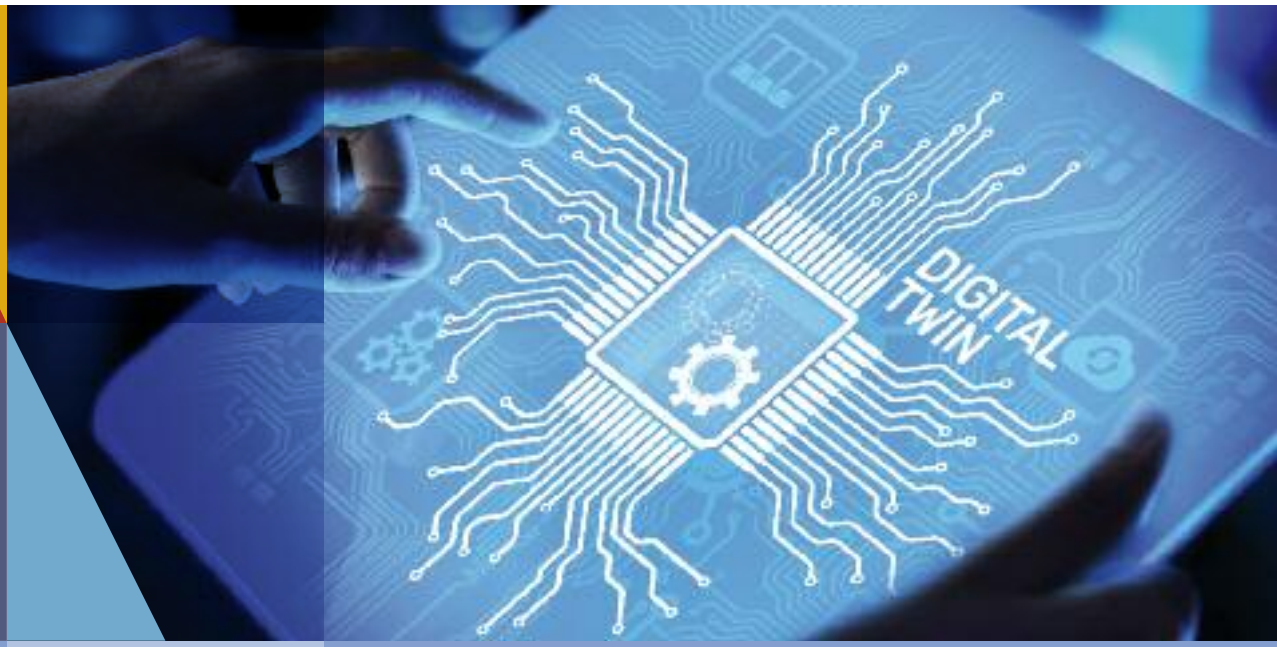
NTT DATA
Trusted Global Innovator



Digital Twin for maximum Cyber Security

Compliance with new UNECE cyber security regulations by using a digital twin of the car

NTT DATA Deutschland GmbH

Digital Twin for maximum Cyber Security

Digitization in the automotive industry makes cyber security a focus topic for vehicle software updates – international regulatory bodies are currently working on security guidelines. For vehicle manufacturers, this means that they have to establish processes and systems in accordance with the new cyber security requirements as quickly as possible. "Digital Twin Computing" can provide significant support in this area. The new Digital Twin Computing initiative from Japan is going beyond the traditional understanding of digital twin.

Modern vehicles are "data centers on wheels": they contain over 100 electronic control units for functions such as engine control, anti-lock braking system, airbag or navigation. Each control unit is a computer with the corresponding (embedded) software. In total, around 100 million lines of code are currently installed in a premium vehicle. Innovations such as automated driving and the increasing networking of vehicles will at least double the software volume in the next ten years. This software must be maintained over the entire lifecycle in order to achieve security and customer satisfaction. On the one hand, software maintenance can consist of correcting errors. On the other hand, it can also enable new functions. In both cases, the software updates must be applied to each individual vehicle. Up to now, this usually required a workshop visit. In the future, this process will increasingly take place over the air, or OTA for short.

Safety is not just security

Functional safety was in the foreground in the historically grown vehicle architectures; it was already defined in ISO 26262 in 2011. In contrast, information security is a newer discipline in this environment. This type of security has quickly become very important due to the increasing number of potential points of attack in intelligent, networked vehicles (see Figure 1).

OTA is just one of many information security risks that must be kept as small as possible with appropriate measures. This is even more true since cyber security and OTA are subject to international standardization and are therefore a prerequisite for type approval (homologation) of vehicles in the individual markets.

New cyber security regulations change type approval process

Vehicles are sold and used globally. In doing so, they must comply with country-specific approval regulations. In Germany, for example, type approvals are granted by the Federal Motor Transport Authority on the basis of the road traffic licensing regulations. To simplify the process of homologation, the "United Nations Economic Commission for Europe", or UNECE for short, has WP29, i.e. the "World Forum for Harmonization of Vehicle Regulations". The rules are agreed there and then transposed into national law. In particular, the Cyber Security and Software Updates OTA task force is working on two regulations that will have a massive impact on type approval in the coming years and pose major challenges for vehicle manufacturers. The digital twin of the vehicle is an essential component of the solution.

SUMS – enormous effort for car manufacturers

The current draft of the regulations from the beginning of 2019 provides that vehicle manufacturers establish processes and systems to ensure information security during development, production and use. Among other things, a software update management system (SUMS) is to be created and audited every three years. The requirements for the SUMS include the identification of all software versions and their dependencies on the hardware and software environment used (compatibility), the identification of target vehicles for a software update, the impact analysis on existing type approvals, information on the vehicle user and the safe implementation of software updates – all combined with extensive documentation.

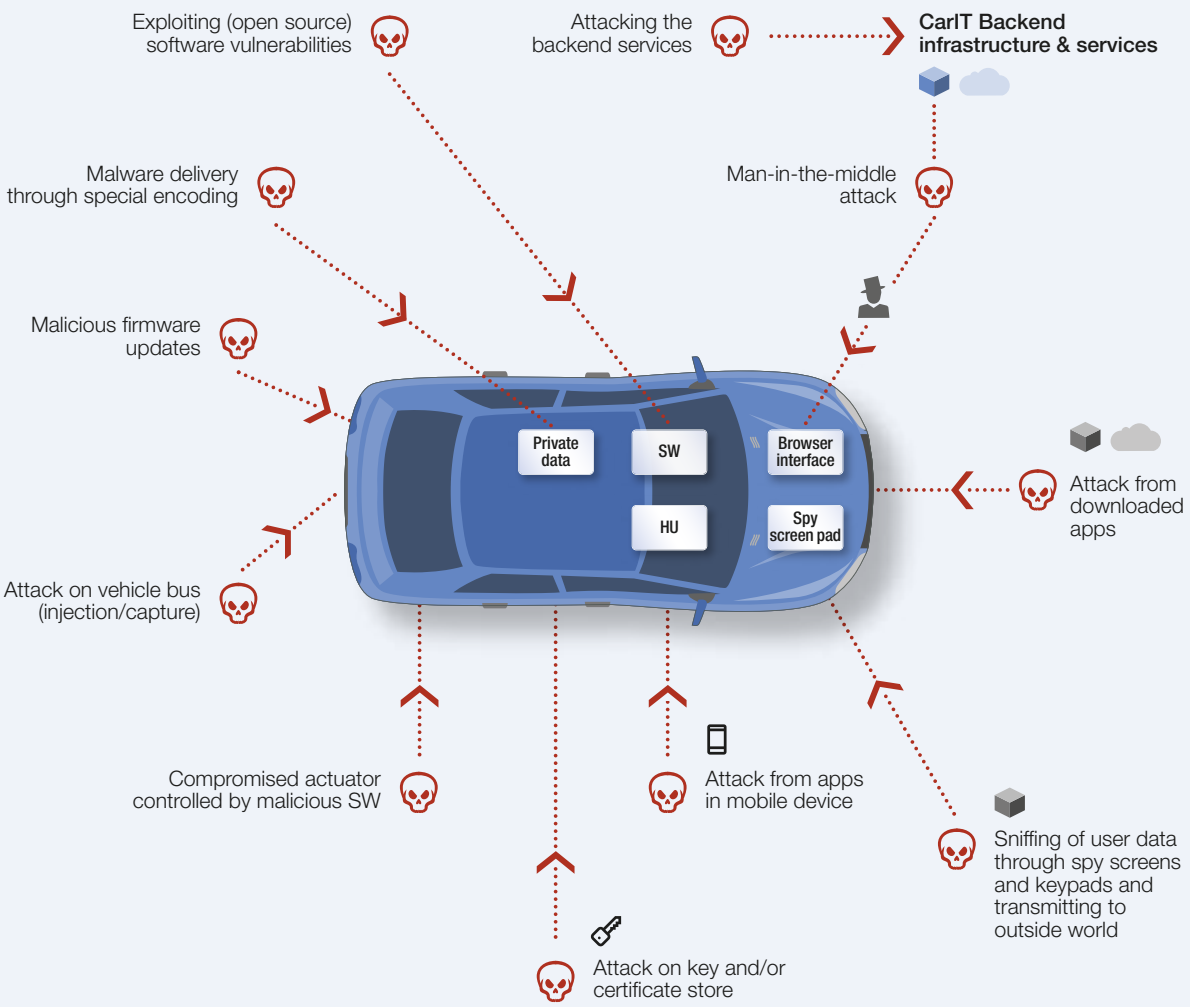


Figure 1: Overview on attack points of a connected car (image source: NTT)

Another requirement in connection with SUMS is the "RX Software Identification Number" (RXSWIN), which contains regulation-specific information about homologation-relevant software. Each vehicle must be able to provide information via standard interfaces (on-board diagnostics, OBD for short) which software versions for functions relevant to type approval are installed on the vehicle.

New challenges for automotive manufacturers (OEMs) and suppliers

OEMs are under great time pressure to have the SUMS & CSMS (Software Update Management System & Cyber Security Management System) and the associated processes and documentation established and audited as soon as the UNECE regulations have been finalized.

The introduction of the software identification number (RXSWIN), which contains information about the approval-relevant software of the electronic control systems and must exist across the entire value chain and the complete product life cycle, requires a comprehensive review and, if necessary, redefinition of processes. Given the many partners and suppliers involved, this is a complex requirement.

Meeting new regulations: Digital Twin reduces effort

To meet cyber security regulations such as SUMS & Co., the digital twin of the vehicle is an essential solution component, as automobile manufacturers can use digital twins to monitor and analyze the real vehicle. A digital vehicle twin thus offers exactly what the new UNECE regulations require in terms of transparency for the highest possible cyber security: The integrity and authenticity of the software in the vehicle can be traced at any time, software updates must be verified and validated at an early stage, for example by simulating cyber attacks.

Digital twin for vehicles

For an efficient software update management system, a digital twin of the vehicle is almost a must. All information on the vehicle's software and control unit configuration is available from the manufacturer at the time of delivery, but can change due to visits to the workshop or accidents, for example. Therefore, the current configuration of each individual vehicle must be checked before installing an update in order to reliably meet requirements such as storage space, libraries, control unit versions and compatibility.

Concepts such as app stores for vehicles can also result in a large number of complex configurations over the product life cycle in the entertainment area.

The combination of the vehicle twin with the owner's driving profile allows further process optimization. For example, a time can be determined at which the vehicle is probably not being used and then the update can be carried out successfully.

Implementation over the product life cycle

The digital twin for the software must be available both at the car manufacturer and on the individual vehicle. The manufacturer builds the digital twin during product development and validates it with virtual and physical tests. The dependencies between electronic control units and software modules and their suppliers must also be managed. Depending on the vehicle equipment, the appropriate software versions and data must then be brought to the control units in production. Finally, in aftersales it is important to provide the dealers and workshops with the latest versions.

These processes are based on IT applications for software configuration management including compatibility management. In addition to the software source code, it is also necessary to manage the executable

binary files and other data for parameterization. This software configuration is linked to the product structure in development and production. The delivery status of the software configuration of a vehicle can be seen as the initial status of the digital twin. This configuration must not only be managed centrally in the vehicle manufacturer's databases, but also stored on the vehicle with the ability to be queried.

Successful automotive OTA

From the smartphone we know the software update process, which is usually initiated by the user. In addition to this pull mechanism, a push mechanism is also required in the automotive sector, for example for recalls and security-critical updates. Some experiences from this environment should also be considered for automotive OTA:

- Sign code: check the safe origin before installation
- Only transmit updates via secure communication channels: encrypt the path from the cloud to the gateway/edge and from there to the vehicle
- Delta updates of the affected code modules: optimize bandwidth requirements and update duration
- Automatic recovery including rollback: create a functional state after connection problems

Outlook: Digital Twin Computing

At the end of 2019, the Japanese NTT presented the first research results with the Digital Twin Computing Initiative (DTC) in order to significantly expand the areas of application of digital twins through modern IT.

The difference between Digital Twin and DTC is as follows: Conventional digital twins are created and used for specific purposes. It is difficult to combine and interact with different digital twins. The DTC vision extends this concept by merging several digital twins in different industries and by expanding existing digital twins. For example, entire supply chains including factory planning and logistics could be mapped. This would require an enormous amount of IT resources. Therefore, an infrastructure based on an "Innovative Optical and Wireless Network (IOWN)", such as that offered by NTT, is an important building block for DTC. IOWN uses the future technology of photonics for ultra-fast data transmission.

The technical solution modules for DTC form an architecture with four layers:

1. **Cyber/Physical Interaction Layer** for the interaction between the real world of humans and things with cyberspace
2. **Digital Twin Layer** for the generation and maintenance of digital twins
3. **Digital World Presentation Layer**, in which digital twins can be combined
4. **Application layer** for running applications

Conclusion: **"DTC is a broad vision. We believe that we have to work with many partners from many different disciplines, for example from the social and natural sciences as well as the humanities and applied sciences, to implement this concept and to advance society."** said Koya Mori, Senior Research Engineer from the NTT Software Innovation Center in Tokyo

Author Biography

Jens Krüger, born in 1966, has a degree in business information technology. After studying at the FH Wedel University of Applied Sciences, he initially worked in engineering IT for a global automotive supplier for 10 years. Since 1998 he has been working for the Japanese IT service provider NTT DATA in Munich as a consultant in the area of product lifecycle management and heads the global Engineering Center of Excellence.

Initial publication in German language:
Krüger, J.: Digital Twin für maximale Cyber Security.
Zeitschrift für Wirtschaftlichen Fabrikbetrieb (ZWF).
Sonderausgabe "Digitaler Zwilling" (2020), S. 29-31.

NTT DATA Deutschland GmbH
Hans-Döllgast-Straße 26
80807 München
Deutschland
Telefon +49 89 9936-0
de.nttdata.com