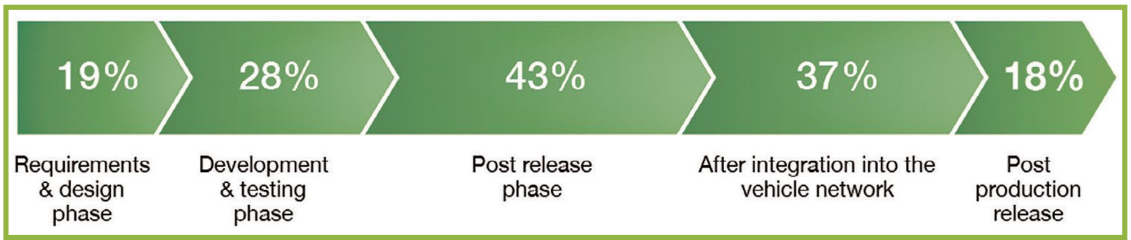
Secure chips from the outset

Pre-silicon verification of hardware security is crucial, argues **Sergio Marchese**, yet more robust, efficient design flows are needed



Percentage of companies that assess security vulnerabilities of automotive software/technology/components at a specific stage during product release

Advanced electronic systems for connected autonomous vehicles (CAVs) and other safety- and security-critical applications use complex software stacks. At the bottom of the stack are ICs which include general purpose and workload-optimised processing engines, and other semiconductor IP.

Hardware vulnerabilities may compromise the entire system. To ensure that ICs – both asics and FPGAs – have high integrity it is necessary to have adequate hardware development flows that deliver evidence of functional correctness, safety (ie. that they can prevent or control failures that could occur during operation due to physical effects), and trust and security (ie. that they do not include unexpected or malicious additional functions).

Sometimes referred to under the title ‘data sanctity’, integrity properties are not an after-thought. All IC and IP development stages, including pre-silicon validation and verification, need adequate tools and methods to achieve high integrity. The safety and privacy of people is at stake.

Proving the functional correctness of complex hardware designs is challenging. Over the past 20 years new electronic design automation (EDA) technologies and methods have emerged to address the task.

Safety requirements used to be confined to niche, low-complexity applications. In the past 10 years, this has changed dramatically. With the advent of advanced driver assistance systems (ADAS) and developments towards self-driving cars, new and established IP and IC providers have deployed functional safety flows for the development of complex electronic systems.

The ISO 26262 functional safety standard for road vehicles has enjoyed widespread adoption since its first draft was published more than 10 years ago. Hardware security, on the other hand, is in its infancy. Industry, academia and governmental institutions openly acknowledge that security is not only a software issue. Moreover, hardware functions implementing intelligent security mechanisms can also be part of the solution, reducing the need for software updates and security patches.

Confidentiality, integrity and availability

Most chips include features that are used by software layers to implement security functions. Examples include authentication, the handling of signatures for secure over-the-air software updates, and fast encryption and decryption of secure data.

Certain hardware memory regions may be reserved and accessible only to applications with high privilege level. Some registers may contain secret data, for example an encryption key.

In more general terms, hardware must ensure that information security is maintained. This includes ensuring information confidentiality, integrity, and availability (CIA).

Attackers may try to extract a secret key, for example, thus breaking information confidentiality, sometimes referred to as data leakage. They could also try to overwrite the secret key, replacing the lock rather than stealing the key, thus breaking information integrity. Both information confidentiality and integrity are critical aspects of hardware security that need rigorous pre-silicon verification.

At present, commercial EDA tools offer proprietary methods to describe and verify information flow requirements.

A standardised method would enable tool interoperability, improve reusability of requirements across design iterations, and allow providers of semiconductor IPs to deliver executable security specifications that could be independently checked by SoC integrators, and reused to ensure chip-level security.

Standardisation efforts

A recent survey, focusing on the security of the automotive supply chain, found that only 47% of companies assess security vulnerabilities during the early stages of the product release process, namely requirements and design phase, and development and testing phase.

The survey report said: “This process is contrary to the guidance of *SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, which advocates for a risk-based, process-driven approach to cybersecurity throughout the entire product development life cycle.”

The ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering Standard, currently under development, promises to improve this situation, using an approach similar to ISO 26262.

Another important initiative, which goes beyond the scope of automotive security, is the Accellera working group on Intellectual Property Security Assurance (IPSA).

The goal of this working group is to provide a security assurance standard for hardware IPs to reduce and manage security risks when integrating IPs in embedded systems.

SAE has also established a Cyber Physical Systems Security Committee (G-32), which aims to deliver a draft standard by 2021.

The safety and privacy of people depends on the security of complex electronic systems used in autonomous vehicles, aircrafts, medical devices, 5G networks and critical infrastructure.

Security needs to be integrated into all hardware development stages and vulnerabilities need to be avoided or detected early, in the design phase, whenever possible.

Pre-silicon validation and verification of security requirements are challenging, critical tasks. New standards will have a crucial role in driving security awareness and expertise in the engineering community, while also enabling faster technological advances and more efficient flows for secure hardware development.

Source: *Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices*, Ponemon Institute

About the author

Sergio Marchese is technical marketing manager at OneSpin Solutions.