DRIVING AMBITION

Graeme Simpson *reports on the challenge of building cyber-secure cars for the unknown future*

For many of the UK's car owners, airbags are an assumed feature in any car. In fact, it's safe to say that any modern car found on our roads in the past decade had airbags. Yet, car manufacturers aren't obliged, legally speaking, to fit airbags – so how has it become an expected standard within the industry?

The answer is not customer safety, but customer expectation. Thanks to initiatives such as EuroNCAP, a five-star rating system assessing a vehicle's safety, rather than simply meeting the legal requirement for safety, car manufacturers have been pushed to continually raise the bar. Clearly some manufacturers, such as Volvo, make good use of safety as a marketing tool and this inevitably leads to others investing in safety features to keep up with growing expectations. The result is that cars are now far safer than they used to be and typically far safer than the minimum legal requirement.

But what about cyber security? When it comes to vehicles, most people will think of cyber security as whether or not someone can steal their car. This might be an inconvenience, but it is hardly life-changing. Security isn't just about physical theft, however, it can be about taking control of or disabling key systems within the car or using personal information such as payment data that's held on a device within it – now that could be life-altering.

A car's cyber security should be considered as important as its safety

What if we call it cyber safety instead? That might make people think about it differently and consider that it is at least as important as their airbags. But a name change alone is unlikely to have a great impact. If we're hoping for consumers to expect cyber protection in modern vehicles, we need to first consider how we drive awareness. So how can we get people thinking about cyber protection (for both safety and security) and the impact it could potentially have on them?

Vehicle cyber protection is on few peoples' radar at the moment, but it should be. Back in 2015, car security researchers Charlie Miller and Chris Valasek demonstrated that they could take control of a number of functions of a Jeep Cherokee remotely, enough to cut the transmission and force the vehicle into a ditch while 'driven' by a terrified journalist. The scariest thing about this demonstration was that Miller and Valasek could have applied the same effects to hundreds of vehicles simultaneously if they had chosen to do so. The potential result would have seen a lot of drivers and their passengers relying on their airbags. Assuming they hadn't been turned off remotely, of course.

Since 2015, a lot of progress has been made with car security, but it's still not keeping pace with the new features being released. Consumers are clamouring for the latest and greatest feature for their cars and manufacturers are unsurprisingly keen to maintain their competitive advantage, even if that means launching a feature without the appropriate cyber protection. As an industry, we need manufacturers to fear launching a new feature without good cyber protection more than they fear launching before their competition or for a greater cost. Unfortunately, it is unlikely to make it onto the priority list until cyber protection impacts how consumers spend their money when they're on the forecourt or legislation drives them to meet a standard. That is, of course, assuming that consumers pick up the importance of cyber protection. At the moment it would still be difficult to determine whether a given car was more or less cyber protected than one of its peers.

This unfortunately is nothing new. How does a consumer currently know whether the airbags in one car are better than those in another? Quite simply, they don't. And what else do you need as well as airbags? Vehicle safety is now a mix of active and passive measures with a layered approach and is a key design consideration from the very outset of any development project. While it's possible to take a very simplistic stance that more airbags are better than fewer, we still don't really know if they are effective. Unless, of course, they do research in advance and use rating schemes such as EuroNCAP.

WE'RE ENCOURAGING MANUFACTURERS TO BUILD SECURE DESIGN INTO CARS FROM DAY ONE

Right now, there is no equivalent to help consumers make an informed decision about the cyber security in a vehicle. However, all that is set to change with 5StarS, a cyber assessment framework in which Roke and Ricardo, together with consortium partners, Thatcham Research, Horiba Mira and Axillium have been working since 2017. The aim of the 5StarS cyber assessment framework is to judge the quality of cyber protection built into a car using a range of measures that follows the complete design life of the vehicle, not just an assessment at the end of the process. This will condense a thorough cyber assessment into a significantly more digestible five-star rating. No-one knows whether one manufacturer's firewall is better than the other, but at a glance it's easy to know that a five-star car should be more cyber secure (and cyber safe) than its two-star competitor.

Such a rating scheme will enable manufacturers to gain assurance for their products, use resilience as a market differentiator and establish meaningful ways of communicating cyber security risks to consumers. And, as a member of the 5StarS project since its inception, I can assure you that confidently assessing a vehicle for cyber security is not without its difficulties. When you crash a car into a wall at 40mph, you can be fairly sure that you'll get the same result if you perform the exact same test on a different day, not least because they are designed against standards and with years of experience in improving the test correlation.

The test is easily repeatable, assuming you've got a good supply of cars to keep crashing. It's not so simple with cyber security as current and emerging threats change over time, often rapidly and this occurs not just during the development time, but after the car is sold. New threats, vulnerabilities and techniques are introduced all the time, making it difficult to judge the likely outcome for a given car 12 months after test day.

One such way to counter this challenge is to balance the practical vulnerability tests performed on the completed vehicle with a measure of how much cyber protection has been built into it from the beginning. We're currently using our newly established, dedicated facility to assess a number of vehicles to establish a cyber security benchmark for cars that are already on the road. This has given us a good understanding of how different manufacturers have approached the topic of cyber security and allowed us to help identify modifications that would improve future vehicles' resilience to cyber attack. For example, as part of our assessment manufacturers are questioned on a range of factors from the level of cyber security training given to their programmers and how they test their code, to whether or not their incident response teams have the full support they need to be able to operate effectively.

This approach isn't without precedent; around the turn of the millennium, Microsoft was enjoying near universal adoption of Windows, but was justifiably being hammered for the lack of security built into the product. Rather than concentrate on just patching the holes, it went back to the beginning and made sure its development processes included security from the start. It wrote several books on the topic – some of which remain key texts for developers to this day.

We're taking the same approach, encouraging manufacturers to build secure design into their cars from the beginning and to adopt a continuous improvement philosophy. The encouragement comes in the form of the 5StarS assessment, which once achieved, manufacturers can boast about to prove their good work and hopefully help them to sell more.

The proposed assurance framework, announced on 26 June, 2019 and explained in the 5StarS white paper *A Roadmap To Resilience: How The Automotive Sector Can Build Trust In Connected Vehicles* outlines four distinct components: product development (concept and design); production, operations, maintenance and decommissioning; cyber security governance and management; and vulnerability assessment.

Vehicles will be scored on each component – in accordance with the UK Government Department for Transport Principles of Cyber Security for Connected and Autonomous Vehicles – and provided with feedback to allow them to resolve any issues. This is a far more positive approach than simply crossing their fingers and hoping the competition falls short before they do.

It's set to inform consumers' buying decisions and lets the industry address cyber threats as they emerge. We're confident that the framework will tackle the issues posed by new technologies, making sure it remains a benefit to both consumers and the industry.

Now is the time for manufacturers to approach cyber protection with the same mature attitude that they have traditionally adopted for safety. Rather than release features and then wait to see what happens, let's build good cyber security in from the very beginning ●

The 5StarS consortium

The 5StarS consortium was created in 2017, funded by Innovate UK. It brings together automotive industry experts: Roke, Ricardo, HORBIA MIRA, Thatcham Research and Axillium. The team has now published a framework for vehicle manufacturers to implement in response to the technological developments that face the automotive industry. It provides vehicle manufacturers with a measurement of their vehicles' resilience and allows stakeholders to quantify their risks from connectivity.

Graeme Simpson – Engineering Service Lead for Cyber Protection at Roke – has 21 years of expertise in the cyber field, working across many industries and global locations. He currently focuses on Digital Resilience for Automotive.

The aim of the 5StarS cyber assessment framework is to judge the quality of cyber protection built into a car