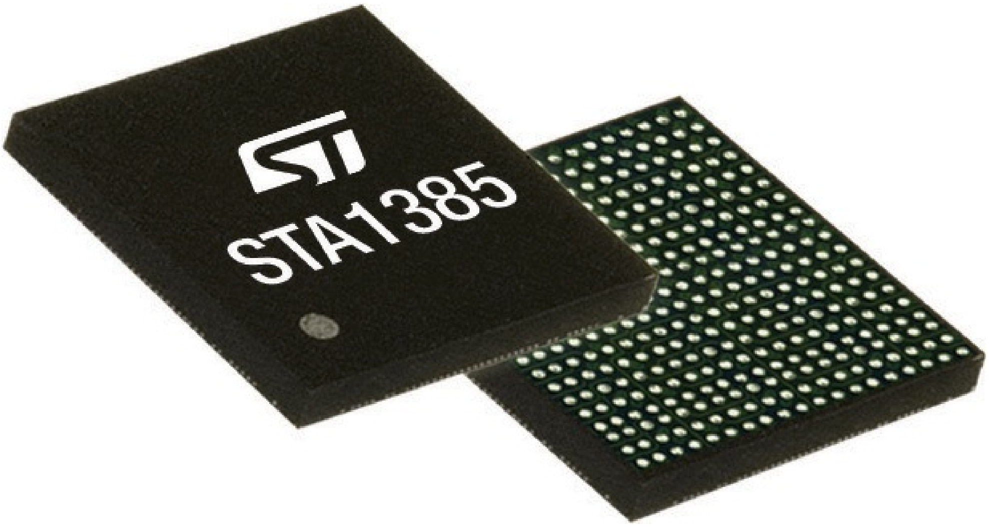
Protecting cars against cyber threats

STMicroelectronics protects connected cars against cyber threats with its latest automotive processors that feature built-in security and CAN moduls.



STA1385 is an automotive, System-on-Chip, targeting processing solutions for telematics and connectivity applications including cyber-security protection (Photo: STMicroelectronics)

Millions of connected cars are already on the road, and industry analysts predict there will be more than250 million by 2020. Connected services supported by on-board telematics units, Wi-Fi hotspots, Bluetooth devices – and aftermarket equipment such as on-board diagnostics (OBD) dongles – enable drivers and passengers to be safe, productive, socially connected, and entertained on their journeys. Unfortunately, all this connectivity builds a real surface of attack for hackers.

Automotive groups are addressing security measures to support growth in valuable markets for connected services. This includes content streaming, location-based assistance, emergency support, and remote software updates over the air of in-car electronic control units (ECU), while preventing hackers exploiting the connections for their own ends. Experts recommend manufacturers employ a range of techniques, including establishing trust in connected devices and securing all connections, to provide multiple layers of defense throughout the vehicle's circuitry and software.

ST claims that its Telemaco3P telematics and connectivity processors (STA1385 and its variants) are the first automotive micro-processors to integrate an isolated Hardware Security Module (HSM), which acts like an independent security guard to watch data exchanges and encrypt and authenticate messages. The HSM checks the authenticity of received messages and any external devices that try to connect and protects against eavesdropping.

With this HSM on-chip, Telemaco3P devices are ahead of the general-purpose application processors typically found in current connected-car systems, which lack dedicated hardware-based security, said the company. ST's chips also comes with a 105 °C maximum temperature rating for use in locations that can become extremely hot, such as on top or directly beneath the roof in a smart antenna. The HSM also runs software-security algorithms, giving freedom for the main high-performance CPU to host more applications.

Integrated CAN FD, Gigabit-Ethernet, and 100-Mbit/s Secure Digital I/O interfaces allow the Telemaco3P family to be used as communication gateways throughout the vehicle, for linking infotainment systems, or ECUs connected to the CAN network. This includes door controllers, engine or transmission management systems, or body electronics. The Telemaco3P features two CAN FD and one Classical CAN interface. Essential power-management circuitry is also integrated.

The STA1385 is designed to comply with the automotive functional-safety standard ISO 26261, up to safety integrity level B (Asil-B), and meet the Autosar specification for protected communication across the CAN network. Telemaco3P devices can run Posix-compliant operating systems (OS), giving users flexibility to choose their OS for a variety of intended use cases.

"Realizing the benefits of connected cars requires strong protection against cyber-attacks," said Antonio Radaelli, Infotainment Business Unit Director, Automotive and Discrete Product Group, STMicroelectronics. "Our new Telemaco3P processors combine ST's proven expertise in hardware security and knowledge of the automotive industry's standards and requirements to lay solid ground for safe and enjoyable connected motoring."

cw