Electronic Design

ALAN R. EARLS, Contributing Editor

Adapting to UN Regulation 155: Automotive Cybersecurity Solutions

Regulations increasingly drive automotive engineering and electronics. This UN regulation is now reshaping markets in dozens of nations, including North America—fortunately established hardware and software options can help ensure compliance.

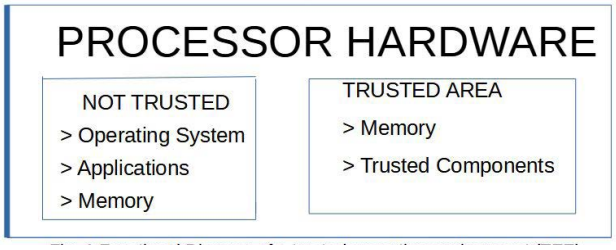
North American automakers have been giving more and more attention to cybersecurity issues in recent years. Given how few actual "hacks" to vehicle systems have occurred, they must be doing something right.

But a recently enacted "global" rule, covering the market in more than 60 countries, combined with an existing standard, means that designers with hopes for export sales or manufacture under license, must make a plan to ensure compliance.

OEMs have been advancing electronics and software to provide drivers with an improved user experience and connections to the outside world. These systems, as well as over-the-air (OTA) updates, provide potential attack avenues that could lead to loss of intellectual property, loss of privacy, and security for vehicle occupants—and even potentially compromise the safety and performance of the vehicle.

OEMs are increasingly looking at the challenge of securing the whole system to ensure safety and security for everyone. And they're recognizing that security needs to start with design, often referencing the ISO/SAE 21434 standard, a joint effort between ISO and SAE to create a global cyber standard for automotive.

That focus on design is now receiving an additional impetus from the implementation of United Nations Economic Commission for Europe Regulation 155 (UNECE R155). It mandates not specific technical details, but rather an end-to-end cybersecurity process that reaches into the supplier community, too.



A trusted execution environment (TEE) is one of the primary tools for ensuring cybersecurity compliance in vehicle electronic systems.

Not yet applicable in the U.S. or China, UNECE R155 is nevertheless expected to become relevant in North America either as a preparation against the future or to ensure the goods and designs can be sold in other markets.

What are the Compliance Requirements of UNECE R155?

UNECE R155 applies only to OEMs, but it requires each OEM to document compliance with the regulation by each supplier. The OEM has a lot to do with defining how this is done and that the whole result meets UNECE requirements. Implementation of ISO/SAE 21434 by OEMs provides guidance, such as a cybersecurity interface document or agreements to establish cooperation and avoid obstacles between suppliers, customers, and others

Some of the team and organizational issues to consider as part of conformance with UNECE R155 ISO/SAE 21434 include risk analysis that looks at the whole vehicle lifecycle. This includes a vulnerability monitoring and management

practice, careful selection of programming languages that can best ensure security, and making sure that there's a plan for dealing with any incident (such as discovery of a vulnerability or an actual breach or hack).

How Can Hardware Help with Cybersecurity?

While most cybersecurity action in vehicle development and operation will likely involve software, some very specific hardware elements can be critical to success. Two of the most prominent are hardware security modules (HSMs) and trusted execution environments (TEEs), which work with hardware.

An advanced driver-assistance system (ADAS) as well as systems that support growing vehicle-to-everything (V2X) communications need security. So, too, do the systems that deliver ubiquitous cloud and telecom network connectivity. These systems can generate large volumes of data movement, which can leave systems vulnerable to attack or corruption.

How Can HSMs Keep Data Safe in Vehicle Systems?

An HSM typically is installed into electronic control units (ECUs) to provide cryptography that can protect vehicle communications and internal control systems. Equipped with its own dedicated memory and firmware, the HSM safeguards vehicle communications and functional control systems with message cryptography. Typically, an HSM will include a dedicated processor and embedded cryptographic technologies, so that it's not dependent on the ECU.

Of course, vehicles with multiple ECUs—and that's a pretty big set, with most cars having dozens—ideally would have an HSM for each one. However, not every ECU needs an HSM, but they're advisable for ECUs requiring robust security. That means where the integrity and authenticity of a system could be compromised and hardening must be assured, and to protect key embedded systems against attacks.

The important job handled by HSMs typically includes performing a variety of cryptographic functions, holding keys, assessing the authenticity of messages passing through, and verifying digital signatures. Thus, it should help keep internal systems safe while also not passing dangerous data to other systems.

But HSMs—because they're hardware, not software—lack flexibility and are challenged in environments where systems are periodically updated; for example, through OTA systems.

The hardware-software segregation in advanced vehicle architectures requires a more flexible approach to cybersecurity. It must ensure cybersecurity measures evolve hand-in-hand with vehicle software developments.

What's a TEE and How Can It Enhance Security?

An alternative to HSM is a trusted execution environment (TEE), which replaces the HSM with a software-based security measure that implements in an isolated hardware area within a given processor, walling-off critical functions and keeping them secure *(see figure)*.

Both HSMs and TEEs can store keys and other sensitive information while also maintaining a secure execution environment.

A big difference is that TEEs are incorporated within the processor chip set and can be initiated and updated via software. As a result, they have a great potential for upgrading and adapting to evolving needs. They use hardware that's already part of the vehicle, potentially reducing some costs while delivering what companies need, customers seek, and regulators demand.

References:

USDOT Releases National Deployment Plan for Vehicle-to-Everything (V2X) Technologies to Reduce Death and Serious Injuries on America's Roadways

EU Cyber Resilience Act