Automotive World
Software-Defined Vehicle
MAGAZINE

Issue 3 | February / March 2025

Timing silicon future-proofs SDV performance, says Renesas

Qualcomm underpins industry evolution to SDVs | **Valeo** outlines a new OEM-supplier dynamic | **SDVerse** provides an 'Amazon' for auto software | **Plus** develops software-defined ADAS | **Aptiv** accelerates OTA with telecom tech | **SOAFEE** aims to standardise software innovation

© iStock/metamorworks

Cyber security strategy: SDVs raise the stakes

With functions and features increasingly defined by software, how can automakers ensure their products are secure?
By Megan Lampinen

Cyber security has been a growing concern within the automotive industry, particularly as cars become more connected. Formal hackathon events and independent white hat exploits by researchers have demonstrated that it's technically possible for a remote actor to access all sort of vehicle systems. From hijacking driving controls and causing sensor hallucinations to capturing the wireless modem that receives over-the-air (OTA) updates, playing video games on the infotainment system and interfering with the windshield wipers, no system is fully secure from intrusion. But in terms of documented, in-the-wild, on-the-road cyber attacks on connected vehicles, these are few and far between.

"Given some of the well-publicised vulnerabilities, one would expect to have seen numerous attacks," notes Dante Stella, a cyber security lawyer with Dykema. "Several things could explain why we haven't."

To start with, there doesn't seem to be an easy way to monetise these vulnerabilities, and Stella notes that many potential cyber criminals remain unmotivated by vehicles. At the same time, the lack of software uniformity across manufacturers makes it more difficult for malicious actors to create economies of scale when developing attack techniques. Stella also suggests that the number of connected vehicles in operation is probably "still too small to excite state actors bent on paralysing infrastructure or inspiring

OTA updates open up new attack vectors

other terror." That said, attackers with sufficient incentives could still cause damage to a targeted vehicle.

So far, most of the cyber attacks within the mobility sector have involved stealing customer data from customer service departments, ransoming production systems, and pranking electric vehicle (EV) charging stations. "None of that is good, but we are not in the 'robotaxi revolt' phase," Stella tells *Automotive World*. "Well, not yet."

Software is in everything

While a fully autonomous ecosystem remains a distant prospect, the age of the software-defined vehicle (SDV) has arguably arrived. The industry has begun to position for a future in which vehicle functionality and the customer experience are shaped by software. With OTA updates, both of these can continually evolve over a vehicle's lifetime.

"Software is in everything," asserts Brian Irwin, Managing Director with Alvarez & Marsal's Automotive and Industrials group. The firm's Global Cyber Risk and Incident Response Services practice advises on cyber resilience and assists with cyber threat hunting, code reviews and penetration testing as well as red teaming. "Software runs throughout the entire vehicle–it's even in the rear-view mirror." Some modern vehicles have upwards of 150 million lines of code. In comparison, an A737 airplane has 75 million lines of code. This new paradigm raises several new potential security concerns.

"SDVs accumulate vulnerabilities by an increasing reliance on a stack of software components–some purchased as commodities, some open-source, some custom-developed," Stella explains. "Every component of the stack can have its own vulnerabilities, including 'inherited' ones." For example, if a car leverages a version of an operating system that has a particular vulnerability, the car could have that same vulnerability as well. This puts the focus on supply chain management and the use of software bills of material (SBOMs) to know exactly what goes into a vehicle.

Stella notes that this software stack offers multiple points of entry for compromise in the SDV's manufacturing or software update process through supply-chain attacks. "Should a threat actor compromise the systems of a supplier that provides one of the software components, a fleetwide vehicle software update could effortlessly proliferate a vulnerability or malware to hundreds of thousands of cars simultaneously."

Ruediger Ostermann, Vice President and Chief Technology Officer of Global Automotive for TE Connectivity, similarly flags the supply chain as a key security focus within the rise of SDVs. "GM and Ford don't build things like high-performance computers themselves," he notes. "They rely on suppliers to provide them and ensure their development processes contain an element of cyber security validation."

Standards and best practice

This is where regulations and guidance on best practice play an important role. The UNECE World Forum for Harmonization of Vehicle Regulations' (UNECE WP.29) regulation on cyber security (R155) requires all new car lines launched from existing electronic architectures to obtain cyber security system type approval as part of the whole vehicle type approval process. R156 issues similar requirements for OTA updates.

At the same time, the industry is establishing SBOM standards and procedures to ensure that software is sourced and deployed in such a way as to ensure the integrity of the stack, identify vulnerabilities, correct or compensate for them, and trace any apparent issues. Auto-ISAC (the Automotive Information Sharing and Analysis Center) is one of the groups leading the push for industry-wide standards, practices, and procedures for SBOMs.

While Stella observes that SBOMs could help curb risks with 'buy' versus 'make' software, he cautions that "automakers will always run into a tension between effectiveness and economic reality. The most secure systems would be built in-house using principles of security by design and least access."

In practice, that's not terribly realistic, at least at the moment. As he elaborates, tremendous cost pressures serve as a powerful incentive to use commodity or lightly customised software components rather than reinventing them. On top of that, automakers are not typically vertically integrated, and some systems are designed by suppliers that may provide the same hardware/software components to numerous OEMs. Similar base hardware and software could create shared vulnerabilities, and "the desire to accommodate future software changes could lead to systems that are more flexible–and vulnerable–than they need to be," he warns.

Playing with fire

The challenge of securing SDVs is made more difficult by the growing industry pressure to innovate at an accelerating rate, and for automakers to be the first to market with new features. "Technology in vehicles is increasing exponentially. Consumers want artificial intelligence (AI), electrification and new customer experiences," says Rocco Grillo, Managing Director and Head of the Global Cyber Risk and Incident Response Services at Alvarez & Marsal. "If you don't bring your idea to market first, 100 other companies could grab it, make it better and bring it to market themselves."

“

A fleetwide vehicle software update could effortlessly proliferate a vulnerability or malware to hundreds of thousands of cars simultaneously

The trouble, as he sees it, is that some players may overlook something or fail to test sufficiently. “That race can’t be at the expense of security,” Grillo emphasises. “You can’t just tack it on at the end. Technology is like fire: it’s good, but if you don’t manage it, it could result in a crisis or even become catastrophic.”

AI in particular has prompted concerns among consumers, but it’s impact on cyber security is currently unclear. “It is difficult to predict the extent to which AI will pose a threat unique to SDVs,” says Stella. “We know already that threat actors use AI for social engineering–tricking people into giving up credentials–and for writing malicious code and defeating endpoint protection. As vehicles lean more heavily into AI for delivering driving dynamics or entertainment, we can expect to see attempts to influence those systems or cause them to fail.”

His advice to developers within the SDV ecosystem is pragmatic: incorporate security, privacy, and data minimisation consistent with emerging data protection laws and DevSecOps principles; explore layered defences, so a single vulnerability does not hand an attacker the keys to every system in an SDV; carefully consider the cost/risk trade-offs in software sourcing choices; and aggressively manage the software supply chain, using SBOMs and other methods, to enhance verification, auditing, traceability, and accountability.

These steps should provide a practical foundation for secure vehicles, though nothing can ensure complete protection. “As technology evolves, cyber risk will evolve too, without question,” says Grillo. “The threat actors will find ways to circumvent controls. It doesn’t mean that we unplug the internet–that’s the only way you’d really be 100% secure.”

Irwin points to the phrase “with great power comes great responsibility”, a sentiment found in various wordings across historic texts but popularised by the Spider Man series. “As we embed greater and greater feature functionality, the opportunity for disruption increases. Those responsible need to up their game and make sure that we’re protected.”