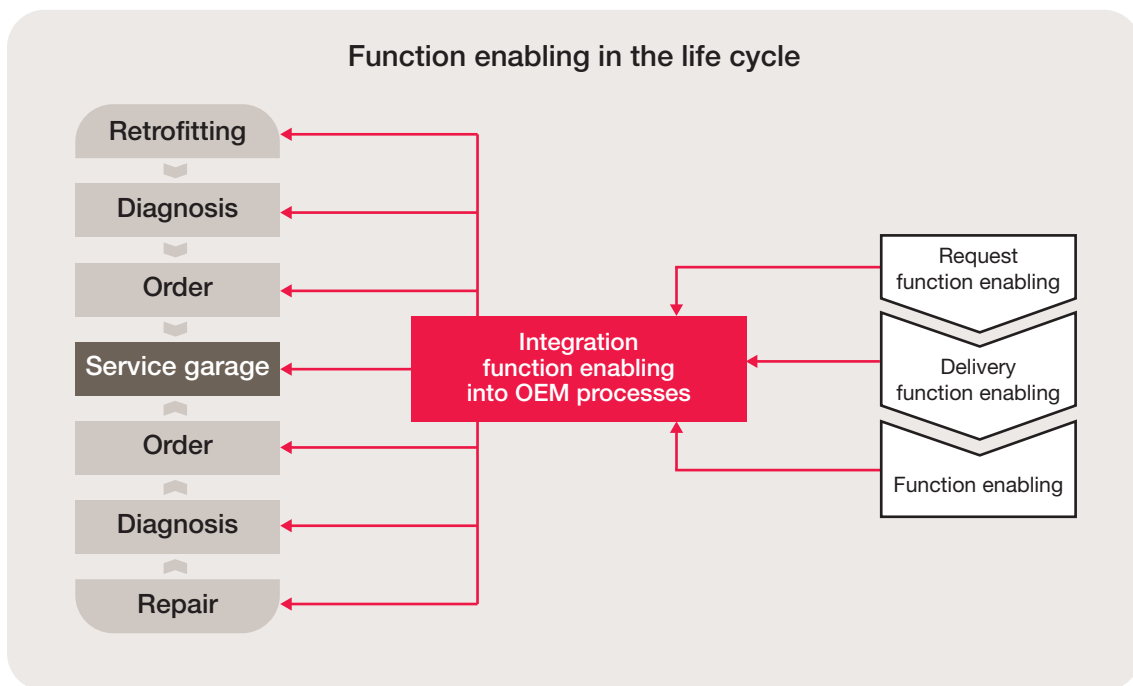


# Automotive Security – Function Enabling

## Secure individual software enabling in vehicles



As a result of the growing number of software functions in commercial vehicles and the possibility to enable these functions, car manufacturers now have completely new business models. At the same time, requirements for protection against misuse are increasing. secunet supports vehicle manufacturers and suppliers in the launch of innovative security solutions for function enabling.

### Security requirements for protecting function enabling

#### Protection against misuse

The integration of secure and controlled software enabling is an effective means of preventing possible misuse of a software function. This kind of limited use is based on the secure assignment of the function to a unique characteristic in the vehicle, e.g. the vehicle identification number. In addition, enabling of the software functions can be made dependent on parameters such as mileage. In this context, feasible authentication and authorisation models must be specified for the user of the functions, and the secure provision of the parameters must be defined for enabling within the vehicle.

### Your advantages:

- Reduction of the number of hardware variants and a corresponding drop in logistics costs
- Reduction of licensing costs as a result of individual software enabling
- New revenue models as a result of controlled software enabling

### Protection of the processes from production to shipment

In order to safeguard function enabling, appropriate processes must be in place for the areas of development, production, distribution, service and billing. This involves analysing whether the required enabling data is made available via a central instance from the background systems or via distributed systems in the vehicle. In the case of central enabling, it is possible to make enabling data available to the vehicle by means of an online connection with the vehicle as well as offline via available service processes.

There are logistical and technical questions to be resolved for the processes. For instance, whether and how the enabling request can be processed independent of the installed hardware as well as how the prompt availability of the enabling data on the line is ensured. The integration of the enabling procedure in the supplier's production process and the quality assurance processes must also be taken into consideration. If enabling is extended to include the service organisation, the data must be available in a global, heterogeneous infrastructure at all times.

### Protection of property rights and billing

If enabling involves software which is charged for, the enabling processes must be integrated into existing billing processes. In the case of a change of ownership, usage rights must be clarified. For an effective and secure implementation of limitations of use, appropriate measures must also be taken with regard to control units. A routine for verifying the authorisation must be integrated and protected. This is supplemented by the definition and implementation of rules governing responses to the respective verification results.

### **secunet – your experienced security technology partner for the automotive sector**

secunet supports vehicle manufacturers and suppliers in the implementation of security infrastructure and security-relevant processes for HIS compliant function enabling in development, production and the service organisation including their integration into logistics and financial systems.

### **secunet Security Networks AG**

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:

# **secunet**

secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen, Germany  
Phone: +49 - 201 - 54 54 - 0  
Fax: +49 - 201 - 54 54 - 123  
E-mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)