

7 Cyber Risks of the Connected Vehicle

The background image shows a white car on a lift in a garage. A dark blue and purple graphic overlay is positioned in the center, containing text. The overlay has a wavy, abstract pattern on its right side.

The purpose of this eBook is to provide insights into top cyber risks for EV OEMs and suppliers.

More importantly, these observations are intended to help product cybersecurity teams to determine what needs to be done in their organizations, to achieve and maintain ISO/SAE 21434 and UN R155 compliance, and reduce operational and cyber compliance costs.

Introduction

In 2021, there were about 237 million connected cars on the roads across the globe. Their number is expected to surpass 400 million by 2025. [1] As connectivity increases, so is the possibility of cyber attack threatens the safe operation of vehicles.

ISO/SAE 21434 certification is mandatory for every supplier of components to OEMs, and OEMs that need to submit their vehicle model for UN R155 homologation. Ratified in August 2021, the standard of cybersecurity inroad vehicles requires OEMs to demonstrate and document a detailed cyber risk handling process for their entire organization, for each specific model undergoing compliance, and for its subcomponents. The standard goes beyond process and requires bespoke automotive & cyber content and expertise.

This requires, among other things, describing organizational cyber processes, performing a detailed Threat Analysis & Risk Assessment (TARA), coming to contractual agreements with each 3rd party supplier regarding cyber risks responsibilities, risk handling, and validation of mitigation implementation.

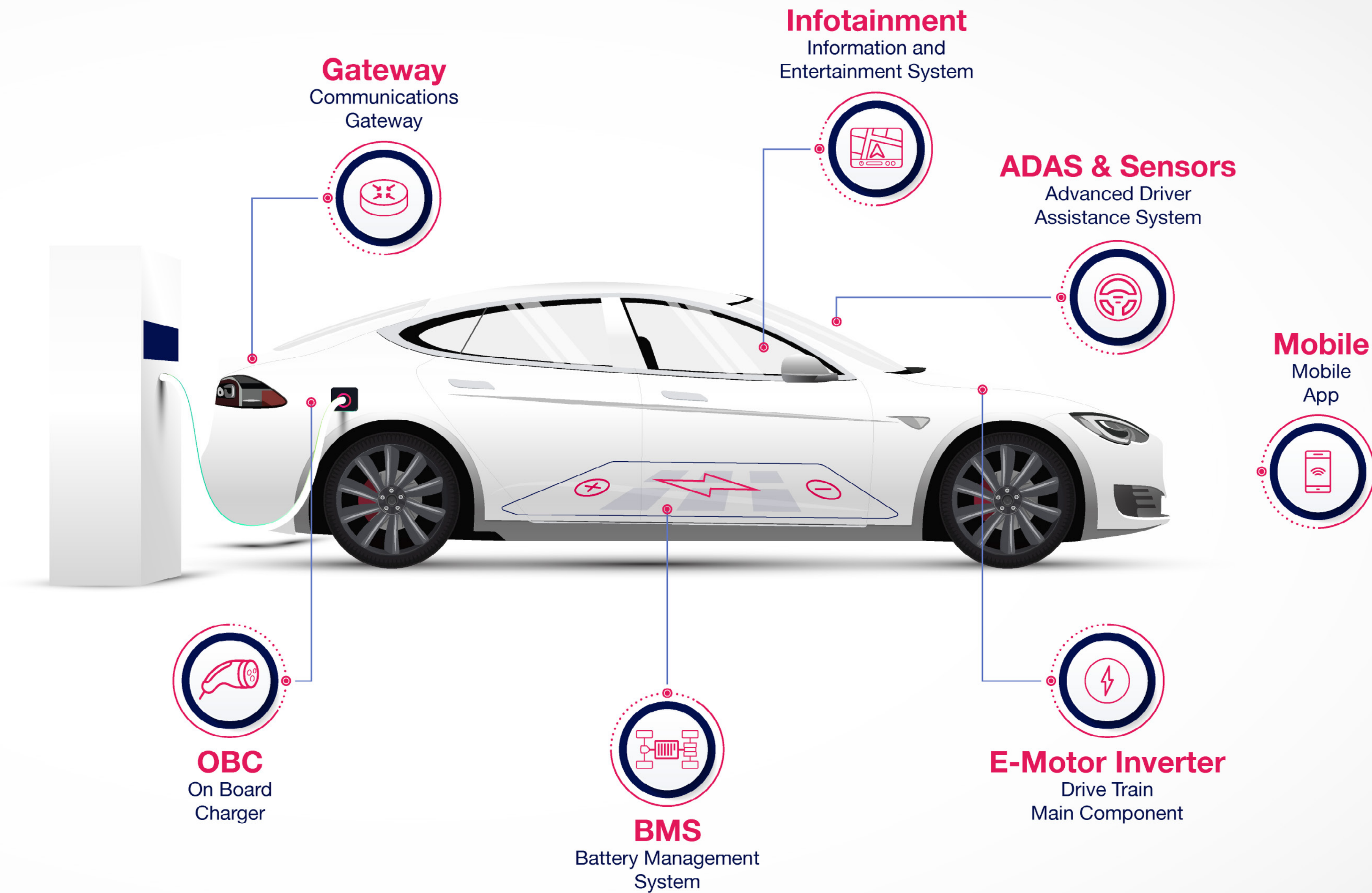
My team has completed over many dozens of projects, covering major EV components and full vehicle architectures. Successfully completing so many projects in challenging timeframes, we've learned a lot along the way. Although high-level, we hope that this e-book will make a difference in your compliance journey, and help you get one step closer to achieving and maintaining compliance and protecting your vehicle types from cyber threats.

[1] Statista.com

Assaf Harel
Chief Scientist, Co-Founder



- 1 **OBC** page 5
- 2 **BMS** page 7
- 3 **E-Motor Inverter** page 9
- 4 **Mobile** page 11
- 5 **ADAS & Sensors** page 15
- 6 **Infotainment** page 17
- 7 **Gateway** page 19






1 On Board Charger (OBC)

On-Board Chargers manage the charging cycle of the car from external AC/DC sources. OBC is ISO/SAE 21434 relevant due to its main risks:

- Hyper-charging, beyond current limits
- Escalated privileged access

By having access to the OBC an attacker can gain access to ECUs in the power domain, directly from the charging port.

Potential breaches/attacks

-  **Safety risk, life risk**
Incorrect charging may cause damage to the battery, and possibly result in overheating and combustion.
-  **Operational and brand damage**
Battery damage, maintenance issues.
-  **Privacy**
With new Plug & Charge, sensitive personal and financial data is exchanged with the charging station (EVSE).

How Karamba helps to secure the OBC



VCode®

- ✓ Automatically identifies and prioritizes vulnerabilities, weaknesses and misconfigurations, and suggests remediations before production.
- ✓ Identify and address cybersecurity issues in 3rd party and in its own software packages (binary analysis).



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Assess attack path impacts and feasibility.
- ✓ Design mitigation strategies for the lifetime of the vehicle.
- ✓ Learn how to meet the requirements of ISO21434 and UN R155.

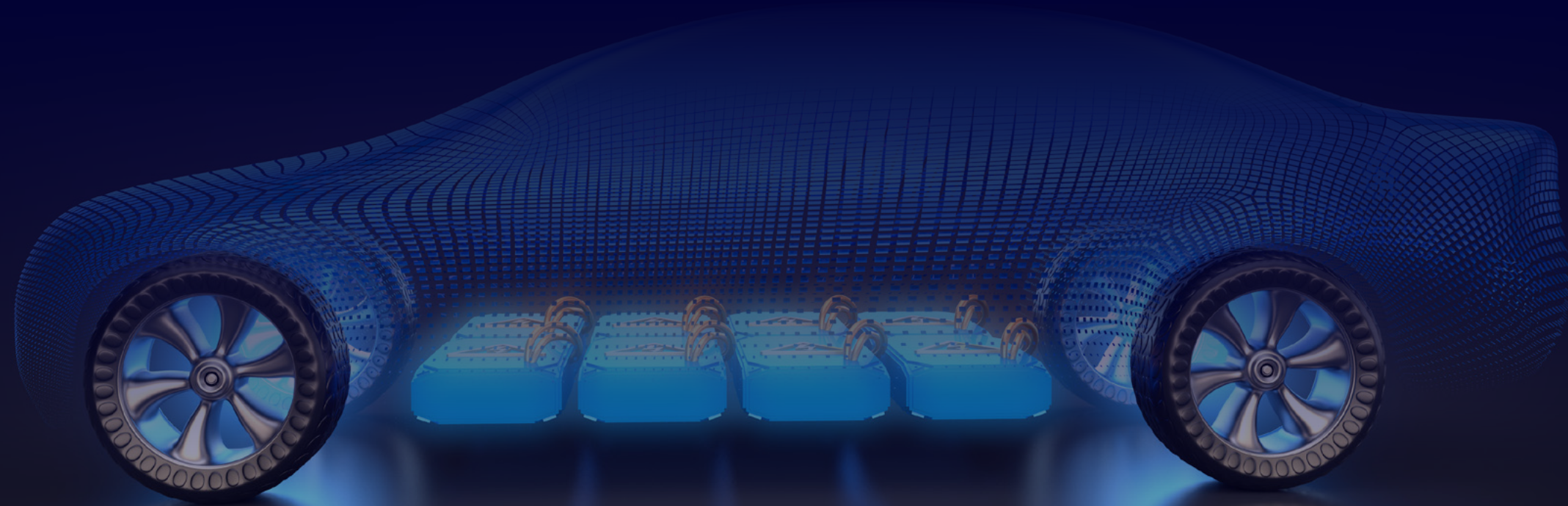


Pen-Test




- ✓ Test interfaces (e.g. ISO 15118) per standard work packages.
- ✓ Find vulnerabilities in the OBC with Karamba's R&D team, leverages proven test suite and hacker's ingenuity, covering the subsystem from mobile charging app to charging station.

2 Battery Management System (BMS)

The most critical component in the EV power chain, the BMS controls the efficiency and behavior of the battery.



Potential breaches/attacks

-  **Battery risk**
Damage to the battery by tampering with the calibration file, maintenance problems.
-  **Safety risk, life risk**
Melting or exploding batteries.
-  **Intellectual property theft / brand damage**
One of the key aspects in maximizing the performance of electric vehicles is the optimization of the propulsion system. A proprietary calibration files are a high value manufacturer's intellectual property and a sought-after commodity by car enthusiasts' communities called "tuners".

How Karamba secures the BMS



VCode®

- ✓ Automatically identifies and prioritizes vulnerabilities, weaknesses and misconfigurations, and suggests remediations before production.
- ✓ Validate cyber posture of 3rd party and in its own software packages (binary analysis).



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Assess attack path impacts and feasibility.
- ✓ Design mitigation strategies for the lifetime of the vehicle.
- ✓ Leverage proven methodology and tools to achieve high quality TARA fast.






Pen-Test

- ✓ Test interfaces (e.g. ISO 15118) per standard work packages.
- ✓ Find vulnerabilities in the BMS with Karamba's R&D team leverages proven test suite and hacker's ingenuity.

3 E-Motor Inverter

This is the main component of the drivetrain. Unauthorized access to the inverter functions can result in safety-critical risks including loss of life.

Potential breaches / attacks

-  **Engine risk**
Damage to the engine by tampering with the calibration file.
-  **Safety risk, life risk**
Lose control of engine, engine damage.
-  **Intellectual property theft / brand damage**
The e-motor calibration files are a manufacturer's intellectual property and a sought-after commodity by car enthusiasts' communities called "tuners".

How Karamba secures the E-Motor inverter



XGuard™

- ✓ Signatures protect against in-memory changes to the data, securing the calibration file.

VCode®

- ✓ Automatically identifies, prioritizes, and advises how to remediate 3rd party risks before production.



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Identify system and implementation vulnerabilities.
- ✓ Develop defense strategies for the lifetime of the vehicle.
- ✓ Learn how to meet ISO/SAE 21434 and UN R155 requirements.



Pen-Test

- ✓ Karamba's R&D team tests your E-Motor system for possible exploits to determine where hackers could gain entry.

4 Mobile Application

The security of this application's storage of personal data, as well as the security of the APIs used by the application, may not have safety impact, but they affect one of the most painful problems for the owner: theft using impersonation, replication and/or replay methods.

Potential breaches /attacks



Car theft

As the owner mobile app serves as the keyless entry system - a compromised application poses a risk of theft.



Operational and brand damage

An owner mobile application can serve as an attack vector to the manufacturer's backend, posing risk to fleet management, Personally Identifiable Information (PII), intellectual property theft and more.

How Karamba secures the mobile app



Hardening Consultancy

- ✓ With a cybersecurity-first approach, Karamba team uncovers 3rd party vulnerabilities as well as security issues in the application code.



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Identify system and implementation vulnerabilities.
- ✓ Develop defense strategies for the lifetime of the vehicle.



Pen-Test

- ✓ Karamba's R&D team tests your system for possible exploits to determine where hackers could gain entry.

3 TARA questions

we get asked frequently and their answers



With dozens of TARAs under his belt, here's what Assaf Harel, Karamba's Chief Scientist, Co-Founder, has to say:

“EV is a feat of modern engineering: It is so sophisticated, intricate and innovative. I am proud to take part in this industry.”

1. What is your recommendation to young OEMs or Tier 1s for handling the new ISO processes?

That's the question we get asked the most! Usually, for young OEMs seeking to start the journey towards ISO/SAE 21434 compliance, we have two key recommendations:

Start with a gap analysis - this is where, together with you, we go over your ISO readiness. It's an effort that takes a few weeks, where we map the process of achieving compliance, breaking it down to the different tasks that are required in order to successfully complete the journey on time.

Threat analysis, for system and vehicle architectures. From this process we measure relevancy of different ECUs so we can further work at the component level and assure vehicle type compliance and homologation.

TARA questions answered by Karamba's Chief Scientist



2. How different is the OBC from other ECUs in terms of cybersecurity?

The difference is that it is externally connected to the charging port which already established a communication channel, so it can be exploited from an external interface, which is connected to the internet. From external interfaces e.g. payment page, through man-in-the-middle (MITM) attacks, hackers can gain control of the OBC. Additionally, the OBC sits on the power domain, i.e. where the Emotor-inverter is. That means that within one “hop” an attacker gains control of the ECU, which is responsible for acceleration - which makes it potentially the most risky ECU in the car.

3. Would you consider FPGA components in the scope for cybersecurity assessments, what techniques would be used compared to a CPU or, (because it's hardware) can it be considered out of scope?

Field-Programmable Gate Array, or FPGA, is an integrated circuit that implements code in hardware to execute a thousand times faster than in a processor. These circuits, or arrays, consist of configurable logic blocks (CLBs), memory, or other elements - no chipset. From an attacker's perspective, it's like you're almost writing code, just different environments and languages. You are still writing firmware that is flashed, you can still reverse engineer it. Now, manipulating an FPGA is a totally different challenge.

First thing is we need to find out what a certain FPGA does and whether it's relevant to cybersecurity. If it does, the next step would be to find out how easy it is to breach (for example tampering or denial of service) - this is usually extremely hard when it comes to FPGA, meaning low risk feasibility and that's why we don't address it as first priority.

5 Autonomous Driving and Assisted Driving Systems (ADAS)

Advanced driver-assistance systems (ADAS) are groups of electronic technologies that assist drivers in driving and parking functions. Through a safe human-machine interface, ADAS increases car and road safety. ADAS uses automated technology, such as sensors and cameras, to detect nearby obstacles or driver errors, and respond accordingly. Having fully autonomous or even L3 assisted driving means that a wrong guidance from the system due to erroneous/malicious sensor input or wrong algorithmic decisions can cause catastrophic results. The ADAS vulnerabilities focus on two scenarios above others: Replacement of firmware, and validation of sensor input.

Potential breaches/attacks



Safety risk, life risk

1. In Autonomy Level 3 and up, ADAS is controlling the car, and can be an attack vector for a vehicle takeover.
2. ADAS is very vulnerable due to sensors and is prone to attack without controlling the ADAS (e.g. blind the LIDAR).

How Karamba secures ADAS systems



Sensor-fusion Cyber Security Consultancy

- ✓ In the field of autonomous driving, sensor fusion is used to combine the redundant information from complementary sensors in order to obtain a more accurate and reliable representation of the environment. Karamba consults how to incorporate cybersecurity elements to the sensor fusion algorithm (e.g. redundancy).



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Identify system and implementation vulnerabilities.
- ✓ Develop defense strategies for the lifetime of the vehicle.
- ✓ Learn how to meet the requirements of ISO21434 and UN R155.






Pen-Test

- ✓ Karamba's R&D team tests your system for possible exploits to determine where hackers could gain entry. Combining a proven set of penetration tests and hacker ingenuity, the Karamba research team thoroughly examines the ADAS communication channels, and subsystems.

6 Infotainment

The Infotainment system has rich functionality and lots of processing power. It often also allows control of windows/doors and remote start of the car. Risks are: remote control of this unit allowing breaking into the car and stealing it, stealing Personally Identifiable Information (PII), and more.

Potential breaches/attacks

-  **Operational and brand damage**
The infotainment system can serve as an attack vector to the manufacturer's backend, posing risk to fleet management, Personally Identifiable Information (PII), intellectual property theft and more.
-  **Car theft**
As the infotainment system serves as the "server-side" keyless entry system - a compromised infotainment poses a risk of theft.
-  **Safety risk, life risk**
Lose control of the car, in case of ADAS L2 autonomous parking.

How Karamba secures Infotainment systems



Hardening Consultancy

- ✓ With a cybersecurity-first approach, Karamba team uncovers 3rd party vulnerabilities as well as security issues in the infotainment code.



XGuard™

- ✓ Signatures protect against in-memory changes to the infotainment files, detecting and preventing malware attacks and in-memory attacks.

VCode®

- ✓ Automatically identifies, prioritizes, and remediates 3rd party risks before production.



TARA

- ✓ Define system adversaries, functionality, and attack vectors. Identify system and implementation vulnerabilities.
- ✓ Develop defense strategies for the lifetime of the vehicle.
- ✓ Learn how to meet the requirements of ISO21434 and UN R155.



Pen-Test

- ✓ Karamba's R&D team tests your system for possible exploits to determine where hackers could gain entry. Combining a proven set of penetration tests and hacker ingenuity, the Karamba research team thoroughly examines every component from infotainment and telematics to UDS, Bluetooth and USB.

7 Communications Hub/Gateway

The communications hub is used to separate outward facing communications from the rest of the car, and thus segment the risk. This makes those units an easy and preferred attack vector, extending any other attack vectors that were initially blocked by a gateway.

In most car architectures, the gateway is connected directly to the telematics unit and OBD2 port, making it exposed to external attacks.

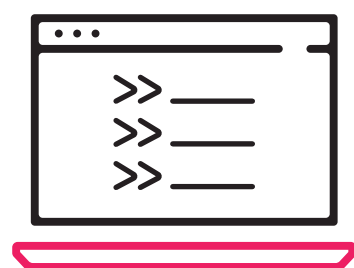
Potential breaches /attacks



Safety risk, life risk

In ASIL levels 2 and up, the gateway serves as the divider between the “dirty sub-network” (Infotainment and telematics) to “clean sub-networks”, where safety systems reside. Hacking the gateway may serve as an attack vector for vehicle takeover.

How Karamba secures the Gateway/Communications Hub



Hardening Consultancy

- ✓ With a cybersecurity-first approach, Karamba's team uncovers 3rd party vulnerabilities as well as security issues in the structure of the code.



XGuard™

- ✓ For AUTOSAR Classic or any other RTOS based systems, automatically protect against in-memory changes to the gateway application in runtime.

VCode®

- ✓ Automatically identifies, prioritizes, and remediates 3rd party risks before production.



TARA

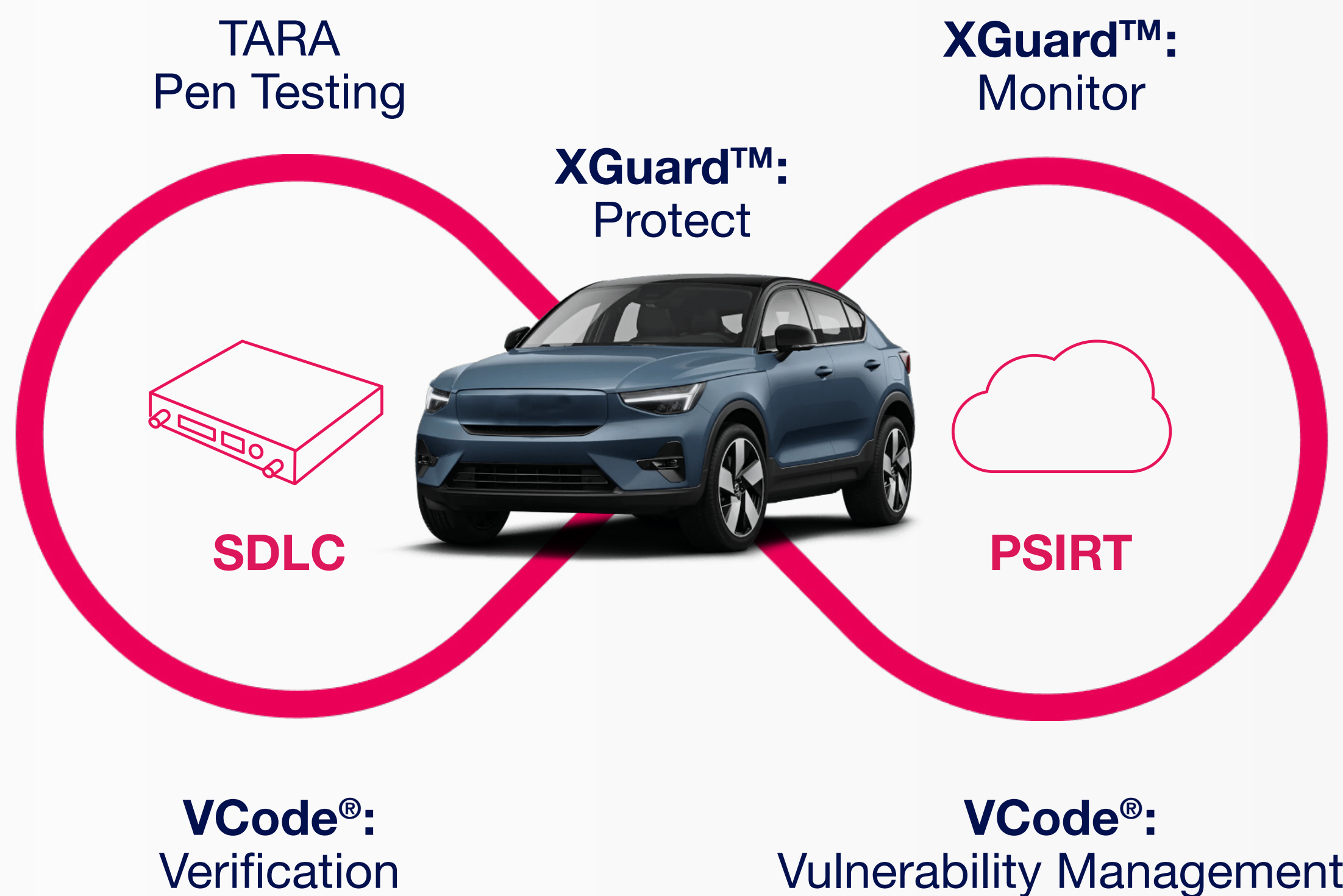
- ✓ Define system adversaries, functionality, and attack vectors. Identify system and implementation vulnerabilities.
- ✓ Develop defense strategies for the lifetime of the vehicle.



Pen-Test

- ✓ Karamba's R&D team tests your system for possible exploits to determine where hackers could gain entry. Combining a proven set of penetration tests and hacker ingenuity, the Karamba research team thoroughly examines the gateway various attack surfaces.

End-to-End Product Security



Karamba's product security portfolio of products and services enables EV OEMs and suppliers to protect their ECU and vehicle types, without interfering their R&D and supply-chain processes.

From threat analysis and risk assessment (TARA) during the design phase, to embedding security into the ECU, without requiring any access to source code, and without affecting R&D and validation processes, to binary analysis to manage supply-chain security, accelerating acceptance with rigorous pen testing, and managing continual security with a vulnerability management system, Karamba Security leads the market of product and automotive security.

OEMs and suppliers from the electric vehicle and smart energy industries rely on Karamba Security to ensure products are continuously protected against cyber threats, stay compliant with the latest standards and regulations, minimize supply-chain risks, and reduce operational costs.

**To learn more how Karamba Security can help you accelerate ISO/SAE 21434 compliance and UN R155 homologation,
Send us an email: ebook@karambasecurity.com or visit www.karambasecurity.com**