Contents [hide]

1 NXP Dynamic Networking in the Software
2 Product Information
3 Product Usage Instructions
4 INTRODUCTION
5 FEATURES
6 Industry standards
7 In summary
8 NXP CoreRide networking
9 Customer Service
10 Frequently Asked Questions
11 Documents / Resources
11.1 References

NXP Dynamic Networking in the Software

Product Information

Specifications

- **Product Name:** Software-Defined Vehicle Networking System
- **Manufacturer:** NXP Semiconductors
- **Networking Type:** Software-Defined
- **Features:** Dynamic network configuration, Over-the-Air updates, Real-time adaptability

Product Usage Instructions

Dynamic Network Configuration

- The Software-Defined Vehicle Networking System allows for dynamic network configuration, enabling real-time adaptability during operation and changing scenarios. This feature ensures that network priorities can adjust as conditions evolve.

Over-the-Air Updates

- Throughout the vehicle's lifecycle, utilise over-the-air updates to implement software improvements, new features, and functional enhancements. This process ensures that your vehicle stays up-to-date with the latest advancements.

Standardized Approach

- Efficiently meet diverse requirements by following a well-structured, standardised approach to network configuration and reconfiguration. This method simplifies the process and enhances overall system reliability.

INTRODUCTION

- Today’s and tomorrow’s software-defined vehicles (SDV) have increasingly complex and dynamic network requirements.
- These requirements evolve not only while the vehicle is in operation but also as software is updated, modified, or newly deployed.
- However, complexity is the enemy of scalability, reliability and efficient implementation.
- Standardising network configuration and reconfiguration presents considerable advantages for the automotive industry.

FEATURES

Network configuration for the SDV

- Modern vehicles are now programmed as much as they are built. Traditional automobiles had fixed characteristics and capabilities defined by the physical components assembled on the production line. In contrast, today’s vehicles are highly adaptable, with fundamental attributes – including driving dynamics – determined by software and controlled through semiconductors in tandem with mechanical parts.
- SDVs are not just programmable, but, even more importantly, continuously reprogrammable. Throughout the vehicle’s lifecycle, over-the-air (OTA) updates enable software improvements, new features and functional enhancements.
- This level of adaptability depends entirely on robust in-vehicle networking. Every component must be able to send and receive data, whether continuously or on demand. Network demands vary widely across different vehicle systems.
- High bandwidth and low latency are crucial for safety-critical functions such as collision detection systems. In contrast, other systems, such as turn indicators, require only intermittent, low-bandwidth communication with some tolerance for latency.

- Meeting these diverse requirements efficiently requires a well-structured, standardised approach to network configuration and reconfiguration.

Why SDVs depend on dynamic configuration

- Dynamic network configuration allows real-time adaptability both during operation and in other scenarios. As conditions change, network priorities can adjust accordingly.
- While physical cables and Ethernet switches remain essential, SDV networks are primarily software-defined, allowing for seamless reconfiguration as an inherent design feature.
- This capability for reconfiguration allows for the optimisation of vehicles for the hardware components in specific vehicle models. It can help it achieve better energy consumption and adapt to diverse driving conditions.
- It will improve fault tolerance, with components monitored in real-time and devices reconfigured to help mitigate against any faults. It will help enable predictive maintenance programs to identify vehicle parts or systems that are likely to need attention.
- And it will assist the personalisation and customisation of a vehicle for its user.

- Network requirements will fluctuate based on the vehicle's current operation, necessitating automated, context-aware configuration.
- **Design and construction:** Parts will be installed and networked at different times and different stages of the design, prototyping, production and testing processes.
- **While driving:** Different driving states and circumstances will require the activation,

deactivation and prioritisation of different components, for example, when parking on busy urban streets, when driving on an open highway, or during different times of day and weather conditions. If a fault is detected, the best strategy for mitigating against that fault is implemented.

- **At the garage:** Mechanics will need to be able to test, replace and repair components safely, both in isolation and in concert with the rest of the vehicle's systems.
- **At home:** While the vehicle is parked in its owner's driveway, many components will be switched off or dormant. But others, such as those used for battery charging, door access and security, will need to be operational.
- The ability to rapidly, safely and automatically configure and reconfigure a vehicle's networking infrastructure is thus fundamental to the development of SDVs.
- However, achieving this flexibility is challenging in today's automotive landscape. Car OEMs and their suppliers will select a wide range of components to meet design requirements, manage costs, and integrate best-in-class technologies.
- While this flexibility is essential, the resulting heterogeneity in network components introduces significant challenges for network configuration and reconfiguration.

Key challenges of non-standardised network configuration:

- **Interoperability:** Proprietary configuration standards from different OEMs and suppliers create inefficiencies, requiring additional software adaptations or even extra physical components.
- Integration issues arise when components require intermediaries to communicate, adding complexity that can impact reliability and safety.
- **Scalability:** OEMs benefit from standardised electronic/electrical (E/E) and software architectures that can be reused across multiple vehicle models. Components that require unique configurations for specific parts hinder this scalability, reducing efficiency and increasing engineering overhead.
- **Integration effort and cost:** Custom configurations drive up costs by increasing validation and testing time. These costs extend to maintenance, as any changes to the SDV architecture may require repeated validation to ensure compatibility and reliability.

Cybersecurity: Inconsistent configurations introduce unknown vulnerabilities, expand the vehicle's attack surface and complicate threat mitigation efforts. Standardisation is essential for enforcing uniform security policies across the network.

A common configuration model

- The automotive industry would benefit considerably from a common network configuration model, a universal protocol and language that can be used to program network connections across all devices. This does not require any change in the components used. As discussed, imposing any such constraints would be very much against the interests of manufacturers and consumers. Rather, this is about changing how those components are connected, configured and reconfigured. In the spirit of the SDV architecture, it's much more focused on software rather than hardware.
- In many ways, the benefits of a common configuration model are the mirror-image of the disadvantages of our current non- standard environment.
- Where interoperability is currently a challenge, with a standardised model, it becomes streamlined and seamless, whether components come from one manufacturer or many. Scalability and re-use of code is enabled because network software configurations are written to a common standard and use the same protocols. Development costs and time-to-market are reduced, since validation, testing and ensuring compliance against various industry standards would be simplified due to a reduction in the complexity of the network designs. Equally, cybersecurity is not just simplified, but more effective because of increased visibility across the entire network.

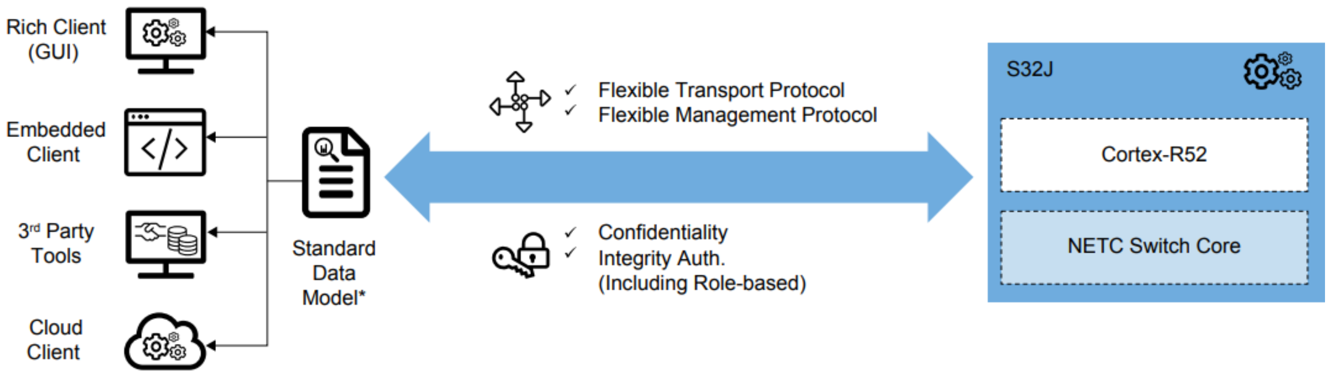
Industry standards

- YANG (Yet Another Next Generation) and MIB (Management Information Base) are both used for network management, but they differ significantly in approach and scope. YANG is a data modelling language designed for modelling the configuration and state data of network devices in a structured way, typically used with NETCONF for automation and dynamic management. YANG supports a wide range of network services and provides better flexibility for modelling complex network configurations, enabling more granular control and configuration. On the other hand, MIB, primarily used with SNMP (Simple Network Management Protocol), offers a static, predefined structure to represent network device data. While MIB is widely used in legacy network management, it lacks the flexibility and extensibility of YANG, particularly when it comes to handling complex, dynamic configurations. YANG is more suitable for modern network management, especially in environments that require automation and real-time adaptability.

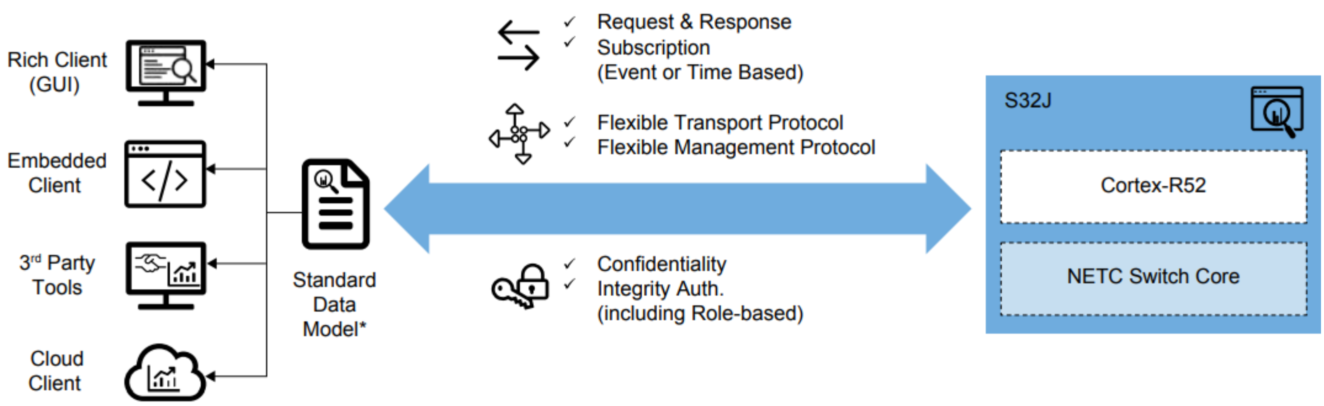
- For automotive use cases, existing YANG models often need extensions to meet the unique requirements of vehicle networks. Traditional YANG models are generally designed for generic networking and communication scenarios, but automotive systems have specific needs. Extending YANG models allows for the integration of automotive-specific requirements, enabling more efficient management of modern vehicle networks.
- Several management protocols are used with YANG, including NETCONF, RESTCONF, gNMI, and CORECONF. NETCONF is widely used for reliable, comprehensive management, offering support for advanced operations. RESTCONF, leveraging HTTP methods, provides a simpler interface, ideal for web-based applications. gNMI, based on gRPC, is particularly well-suited for high-performance, telemetry, and streaming use cases. CORECONF, a more lightweight protocol, offers a streamlined approach with minimal overhead, making it a great choice for environments requiring quick, real-time configuration changes with low-latency demands. Its simplicity and focus on essential configuration tasks make it a compelling option for modern network automation, particularly when ease of use and efficiency are prioritised. While not as widely adopted as NETCONF or RESTCONF, CORECONF's straightforward design ensures it delivers fast and efficient management for network devices.
- CORECONF uses CoAP (Constrained Application Protocol) methods to access structured data defined in YANG. CoAP is a lightweight protocol designed for resource-constrained devices and networks, commonly used in IoT applications.
- It operates over UDP for lower overhead, prioritising speed and efficiency. CoAP follows a client-server request/response model and uses CBOR for compact data encoding. Despite using UDP, CoAP includes features for reliability, like retransmissions and acknowledgements.
- CoAP also supports DTLS for security, ensuring encrypted communication. Its low-overhead design makes it perfect for less powerful devices.
- In some cases, data encoded in CBOR can be transmitted directly over raw Ethernet without the need for a TCP/IP stack. This is particularly useful for resource-constrained devices that don't require the full overhead of a traditional network stack.
- By bypassing the TCP/IP layers, these devices can communicate more efficiently,

reducing latency and conserving resources such as memory and processing power. This approach is often used in specialised applications like industrial IoT or automotive systems, where low-latency communication and minimal resource consumption are essential for real-time operation.

- Standardising the data model is crucial for ensuring consistency and interoperability across various systems, particularly in complex environments like automotive or IoT networks.
- A well-defined data model provides a unified approach for managing configuration, monitoring and control, enabling seamless communication between different components. However, flexibility in the transport protocol is equally essential. Different devices have varying resource constraints, communication needs and network environments. By supporting multiple transport protocols, the system can adapt to these diverse requirements, ensuring efficient and reliable communication across a wide range of devices, from low-power sensors to high-performance controllers.



- Extensions are added only when standards are not sufficient
- **Figure 2:** Standardised configuration options.
- **(Note:** Standardisation started in OPEN Alliance TC-19)



- **Figure 3:** Standardised monitoring and diagnostic options.
- **(Note:** Standardisation started in OPEN Alliance TC-19)

In summary

- The lack of standardised network configuration is adding unnecessary complexity for vehicle manufacturers as they develop the next generation of software-defined vehicles. A unified approach is essential to ensure scalability, security and efficiency.
- This challenge affects the entire automotive ecosystem—OEMs, electronic equipment suppliers, and software providers alike. Addressing it requires a coordinated, industry-wide effort to develop and adopt harmonised network configuration standards. Standardisation is not just a technical necessity—it is a strategic imperative for accelerating innovation while reducing complexity and cost.
- There are gaps in current alternatives for network configuration in automotive-specific use cases, which is why there is this variety of solutions in play.
- But these gaps are far from insurmountable. A concerted, collaborative effort to evolve open standards and a parallel push to adopt these standards across the automotive sector will yield rich rewards. Every company in our sector will benefit.

- **Figure 4:** The S32J100 empowers manufacturers to create streamlined vehicle networks

NXP CoreRide networking

- While a single, standard model for dynamic networking remains a challenge for the auto industry, NXP has already simplified modern vehicle networking through its introduction of NXP CoreRide networking, with the S32J family of high-performance Ethernet switches at its core.

- The S32J family shares a common switch core, NXP NETC, with NXP's latest S32 microcontrollers and processors. The common switch core streamlines integration, providing manufacturers with more efficient, scalable and flexible networking solutions.
- Historically, ECU development has involved integrating numerous semiconductor and software components from different providers, each requiring distinct configuration and support.
- The absence of common standards has led to increased complexity, slower design and development timelines, and a higher risk of faults.
- NXP CoreRide networking revolutionises this process and simplifies network management for every node within the vehicle's network by providing a unified approach to network management.
- This approach enables OEMs to design and build streamlined, flexible vehicle architectures that can easily adapt to varying requirements across different vehicle models and production tiers.

Customer Service

How to reach us

- Home Page: nxp.com
- Web Support: nxp.com/support
- **USA/Europe or Locations Not Listed:**
  - NXP Semiconductors USA, Inc.
  - Technical Information Centre, EL516
  - 2100 East Elliot Road
  - Tempe, Arizona 85284
  - +18005216274 or +14807682130
  - nxp.com/support
- **Europe, the Middle East, and Africa:**
  - NXP Semiconductors Germany GmbH
  - Technical Information Centre Schatzbogen 7
  - 81829 Muenchen, Germany
  - +441296380456 (English)
  - +468 52200080 (English)

  - +4989 92103559 (German)
  - +33169354848 (French)
  - **nxp.com/support**
- **Japan:**
  - NXP Japan Ltd.
  - Yebisu Garden Place Tower 24F,
  - 4-20-3, Ebisu, Shibuya-ku,
  - Tokyo 1506024, Japan
  - 0120950032 (Domestic Toll Free)
  - **nxp.com/jp/support**
- **Asia/Pacific:**
  - NXP Semiconductors Hong Kong Ltd.
  - Technical Information Centre
  - 2 Dai King Street
  - Tai Po Industrial Estate
  - Tai Po, N.T., Hong Kong
  - +80026668080
  - **support.asia@nxp.com**

Razvan Petre

- Senior Marketing Manager, NXP Semiconductors
- Razvan Petre leads the product strategy for automotive Ethernet switches, including the innovative S32J family, within the Ethernet Networking Solutions team at NXP.
- With a strong focus on innovation, market trends and customer needs, Razvan advances networking solutions that meet the evolving demands of the automotive industry.

- **nxp.com/S32J100**

- **Document Number: DYNAMICNETWORKINGA4WP REV 0**

Frequently Asked Questions

- **Q: Why is dynamic network configuration essential for Software-Defined Vehicles?**
  - **A:** Dynamic network configuration allows for real-time adaptability, ensuring that network priorities can adjust based on changing conditions during vehicle operation.
- **Q: What are the key benefits of over-the-air updates for SDVs?**
  - **A:** Over-the-air updates enable software improvements, new features, and functional enhancements throughout the vehicle's lifecycle, keeping it up-to-date with the latest advancements.
- **Q: How does a standardised approach to network configuration benefit the automotive industry?**
  - **A:** Standardising network configuration and reconfiguration offers considerable advantages for the automotive industry by improving scalability, reliability, and efficient implementation.

Documents / Resources

	NXP Dynamic Networking in the Software [pdf] User Guide Dynamic Networking in the Software, Software

References

- User Manual

Dynamic Networking in the Software, NXP, Software

NXP

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search