SERVICE-ORIENTED VEHICLE DIAGNOSTICS

WHITEPAPER

Jay horak
OPUS IVS
August 2025

TABLE OF CONTENTS

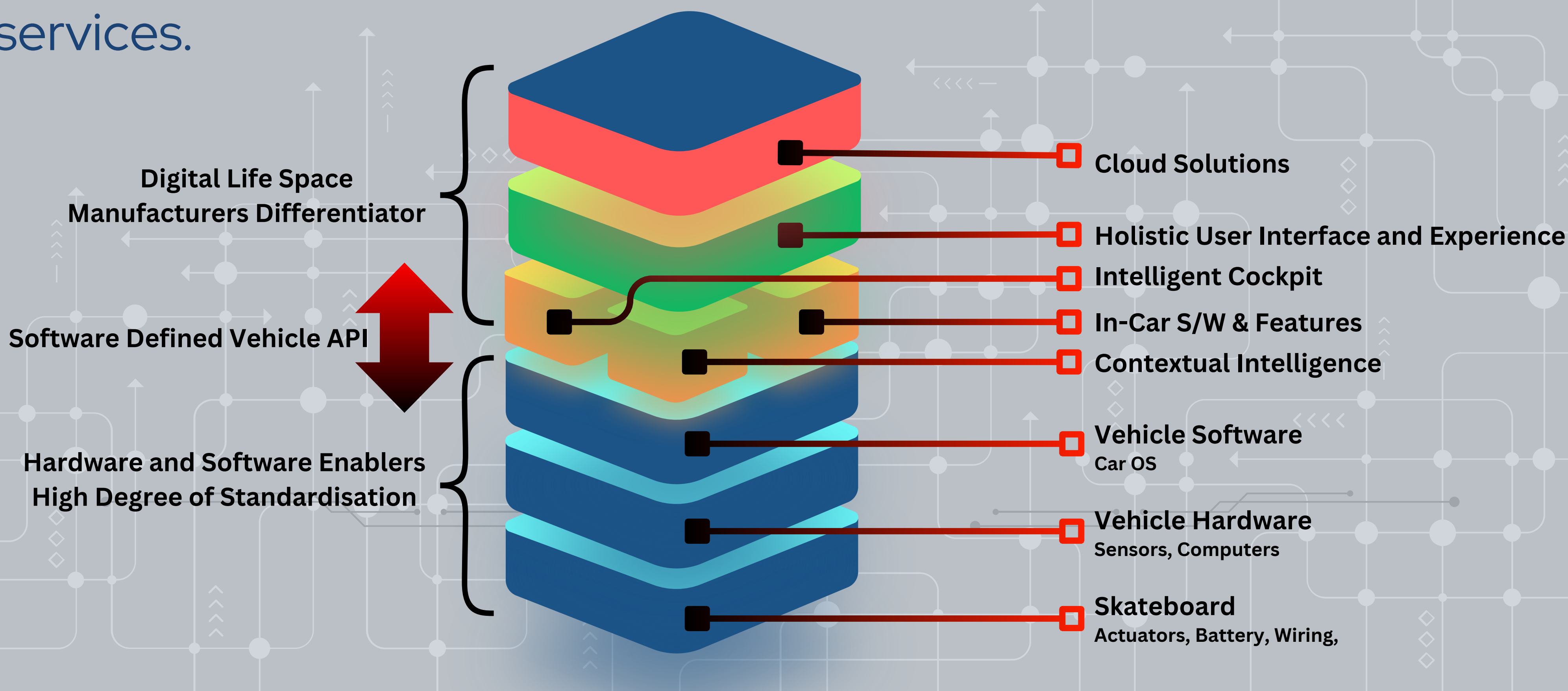
Preface :

This whitepaper was prepared by Jay Horak of OPUS IVS, an ETI member company, to support broader industry understanding of Service-Oriented Vehicle Diagnostics (SOVD). The views, interpretations, and technical insights presented herein are those of the author and do not necessarily reflect the official position of the Equipment and Tool Institute (ETI).
ETI maintains a neutral stance in matters involving OEM strategy, tool design preferences, or regulatory interpretation. Our goal is to provide a forum for technical collaboration, education, and open dialogue among all stakeholders in the automotive service ecosystem.

INTRODUCTION:

The automotive industry is undergoing a significant transformation with the rise of software-defined vehicles (SDVs). Traditional vehicle diagnostics, primarily based on UDS (Unified Diagnostic Services) over CAN or DoIP, are no longer sufficient to manage the growing complexity of modern vehicle electronics. In response to these challenges, Service-Oriented Vehicle Diagnostics (SOVD) emerges as a forward-looking diagnostic architecture.

SOVD redefines diagnostics by leveraging web-based standards such as HTTP/REST and JSON, promoting a more flexible, modular, and scalable approach. Rather than relying on hard-coded byte-level commands, SOVD facilitates high-level, human-readable interactions between diagnostic clients and vehicle modules. This paradigm shift allows for greater interoperability, especially as vehicles become more connected and reliant on cloud-based services.



INTRODUCTION:

- On its face SOVD is a dynamic distribution of vehicle module data sets
- GOAL:
  - Simplifies the data set distribution by including it with the module instead of separately
  - Standardizes the distribution model using a txt-based command / request exchange
  - Allows dynamic distribution of data sets
  - Allow for more specific control through procedures as opposed to sending bytes
  - SOVD accomplishes this by using a defined exchange language that allows for the transmission of data sets. More specifically an exchange of functions and features for a vehicle module
- Motivation for SOVD is the large data sets for HPCs and large module sets

SUPPORTING COMPANIES:

OEM Adoption of SOVD (Indicative Overview)

SOVD is being explored and implemented by multiple global vehicle manufacturers, particularly those transitioning to centralised and software-defined vehicle (SDV) architectures. While public disclosure varies, the following groups have either released technical documentation aligned with SOVD principles or are known to be piloting the architecture through industry collaboration:

- Several German premium OEMs have implemented SOVD for diagnostics over Ethernet, particularly in EV and high-performance platforms.
- Luxury and performance divisions within major automotive groups are using SOVD as part of their shift to modular, updatable vehicle platforms.
- Global OEMs in North America and Europe have shown alignment with SOVD as part of broader cloud diagnostics and OTA update strategies.
- Electric vehicle pioneers and new entrants are adopting SOVD-like architectures to simplify in-vehicle service integration and remote diagnostics.
- Tool vendors and Tier 1 suppliers report increasing demand for SOVD support in vehicle ECUs and test systems, especially those built on AUTOSAR standards.

This indicative list reflects the general trend toward service-oriented diagnostics, even where full public declarations of SOVD adoption are not yet available.

HOW DOES SOVD WORK?

At its core, SOVD enables service-based communication between a diagnostic tool and vehicle control units (ECUs). This is achieved through a layered architecture:

- The transport layer utilises HTTP, ensuring compatibility with existing internet infrastructure.
- Data is transmitted using JSON, providing a structured and readable format for requests and responses.
- Access is gated by Secure Gateways (SGWs), which use OAuth2 or certificates to authorise communication.

This setup enables tools to dynamically request available diagnostic services from a module, and interact using standardised function names like 'readDTCs' or 'performActuation'. These abstracted services replace legacy commands, simplifying integration and promoting transparency.

USE CASES AND BENFITS:

SOVD is designed to meet the needs of a connected, digital automotive ecosystem. Its use cases include:

- Remote diagnostics: enabling OEMs or third parties to access vehicle data over-the-air for fault analysis.
- OTA feature enablement: activating premium features post-sale through authenticated service calls.
- Predictive maintenance: feeding real-time diagnostics into analytics platforms to schedule servicing proactively.
- Line diagnostics: supporting automated testing of vehicles during production.
- Independent access: potentially enabling secure, vetted access for non-OEM tools under Right to Repair frameworks.

These capabilities provide cost savings, faster issue resolution, and improved vehicle uptime for all stakeholders.

ARCHITECTURE OVERVIEW:

SOVD architecture aligns closely with modern IT systems. Vehicle ECUs act as servers, hosting diagnostics services. A diagnostic client sends RESTful requests to these endpoints, and receives JSON-formatted responses. This modular design is highly scalable, especially as vehicles adopt centralised computing models.

Secure Gateway (SGW) acts as an access controller, ensuring that only authorised users can interact with sensitive functions. Communication flows can extend beyond the vehicle to cloud services, enabling powerful new diagnostics paradigms such as remote testing or AI-assisted issue triage. This distributed model is particularly effective for fleets, EV platforms, and complex modular ECUs.

TECHNICAL DEEP DIVE:

Traditional diagnostics relied on proprietary data and byte-specific commands, often hidden behind expensive licensing schemes. SOVD revolutionises this by offering a transparent, extensible model based on open technologies. Each SOVD-capable module exposes a set of endpoints representing supported functions. These can be queried with requests such as: { "action": "getSupportedServices" }

Responses are structured JSON objects that may include diagnostic routines, sensor data access, or control commands. This model allows for asynchronous operations, essential for long-running tasks such as firmware updates or calibration routines.

The use of human-readable descriptors and standardised schemas enables faster development, easier debugging, and better cross-OEM tooling.

SOVD BLIND SPOTS:

Standards Aren't Always A Standard

Despite its advantages, SOVD faces challenges rooted in implementation inconsistency and the history of failed standardisations. Different OEMs may interpret the specification differently, leading to fragmented tooling support. Similar issues plagued earlier formats such as ODX and even Excel-based data sets, where inconsistent layouts made universal parsing difficult.

Language localisation is another concern, with many JSON responses relying on human-readable terms that may include errors or regional terminology. Without strict enforcement of a naming convention or translation layer, global deployment remains a challenge.

Lastly, while the interface is technically defined, OEMs may still implement proprietary protections or limit functional access under different policies.

SOVD HEADWINDS:

SOVD requires specific technologies that are at the center of legal challenges.

SOVD's technical model introduces potential vulnerabilities, especially around data access and encryption. If each module contains its full feature/function set, every deployed vehicle becomes a potential target, if you sell 6 million cars, you have six million possible breaches. While SGWs mitigate some of this risk, they are also at the centre of legal challenges tied to Right to Repair and DMCA.

A successful challenge to SGW use could undermine the entire SOVD model. Additionally, offline vehicles may be left without robust protection, requiring Mode 27 locks or similar security mechanisms to prevent tampering.

This friction between openness and security continues to be a central issue in the evolution of diagnostic frameworks.

SECURITY MODEL:

Security is a cornerstone of SOVD design. It uses OAuth2 tokens or cryptographic certificates to verify the identity and permissions of any client tool. These credentials are validated by the Secure Gateway before any diagnostic operation is authorised.

All communication is conducted over encrypted HTTPS (TLS), protecting against eavesdropping or tampering. Vehicle-side logging enables traceability, and misuse can trigger alerts or revocation of access rights. This framework supports remote access policies, ensuring even off-board tools operate within controlled parameters.

ECOSYSTEM IMPACT:

The introduction of SOVD will reshape the diagnostic and repair ecosystem:

- OEMs will benefit from improved security and consistent service interfaces.
- Tool manufacturers will face the challenge of supporting web-native architectures.
- Repair workshops must invest in new infrastructure and training.
- Regulators are being pressured to ensure fair access under Right to Repair frameworks.

This shift is not just technical, but strategic, requiring cooperation across the supply chain to ensure transparency, compliance, and innovation.

FUTURE OUTLOOK:

SOVD is a foundational element for next-generation diagnostics. As vehicles integrate more centralised computing and connectivity, SOVD will serve as the diagnostic backbone for SDVs. Emerging trends include:

- AI-driven diagnostics using structured JSON logs.
- Digital twins for simulation and service forecasting.
- Cloud-native diagnostics, enabling real-time triage at scale.
- Integration with blockchain for audit and traceability.

As standards like AUTOSAR and ISO evolve, SOVD will play a critical role in ensuring diagnostics keep pace with vehicle technology.

GLOSSARY AND REFERENCES:

Glossary:

- SOVD: Service-Oriented Vehicle Diagnostics
- SDV: Software-Defined Vehicle
- SGW: Secure Gateway
- DoIP: Diagnostics over IP
- JSON: JavaScript Object Notation

References:

- AUTOSAR SOVD Specification
- ISO 14229 (UDS)
- ISO 21177
- SAE J1979-3