How Do I Come To Trust An Electronic Component?

Determining what makes a dependable system.

By: Roland Jancke

Can I trust all of the electronic systems in my vehicle, for example if I'm driving my car at a high speed on the highway or in city traffic at a confusing intersection? Will all of the vehicle's sensors work as they should and correctly recognize all of the possible dangers around me?

In modern vehicles and complex industrial plants today, a number of sensors and many electronic components work to process signals and control commands. Reliable, safe operation of the overall system is possible only if they work flawlessly. With vehicles, safety relates to the physical well-being of passengers as well as other users of the road, while for large industrial plants a safety incident can in principle affect an entire population.

So how is trust in an electronic component gained? What is the meaning of trust in electronics and how can we achieve it?

The challenge is for us to be able to rely on components and devices, on their doing the right thing when it matters the most. The issue essentially concerns dependability and the question of what we consider to be a dependable system.

First of all, the wish in general is for the electronic system – like other systems – to react as expected and perform its intended function correctly at all times. This already leads to more specific questions: What functions must be performed? When is a function correctly performed? Generally, it can be said that complete specifications are necessary and must be met exactly and exclusively.

While these tend to be soft criteria, there are properties that can be tested rigorously. For example, high quality electronic components and assemblies are expected to operate reliably in the field for their entire service life. There are international standards that establish requirements that must be met for the quality and reliability of electronic circuits and systems.

Just as important are the safety and security of electronic systems – data security against external attacks and suitability for safe operation. Internationally agreed standards for such already exist for different applications or are currently being prepared. Critical to data security is sufficient hardening to protect against external attacks. This requires security measures in the specifications, and no relevant vulnerabilities may arise outside of the specifications.

Another essential feature for trusted electronics is a transparent supply chain: Can I trust my supplier and how do I "deliver trust" myself? Who will be handling my component over the course of international development and production processes? Is the manufactured and delivered product really identical to the one that was developed and commissioned?

It is tremendously important to recognize and examine possible attack vectors and scenarios in order to be able to find valid answers to questions related to trust in electronics. In principle, there are three different categories: intentional backdoors, unintentional vulnerabilities, and fraudulent products. All of these potential points of attack can have causes and effects at different points in the value chain.

Trust can develop only if it is taken into consideration and implemented end-to-end along the entire chain of suppliers, manufacturers, integrators, and OSATs (Outsourced Semiconductor Assembly and Test). Preferably, trust develops naturally based on effective monitoring based on verifiable criteria. Besides the standard-based criteria already named, additional properties will have to be defined as verifiable rules and standards in the future.

Many activities currently focus on making it difficult to copy integrated circuits and systems. In addition to purely financial damage, copying also results in a loss of trust due to the insufficient quality that results from changed production processes and possibly a lack of qualification.

Of course, a discussion as to what level of protection is actually required for a given application is also always a necessity. Different protection classes have to be defined and the effort needed to reach a specific level of protection has to match the protection goals. That is why the best possible estimates regarding the effort in implementing protective measures will be an important direction for development in the future.

Overall, the path to a trusted electronic system is long: from a custom schematic/layout with the corresponding synthesis tools and integrated third-party IP, to mask production and manufacturing, to testing, verification, and integration. The many single steps and partners involved in international trade relationships result in a large number of possible points of vulnerability and reflect the magnitude of the future challenge in developing more secure, reliable electronic systems.