# Integrating V2X Into Telematics Architectures

Next-generation self-driving cars will need advanced telematics to wirelessly exchange safety and operational data between vehicles and roadway infrastructure. Vehicles manufactured now already feature innovations to keep us safer, such as blind spot detection, lane departure warning, lane keeping technology and automatic emergency braking. But for self-driving cars to become accessible and gain regulatory approval, systems must be faster, more responsive and more reliable.

The next wave of automated driver-assistance system (ADAS) improvements will be brought about by telematics integration with 5G and vehicle-to-anything (V2X) communication. These are the technologies allowing vehicles to listen and talk to each other, to smart devices on pedestrians, and to road infrastructure. Micron's online article, "When Cars Talk, Accidents, Emissions and Traffic Congestion Reduce" from Robert Bielby, V2X expert and senior director of automotive system architecture in Micron's Embedded Business Unit, features more about these technologies.

This white paper discusses options on architectural integration of automotive electronic control units (ECUs) and vehicle telematics systems, including the challenges to integrate V2X into current telematics architectures and several options to position solutions for regulatory approval.

## Car Network Topologies With Telematics

Usually, a telematics control unit (TCU) is a component of the so-called unsecure or exposed domain of the in-car network because a TCU has — by its nature — interfaces to the external world. The same is true for the infotainment system and the onboard diagnostics unit (OBDU). A security gateway separates the unsecure domain from the secure domain (Figure 1). All communication running between unsecure and secure domains is controlled by the security gateway.

An automotive Ethernet (100BASE-T1 or 1000BASE-T1) is commonly used to connect the TCU. In contrast to standard Ethernet, automotive Ethernet uses unshielded twisted pair cables to reduce weight as well as cost. The drawback of automotive Ethernet is that it lags behind standard Ethernet maximum throughput: 100BASE-T1 and 1000BASE-T1 support a peak symmetric throughput of 100 Mbit/s and 1000 Mbit/s respectively.

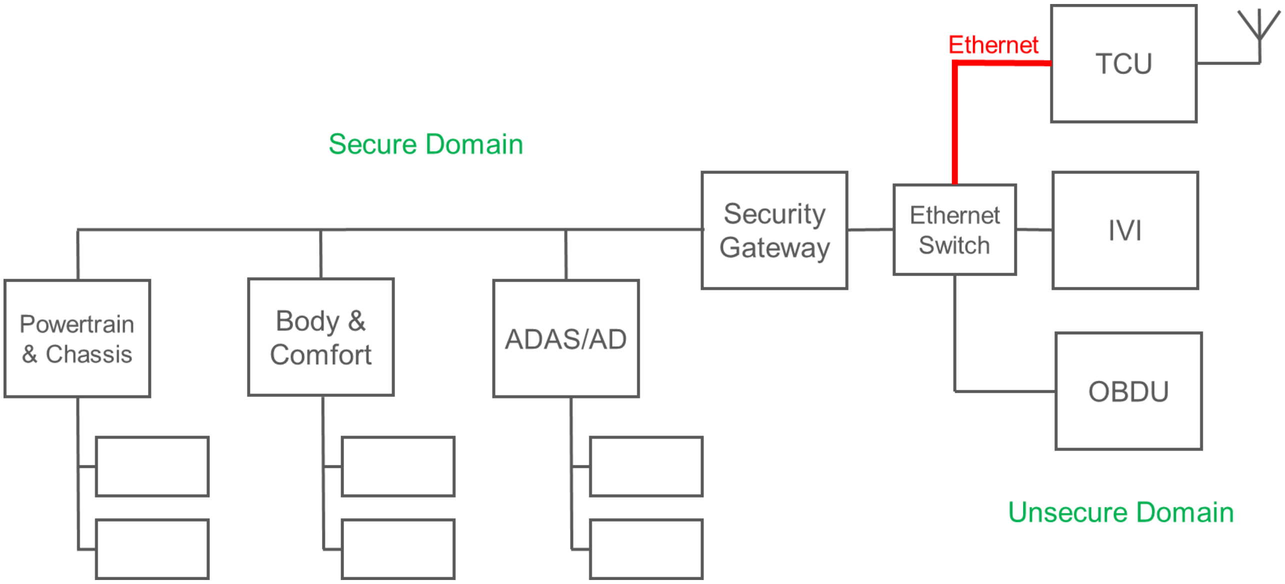

**Figure 1: Typical in-car network topology and how a telematics control unit is connected to other ECUs**

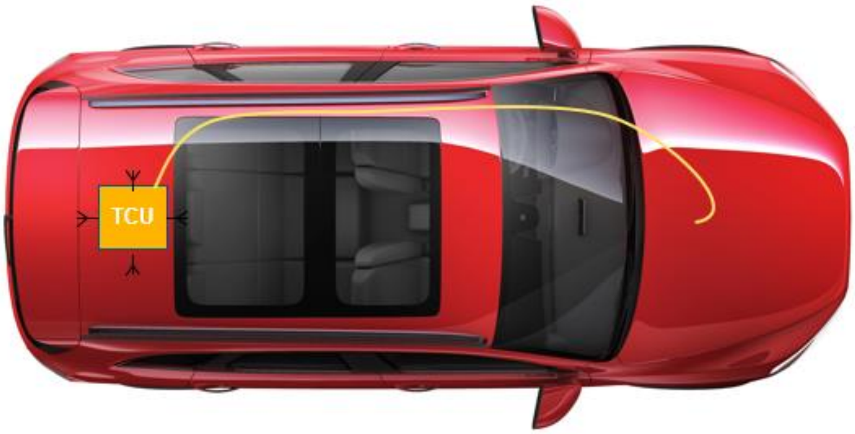

**Figure 2: TCU placement in the car**

With state-of-the-art cellular modems supporting up to 2Gbit/s (4G, Release 14) or even up to 5 to 6Gbit/s (5G, Release 15), the Ethernet connection becomes the system bottleneck. For this reason, higher-speed Ethernet (up to 10Gbit/s and higher) and PCIe-over-cable technologies are being developed.

Figure 2 depicts the TCU placement in cars. TCUs are usually placed in the back of the car under the roof below the shark fin. The shark fin contains the antennas needed for cellular, global navigation systems (GNSS), digital video broadcasting (DVB), digital audio broadcasting (DAB) or satellite radio systems. This placement minimizes problems stemming from expensive and lossy antenna cables. But the challenge with this arrangement is that temperatures under the roof can become quite high when the car is parked in the sun. This in turn affects the temperature-grade requirements for V2X and telematics components.

# TCU Architectures

There are two main topologies for TCUs. Historically, so called **smart modems** were dominant. A smart modem is a cellular modem that — besides baseband physical layer (PHY) and protocol stack processing, radio frequency (RF) chip, RF front-end components and power management unit (PMU) — also contains a small application processor (AP) that is integrated into the baseband chip (Figure 3). In this architectural approach, software applications managing the TCU and any potential applications running within the TCU are executed on this small integrated AP.

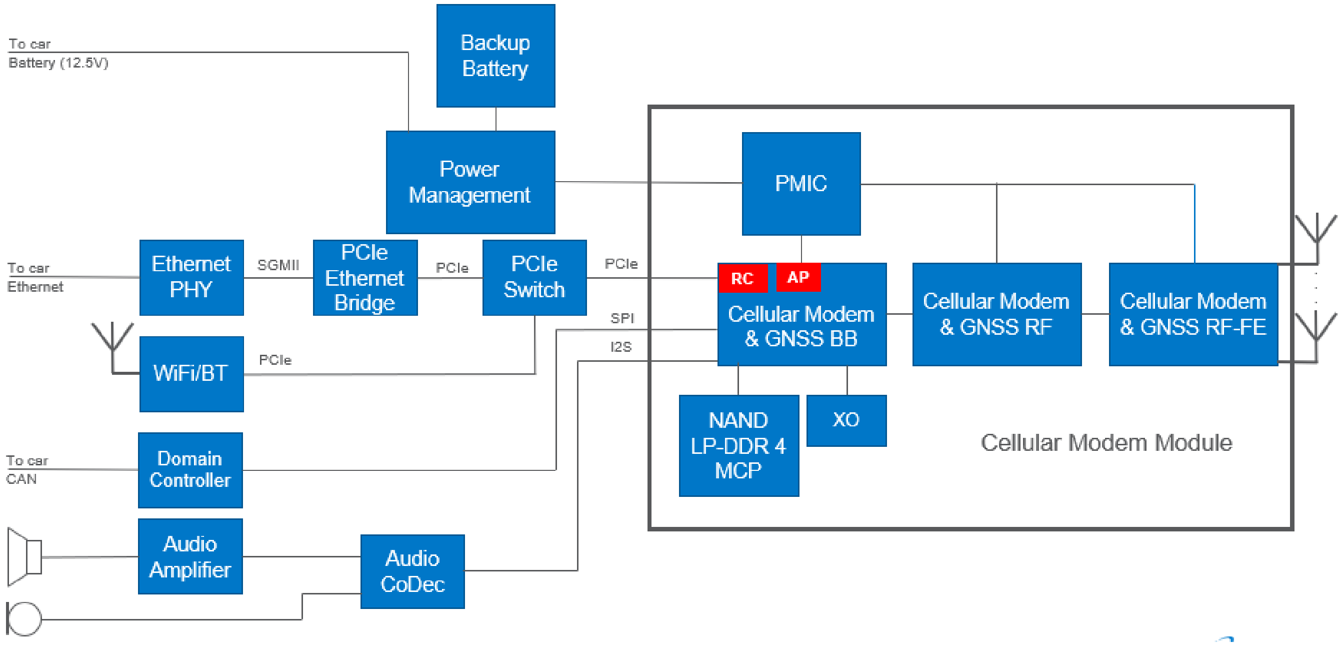

**Figure 3: Smart modem TCU block diagram**

**AP+slim modem** is the second alternative that has emerged recently because processing requirements keep going higher to manage a TCU and more applications that run directly there (Figure 4). A classical AP+slim modem approach is used in high-end mobile phones (such as Apple iPhones).

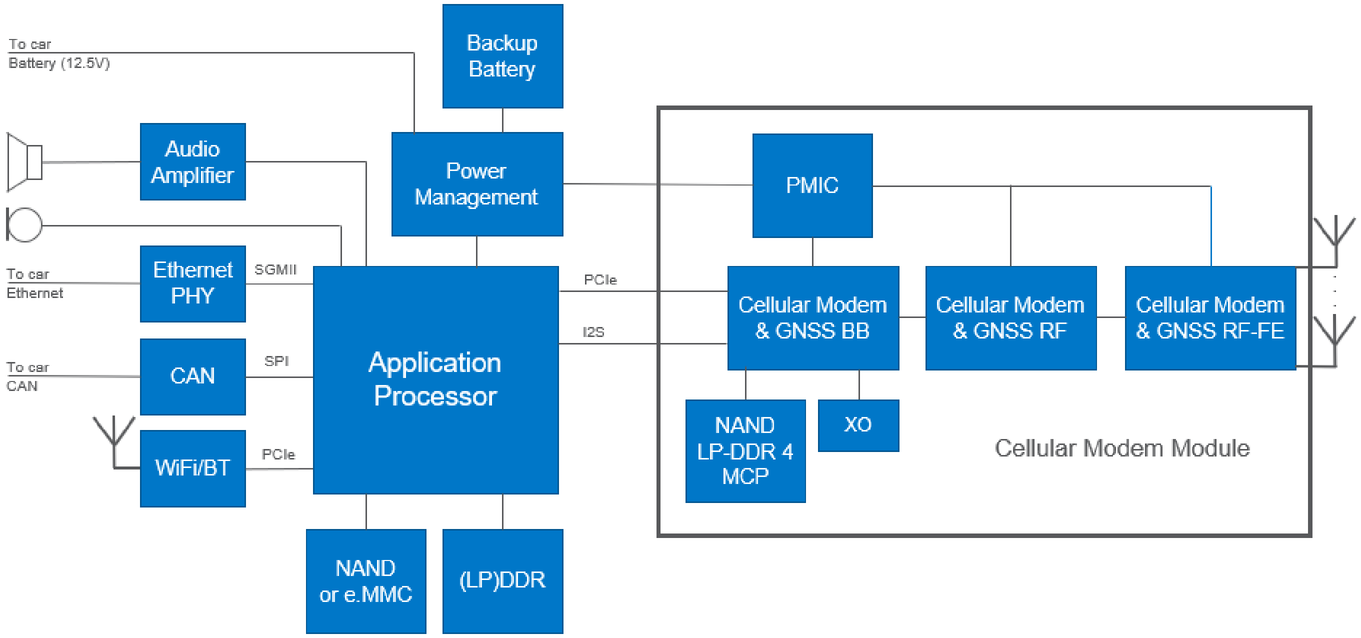

**Figure 4: TCU with application processor and slim modem**

The modem portion in the black box in both approaches is commonly put into a dedicated module — the so-called NAD (network access device) module. This module is then soldered onto the main printed circuit board (PCB) by the TCU manufacturer. A backup battery and spare audio subsystem are required to place and receive e-calls after an accident that disconnects the main car battery or causes the main audio system to fail.

The main advantage of the smart modem approach is its lower product cost while the AP+slim modem architecture offers better AP performance and is more scalable. Table 1 compares advantages and disadvantages of both architectures. As of today, most car OEMs use the smart modem architecture. However, the AP+slim modem is gaining momentum.

**Table 1: Advantages and disadvantages of both TCU architecture topologies**

| | AP+Slim Modem | Smart Modem |
|---|---|---|
| Estimated Share | 20% | 80% |
| Pros | • More performance (e.g., for routing, firewall and cellular V2X stack)<br>• Modularity and easier upgrade path to new modem generations | Lower product cost |
| Cons | Higher product cost | • AP performance limitations<br>• Stronger modem vendor dependency |

# Integration of V2X

There are two competing V2X standards under discussion at this point: 802.11p standardized by IEEE vs. cellular V2X (C-V2X) standardized by 3GPP as part of the 3GPP cellular standard. The first version of 802.11p was published in 2002 while C-V2X — sometimes called LTE-V — was introduced by 3GPP as part of LTE Release 14 in 2017. Both standards use the same frequency band (5.9GHz band), which might create coexistence issues. Other frequency bands might be added in the future, such as millimeter wireless access in vehicular environments (WAVE) bands for 5G NR V2X. Table 2 shows a comparison of advantages and disadvantages of both standards.

**Table 2: Advantages and disadvantages of 802.11p and C-V2X**

| | 802.11p | C-V2X |
|---|---|---|
| Pro | • Mature technology with a million kilometers of test driving<br>• Moderate complexity | • Strong roadmap<br>• Said to have better range and performance<br>• Integration with cellular allows direct and indirect communication paths |
| Con | • Virtually no technology roadmap anymore<br>• Said to have lower range and higher error rates than C-V2X | • Relatively new and unproven technology<br>• Comparatively high complexity because of integration of direct (SL) and indirect communication (UL/DL) and centralized vs. decentralized network |

Another important item to consider for V2X integration strategies is that 3GPP does not standardize a middleware for V2X communication. 802.11p and C-V2X will use the same middleware based on IEEE 1609 WAVE.

Because of the tighter integration between indirect (traditional cellular Uplink [UL] / Downlink [DL] via base station) and direct (Sidelink [SL]) communication, stronger roadmap and lower additional costs, Micron believes that C-V2X will eventually prevail. But to be safe, an integration of V2X should include both standard variants.

In "Accelerating Global V2X Deployment for Road Safety," Autotalks summarized the main considerations for V2X integration into telematics units for an easy deployment in the early phases of the market introduction of V2X technologies. The company listed these benefits:

- Flexibility — be able to support both standards
- Modularity — incur additional costs for V2X only if needed
- Security — support regulatory security requirements
- Safety — support use cases with functional safety requirements
- Boot — start operation quickly with fast boot time
- Temperature — accommodate up to 105 C $T_{roof}$ with the TCU mounted under the roof

Another important requirement is the cryptographic performance required to authenticate received messages. For security reasons, each V2X message is protected by a signature that is based on elliptic curve cryptography (ECDSA). This signature makes it impossible to inject false messages. Each car will transmit 10 V2X basic safety messages (BSM) per second, which can be received within a perimeter of up to 1 km$^2$ from the sending car. On a four-lane highway with traffic jams in each direction, up to 300 cars could be generating messages. Authenticating each message by checking the validity of the signature could entail up to 3,000 signatures per second to be verified using elliptic curve cryptography. Today, standard crypto accelerators in commonly used automotive microprocessors can handle only 100 to 200 messages per second. So, an application processor with high-performance hardware accelerators is required.

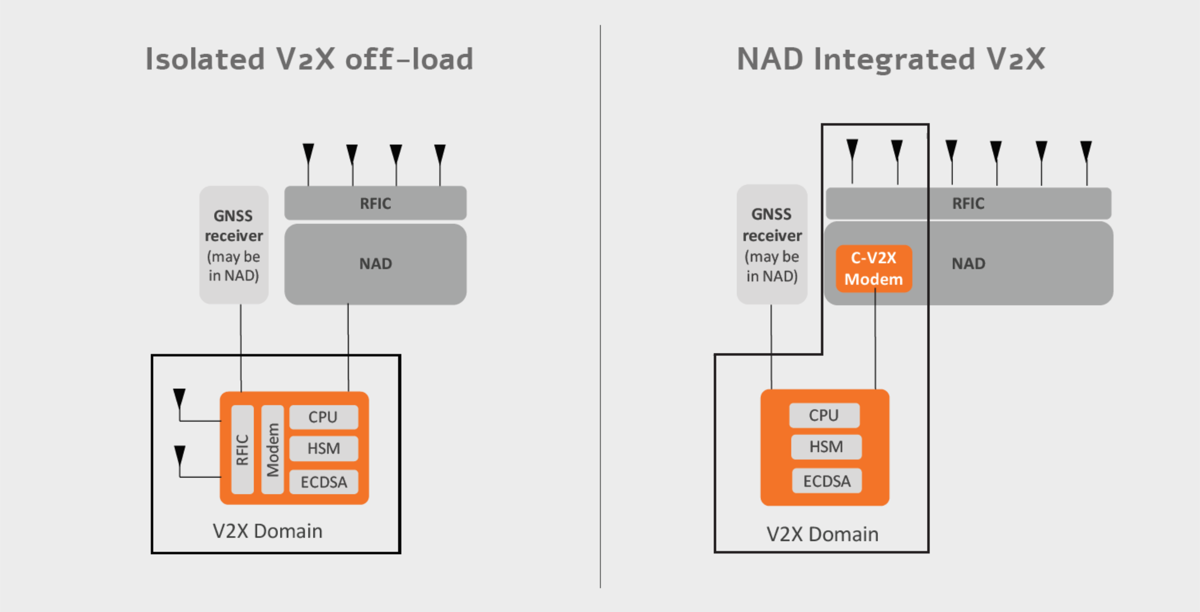

**Figure 5: Modular architectural approach for V2X integration into TCUs proposed by Autotalks**

Figure 5 depicts architectures proposed to fulfill the above requirements. In the left variation, the complete V2X functionality is separated from the cellular modem as well as the TCU control functionality. This is, of course, the most modular and flexible approach. A dedicated V2X module can be mounted when V2X is required but not mounted in regions without a V2X mandate.

The V2X module contains these components:

- Radio frequency (RF)
- Physical layer (PHY)
- High-security module (HSM)
- Cryptographic accelerators (ECDSA)
- IEEE 1609 middleware

This approach is best applied for 802.11p. It is also technically possible to separate the C-V2X PHY and RF functionality from the cellular modem. However, it would, for certain C-V2X operating modes, be quite challenging to manage this separation in the control plane because these operating modes require close interaction between base station and V2X sidelink. Using the architectural approach for C-V2X (shown on the right in Figure 5) might be preferred. Here, RF, PHY and control plane for the sidelink remain part of the cellular modem. Leading modem suppliers such as Qualcomm support C-V2X with their 5G product lines. The V2X module still handles the V2X middleware, signature verification and security requirements.

The above architectural approach supports fast time to market for V2X introduction and leads to very cost-efficient solutions because of its modularity in the introductory phase of V2X. At some point, if one of the two V2X standards prevails and the penetration rates converge to 100%, an even tighter integration of telematics and V2X might evolve to further reduce product cost. Figure 6 depicts a possible architecture with cellular, V2X, TCU control and applications fully integrated.

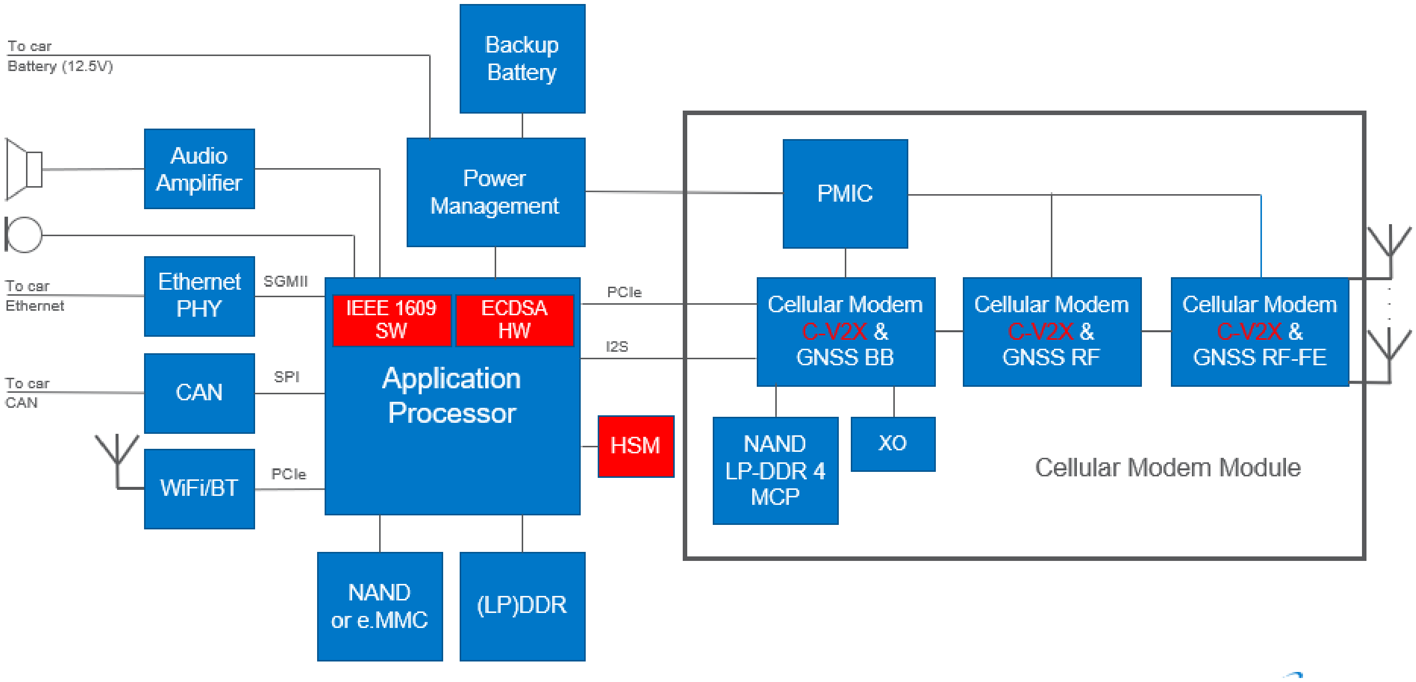

**Figure 6: Possible full integration of C-V2X with telematics, cellular, V2X, TCU control and applications**

Mirroring the requirements for V2X integration described above, modularity and flexibility are less important when the standard is decided and penetration rates of V2X approach 100%.

Security can be addressed by using a dedicated small HSM — such as the Infineon SLE97 (Infineon Technologies AG) — that can fulfill the high-security requirements expected for V2X mandates (FIPS 140-2 level 3 in the U.S., Common Criteria EAL4 in the EU). This HSM stores secret keys and compute signatures used to transmit messages, which are based on the secret keys. Since only 10 messages per second need to be transmitted, performance requirements for signature generation are moderate. In cases where multiple thousands of messages might be received and need to be verified, cryptography based on public keys is used, so security requirements can be lowered. The high-performance ECDSA engine used to verify the signatures of received messages could be integrated into the application processor.

The remaining requirements — functional safety, fast boot and temperature range — can be tackled by state-of-the-art methods applied in automotive microcontrollers or application processors.

# Micron Memory Offering for Telematics and V2X

Micron has been recognized as an industry leader in memory solutions for automotive, with long-standing expertise with automotive processes and business practices. All products of the Micron memory portfolio for automotive, including a variety of DRAM, NAND, mNAND and NOR products, are qualified according to automotive standards AEC Q100 for components and AEC Q104 for multichip packages (MCPs). To our customers, we deliver PPAP (Production Part Approval Process) documentation according to IATF 16949.

Micron remains committed to the automotive industry goal of zero defects and offers significant lab capacity to analyze field returns based on the 8D methodology. Our labs also support our customers during the product design-in phase. Micron's Manassas, Virginia, fabrication site manufactures our long-lifecycle products to ensure supply continuity for the automotive market.

Micron offers DRAM and NOR products up to AEC Q100 grade 1 (-40 C to 125 C $T_{case}$) and NAND and managed NAND products up to AEC Q100 grade 2 (-40 C to 105 C $T_{case}$). We also provide support for thermal design.

Micron designs and manufactures multichip packages (MCPs) driven by the requirements of the telematics market. This product features a volatile and a nonvolatile memory die stacked on top of each other, as depicted in Figure 7. Another often used MCP combination for automotive is LP-DDR DRAM plus single layer cell (SLC) NAND in one package. Other combinations are NOR plus DRAM or e.MMC plus DRAM.

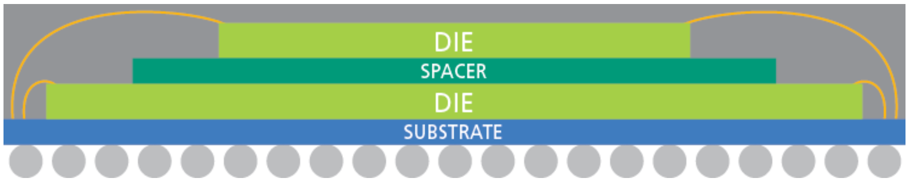

**Figure 7: Typical two-die multichip package stack for a telematics memory solution**

A major challenge for MCPs in telematics is how little board space is available in small cellular modem (NAD) or V2X modules. Micron designs its MCPs to save 30% to 40% of board space through the vertical stacking of the two die and shared common pins, such as supply or ground pins. Additional advantages are reduced product cost because of package and pin savings and simplified logistic and manufacturing processes, since only one component is sourced and mounted during production, not two.

# Conclusions

In this white paper, we have reviewed integration approaches of V2X into telematics platforms starting from the overall car network topology and different TCU architectures. The two main architectural approaches are so-called smart modems and AP+slim modem. Flexibility and modularity are key considerations when integrating V2X, especially during V2X market introduction when penetration rates are still in flux and two competing V2X technologies are available in the market. Autotalks with its Craton™ product family facilitates fast integration and a modular design approach for contending V2X technologies. At a later stage in a more mature market, we might see an even tighter integration with further cost savings.

Micron, as a market leader in automotive memories, also offers competitive solutions for telematics and V2X. MCPs that combine DRAM and NAND not only save significant board space in NAD and V2X modules but also reduce product and manufacturing costs for our customers.

## For More Information

Follow the latest news on our automotive memory on Twitter @MicronTech, and learn about V2X, MCPs and more at micron.com/automotive.

**micron.com**