Technical Article

Three Considerations for Automotive Powertrain Safety and Security

Bharat Rajaram

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

With functional safety and security concerns in automotive electronics gaining attention, including in standards bodies, it's important for automotive designers to enable functionally safe and secure automotive electric powertrains. Functional safety, cybersecurity and high-voltage safety play an important role in the design, development and mass production of modern electric vehicles.

Functional safety

A prevalent estimate for the amount of software in a modern vehicle is between 100 and 200 million lines of code. This software runs on a large variety of programmable electronic control units and provides functions for advanced driver assistance systems and safety features in the vehicle. Examples of such systems include blind-spot monitoring, automatic emergency brakes and adaptive cruise control. Vehicles with autonomous and electric features require functional safety for safe operation.

Cybersecurity

The increasing sophistication in the type and amount of connectivity available makes vehicles more vulnerable to digital attacks. What was once considered the gold standard in the prevention of cyberattacks is no longer valid. Given the implementation of communications protocols like Controller Area Network and *Bluetooth*®, and now Global System for Mobile Communications and Wi-Fi® networks for vehicle-to-vehicle communication, automobiles are no longer protected by the “air gap” between them and networks that hackers may employ. Imagine a scenario where a hacker immobilizes a vehicle and only unlocks it after being paid a ransom in bitcoin.

High voltage

Additionally, all aspects of the electric drivetrain – such as the onboard charger, high-voltage to high-voltage or high-voltage to low-voltage DC/DC converter, and electric vehicle traction inverter – all use programmable microcontrollers (MCUs) such as C2000™ real-time MCUs. And with electric vehicle battery voltages approaching 600 to 800 V, it is equally important to understand and apply the requirements for high-voltage safety systems.

Automotive safety and security standards

These international standards address safety and security aspects:

- International Organization for Standardization (ISO) 26262:2018 outlines the functional safety requirements of road vehicles.
- ISO 6469:2018 specifies high-voltage electrical safety requirements for electrically propelled road vehicles.
- United Nations Economic Commission for Europe WP29:2020 details automotive cybersecurity requirements for automakers worldwide.

Additionally, automotive Tier 1s (subsystem manufacturers) follow:

- ISO DIS 21434:2020, which is still a draft international standard and a superset of Society of Automotive Engineers (SAE) J3061. ISO DIS 21434:2020 outlines a cybersecurity management framework and activities in deference to the ISO 26262 functional safety-compliant V-model-based product development life cycle.
- SAE J3061:2016, the original “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” on which ISO/SAE DIS 21434 is based.

Electric vehicle system designers must consider aspects of all three safety and security measures.

ISO 26262 defines four automotive safety integrity levels (ASILs), as listed in Table 1.

Table 1. ISO 26262 quantitative random hardware diagnostic coverage metrics per each ASIL class

ASIL class	Single-point fault metric	Latent fault metric	Probabilistic metric for hardware random fails
ASIL A	n/a	n/a	n/a
ASIL B	≥90%	≥60%	≤100 failure in time (FIT)
ASIL C	≥97%	≥80%	≤100 FIT
ASIL D	≥99%	≥90%	≤10 FIT

ISO/SAE 21434 defines four cybersecurity assurance levels (CALs) based on attack vector and impact, as listed in Table 2.

Table 2. ISO/SAE 21434 cybersecurity assurance levels

		Attack vector			
		Physical	Local	Adjacent	Network
Impact	Negligible	n/a	n/a	n/a	n/a
	Moderate	CAL 1	CAL 1	CAL 2	CAL 3
	Major	CAL 1	CAL 2	CAL 3	CAL 4
	Severe	CAL2	CAL 3	CAL 4	CAL 4

SAE J3061 defines four cybersecurity integrity levels (CSILs) and recommends the application of a cybersecurity process for all automotive systems responsible for functions that are ASIL rated per ISO 26262, or for functions associated with subsystems such as propulsion, braking and steering. These are CSIL A, CSIL B, CSIL C and CSIL D.

ISO 6469 describes four classes that depend on the maximum working voltage range "U" of an electric circuit, as listed in Table 3.

Table 3. ISO 6469 permissible maximum voltage levels per each voltage class

Voltage class	Highest (maximum) working voltage	
	DC voltage (in V)	AC voltage (in root-mean-square value)
A	0 < U ≤ 60	0 < U ≤ 30
B	60 < U ≤ 1,500	30 < U ≤ 1,000
B1	60 < U ≤ 75	30 < U ≤ 50
B2	75 < U ≤ 1,500	50 < U ≤ 1,000

There is significant synergy between ISO 21434 and ISO 26262 in terms of how to implement their recommendations during the design, development and mass production of an electrical/electronic/programmable electronic system.

Conclusion

With the increasing complexity of automotive subsystems in hybrid electric vehicles and electric vehicles and the electrification of the powertrain, safety and security are becoming higher priorities. Fortunately, commonly accepted normative international standards address these safety and security aspects.

TI can help you make security and safety assessments and achieve security and safety goals in your automotive designs. For example, while developing a powertrain solution with a C2000™ real-time MCU, the online safety material is a great starting point.

Additional resources

- Watch the training, "Functional Safety at TI."
- Read these white papers:
  - "Understanding Functional Safety FIT Base Failure Rate Estimates per IEC 62380 and SN 29500."
  - "Streamlining Functional Safety Certification in Automotive and Industrial."
  - "Functional Safety Considerations in Battery Management for Vehicle Electrification"
  - "Wired vs. Wireless Communications in EV Battery Management"
  - "Functional Safety-Relevant Wireless Communication in Automotive Battery Management Systems"

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