magility
cyber security

Presentation of the company and consulting approach

Magility Cyber Security GmbH

Dino Munk,
Managing Partner

Contents

Short profile Magility Cyber Security (MCS)

Business purpose of Magility Cyber Security GmbH (MCS)

Who we are and what we aspire to

- MCS is a spin-off of Magility GmbH, a high-tech consulting company with a focus on strategy, business model development and management consulting.
- MCS implements holistic and compliant Cyber Security Management Systems (CSMS) and Software Update Management Systems (SUMS) along the supply chain.
- Currently, our customers come from the automotive industry and vehicle construction, from medium-sized companies to OEMs from the German and European market.
- Thanks to the longstanding eco-system of our shareholders and our experienced cyber security experts, we are optimally positioned.
- We are closely networked and work trustfully with leading cyber security providers, e.g. from the Cyber Hub Israel.
- We are also active in other sectors such as high-tech, mechanical engineering, aviation/transportation and implement the standards in a sector- and customer-specific, practice-oriented manner.
- We always have our finger on the pulse and adapt our offer in real time to new regulations and best practices specific to the industry.

The shareholders of Magility Cyber Security

"We believe in the future viability of our advisory approach and are committed personally, financially and with many years of expertise."

Dino Munk

Managing Partner

formerly Business Unit Director at Staufen.AG Beratung und Beteiligung

Dr. Michael W. Müller

Shareholder

Managing Partner Magility GmbH, formerly Managing Director MBtech Consulting

Stefan E. Buchner

Shareholder

Member of the Supervisory Board of various companies such as Continental AG and thyssenkrupp AG, formerly Member of the Board of Management of Daimler Trucks,

Ralf Stokar von Neuforn

Shareholder

Founder of Staufen.AG and numerous start-ups, successful implementation of various company successions

Typical Cyber Security Challenges

Cyber security must be anchored at different levels

Classic IT

e.g. cloud, servers, networks, PCs, laptops, mobile devices, software

Infrastructure

e.g. buildings, IIOT, OT, data buses, plants, machines, Industry 4.0, smart cities, software

Products & Services

e.g. IoT products, end-to-end solutions, V2X, vehicle fleets, services, software

Through modern connectivity,

End-to-End Security

becomes a critical success factor for companies

End-to-end security along the lifecycle and the value chain

Supply chain cyber security management and OTA software updates become critical success factor

HW and SW Value Chain

OEM – Tier 1 – Tier 2 – Tier n

Product Life Cycle

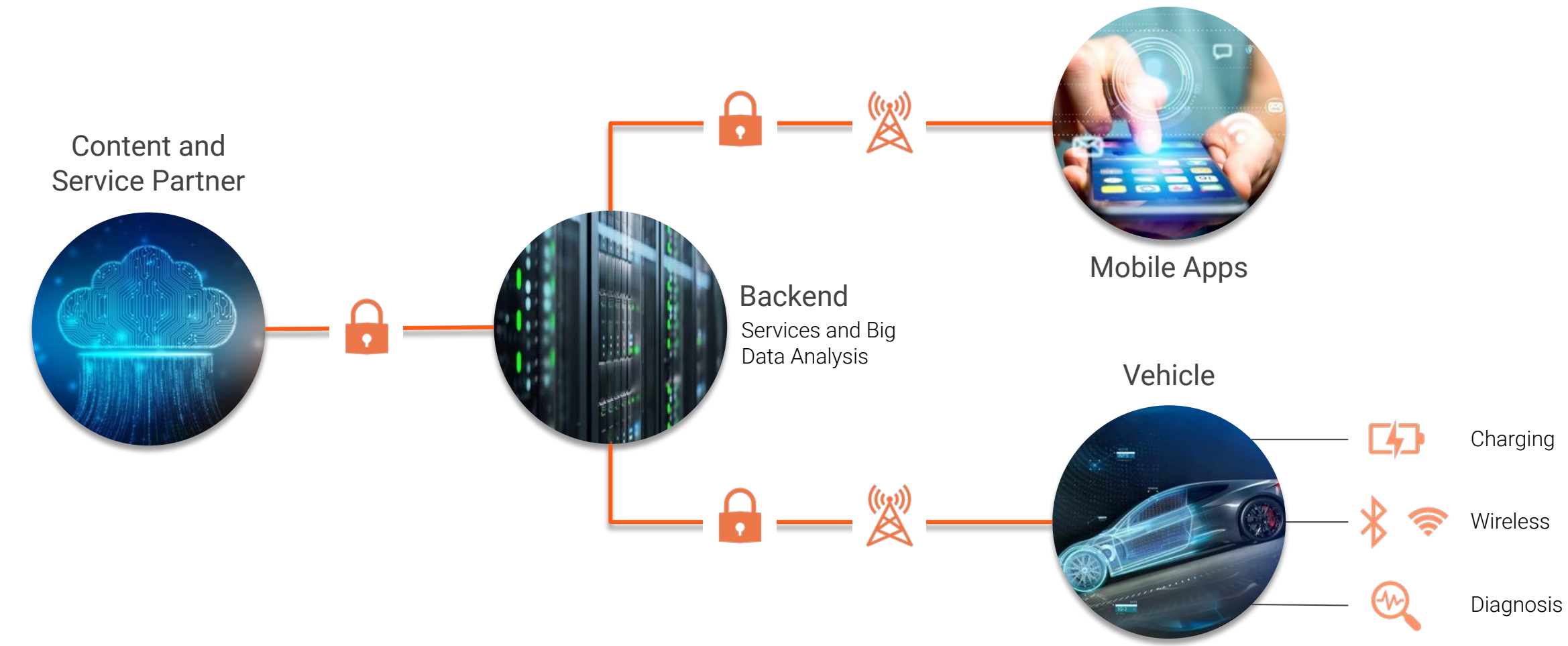
R&D, Production, Sales, Aftersales,
Waste Management

End-to-End Overall System

Vehicle, Backend, Cloud Services,
Mobile Applications

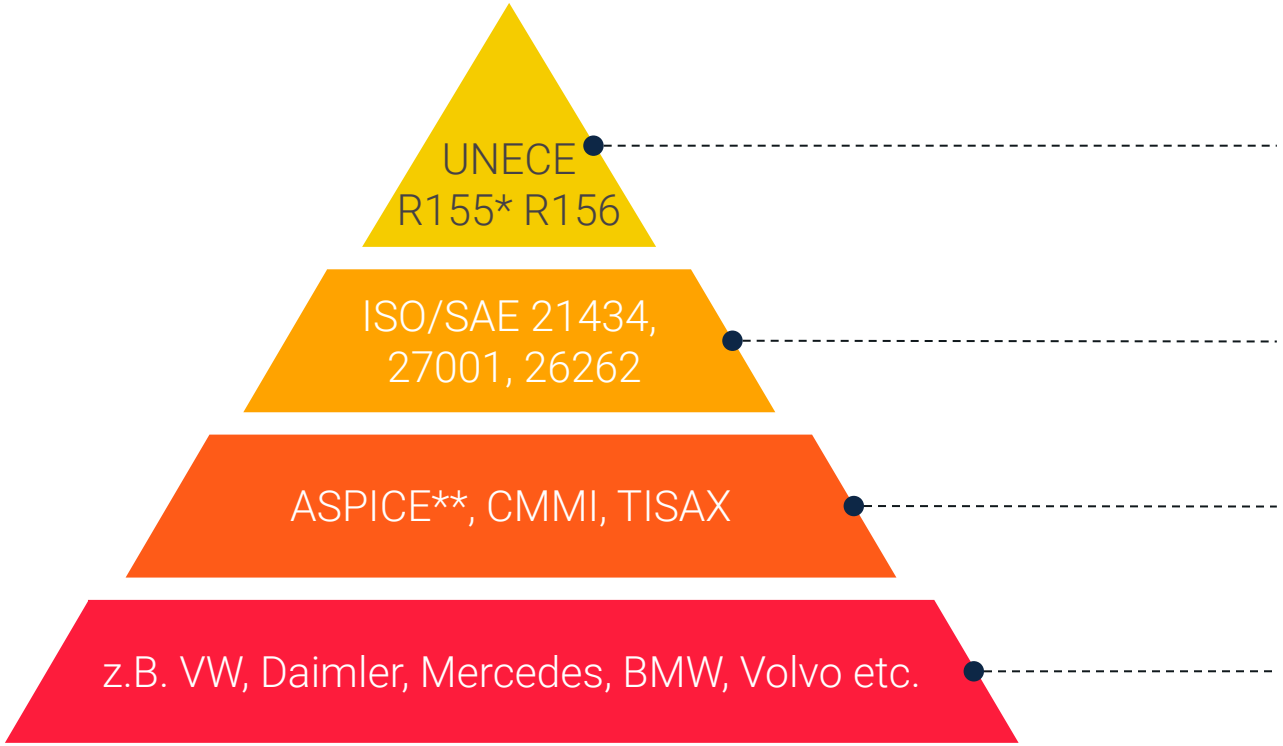
Example Automotive – end-to-end security is necessary

All connections to the outside and inside must be protected



Regulations for automotive CSMS set by UNECE law

Implementation through co-applicable standards and overarching, as well as internal company lines



Laws (e.g. worldwide, EU-wide, state-wide)

Standards (e.g. USA, EU, etc.)

Guidelines/assessments
(e.g. from associations (VDA), etc.)

Internal company guidelines

*UNECE R155 „UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (CSMS)"
**ASPICE: Automotive Software Process Improvement and Capability Determination

The UNECE-WP.29* sets requirements for the OEM from the automotive industry

OEMs must adapt their organization and processes

Cyber Security (ISO/SAE 21434, UN R155)

Cyber Security Management System (CSMS)

External certification valid for three years

- Risk management in processes is implemented
- Processes for risk handling are established

Vehicle requirements

Type testing

- Proof of vehicle safety and cyber security over the entire product life cycle

Software Updates (ISO/SAE 24089, UN R156)

Software Update Management System (SUMS)

External certification valid for three years

- SW update management processes are established
- Security and OTA requirements are secured

Vehicle requirements

Type testing

- Compliance with requirements SW updates and OTA updates throughout the lifecycle

UNECE-WP.29 ("World Forum for Harmonization of Vehicle Regulations")
Working Group GRVA ("Working Party on Automated/Autonomous and Connected Vehicles")

* WP.29 UNECE Working Group, World Forum for Harmonization of Vehicle Regulations

Focus on organization and processes

Focus on vehicle and end-to-end technologies

Legal Regulation for Automotive Cyber Security

UNECE R155/R156

Evidence of how the processes related to cyber security management are subject to a continuous updating process and are thus always up to date

Evidence of an appropriate approach to risk management in relation to suppliers, service providers or other third parties

Demonstrate how cyber risks are managed from identification to categorization, assessment, and treatment

Evidence of how cyber security is verified from development is checked and validated throughout the production phases

Demonstrate cyber security tools, processes, and technologies to monitor, detect, and respond to cyber threats, -vulnerabilities and attacks

Demonstration of processes suitable for special use cases

MCS consulting approach

CSMS – Cyber Security Management System

Our approach integrates cyber security holistically and sustainably into the organization

Empowerment Management

Cyber security awareness and importance; Announcements by top management/corporate culture
Scope/goals

Audit

Independent effectiveness monitoring of the cyber security management system (audit)

Cyber Security Effectiveness Monitoring

Monitoring of the effectiveness and efficiency of the cyber security management system and continuous improvement

Cyber Security Transformation

Implementation of cyber security measures

Enablement, Qualification & Communication

Informing and training employees about cyber security risks

Redesign organization & processes

Establishment of the organizational structure; Roles, responsibilities and processes

Risk Identification

Systematic and holistic approach to identifying and assessing cyber security risks

Risk Management

Measures to mitigate cyber security risks

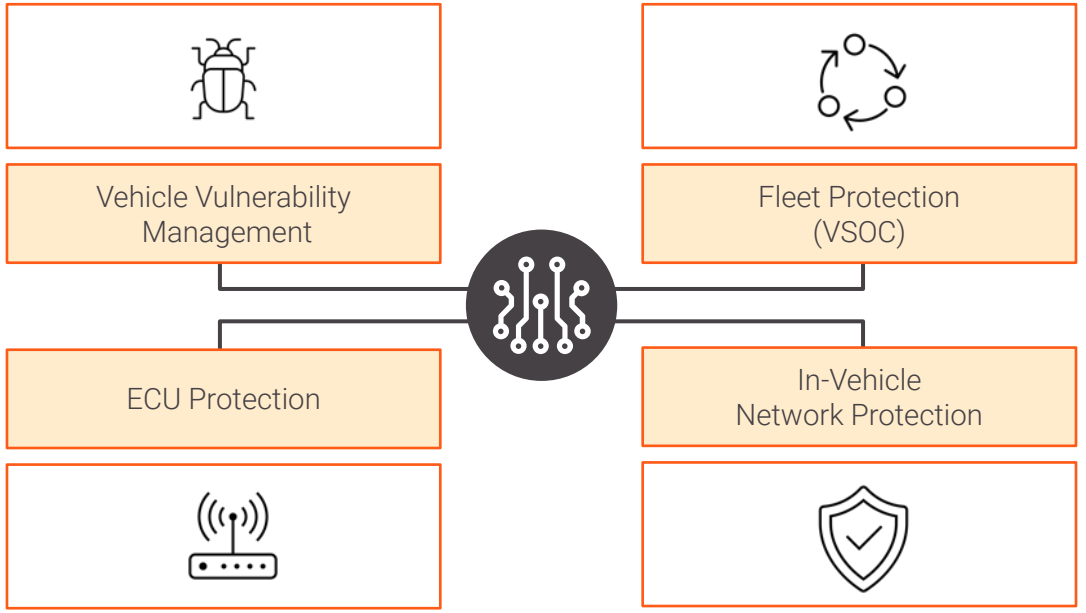
- CSMS Targets set by management
- Organization setup
- Cyber Security Framework

The magility ecosystem enables CSMS implementation as a one-stop shop

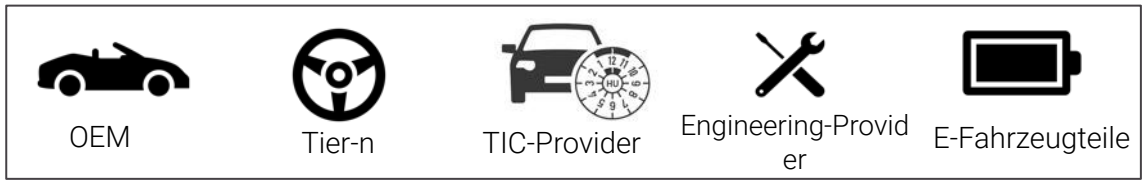
Holistic technology footprint across the entire value chain and end-to-end

Cyber Security Process Footprint – Core Competence MCS

Cyber Security Technology-Footprint – Core Competence Ecosystem



Our references – a selection



The certification process for OEM for a CSMS compliance test

OEMs must be able to demonstrate compliance at any time to a certified authority or service

Phase 2 – CSMS Evaluation and Review

- by technical service and assessment based on maturity level in relation to necessary requirements by approval authority

Phase 1 – CSMS Consulting and Implementation

- Ensuring cyber security throughout the lifecycle and value chain
- Processes for risk assessment, testing, monitoring and response
- OEM is supported by magility and Argus

Phase 3 – CSMS Compliance Certificate

- Required for future approval for type testing
- State authority can check, reissue or withdraw validity at any time
- State authority: KBA (Federal Motor Transport Authority)

MCS provides support for the implementation of a CSMS

Phase model approach for sustainable project progress

1. creating an understanding of **WP.29** and evaluating the requirements

2. deriving the corresponding **organizational implications**

3. setting up an action plan, adapted to the maturity l**evel of the organization**

4. internal **check audit** and subsequent **implementation of measures**

The MCS consulting approach is customer-specific scalable

Detailed and sustainable support in all or only individual phases

1 STATUS QUO ANALYSIS

- Carrying out the detailed CSMS as-is analysis of the company
- Inventory for further strategy definition

2 CONCEPT/ BUSINESS MODEL

- Further development of the CSMS by setting the goals
- Derivation of the strategy in the areas: products, services, processes, competencies

3 IMPLEMENTATION/ TRANSFORMATION

- Support of the CSMS implementation and transformation process
- Involvement of all stakeholders for targeted and holistic implementation

Contact

Your contact to magility cyber security

Magility Cyber Security GmbH | Heinrich-Otto-Str. 71 |
73240 Wendlingen am Neckar | Germany

+49 177 698 2021 | contact@magility-mcs.com | www.magility-mcs.com

magility

together. cyber. secure.

Disclaimer

Magility Cyber Security GmbH

Liability for contents

As a service provider, we are responsible for our own content on these pages in accordance with § 7 Para. 1 of the German Telemedia Act (TMG). However, according to §§ 8 to 10 TMG, we are not obliged as a service provider to monitor transmitted or stored third-party information or to investigate circumstances that indicate illegal activity. Obligations to remove or block the use of information in accordance with general laws remain unaffected by this. However, liability in this regard is only possible from the point in time at which a concrete infringement of the law becomes known. If we become aware of any such infringements, we will remove the relevant content immediately.

Although the greatest possible care has been taken in the preparation of this presentation, we cannot accept any liability for the completeness, up-to-dateness or correctness of the information contained therein. The information in this documentation is provided for information purposes only and should not be construed as an offer or public advertisement soliciting the use of services.

Liability for any damage or loss claimed on the basis of the information contained in this documentation is excluded.

Liability for links

If there are links to external websites in our presentation, we have no influence on their contents. We do not assume any liability for external contents. The responsibility for the contents of linked pages always lies with the respective provider and operator of the pages. Constant monitoring of the content of linked pages is not reasonable as long as there are no concrete indications of a violation of the law. If such become known, we will remove such links immediately.

Copyright

Managing Director: Dino Munk | Magility Cyber Security GmbH | European Metropolitan Region Stuttgart
Heinrich-Otto-Str. 71 | 73240 Wendlingen am Neckar | Germany
E-Mail: dino.munk@magility-mcs.com | Tel. +49 177 698 2021
Stuttgart | HRB-Nummer 78 4630
www.magility-mcs.com