Automotive engineering: Careful! Speed bumps ahead

by Oana Lazar from the University of Southampton

What comes to mind when you think of future cars? I'll take a guess: self-driving cars, cars-as-a-service, cars you can call to your front door...you name it! These exciting ideas, known as connected and autonomous vehicles or "CAVs", are quickly becoming a reality. We're no longer talking about the future, but about technology already hitting the road.

CAVs will give freedom to those whose age or reduced mobility prevents them from driving. CAV fleets will enable businesses to send out cars to any location, and will revolutionise emergency services while being the connecting glue of future smart cities. Cars-as-a-service will provide options to those with limited income or space. The automotive industry's concerns are not with the direction CAVs are taking, but with the pace of these developments. The time-to-market is accelerating, and AESIN's April 2020 CyRes report predicts that by 2025 every new car will be somehow connected. Fully autonomous cars are estimated to reduce accidents by 90% if *every* car is fully driverless, achieving SAE/J3016 Level 5 autonomy. But for the time being, it's difficult to imagine this revolution without a transition period, and when human drivers coexist on the road with driverless cars, things become difficult.

When we think of accidents involving CAVs, we immediately think of risk to the safety and security of the passengers. But safety and security are not equivalent, and although it's more exciting to imagine foiling a black hat's attack, we mustn't overlook the importance of finding bugs in software, which lead to systematic failures.

Security is meaningless without safety. It's one thing for several cars to be hacked, causing significant but limited damage, and a completely different thing for every unit running specific firmware to enter the same erroneous states, with distributed but collectively massive impact potentially affecting millions. This makes automotive electronics a high-risk industry, as failures in safety-critical software can lead to fatalities.

In real-time systems, correctness is not just determined by a result, but by the timeliness of that result. For example, an airbag deployed too late is just as useless as an airbag which never deployed. Indeterminism from multicore and parallel processing only make correctness harder. Even today, modern cars have as many as 150 electronic control units (ECUs). Cars are computers on

wheels, with millions of lines of code (LOC) rendering the automotive ecosystem so complex that it can't be understood by a single person. This makes software both difficult to verify, and impossible to exhaustively test. Such complexity and connectivity increase attack surfaces, but also makes debugging more difficult. Additionally, increasing cyber resilience could mean engineering significant differences into different models to eliminate similar single points of failure. Integrating IP from multiple companies further increases complexity, obliging a tradeoff between safety and security.

ASIL (automotive safety integrity level) puts risks at different levels depending on their impact and likelihood. While the impact of a successful hack could be disastrous, its likelihood is expected to be minimal. But when it comes to software bugs this likelihood jumps close to 100%, as we have yet to write entirely error-free code, and it's hard to believe formal methods will save us from errors as these methods have been around for 40 years. "Secure by design" is a great but ultimately unachievable goal, especially for a product with a minimum lifespan of 8 years. With CAVs, unlike phones, one can't stop offering updates, but likewise, backwards compatibility cannot be sustained forever. Even by replacing ECUs entirely, the issue of interfacing with sensors which could be a decade old will not be solved. Additionally, hardware is physical and will at some point fail, just how brake lights sometimes stop working, but we need to ensure the systems in place can detect and signal this, allowing the software to recognise and adapt to the change, and the CAV to fail safely.

Failures don't necessarily originate from external malicious attacks, but could very well be generated from within the system, so any supervision solutions should not just detect attacks, but also variances outside acceptable parameters. We don't necessarily need to focus on building a hacker-proof system, as there will always be the 0-day vulnerabilities. A better way would be to create systems which detect changes and allow CAVs to respond to those changes accordingly. On-board diagnostics data such as from OBD-II ports shouldn't be used just for monitoring, but also for launching timely countermeasures through embedded analytics to manage a CAV's life-cycle. But maintainability is not just about patches, but also about adding new features, which could in turn lead to new bugs or break previously functional systems.

This is where the concept of digital twins comes in: a virtual representation of the car which is updated over-the-air (OTA) using on-board diagnostics data such as from OBD-II, especially useful if cars have malfunctioned or entered scenarios not predicted. Simulations and emulations, together with AI, can equally be used on the digital twin to evaluate the CAV's adaptability and response to different situations, and these can create feedback loops to continuously improve safety.

People aren't specifically afraid of hacking, but more of its end result: malfunction, regardless of what caused it. A single plane crash can scare people from flying, despite the statistics showing that flying is almost guaranteed to be safe. Likewise, a single bug-induced CAV crash will make world news whereas thousands of drunk drivers will not. And when it comes to CAVs, it's not just about those who choose to buy them, but also about those who will have to share a road with them, and thus share the risk.

Although safety risks can come from within, so can the solutions, and all of us can be part of this exciting future! Regardless of whether we're directly working in the industry or as future customers, we will have an impact on the future of cars.