive use, developers can meet these challenges, including the risk of cyberattacks, by choosing a software compiler and linker that is tightly integrated with its embedded HSM.

REFERENCES

(1) ABI Research Anticipates Accelerated Adoption of Automotive Software Over-the-Air Updates with Nearly 180 Million New SOTA-Enabled Cars Shipping Between 2016 and 2022, https://www.abiresearch.com/press/abi-research-anticipates-accelerated-adoption-auto/

(2) Over-the-air updates on varied paths, Gabe Nelson, http://www.autonews.com/article/20160125/OEM06/301259980/over-the-air-updates-on-varied-paths

LEARN MORE

- Software Updates Over the Air Secured by Infineon's Security Controllers
- Infineon and Argus enhance the security of the connected and automated car and present a cyber security solution for central gateway protection
- http://www.infineon.com/cms/en/about-infineon/press/market-news/2016/INFATV201610-005.html
- Cybersecurity and Recalls Will Mean Over-The-Air Updates for 203M cars by 2022
- Opportunities and challenges of over-the-air software updates in automotive