With cars becoming more connected, OEMs (original equipment manufacturers) need telematics solutions that facilitate seamless communication within and outside the vehicle. The device should be cloud-enabled, connectable to servers for real-time computation and analysis, and offer an intuitive user interface that allows users to interact and control various operations.

Telematics gateway choosing criteria

When choosing a telematics gateway, various factors should be considered. These include the type and nature of clients, geographical conditions, the average distance to cover, and the vehicle type. The following considerations should be taken in account:

- **Connectivity options:** Reliable connectivity solutions are critical for the connected mobility data transformation. The telematics gateway should be able to scale up and down communication standards based on the connectivity infrastructure required for a vehicle. Depending on the end application, a telematics gateway should be able to support multiple wireless communication infrastructures such as Wi-Fi, Bluetoooth, LTE, DSRC (dedicated short range communication), and so on.

- **Type of data to be collected:** The increasing number of vehicle makers, models, and options necessitate a telematics gateway with a modular architecture capable of supporting multiple interfaces to the in-vehicle networks such as CAN (e.g. using CANopen or J1939 higher-layer protocols), Ethernet, EIA-232, EIA-485, and others.

- **Software flexibility:** A scalable software is a must for the simultaneous tracking of diverse assets and vehicles. The software stacks supported on the gateway should ensure interoperability among different vehicles and mobility infrastructures as well as reduce the development time of customized applications.

Available functionality

The telematics gateway from Iwave offers car manufacturers a modular computing platform, which allows data exchange between multiple electronic control units (ECUs) and servers. It provides a secured execution environment and prevents unauthorized access to the device while maintaining data integrity.

**Figure 1:** Features of the telematics gateway (Source: Iwave)
The device integrates a range of interfaces to collect data from vehicles and to provide it to users for further actions. Wireless communication possibilities include 4G/LTE (long term evolution) cellular network connectivity for M2M/IoT (machine-to-machine/Internet of things) applications. Other options include Wi-Fi, Bluetooth 5.0, and UWB (ultra-wideband) wireless transceiver, enabling data transfer from vehicle to the cloud. Provided wired interfaces such as CAN FD, EIA-232, EIA-485, Automotive Ethernet, and analog inputs enable interconnection with ADAS (advanced driver assistant systems), within self-driving cars, vehicle-to-everything connectivity, and more. For real-time vehicle monitoring five CAN-FD ports supporting data bit-rates up to 5 Mbit/s are provided. The gateway implements protocol stacks for such higher-layer protocols and applications as ISO 15765-4 (diagnostic communication over CAN), SAE J1939, CANopen, and CiA 447 (CANopen application profile for special-purpose car add-on devices). Thus, the device is suitable for deployment in heavy-duty trucks, off-road vehicles, special-purpose and emergency vehicles as well as further transportation and mobility infrastructures.

The gateway is based on the i.MX 8 DXL CPU (central processing unit) by NXP with 64-bit ARMv8 architecture. Processing power scaling with ARM Cortex A35 and ARM Cortex M4 processors and an internal memory of 2 GiB is possible. The device supports advanced fleet management, configurations, and remote management. For uninterrupted vehicle location, a high-precision GNSS (global navigation satellite system) module is integrated in the telematics unit. GPS (global positioning system), Glonass, Beidou, and Galileo satellite-based systems are supported. The telematics device also includes a three-axis gyroscope, accelerometer, and magnetometer for continuous real-time motion monitoring, driver behavior analysis, and auto-calibration.

Regarding security, the device offers an eSIM (embedded subscriber identity module) data encryption, multiple IMSI (international mobile subscriber identity), and a multiple-profile UICC (universal integrated circuit card) SIM technology remote file/applet management. The protection functions of the implemented Hardware Secure Element (NCJ38A) restrict unauthorized installation of applications on the gateway. Thus, only trusted applications and devices can access the telematics device. The provider also offers a security suite that includes a secure boot, secure storage, and Wi-Fi security functions.

The telematics gateway is FCC, CE, and ISED certified. The company also supports country-specific certifications such as Kominfo and E-Mark. To shorten the pre-programming cycle, available user-friendly APIs (application programming interfaces) eliminate the effort with complicated embedded scripting and proprietary device management tools. Based on the requirement, the manufacturer also provides customization options on hardware features, type of enclosure, and branding for the telematics gateway.

**Telematics gateway use cases**

For example, a telematics gateway can be deployed in the following use cases:

- **Predictive maintenance in electric vehicles**: Drivers of electric vehicles must be aware of their battery health, the charge level, and the nearest charging station to plan the trip appropriately. Telematics gateways with various on-board features and wired as well as wireless interfaces can provide valuable data needed to improve the vehicle algorithm.

- **Control and track farm equipment**: Manufacturers of farm equipment strive to improve farmer operations by securely sharing information about their daily operations. Telematics gateways installed in tractors, vehicles, and other farm equipment enable tracking of vehicle movement, location, driver status, gasoline usage, and more.

- **Fleet management**: Failures in fleet management, such as vehicle recalls resulting in service interruption, can be very costly. A telematics device reduces this risk with built-in interfaces such as CAN, EIA-232, and EIA-485 to collect and securely share fleet information with owners. As a result, it enhances fleet productivity and reduces costly failures.

- **Heavy-duty and off-road vehicles**: Forklifts, cranes, and heavy-duty trucks are often used in extreme conditions for long hours, making them vulnerable to frequent breakdowns. Via the integrated J1939 interface, the telematics gateway is able to retrieve diagnostic information and real-time data from the in-vehicle ECUs, which ensures vehicle uptime and predictive maintenance.

---

**Author**

Tawfeeq Ahmad

Iwave Systems

tawfeeq.ahmad@iwavesystems.com

[www.iwavesystems.com](http://www.iwavesystems.com)
This CiA technology day focuses on CAN XL. During this onsite event the speakers discuss all relevant CAN XL topics such as technical details, implementations, availability, and addressed markets. Additionally, they provide an outlook to the usage of CAN XL as embedded backbone network. The event is accompanied by an exhibition of CAN XL demonstrators, provided by companies offering CAN XL-based solutions.

Agenda*

08:30 to 09:00  Registration
09:00 to 09:15  Welcome (Holger Zeltwanger, CiA)
09:15 to 09:45  Excursus CAN FD Light (Fred Renning, ST)
09:45 to 10:15  General introduction to CAN XL technology (Arthur Mutter, Bosch)
10:15 to 10:45  Coffee break
10:45 to 11:15  CAN XL physical layer implementations (Teun Hulman, NXP)
11:15 to 11:45  CAN XL physical layer network design (Magnus-Maria Hell, Infineon)
11:45 to 12:00  Availability of CAN XL solutions (Holger Zeltwanger, CiA)
12.00 to 13.30  Lunch break
13.30 to 14:00  Cybersecurity and CAN XL (Wes Mir, Aptiv)
14:00 to 14:30  CAN XL and Autosar (Peter Decker, Vector)
14:30 to 15:00  CANsec implementation (CAST)
14:30 to 15:00  CANsec implementation (CAST)
15:00 to 15:30  Coffee break
15:30 to 16:00  CAN XL conformance and interoperability testing (Maen Mohammad, C&S)
16.00 to 16.30  Discussion (Q & A)

* Agenda may change without notice.

For more details please contact CiA office at events(at)can-cia.org

www.can-cia.org