Technical Article

Enabling Functionally Safe and Secure Electric Automotive Powertrains Using C2000™ Real-time MCUs

Bharat Rajaram

Jürgen Belz, senior consultant, functional safety and cybersecurity at Prometo, co-authored this technical article.

The migration from internal combustion engines (ICEs) to electric vehicles (EVs) requires at least five new electrical/electronic/programmable electronic (E/E/PE) systems. Figure 1 depicts these systems within an EV.

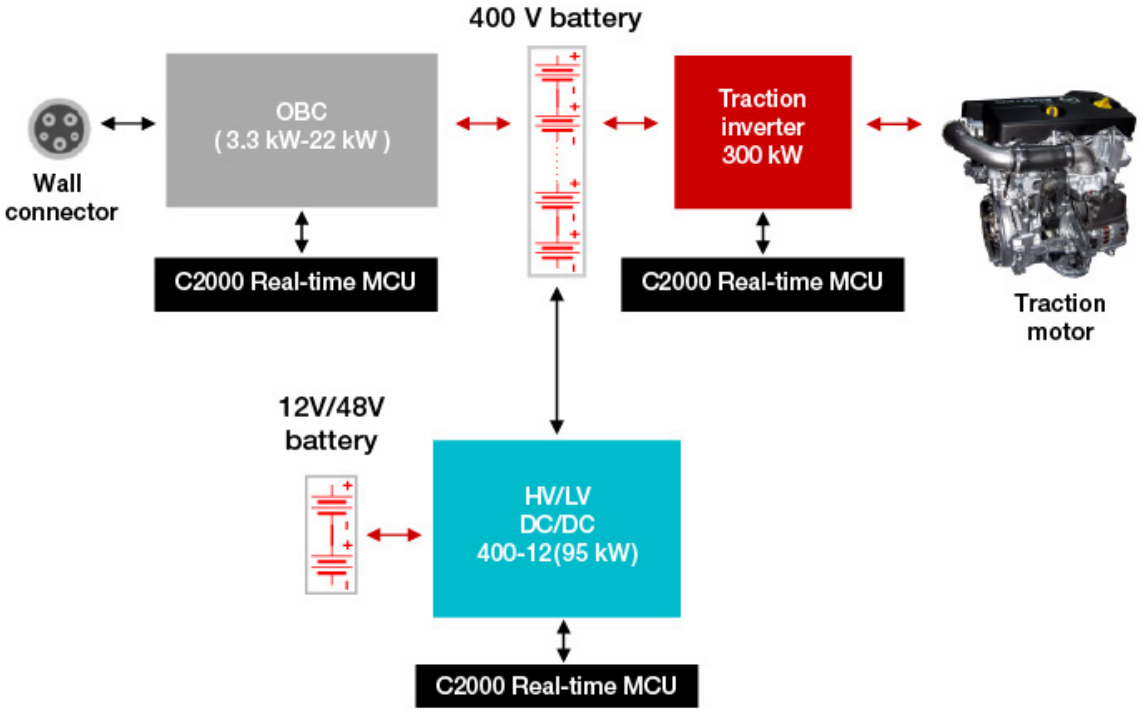

Figure 1. Block diagram of a typical EV powertrain

In order to zero out tailpipe emissions and reduce continued reliance on fossil fuels, refuelling EVs happens at a charging station. These EV charging stations could be supplied with renewable energy sources like solar and wind, which increases the positive impact of EVs on the environment. The onboard charger forms a functional unit with the high-voltage battery, which ensures fast, efficient charging while still protecting the battery from overcharging. These and other safety requirements are described in International Organization for Standardization (ISO) 6469 parts 1, 2 and 3 – the standard that governs the high-voltage electrical safety requirements for electric road vehicles.

All Electronic Control Units (ECUs) in an EV require a 12-V battery charged by a high-voltage-to-low voltage DC/DC converter, which helps establish galvanic separation between the low-voltage (12-V) battery and the high-voltage (400 V or 800 V) battery. The inverter and the electric machine (propulsion motor) deliver torque for controlled motion. Very compact and high-power-density permanently excited synchronous machines are usually deployed in an EV propulsion motor. At lower power levels, asynchronous machines have found limited use in EVs. Functional safety aspects of this high-voltage-to-low voltage DC/DC converter help guarantee the

operation of all ECU features while the EV is in motion and the EV Traction Inverter (EVTI) are outlined in ISO 26262:2018.

For instance, for a vehicle with an ICE, the operating time (or power-on hours) of a semiconductor component is between 8,000 and 10,000 hours. With an EV, this increases to 30,000 hours or more. The reason: semiconductor components have to remain powered up not only when the vehicle is being driven, but also when the vehicle is charging. This amount of power influences, for example, the calculation of the probabilistic metric for random hardware failures according to ISO 26262. For engineers, this amount of power means that they must develop a system that on average has a fivefold lower probability of dangerous component failures or failure in time.

In an electrified powertrain, the C2000™ real-time microcontroller (MCU) typically addresses power conversion and communicates with a general-purpose MCU connected to the bus vehicle, managing the highest level of security, shown in Figure 2.

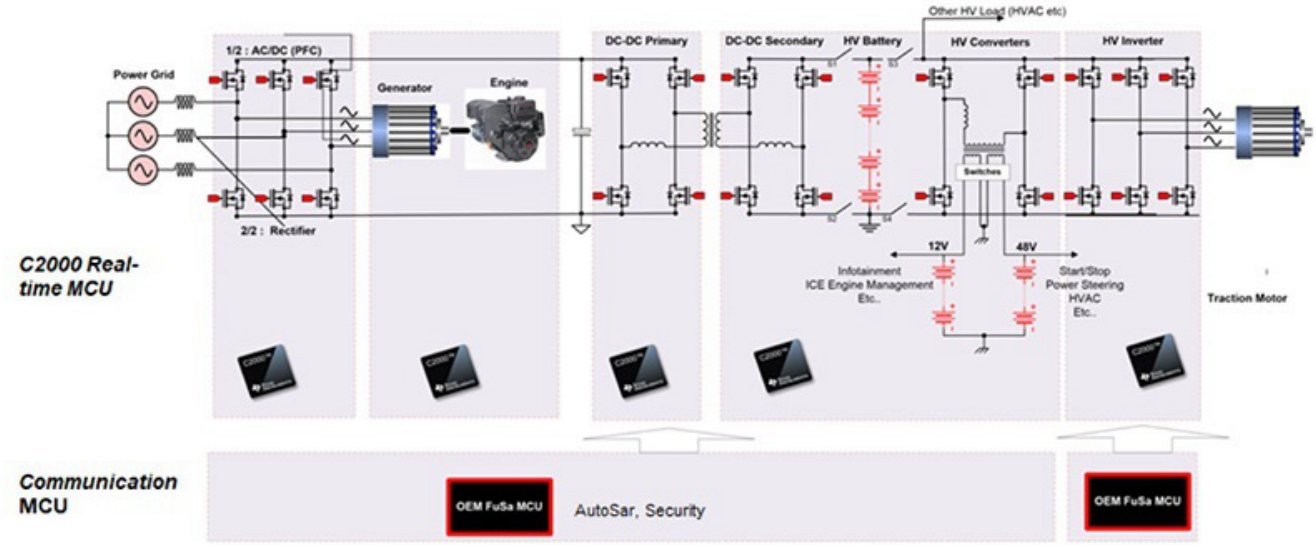

Figure 2. C2000 real-time control in an electric powertrain

You might still want to consider encrypted communication between the communication MCU and the C2000 real-time controller, typically used for over-the-air upgrades. In such cases, you need to assess the threat level and define a security strategy at the system level to leverage the various security enablers that the C2000 real-time MCU offers, listed in Figure 3.

Enabler	Feature	F2838x	F2837xD	F2837xS / F2807x	F28004X	F28002X
Cryptographic acceleration	AES: 128, 192, 256 engine	✓				
Device Identity	UID programmed into OTP	✓	✓	✓	✓	✓
Secure boot	User programmed OTP setting‡	✓				
	128b AES-CMAC based	✓				
	Partial authenticated boot (16KB each core)	✓				
Debug security	Password controlled / permanent JTAG lock	✓				
	Security-aware debugging	✓	✓	✓	✓	✓
Trusted execution enviroment	Via multiple cores w/ IPC communication	✓	✓			
Secure storage	Via multiple cores w/ IPC communication	✓	✓			
Software IP protection	Secure memory zones	✓	✓	✓	✓	✓
	Excute only memory	✓	✓	✓	✓	✓

† Advance information ‡ Application report https://www.ti.com/lit/pdf/spract3

Figure 3. C2000 supported enabler status

Some of the technical features supporting these security enablers include:

- The ability to protect memory blocks.
- Memory zone ownership by bus masters such as the C28x central processing unit (CPU), control law accelerator and direct memory access.
- Execute-only protection for certain memory regions (with callable secure copy and secure cyclic redundancy check software Application Programming Interface functions available in the boot read-only memory).
- Protecting the CPU from improper access through debugging ports and logic while it is executing code from secure memory regions (also called secure Joint Test Action Group).
- Unique identification for each product.
- Hardware acceleration engine for 128-bit Advanced Embedded Standard (AES) encryption.
- Secure boot.

Conclusion

Because the electric drives or voltage converters have to be functionally safe, high-voltage safe, power-efficient and cost-effective, the challenges and complexities increase exponentially. Designing with C2000 real-time MCUs can help solve these challenges by giving EV charging designers the option to use a single device that enables all of these requirements.

Additional resources

- Watch the training, "Functional Safety at TI."
- Read the white paper, “Achieving High Efficiency and Enabling Integration in EV Powertrain Subsystems Using C2000 Real-Time MCUs.”
- Read the application report, “Secure BOOT on a C2000 Device.”
- Read the technical article, “Three considerations for automotive powertrain safety and security.”
- Review the presentation, “Integrating a High RPM Traction Inverter, Software Resolver Interface and DC/DC Converter with ASIL D concept assessed C2000 Reference Design”
- See the demonstration video High voltage on-board charger using TI GaN and C2000 real-time MCUs

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265