Focus on security in embedded computing systems

By Harald Maier, TQ Group

In the future, everything will be networked to everything else. The Internet of Things and Industry 4.0 are the key terms in this case. This creates new vulnerabilities for spying and tampering. To counter this, system designers and developers view security as the focus of new developments.

Figure 1. Security plays a central role as early as the product definition and development phases and can sometimes be crucial for the success of the product.

The success story of embedded PC systems began many years ago. Standardization together with the compatibility and replaceability of hardware and software all played and still play a decisive role in this success. Existing printed circuit board assemblies and circuit elements are reused as are software functions and applications. This reduces development costs and schedules. However, it is precisely these advantages that present the greatest vulnerabilities for malicious attacks, abuse, manipulation, the theft of intellectual property (IP) and plagiarism. The topic of the Internet of Things (IoT) and the networked future are exacerbating the situation more and more.

Everyone is talking about IoT. This provides the motive to consider topics such as security with more deliberation. In the networked future, there will be various communication paths together with a large number of interfaces and standards. Being linked to the internet presents a new type of accessibility, too. Going hand in hand with this, several new vulnerabilities for unauthorized access, piracy and abuse are looming. And this is just what is stopping many companies from launching into the new era. The fear of spying and tampering is enormous. Sensitive data, but mainly the systems themselves, need adequate protection and security. Hardware and software packages coordinated with one another to the maximum extent are the best solution to minimize the risks.

Systems and infrastructures used until now were cut off from the outside world and had security measures that were weak or non-existent for this reason. Sensitive data, both user data and special application programs, algorithms and licenses, were stored and managed in the system or in local networks. Even the systems themselves presented little vulnerabilities for tampering or piracy. Direct, on-site access was needed to maliciously cripple a system. Specialized knowledge on the system level was often implemented using a combination of proprietary hardware components and special purpose applications. It was very difficult to copy this.

The possible access modes to systems and data have changed. In addition, IP that should be protected is found more and more in the upper application layers, in the area of software. The desire for update and service demands new concepts and potential access modes. The demand for flexible use and licensing models requires new mechanisms to manage these models. All in all, system designers and developers are facing new challenges and security is playing a major role in all of this. It is necessary to put the focus on the topic of security for new developments and this is not just being driven by buzzwords like IoT and Industry 4.0.

Embedded PC technology can be used in a lot of areas and handles broad application areas due to the flexibility coming from expansions, software compatibility and the availability of the most varied performance classes. The spectrum extends from an intelligent IoT gateway to high-performance computers for demanding automation tasks. Embedded PC applications can also often be found in the medical area. This is precisely where demands for security on extremely different levels come together. These demands include the protection of sensitive data, protection against tampering, protection of application intellectual property, flexible licensing of additional options, usually implemented as software features, and secure communication with the environment.

The system can only satisfy requirements nowadays when the security aspect has been incorporated during the development phase or when embedded PC components are used that already contain the necessary security components and mechanisms. If data and programs are to be stored on a local drive in an encrypted form, functions such as BitLocker from Microsoft – available since Windows 7

Figure 2. The medical PC platform from TQ shows one example of the implementation of all basic security features: TPM support, security controller and wireless options that allow for secure communication and comprehensive protection.

– can be used. These tools access hardware components such as the TPM (Trusted Platform Module) chip to protect the keys used for decryption. The data are only accessible to authorized users. The encryption is also linked to the device so that hackers cannot read any passwords or data even if they remove the hard disk or SSD (solid state drive) and install it into a different system.

In addition, a TPM chip integrated into a system can be used for encrypted communication and for uniquely identifying the hardware to higher-level systems. TPM can also be used to detect hardware and software tampering and, based on this, initiate a secure boot or Roots of Trust. TPM cannot be retrofitted because, besides the hardware chip, the needed functions must be implemented in the BIOS (basic input/output system). More and more intellectual property is in the software, making this a favorite target for hackers and reverse engineering. The ever-increasing network density makes access to this IP substantially easier in the case of systems with weak security. Once the core software is extracted or the license key cracked, the software can be transferred completely or in parts to other systems and used there. Individual algorithms and special functions can be extracted from unprotected program code using reverse engineering and then integrated into other applications. This represents tremendous damage that must be prevented. Security controllers can provide protections here. These are soldered into the system and integrated there.

Functions that need to be specially protected, usually small blocks of code suffice, are encrypted during compilation so that they later cannot be executed on the computer CPU but only in the dedicated security controller of the target system. The software can only run on the intended target system. The encrypted program code blocks can also not be tracked and reverse-engineered during runtime.

The same applies to optional added features that can be activated with a license. If the activation only uses software, it is usually just a question of time and effort until the needed license strings or activation routines are cracked. For secure protection, hardware and software must be coordinated and the license activations (license keys and activation routines) must be run remotely, for example, in the security controller mentioned already. A similar feature is known from the end user arena in the form of hardware dongles that are inserted into a USB port. For embedded PC systems, however, it is advisable to implement this feature using permanently integrated chips. This ensures a fixed assignment to the device or system. Secure licensing processes can only be implemented and the IP and extra options for a fee be appropriately protected against abuse if this has been specified during the development phase.

Hard-wired communication paths are usually used within local networks or IT infrastructures. These paths are well protected from the outside world by firewalls or the like. However, there is a greater risk if the communication is wireless. This is mainly the case if the communication path runs directly to the internet. When selecting communication components, pay attention to which security features are already included, especially when cellular communications (2G/3G/LTE) is used to expand integrated IoT solutions. The entire communication chain, from the system to the cloud, should be considered during development. It is usually advantageous in this case to use manufacturers who offer the communication modules with suitable software routines for connecting to the cloud together with the cloud services as a package deal.

New applications in the IoT area and for the networked future often give rise to uncertainty and doubts because it is difficult to judge the topic of security. Security plays a central role and, as a basic requirement, must be incorporated as early as the product definition phase and during development. To close any gaps in experience and to answer open questions, it can be smart to include partners in the process and to use platforms already in existence. This can happen both on the component level and on the system level. ■