Automotive cybersecurity

Turning the threats of connected mobility into secure innovation. Approved.

EY, GIGATRONIK and Code White.
By 2020, almost every new car will be connected, putting OEM’s current structures at risk

Future connected mobility …

► Built-in internet connectivity will grow from 10% today to 90% in 2020.
► Urbanization, increased logistics and mobility require connectivity-to-X as a key enabler.
► Shared mobility services will be an alternative to owning cars or using public transport. This will become even more relevant when cars drive autonomously.
► Intercity logistics and public transportation based on connected buses and trucks will reduce costs, increase revenues and offer better services.

... and its implications for automotive OEMs

► Historically isolated in-vehicle networks, including electronic control units, sensors and actuators, become part of a network of networks.
► Along with this exposure to other networks come new vulnerabilities with potential impacts on driving safety, data privacy, brand value, warranty or repair costs and their legal consequences.
► The network of networks has to be considered end-to-end when products and services are designed, developed and operated.
► Organizational structures, processes, supplier and partner relationships require adaptation to deal with higher complexity, threats, competition and customer expectations.
► Compliance with legal and regulatory requirements regarding data protection, product safety and security need to be met or exceeded.

Sources: Information-technology Promotion Agency Japan, Machina Research (2013), EY analysis
Attackers combine knowledge about different entry points to win the jackpot, potentially causing severe damage.

- Telematics units are attractive entry points for cyberattackers because they communicate both with the outside environment and connect with parts of a car's internal network.
- The nature of the automotive industry means that a vulnerability in one link of the connected ecosystem can impact many others.

TPMS: Tire Pressure Measurement System
CAN: Controller Area Network
LIN: Local Interconnect Network
MOST: Media Oriented Systems Transport
We combine our complimentary services to a uniquely effective and comprehensive automotive cybersecurity offering.
Our comprehensive automotive cybersecurity and privacy framework

A robust connected vehicle cybersecurity strategy ...

Strategic influences
- Business and product strategy
- IT strategy
- Mobility and industry trends
- Compliance
- Emerging technologies

Practical influences
- Assessment
- Technical reviews

Connected vehicle cybersecurity strategy

Desired outcomes
- Safe vehicles
- Safe customers

requires a structured framework ...

Connected vehicle risk management governance and strategy

Security and privacy process, risk and control framework

Product life cycle
- Design and development
  - V-Model
    - Threat and risk analysis
    - Protection concept
    - Documentation of test cases
    - Comprehensive test coverage
    - Acceptance test concept
- Vehicle production
  - Protection measures
- Vehicle on the road
  - Tools and technology
  - Partner and supplier management

Compliance monitoring and reporting

EY’s automotive cybersecurity and privacy framework
Our three-fold approach to assess cybersecurity risks, perform audits and set up a sustainable security management framework

Dynamic environmental influences

Customer expectations

Technical innovation

1: Penetration testing
Asset identification and threat analysis

2: Cybersecurity audit
Audit of protection concept and requirements specification

3: Security management framework
Risk management

Connected vehicle cybersecurity strategy

Audit of security & engineering processes
Data protection and security analysis
Audit of test cases & test concepts
Penetration testing (holistic / test plan based)
Technical assessment

Risk Assessment

Risk Report and improvement plan

*) Development of cyber security certification standards and offerings in progress

Mobility service innovation

New threats and vulnerabilities

Multiple regulation and compliance requirements

Automotive cybersecurity
The Code White approach of automotive security product testing covers attack paths holistically based on four distinct threat levels.

**Threat level 1**
- **Beginner level** (script kiddy)
  - Has a basic security understanding
  - Is able to use public exploits or reproduce trivial security findings

**Threat level 2**
- **Professional level** (experienced attacker)
  - Profound security understanding and experience
  - Able to adapt existing exploits
  - Has some basic hardware-level exploitation experience

**Threat level 3**
- **Expert level** (advanced attacker)
  - Professional level skills but with the added ability to develop new exploits and find new vulnerabilities

**Threat level 4**
- **State-sponsored level** (foreign government intelligence/military)
  - Expensive long-term targeted attack campaigns

<table>
<thead>
<tr>
<th>Attacker level</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginner</td>
<td>- Has a basic security understanding</td>
</tr>
<tr>
<td></td>
<td>- Is able to use public exploits or reproduce trivial security findings</td>
</tr>
<tr>
<td>Professional</td>
<td>- Profound security understanding and experience</td>
</tr>
<tr>
<td></td>
<td>- Able to adapt existing exploits</td>
</tr>
<tr>
<td></td>
<td>- Has some basic hardware-level exploitation experience</td>
</tr>
<tr>
<td>Expert</td>
<td>- Professional level skills but with the added ability to develop new exploits and find new vulnerabilities</td>
</tr>
<tr>
<td>State-sponsored</td>
<td>- Expensive long-term targeted attack campaigns</td>
</tr>
</tbody>
</table>
Cybersecurity should be part of the vehicle development life cycle from the very outset

The EY certification framework allows the application of diverse certification standards and criteria as industry standards are still developing. We recommend to certify against established legal, regulatory, subject matter (e.g., ISO 26262 or ISO 27001) and custom criteria. The integration of suppliers and partners completes the comprehensive but appropriate approach.

Security engineering process

- Current state assessment of security engineering processes
- Joint workshops to define target maturity level and custom measurement criteria-based on our automotive cybersecurity maturity model
- Identification and prioritization of improvement measures, definition of implementation road map
We guide you to set up or improve your automotive security management

Automotive risk management

Risk management process documentation and product specifications
- Integration of findings from penetration testing, risk assessment and security audits
- Alignment with existing processes
- Implementation, including trainings and services

Tool evaluation, risk management and information security (IS) management system
- Usability
- Integration with existing tools
- Roles and responsibilities

Automotive information security management process

Objective-driven implementation of security triggers, along software, embedded systems and vehicle development processes - as many as necessary, as few as possible.

Software development

(Agile) software development: 6-12 months

Vehicle development cycles: 3-5 years

Operative data security analyses

Risk assessment, protective measures, tracking mechanisms
- Protection requirements analysis for individual components
- Threat and risk analysis
- Definition of risk mitigating measures
Our solution at a glance

**EY Automotive cybersecurity**

Iterative and integrative

- Control framework monitoring and reporting
- Program management

Protect the business

- Maturity assessment
- Security audits
- Product and service testing

Improve processes

- Information Security Management System
- Certification
- Process improvement
- Design improvement

Drive innovation

- Vehicle risk management strategy

EY

- Concept and program management
- Risk management governance & strategy
- Control framework
- Threat modeling & risk assessment
- Audit and certification
- Information Security Management
- Security operations managed services

GIGATRONIK

- Structured security testing (hardware and software)
- Functional testing
- Car IT architecture
- Design and development
- Processes and tools

Code White

- Security intelligence service
- Embedded hardware security reviews
- Holistic penetration testing
- Strategic consulting
Five reasons to choose us

1. Top ratings for EY as security and privacy consulting firm
   ► In 2013, Forrester rated EY highest in their Information Security Consulting Services Wave.
   ► EY’s globally connected cyber professionals take an economical and geopolitical perspective towards cyber risk - giving a truer, fuller risk picture that aids strategic awareness and intelligent decision-making.

2. Automotive embedded systems know-how
   ► Gigatronik is a key supplier of embedded systems development for world-class automotive OEMs.
   ► Code White is a start-up founded by world-class security experts with deepest embedded systems know-how.

3. Code White’s holistic combined with GIGATRONIK’s plan-driven penetration testing approach
   ► Gigatronik’s V-model-based structured penetration testing ensures a comprehensive test coverage while Code White’s holistic approach reflects the real world of hacking, across any system borders - the best of both worlds.

4. Trust and confidentiality
   ► As an audit firm, confidentiality is in EY’s DNA. Also, Code White and Gigatronik are trusted partners within the automotive industry.

5. EY CertifyPoint
   ► EY’s global ISO certification practice (EY CertifyPoint) is headquartered in the Netherlands, manages ISO certifications worldwide, and provides individual client trainings. EY CertifyPoint is growing its offerings continuously, including the fields of connected vehicles, mobility services and related cybersecurity topics.
Sample credentials

Large industrial manufacturer cybersecurity transformation and full security outsource

4000
EY has the capacity for over 4,000 man days of security testing per month.

400
EY has a talent pool of 400 experienced security testers across the globe.

Cyberthreat assessment at manufacturer of industrial-grade turbo-machinery

Global automotive OEM required executive understanding of their enterprise security risk posture. EY applied the cyber transformation method to assess the cybersecurity capabilities and executed a number of targeted, red team, testing procedures.

EY mobility innovation center with in-vehicle electronics expertise
Contact us: automotive.cybersecurity@de.ey.com

Dr. Rainer Scholz  
Executive Director  
GSA Mobility Innovation Group  
Advisory Services, Ernst & Young

Siegfried Adam  
Senior Manager  
GSA Mobility Innovation Group  
Advisory Services, Ernst & Young

Tim Best  
Executive Director, Advisory Services, Ernst & Young

Dr.-Ing. Achim Wohnhaas  
CEO, GIGATRONIK Embedded Solutions

Lüder Sachse  
Managing Partner, Code White

Ernst & Young GmbH  
Wirtschaftsprüfungsgesellschaft  
Rothenbaumchaussee 78  
20148 Hamburg, Germany

Ernst & Young GmbH  
Wirtschaftsprüfungsgesellschaft  
Arnulfstraße 59  
80636 Munich, Germany

Ernst & Young AB  
Jakobsbergsgatan 24  
111 44 Stockholm, Schweden

GIGATRONIK Holding GmbH  
Magirus-Deutz-Straße 2  
89077 Ulm, Germany

Code White GmbH  
Magirus-Deutz-Straße 18  
89077 Ulm, Germany
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY’s Global Automotive and Transportation Sector

In the Automotive and Transportation Sector, we’re doing our part to enhance human mobility, getting people and products where they need to go — better, faster and smarter — in a rapidly changing environment. Through our globally expansive sector network, we bring a strong point of view on the emerging issues across automotive and transportation, connecting more than 13,000 professionals with deep industry and technical expertise who understand what the trends of the future mean for the present. We work with our clients to deliver innovative yet pragmatic solutions to address their imperatives and deliver tangible business value around the disruptive trends and transformational challenges shaping tomorrow’s industry, today.

© 2016 Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft.
All Rights Reserved.

V1.1

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/automotive
www.de.ey.com/futuremobility
Contact us: automotive.cybersecurity@de.ey.com