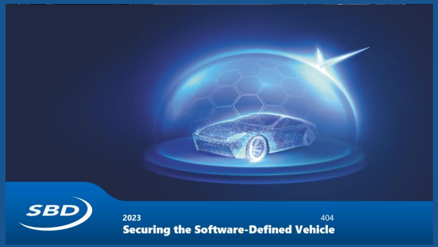


TABLE OF CONTENTS

RELATED SBD REPORTS

402 – Software Defined Vehicle Forecast

The Software-Defined Vehicle Forecast provides a grounded assessment of the growth enabling SDV technologies in different regions and vehicle segments. Its ten-year forecast understands how major OEM groups will deploy future E/E architecture elements, while assessing how these elements are expected to evolve. An adjacent Excel version offers detailed, data-driven, analysis sorted by brand and country in addition to revenues.

SBD

#404

SEC

Security

Securing the Software-Defined Vehicle

In recent years, software has become a mutual focus for many automakers across the industry and around the globe. Legacy OEMs, automotive brands, and newer start-ups alike are increasingly integrating technologies that put software first in many areas of the vehicle lifecycle – from its design and core user experience, through to the ways it can help maintain and extend the lifecycle.

While this focus continues to shift from hardware to software, and from discrete ECUs to advanced computing systems, new cyber security threats and attack points that exploit their vulnerabilities will be introduced. As such, OEMs and suppliers working with, or producing, a software-defined vehicle must be well equipped to manage new risks while adopting new mitigation technologies.

SBD Automotive's Securing the Software-Defined Vehicle report takes a detailed, chip-to-cloud look at SDVs. In doing so, it provides a high-level threat model of a typical SDV architecture and identifies the best practices for preventing, detecting, and containing malicious cyber security attacks at each layer of the technology stack. For IT and security teams newly supporting the development of a SDV, the report maps out the key differences between traditional and SDV architectures from a cyber security perspective.

COVERAGE	FREQUENCY	PUBLICATION FORMAT	PAGES
GLOBAL NA CHINA EUROPE	ANNUALLY QUARTERLY 1 ONE-OFF	PDF POWERPOINT EXCEL ONLINE	150+

Request price ›

Key questions answered

- > What are the fundamental differences from a cyber security point of view between a traditional vehicle architecture and an SDV?
- > What new attack points does an SDV introduce and how will OEMs need to change their approach to protecting their vehicles?
- > What are the emerging solutions for securing SDVs and where are the gaps that may require further research and development?
- > What impact will the shift to SDV have in terms of initial and on-going compliance to UNECE R155?

This research supports

Product Planners

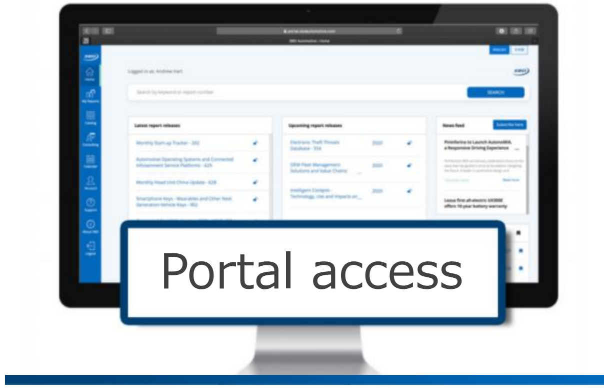
Cyber

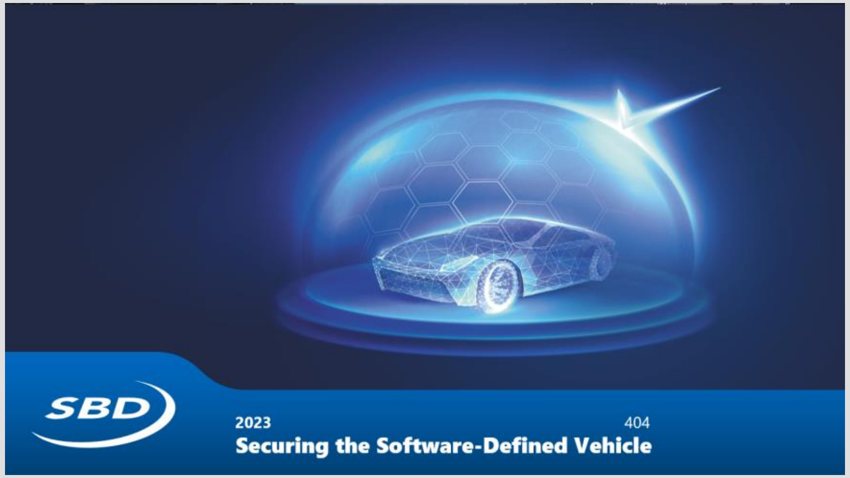
IT

Engineering

Do I have access?

100+	50k+	4,000+
Reports published per year	Slides of insights, forecasts & data	# of auto professionals who access our reports




SBD

2023

404

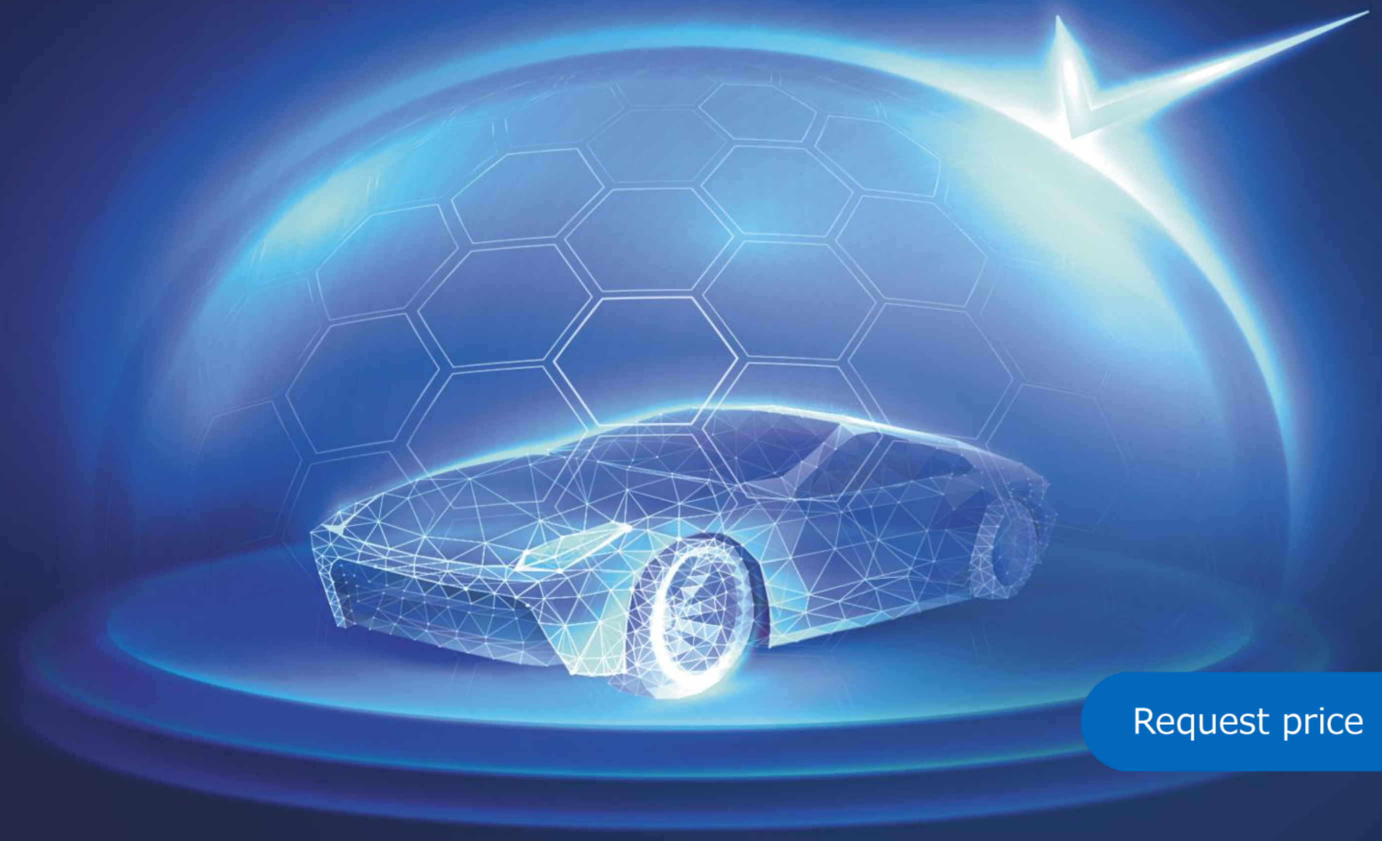
Securing the Software-Defined Vehicle

Request a quote for

Securing the Software-Defined Vehicle

One-Off Report for 2023

Request price >



Request price

SBD

2023

Securing the Software-Defined Vehicle

404

Introduction

Introduction

The transition towards software defined vehicles is already enabling OEMs to realize opportunities which could not be achieved with traditional automotive architectures. New technologies are bringing more features to the vehicle, and also to the OEM business model. Thanks to more advanced software and hardware, the automotive industry can provide safer features, more convenient operations and a better user experience. However, at the same time, the automotive security mindset needs to be updated, as the risk of vulnerabilities also increases because of the increasing number of attack surfaces.

Automotive security is already being taken seriously. In recent years, cybersecurity attacks on vehicles have resulted in serious impact to financial, safety, operational and privacy aspects. Making the industry aware that building a holistic standard that considers security in the early project development, and that working across the industry, is vital to protect vehicles from potential attacks.

Technologies keep evolving, which presents more challenges that stakeholders need to react to. For example, quantum computing and digital twins' applications are bringing new security vulnerabilities. Stakeholders need to adopt an agile and comprehensive approach to address incoming threats. In the early phase of product development, the stakeholders need to adopt a security mindset to conduct the potential threat analysis and deploy forward-looking security mechanisms.

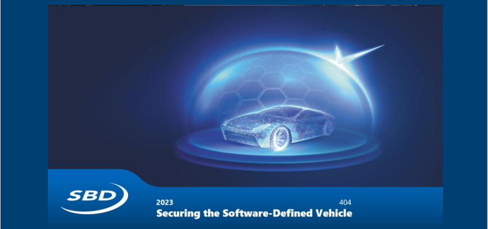
The motivation of attackers comes from various perspectives. New targets now include private user data and bypassing the FaaS to gain financial benefits. In the foreseeable future, more forms of attacks will emerge.

This reports discusses the security-related topics for each of the five layers of the SDV. These are Cloud, Chipset, Software, E/E and Organization & Strategy. The vulnerabilities of each layer, potential impacts, source of threats, security goals and what solutions can be considered for deployment.

A simplified version of TARA modelling is provided to help cybersecurity engineers consider various aspects before deciding the best security mechanism.

	Content
Bird's Eye View	A brief overview of the journey to the Software Defined Vehicle, considering the different layers of the SDV, and SBD's SDV Report Series.
Executive Summary	From the security point of view, the chapter evaluates what are the key approaches considered to follow, the impact, threat, limitation, goals and solutions in each SDV layer.
The Basics	What do you need to know about Software Defined Vehicles? What does SDV mean to security strategy?
Analysis	Five SDV layers (Chipset, Cloud, E/E, Software and Organization & Strategy) analysis, including the cybersecurity assets analysis, impact analysis, threat analysis, limitation analysis, Goals analysis and Solution analysis. A simplified TARA modelling is also conducted for reader example
Next Step	How SBD can help?

Example slides from the report



SBD

2023

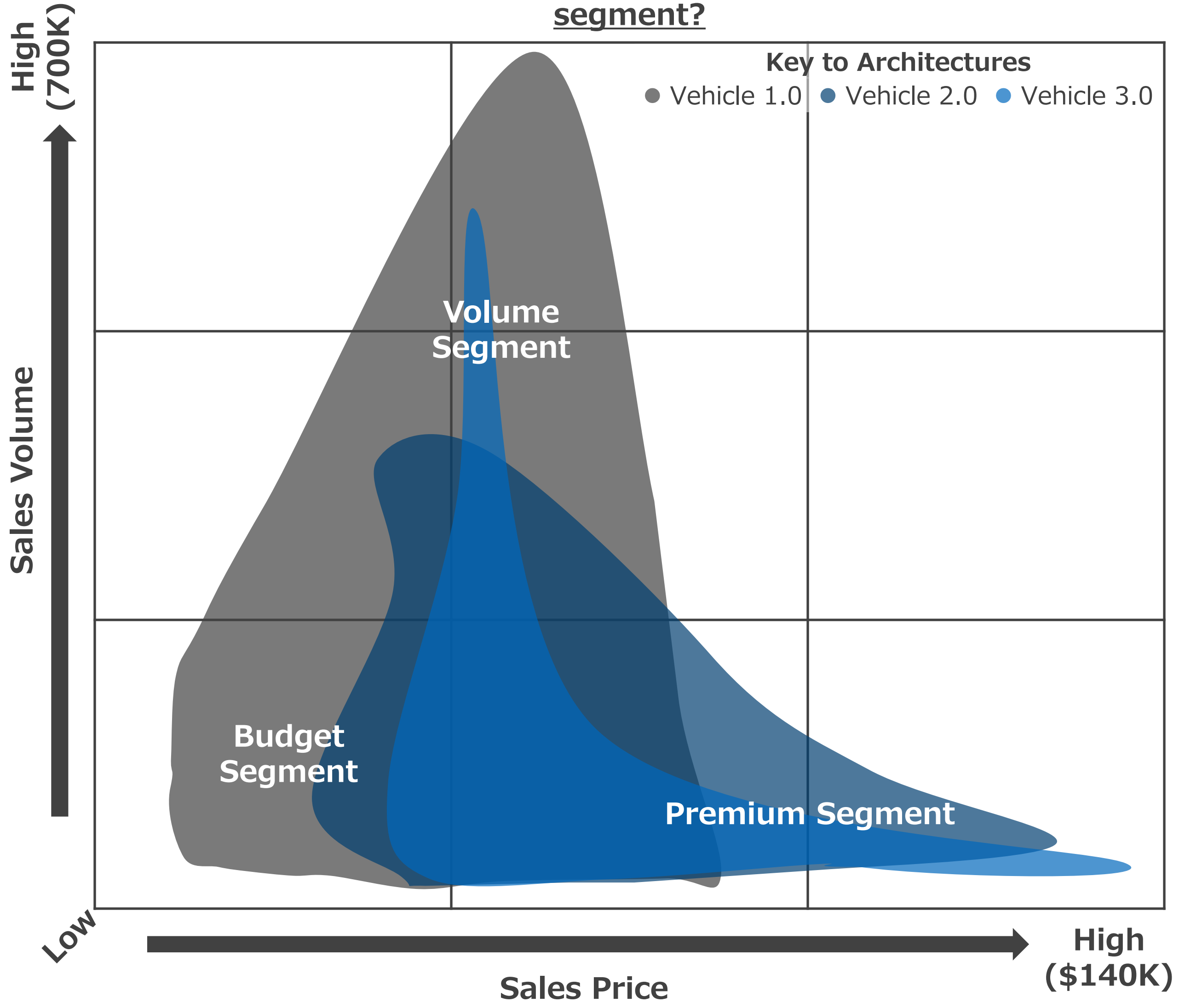
404

Securing the Software-Defined Vehicle

Request price >

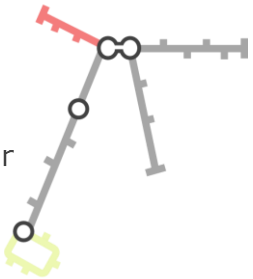
Vehicle 4.0 will evolve across the volume and premium segments

Which generation of architectures are used in which market segment?



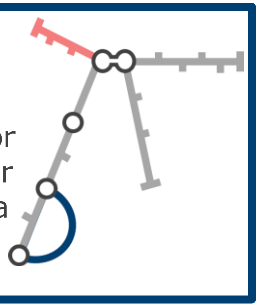
Vehicle 1.0

CAN based topology built around a gateway module. May feature **MOST** or **Flexray** for specific functions



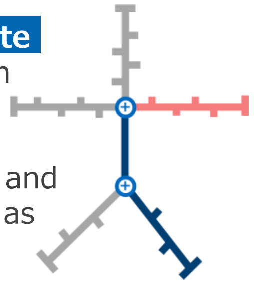
Vehicle 2.0

Introduction of secondary point-to-point high bandwidth **Ethernet** channels for specific functions - for example connecting a modem to infotainment



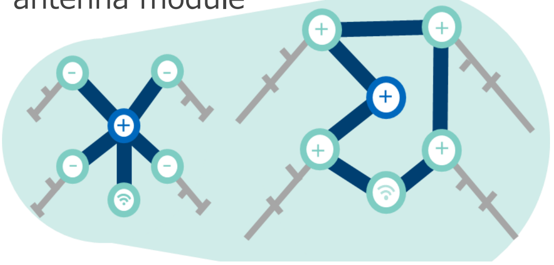
Vehicle 3.0

Centralized Compute or Functional Domain High Performance Compute with decoupled software, and Ethernet being used as a primary network



Vehicle 4.0

Scalable network from distributed **Zonal 'Switches'** to **Zonal Computes**; perhaps with an ethernet ring and a smart roof zone antenna module



E/E Architecture Guide

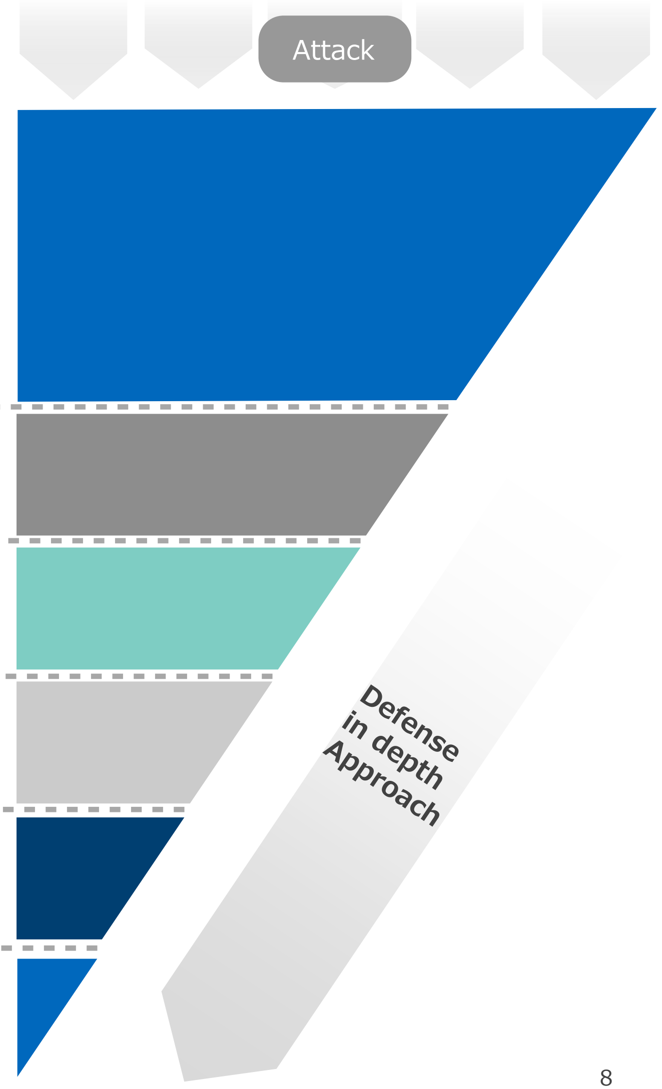
Right decisions on E/E architecture leads to increased vehicle safety, security, and system usability

Learn more ❯

SDV calls for defence-in-depth with a secure by design approach

OEMs need to prioritize security decisions based on the impact of the functions they protect and move away from prioritizing primarily on attack feasibility. This multi-layered methodology should be the basis for any new vehicle development.

Chipset	Cloud	E/E	Software	Organization and Strategy	
ECU Auth (PUFs) Secure Diagnostics Secure Debug	IAM Message-level protection API management Secure gateways Firewall Penetration testing	Secure Gateway Message-level protection mTLS IP-SEC MAC-SEC Segregation of networks Network IPS	App Vetting Code Signing Sandbox Secure boot Secure Storage Crypto agility	Training Regulatory Compliance DevSecOps IAM Simplify organizational complexity Supply chain and open-source oversight	Prevent
	VSOC Monitoring Resources IAM	Network IDs	Host IDS	IAM VSOC Monitoring team Cyber team building	Detect
	VSOC Cloud containerization IAM	Network IPS V2X isolation	Host IPS Sandbox	VSOC Cyber team building Simplify organizational complexity Strong SIEM team Regulatory compliance	Contain
Secure Execution	Cloud backups OTA Updates			Strong backup/ recovery team Simplify organizational complexity Cyber team building	Recover
	OTA Updates Cloud backups Penetration testing		OTA Updates	OTA team starting with R156 VSOC Cyber team building	Fix
	Tamper-proof data storage Penetration testing		Forensic Storage	Data Forensics team Cyber team building	Forensics



New features, software, technologies keep evolving, which requires continuous monitoring

Middleware

Signal-based communication (Classic AUTOSAR) has been replaced with service-oriented communication (Adaptive AUTOSAR), in which new applications can be easily integrated into the entire system.
For OTA software updates, Adaptive AUTOSAR provides key functions for purposefully updating features and components. Classic AUTOSAR requires a full update of the application software. Adaptive AUTOSAR supports differential updates.

Centralising

A high-performance computing (HPC) system in E/E architecture is a centralized computing platform used to process large amounts of data and perform complex calculations. Both OEMs and suppliers are rolling out vehicle HPCs. The presence of such HPCs makes this new architecture vulnerable for cyber attacks, especially if strong security measures are not thoroughly considered. Centralized architecture may unify attackers to focus on the core

Virtualizing

Centralized architecture drives the need for hypervisors. Hypervisors support multiple functionalities on the same device. Hypervisors allocate resources to the SDV virtual machine, providing a configurable, controllable interface between applications and the vehicle.

Known hypervisor vulnerabilities like device escape and memory corruption can have catastrophic effects on the vehicle when the combination of mixed criticality functions are running on the same core.

More personalization

The technologies enable more advanced personalization features are being implemented in the vehicles. Biometrics is expected to be increasingly implemented in various areas, including vehicle access, user authentication, shared services, etc, which will expand beyond the basic safety authentication functions.

Managing the biometric data is a new task for security engineers as the increased privacy requirement.

Innovative Technologies

Looking forward, stakeholders need to consider to react to those emerging technologies, including quantum computing, Neuromorphic computing, Affective computing, mesh networking and 6G, Digital Twin, satellite networking, etc.

A process to evaluate the potential impact from these technologies need to be established and implement corresponding technologies to mitigate the risks.

Implementing security mechanism on Chipset is not straight-forward

Cyber assets
Impact
Threat
Limitation
Goals
Solutions

1	**Complexity of the hardware architecture**	Automotive SoC with multiple computing islands and heterogenous architecture is complex. Complex automotive SoC host powerful software functionality, which increases system vulnerabilities and threats. The security spans multiple computing nodes of different design and capabilities on the same chip. Meanwhile there are **significant differences in SoC architecture** at the different level of usage.
2	**No easy fix for Semiconductor Chips**	Software vulnerabilities cannot be fixed by patching and rebooting once they have been identified. Cybersecurity implementation in chipset requires a **proactive product planning in the early phase of development**. This puts a heightened emphasis on the identification and proactive design of strategies to mitigate potential vulnerabilities. Any chip vulnerability detected by an OEM late in the design cycle will delay the delivery of vehicles to customers.
3	**Long lifecycle**	Semiconductor chips are designed to maintain functionality for over a decade. The long lifecycle means a higher cost because security measures must be well-built to protect against **threats that may emerge throughout the chip's operational lifespan**.
4	**Hard to define the robustness**	There is an increasing risk of cyberattacks and unauthorized access. The performance requirements are being enhanced so the security solution should be robust. It is **difficult for manufacturers to validate the robustness of the chipset's cybersecurity countermeasures** as the attack method is evolving daily.
5	**Improved need for cryptographic processing**	Due to the increasingly **large amount of streaming data** from sensors and cameras to serve new emerging SDV functionalities, it is hard for only one HSM in one ECU to handle the whole cryptographic processing. This is due to the high security demand on performance. Cryptographic platforms need to process large amounts of data in a time sensitive-manner. One option to meet the increasing need is to set several security processing modules outside HSM and to consider an embed security accelerator on the chip.

The shift to the cloud-trust

Cyber assets
Impact
Threat
Limitation
Goals
Solutions

Secure Diagnostics

If the service tools provided to dealers and 3rd parties have no security mechanism applied, it can become a vulnerable point to be attacked. Hackers can utilize the chance to crack the security features and reverse-engineer the shared security keys on the tool itself.

One solution is to adopt a cloud-based crypto solution to prevent key sharing and support role-based authentication. By implementing the end-to-end authentication between the ECU and Cloud, the reliance on diagnostics tools can be further reduced to avoid associated risks.

Some OEMs are adopting the new ISO standard known as UDS service 0x29, which includes the key standards of making the diagnostics more secure, for example, the back-end authentication for diagnostic security access, compared to the older service 0x27 solution that relies on device security.

Cost

Low	**Medium**	High

Maturity

Theoretical	In development	**Ready to use**

When it fits

Planning	Design	Development	**Operations**

Where it fits

Prevent	Detect	Contain	Recover	Fix	Forensics

Advantages/strengths	Disadvantages/challenges
Reduce the risks associated with the cryptographic keys stored in service tools.	The implementation should consider some other legislation, for example, right to repair.
Supports differentiated role-based authentication	Requires a new diagnostics infrastructure to be deployed globally

Attack resistance

Spoofing:	High
Tampering:	Medium
Repudiation:	Low
Information Disclosure:	Low
Denial of Service:	High
Elevation of Privilege:	Medium

Threat modelling example – Threat analysis

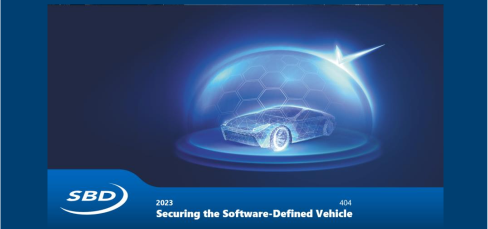
- Cyber assets
- **Impact**
- Threat
- Limitation
- Goals
- Solutions

	Assets	Cyber properties			Damage scenario	Impact Analysis			
						S	F	O	P
V2X	Vehicle module storage	C	I	**A**	Safety impact resulting from the loss of confidentiality of the vehicle V2X module storage	M			
	Vehicle module storage	C	**I**	A	Operational and safety impact resulting from the loss of integrity of the vehicle module storage	M		H	
	Vehicle module runtime	C	I	**A**	Safety impact resulting from the loss of availability of the vehicle module runtime	M			
	Interface to HPC	**C**	I	A	Operational and Privacy losses resulting from loss of Confidentiality of diagnostics interface			H	M
	V2X wireless interface	C	I	**A**	Operational and safety loss resulting from loss of Availability of the vehicle V2X wireless interface	M		H	
	Vehicle Module	C	**I**	A	Safety, Financial, Operational and Privacy loss resulting from loss of Integrity of the V2X vehicle module	H	M	H	M
HPC	HPC communication interfaces	C	I	**A**	Safety and Operational loss resulting due to loss of Availability of the HPC comms interfaces	H		H	
	ADAS sensor safety critical data	C	**I**	A	Safety and Operational loss resulting due to loss of integrity of the ADAS sensor safety critical data	H		H	
	HPC storage	**C**	I	A	Privacy losses due to extraction of raw in-vehicle operational data from the HPC storage, resulting in loss of confidentiality				H
	HPC runtime	C	**I**	A	Safety impact resulting from the loss of availability of the vehicle's HPC runtime	H			
FaaS	Vehicle configuration	C	**I**	A	Safety and Operational impact due to loss of the integrity of the vehicle configuration	H		H	
Edge computing	In-vehicle module	C	**I**	A	Safety and Operational impact due to loss of integrity of the Edge computing in-vehicle module	H	M	H	

Impact Analysis – **H** – High **M** – Medium **L** - Low

Cyber Properties – **C** - Confidentiality, **I** - Integrity, **A** - Availability

Request the price



2023 404

Securing the Software-Defined Vehicle

Request price >

Contact SBD Automotive

Do you have any questions?

If you have any questions or feedback about this research report or SBD Automotive's consulting services, you can email us at info@sbdautomotive.com or discuss with your local account manager below.

✉ info@sbdautomotive.com

Book a meeting

USA | UK | Germany | India | China | Japan

Garren Carr
North America
garrencarr@sbdautomotive.com
+1 734 619 7969

Luigi Bisbiglia
UK, South & West Europe
luigibisbiglia@sbdautomotive.com
+44 1908 305102

SBD China Sales Team
China
salesChina@sbdautomotive.com
+86 18516653761

Andrea Sroczynski
Germany, North & East Europe
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

SBD Japan Sales Team
Japan, South Korea & Australia
postbox@sbdautomotive.com
+81 52 253 6201