TASKING®

TAKING THE BUSINESS RISK OUT OF ADAS DEVELOPMENT

TAKING THE BUSINESS RISK OUT OF ADAS DEVELOPMENT

Two of the most valuable assets your company possesses are its reputation and its competitive edge. Protecting both can be a balancing act – you want to mitigate business risk and yet stay ahead of the competition by developing innovative products and services. Never has that balancing act been more delicate than for companies competing in the race to build the fully connected car, and, eventually, the completely autonomous vehicle.

In this race, consumer interest in fuel efficiency, safety, and connectivity are making advanced driver assistance systems (ADAS), vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications, and in-vehicle infotainment (IVI) three hot spots of automotive development:

- The global ADAS market is expected to reach a 16% to 18% compound annual growth rate (CAGR) through 2020. (1)
- The V2X market is currently valued at $767.5 million and is expected to reach a whopping $2,815.5 million by 2022 (a CAGR of 29.69%). (2)
- Predictions place the IVI market CAGR at almost 5% through 2018. (3)

ADAS technology relies on electronic powertrain controls and many types of sensors, resulting in features such as adaptive cruise control, blind spot detection, park assist, lane departure warnings, tire pressure monitoring, and many others. V2X and IVI services use communication networks and other connected cars and infrastructure to stream music from the cloud, provide real-time traffic information, and other personalized services.

All this technology – and the potential revenue it represents – is tantalizing to automotive developers. The opportunity is real, but so are the risks. Malfunctioning electronics, whether in engine control, ADAS, V2X components, or IVI, could lead to an expensive recall, or to catastrophic injuries or even death. Malfunctioning electronics could also cause monetary loss, and more importantly, irreparable damage to your company's reputation. For example, consider that Volkswagen AG's stock price fell by almost a quarter of its market value after it became clear the company's electronic emissions controls were not functioning as advertised. (4)

Choosing safety-certified, high-performance hardware and software development tools (compiler with OTA support, debugger, linker, and performance libraries) can significantly mitigate the business risks associated with developing electronic automotive systems by integrating safety and information security into every system component.

REVVING UP ENGINE CONTROL SAFETY

Regulation of emissions and fuel efficiency is on the rise worldwide. In response, electronic control of the engine, transmission, and other elements of a vehicle's powertrain is becoming increasingly complex (see Figure 1).

Engine control modules (ECMs) optimize engine performance by using input from sensors that monitor fuel mixture, ignition timing, variable cam timing, idle speed, and emissions control (just to name a few). Beyond the engine, powertrain control modules (PCMs) control the automatic transmission, braking, and other aspects of a vehicle's movement.

ECMs and PCMs use embedded high-performance hardware (microprocessors) and software applications to translate sensor data into actionable outputs (such as adding more air to the fuel mix, or shifting from second gear to first on a steep hill). If you've used a PC, you know that both hardware and software can fail. The same is true of automotive electronics. And in a vehicle, such failures can pose serious risks. For example, if the fuel/air mixture is slightly off, the engine may have to work a little harder. If it's really off, the car may not pass its next emissions test without a tune-up. But if a car inadvertently slams into reverse instead of shifting down as the driver brakes for a stoplight, there could be serious consequences.

When contributing to the development of safety-critical ECMs and PCMs, the following three best practices can help minimize the likelihood of failure of the embedded solution:

- Become familiar with automotive safety standards and integrate them into your development cycle. For example, the ISO 26262 standard ensures the functional safety of electrical and electronic systems in road vehicles, while Automotive SPICE® provides a mechanism for controlling risk in the software development cycle.
- Use safety-certified hardware. In particular, while somewhat more complex than single-core architectures, multi-core architectures support better safety checking and the higher performance necessary for today's automotive electronic applications.
- Choose a compiler and other software development tools that are ASPICE Level 2-certified and that are able to take advantage of safety and performance features in the hardware.

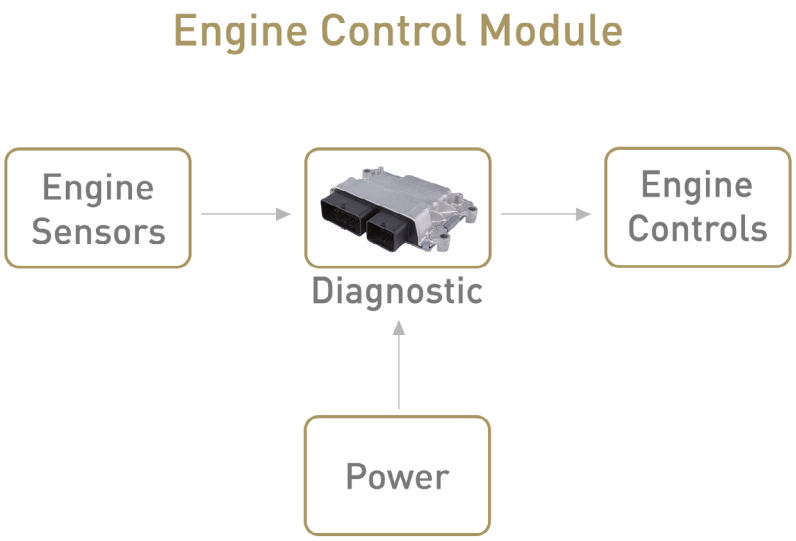

Figure 1. Serving as the brains behind a vehicle's ability to move, the engine control module (pictured here) and the powertrain control module are responsible for many safety-critical functions. These embedded solutions must be developed with reliability as a top priority.

PREVENTING DISTRACTIONS FOR DRIVERS

As seen in Figure 2, IVI systems can provide a wide range of services, including audio and visual entertainment and news, navigation assistance, heads-up display of information such as speed and temperature, and the recording of video and data input (similar to an airplane's "black box recording"). Increasingly, IVI systems are being integrated with smartphones.

You may be surprised to see IVI systems on the list of safety-critical automotive functions. After all, if the radio stops streaming music, no one will be injured. Even if the GPS fails, the driver can always ask for directions or buy a printed map. But in actuality, IVI systems do pose some business risks. First, malfunctioning IVI systems could, like any other component failure, spark recalls – which can cost millions in repairs, legal fees, and brand damage. Companies can also lose royalties associated with streamed content. But more importantly, IVI systems have an important role to play in keeping our roads safe.

Roughly 25% of motor vehicle accident fatalities are a result of distracted driving (5); in 2014, over 3,000 people were killed and 431,000 were injured in motor vehicle crashes involving distracted drivers (6). Drivers do some unbelievable (and dangerous) things behind the wheel, including putting on makeup, brushing teeth, shaving, and changing clothes. And IVI systems could potentially be yet another thing that distracts a driver's attention.

To reduce the risk of driver distraction, IVI applications should use hardware and software to create solutions that prevent drivers from engaging in activities that would distract them. Here are some ideas for creating an IVI system that is safe and secure:

- Use an in-cabin camera to detect driver inattention and sound an alarm or vibrate the seat to refocus the driver.
- Ensure visual displays do not block the driver's view or require turning their head away from the view of the road.
- Support simple, intuitive voice commands (through natural language recognition) to reduce driver distraction and frustration.
- Integrate intelligence into the system so it can function appropriately whether the vehicle is moving or at rest.
- Support secure methods for updating the IVI system components (see "Boosting Security for OTA Updates" for more details).

Figure 2. In-vehicle infotainment systems can provide a wide variety of useful and entertaining services – but it is important that they do not distract the driver's attention.

RISING TO THE FAIL-PROOF CHALLENGE

ADAS technologies are developing rapidly and can dramatically increase vehicle safety (see Figure 3). For example, ADAS features help drivers avoid collisions and accidents by alerting them to potential problems and implementing safeguards. Soon, some form of ADAS will be integrated into every car sold in the United States. In 2014, the US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) announced that it will require all new light vehicles to have rearview cameras by mid-2018 (7). Both the European Union and the United States have mandated that all new vehicles be equipped with autonomous emergency-braking systems and forward-collision warning systems by 2020. (8) In December 2016, the NHTSA issued a proposed rule mandating V2V communication, which can help avoid crashes on all light vehicles. (9)

But while ADAS features have proven reliable and valuable, the technology is not yet mature and poses significant challenges to developers striving to create solutions that are 100% safe. For example, can a camera distinguish a police car from a taxi or a pizza delivery car? What about telling the difference between an ambulance and a delivery truck? What if a speed limit sign is partially obscured by a bush? Does the lane-keeping function work during a snowstorm? What happens when a car equipped with adaptive cruise control encounters a road construction zone or a detour sign? How can mere hardware and software predict the outcome of a situation involving the moods of drivers and passengers? To be truly safe, ADAS must be able to correctly react to situations that haven't been encountered before – and mistakes can be deadly.

By nature, ADAS features are complex. The simple term "adaptive cruise control" barely hints at the sensor fusion, integrated image and data processing, probabilistic algorithms, and other hardware and software tasks that must take place at lightning speeds with no errors. ADAS security requirements are also stringent; a hacker's interference with braking or steering could be tragic.

Although many current ADAS features require the driver to pay attention and take over vehicle control at any time, and as ADAS evolves into autonomous driving, more and more embedded solutions will be rated at Automotive Safety Integrity Level D (ASIL-D). This level of classification of the ISO 26262 standard is reserved for components or systems where a malfunction poses the risk of injury or death. The proposed IEEE 2020 project, which proposes global standards for automotive system image quality is receiving widespread industry support.

Companies that are developing embedded ADAS and autonomous driving solutions should familiarize themselves with ASIL risk-analysis methods and apply them early in product development. Solutions should include monitoring and redundancy to detect errors in real time. At later stages of development, extensive testing is necessary to evaluate the safety of the ADAS component and the entire system under different environmental and operational conditions.

You can reduce the effort and cost associated with testing by choosing an ASPICE-certified compiler, which generates trustworthy code and safety-certified, high-performance microprocessors with built-in security features. Additionally, the compiler must support the safety functions on board the microprocessor, and together with the real-time operating system (RTOS), the compiler should also support over-the-air (OTA) updates (see also the "Boosting Security for OTA Updates" section).

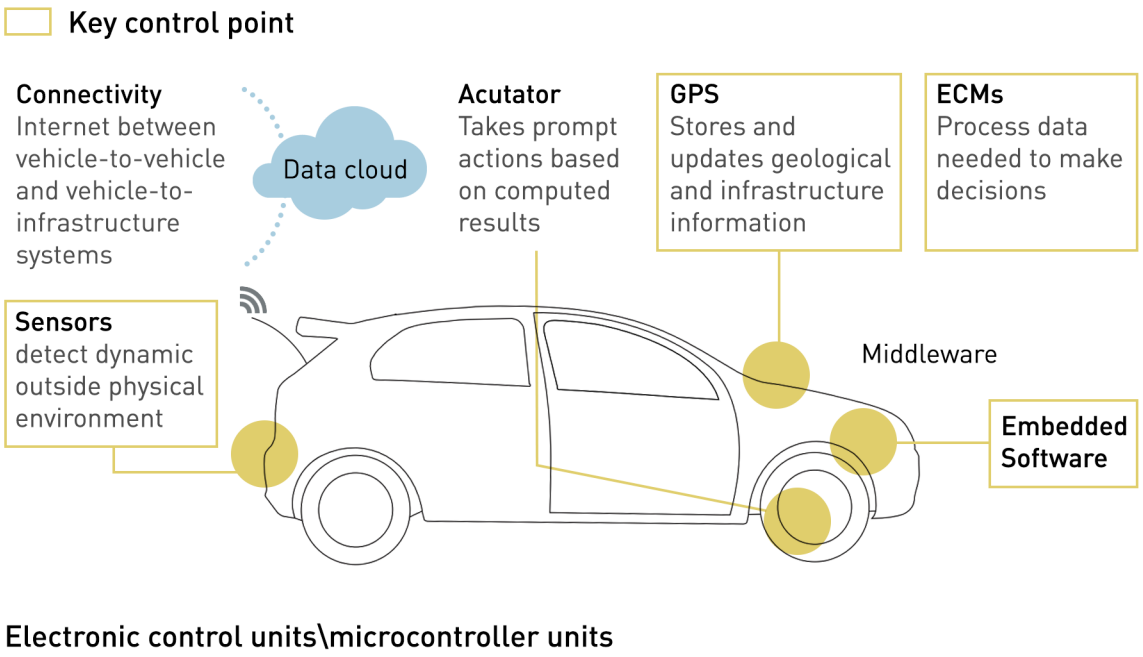

Figure 3. ADAS relies on a combination of hardware and software – both of which must be safety-certified to minimize risk.

TAKING ADAS TO THE NEXT LEVEL: AUTONOMOUS VEHICLES

Nissan® promises a driverless car for 2020; Tesla® tested a 90%-autonomous car in 2016; Volvo®, BMW®, Google®, and Uber® are other major players in the dash for driverless cars. Uber even took an autonomous 18-wheeler for a test drive – delivering 50,000 cans of Budweiser® beer on a 120-mile run in September 2016. Some pundits predict fully autonomous cars will be commercially available by 2025, while Bosch® and NVIDIA® are working on a project that could provide a Level 4 (completely autonomous) car by the end of 2018. (10) Several states, including Nevada and California, have already passed laws allowing driverless vehicles on state highways.

If the legal battle between Google (Waymo®) and Uber is any indication (11), the stakes are high and some of the biggest names in the auto industry will be vying for first place. Therefore, any ADAS technology that gains early support could have an advantage by being adopted as an industry standard. Royalty payments for companies that secure intellectual property for their ADAS technology early can be collected for a longer period of time.

But the risks are substantial. The driver of a Tesla Model S electric sedan was killed in an accident in 2016 when the car's vision system failed to react to a tractor-trailer making a left turn in front of the Tesla (following that crash, the NHTSA reported that no safety defects contributed to the crash) (12, 13). The same year, a self-driving Google vehicle was involved in a crash, striking a bus while attempting to navigate around an obstacle. In March 2017, one of Uber's self-driving SUVs crashed onto its side after another car failed to yield to the Uber car. (14) Obviously, such incidents could result in recalls, legal action, and reputational harm.

The Perfect Autonomous Driving Solution

Process 1 GB of data every minute

Provide 360° awareness

Detect errors and threats instantaneously

Be secure

Be flawless

Still, these sorts of problems may not be the most serious risk automotive developers face. The autonomous vehicle market is moving fast, and companies that hesitate due to fear of risk may never catch up – something no company can afford. The secret is to minimize risk while developing cutting-edge, next-generation technology:

- Use proven, certified software development tools combined with hardware designed specifically for ADAS applications.
- Choose a compiler that can efficiently exploit the hardware's safety and security features.
- Choose tools, including performance libraries, that allow you to write efficient, high-performance software that is also safety-enabled.

Other best practices include protecting the entire data path from sensor to actuator, validating input and detecting and preventing attacks (see the next section), and educating vehicle owners through compelling channels so they know how their ADAS features work and can use them optimally.

BOOSTING SECURITY FOR OTA UPDATES

Software is a big part of the embedded solutions that make up ECMs, PCMs, ADAS, V2X, and IVI systems. GM recently hired more than 8,000 software developers, while Bosch employed about 14,000 software engineers in 2016 alone (15). All this software will need to be updated frequently. But taking the family van into the dealer for monthly ADAS system updates is more than most consumers are willing to deal with. Therefore, the industry is moving toward over-the-air (OTA) updates (see Figure 4). In a similar vein, as V2V and V2X technologies gain ground, connected cars will learn from each other and send each other updates.

While OTA updates are convenient for both automotive companies and consumers, and essential to the connected car, they do raise cybersecurity and privacy concerns. In October 2016 the NHTSA issued guidance for increasing automotive cybersecurity, which underscores the importance of making cybersecurity a top leadership priority for the automotive industry. In addition to product development, the guidance suggests best practices for researching, investigating, testing, and validating cybersecurity measures.

To increase cybersecurity for OTA updates, it is crucial to use hardware and software featuring built-in security features. For example, some microprocessors include an integrated hardware security module (HSM). Compilers can help increase security through the use of cryptography libraries. And of course, as for all automotive electronics solutions, embedded solution developers must embed security in the development process and rigorously test for quality.

Compilers can assist with RTOS configuration and debugging of time-critical embedded applications that require a high degree of modularity and configuration. In particular, OTA updates require the combination of compiler and RTOS to support position-independent executables (machine code modules that are placed somewhere in primary memory and execute properly regardless of their absolute address).

THE TIME TO ACT IS NOW

The modern car is software-intensive; it's essentially a computer on wheels. As ADAS features, IVI systems, electronic control of the engine and powertrain, and increased connectivity become even more ingrained in the industry, those companies that can manage risk while at the same time move quickly in this super-competitive market will be the winners. Proven safety will be a significant differentiator. For example, Toyota has announced that it will invest more than $1 billion in artificial intelligence over the next five years to improve car safety. Its business case? Better safety can be used as a major selling point for its cars. (14) In addition, customers can potentially save significant costs by using autonomous vehicles, such as trucks, buses, and taxis.

With significant revenue – and your company's reputation – on the line, you can't afford mistakes. Like a sports car, you need to move quickly and accurately. It's smart to invest in the best hardware and software available, so you can create the best, highest performance embedded solutions possible.

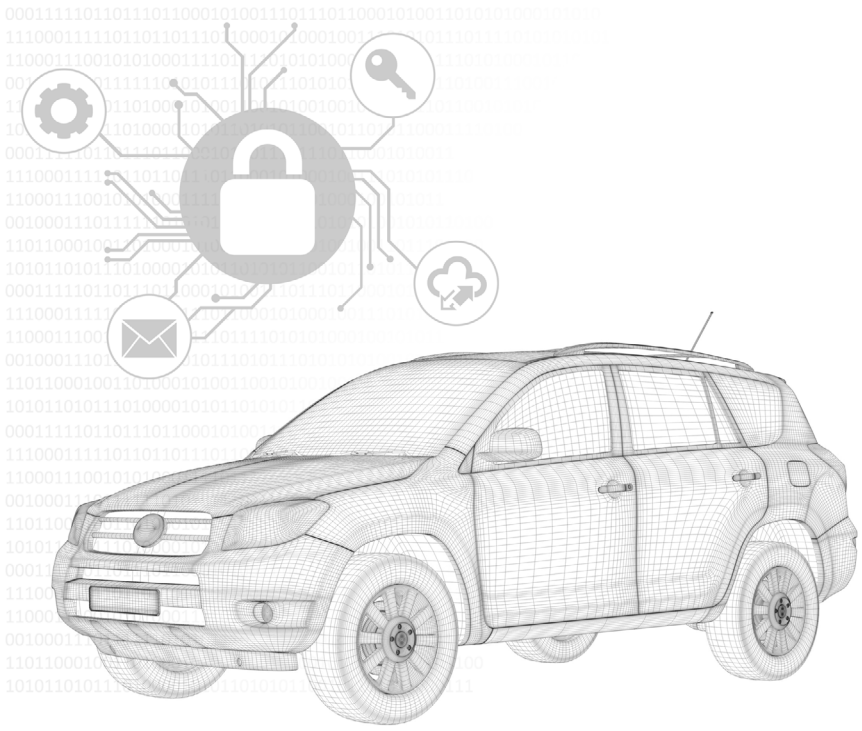

Figure 4. OTA updates are convenient, fast, and essential to the connected, modern car. Choosing the right hardware and software to develop solutions can enhance OTA cybersecurity.

REFERENCES

(1) Advanced Driver Assistance Systems (ADAS) Market: Global Industry Analysis and Opportunity Assessment 2014 – 2020, http://www.futuremarketinsights.com/reports/advanced-driver-assistance-systems-market

(2) Global Forecast, http://www.marketsandmarkets.com/Market-Reports/automotive-vehicle-to-everything-market-195646098.html?gclid=CKT-ssnR79ICFQ5EfgodT_0OIA

(3) Regulation, consumer demand drive future IVI and ADAS markets, http://embedded-computing.com/articles/regulation-future-ivi-adas-markets/

(4) Volkswagen Drops 23% After Admitting Diesel Emissions Cheat, https://www.bloomberg.com/news/articles/2015-09-21/volkswagen-drops-15-after-admitting-u-s-diesel-emissions-cheat

(5) Top 10 Causes of Distracted Driving—and What They All Have in Common, https://safestart.com/news/top-10-causes-distracted-driving-and-what-they-all-have-common

(6) Distracted Driving, https://www.distraction.gov/stats-research-laws/facts-and-statistics.html

(7) NHTSA to require backup cameras on all vehicles, http://www.usatoday.com/story/money/cars/2014/03/31/nhtsa-rear-view-cameras/7114531/

(8) Advanced driver-assistance systems: Challenges and opportunities ahead, http://www.mckinsey.com/industries/semiconductors/our-insights/advanced-driver-assistance-systems-challenges-and-opportunities-ahead

(9) U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes, https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands

(10) NVIDIA and Bosch Announce AI Self-Driving Car Computer,

https://blogs.nvidia.com/blog/2017/03/16/bosch/

(11) Waymo asks court to BAN Uber from testing self driving cars after claiming it stole 14,000 secret sensor documents,

http://www.dailymail.co.uk/sciencetech/article-4302508/Google-s-Waymo-asks-curt-BAN-Uber-s-self-driving-cars.html

(12) Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says, https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html?_r=0

(13) Uber Suspends Self-Driving Car Program After Arizona Crash, http://www.nbcnews.com/tech/tech-news/uber-suspends-self-driving-car-program-after-arizona-crash-n738591

(14) Tesla Model 3 could be 10 times safer than the average car, says analyst, http://www.cnbc.com/2017/03/23/tesla-model-3-could-be-10-times-safer-than-the-average-car-says-analyst.html

(15) Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles, http://www.strategyand.pwc.com/reports/connected-car-2016-study.

LEARN MORE...

Automotive Safety Standards:

ISO 26262

IEEE 2020

ASPICE

Other Documents:

ADAS Development

ADAS Security

In-Vehicle Infotainment

The Connected Car