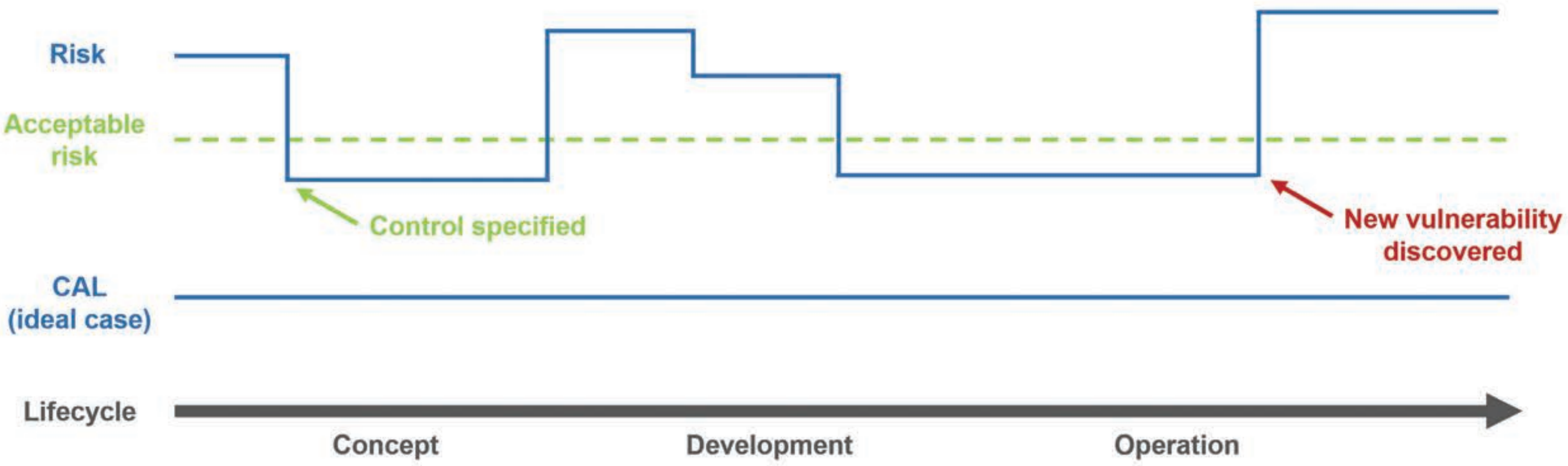
Securing microelectronics for safer automobiles

By John Hallman, product manager for Trust and Security, OneSpin Solutions



Security researchers have demonstrated extensively how cybersecurity attacks can have disastrous consequences in automotive systems. A successful car hack could be extended to an entire fleet of vehicles and put many lives in danger. Moreover, car owners' privacy and the protection of intellectual properties (IPs) and other assets of car manufactures and their supply chain are also at stake. Unlike safety, however, automotive cybersecurity is in its infancy. The upcoming "ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering" standard promises to modernise and harmonise cybersecurity activities across the automotive supply chain.

Hardware security

The ISO/SAE 21434 standard addresses the entire life cycle of electrical and electronic (E/E) systems for road vehicles, from the concept phase to decommissioning. While security has historically focused on software, it has become evident that attacks increasingly involve hardware and firmware weaknesses and vulnerabilities. The MITRE CWE database recently introduced, in version 4.0, a section dedicated to hardware. Hardware development relies on a global, fragmented supply chain, which involves service companies, semiconductor IP and IC suppliers, foundries, and distributors. Trustworthiness and quality of third-party components cannot be assumed but needs to be supported by adequate processes and evidence. A security-by-design methodology, rigorous pre-silicon verification and assurance strategy are crucial to increase confidence and generate objective, auditable metrics and reports. Dedicated electronic design automation (EDA) tools and solutions for functional correctness and trust and security of semiconductor IPs and ICs, such as the ones provided by OneSpin Solutions, can be used to implement automated, scalable hardware security assurance flows.

Threat analysis and risk assessment

TARA is the security counterpart of the ISO 26262 hazard analysis and risk assessment (HARA) process. It is important to list a system's assets and their cybersecurity properties, including confidentiality, integrity, and availability. What is perhaps more challenging is identifying threat scenarios that could violate cybersecurity goals and perform a risk assessment. ISO/SAE 21434 demands that for any identified threat scenario, a risk value is determined. This is a number between 1 (lowest risk) and 5 (highest risk). The risk associated with a threat scenario depends on the feasibility of the attack and its impact. If the attack requires a team of expert hackers and costly equipment, the risk is lower than an attack that anyone can execute and lead to the same damage. In the worst-case scenario, the attack is easy to carry out and has severe consequences. The standard does not prescribe a specific method to analyze the system and calculate risk values, but it does provide some guidance and examples. As may be expected, threat scenarios that could lead to high-severity consequences deserve more attention and, potentially, require the specification and implementation of controls for risk reduction (see Figure 1).

The CAL is an attribute that can be associated with a system, a component, or a specific cybersecurity goal. It expresses the level of assurance required for assets. There are 4 CALs, CAL1 being the least stringent, and CAL4 the most demanding. Depending on the target CAL, certain cybersecurity activities can be omitted or carried out with less rigor. A component classified as CAL4 indicates that it might be suitable to perform critical functions that require a high level of security assurance and protection of critical assets. CALs are important to tailor cybersecurity activities according to the target assurance level and simplify communication among stakeholders and parties in the supply chain. Engineers familiar with ISO 26262 will see a strong resemblance between CALs and automotive safety integrity levels (ASILs).

While CALs and risk values are related concepts, they have significant differences. CALs are described in an annex of the standard, an informative (as opposed to normative) section. This could change in the first release of the standard. The concept of risk value and its determination, on the other hand, is part of ISO/SAE 21434 requirements. Moreover, while CALs are, at least in an ideal case, constant, risk values may change during the product lifecycle. A risk value that is deemed too high may require additional controls until it is reduced to an acceptable level.

Incident response

It is critical to continuously monitor new vulnerabilities discovered in hardware and software components and reassess the risk values associated with automotive systems. If necessary, remediation actions must be taken. This is an area where ISO/SAE 21434 differs profoundly from ISO 26262, which has no concept of incident response. Considering that automotive hardware components have a long life cycle, typically spanning many years between deployment and end of support, and involve a complex supply chain, cybersecurity monitoring and incident response are challenging. Rigorous pre-silicon verification and security assurance may have a huge impact on reducing the cost of these activities. Efficient post-silicon analysis, supported by appropriate tools, is also crucial to identify the root cause of a vulnerability and design and validate remediation actions. OneSpin's tools, for example, are also used to analyze and debug post-silicon bugs and flaws in the hardware model.

onespin.com