Press Release:
Reference: RiTech/PR16-002
Date: Friday, 11 March 2016

Rugged interconnect™ TECHNOLOGIES

Security with embedded systems

Harald Maier, Business Development Manager x86 / Embedded PCs at TQ

Embedded systems are becoming an ever more important part of machines and systems. And system networking is increasing at a breathtaking pace, described under the heading of "Industry 4.0" and "IoT – Internet of Things“. But how secure are these systems? Which aspects and functions can developers take into account during the concept design stage already?

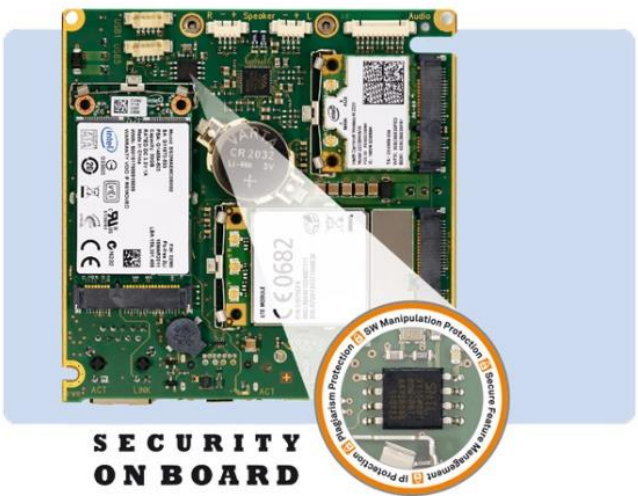
Embedded PC applications benefit from high compatibility and easy software integration. Standard operating systems such as Windows and Linux can be installed quickly and easily on these systems so that, from the software point of view, the focus is usually on the actual application itself. In this connection, the subject of security is still handled very carelessly in many areas. Isn't this actually supposed to be covered by the operating system already as a standard feature? If special security features are taken into account at all, this is often done in the style of standard PC technology where the issue of "security" is covered by means of firewalls and virus scanners. These measures, however, are insufficient in the embedded sector.

Virus scanners in combination with security updates serve well for office applications using standard PCs. New threats from the internet arise every day so that continuous updating plays a decisive role in the quality of protection. And that is exactly where the limits of embedded systems, which are commonly required to be remain as unchanged as possible and available for shipping and installation for a long period of time, are quickly reached. Thus, the problem that the system is not equipped with the latest security updates and the most up-to-date lists of potential viruses exists at the time it is delivered already. Also, the connection to update servers during operation is usually possible to a very limited extent only, often even not at all. The risk of manipulation or damage from the outside therefore increases as each day of operation goes by.

Unlike office systems, embedded systems have one distinctive feature, however, which should absolutely be taken advantage of: software functionality is precisely defined and consequently the programs and services which may be executed are known as well. Thus, if the developer allows only these routines to be executed and excludes everything else, he has optimum protection against harmful software from the outside, without continuously having to install updates. This so-called whitelisting procedure is addressed, for example, by producers such as McAfee under the name "embedded security“. This approach is particularly interesting and cost-effective for systems with Intel's latest low-power CPUs "Quark“ and Atom "BayTrail" (E3800) for with these two processor families, Intel offers the so-called "Moon Island" platform which, in addition to a ready-made WindRiver Linux BSP, also contains the "McAfee Embedded Security" package mentioned above, making implementation and licensing particularly easy.

When also considering the additional security features introduced by WindRiver, it is obvious that the "Moon Island" is a package where particular importance is attached to the issue of security: secure package management, key management, resource control, integrity measurement, secure update and trusted boot.

To fully support all of these features, the matching hardware is required. First, the processor, the central unit, is in demand. Intel deals with this subject matter for the first time in its low-power product line as well, with dedicated hardware support with the Intel Atom family E3800 ("BayTrail"). Thus, for example, processors have a stand-alone AES-NI hardware unit which supports the popular AES encryption mechanism. Since data are processed outside of the actual CPU, the full



resources of the CPU are available for the tasks performed by the application. Data to be transferred or stored data can thus be efficiently encrypted or decrypted in real-time, regardless of CPU load. This allows users to take into account new aspects with regard to security in embedded systems.

Another hardware mechanism for a secure embedded system is TPM (Trusted Platform Module). TPM modules which have to be connected to the CPU as external components, make hardware functions available which are necessary, among other things, to implement functions such as secure boot. This security mechanism is effective during the boot process already. This is necessary in order to ensure that only the operating system permitted for this embedded system is booted up. Boot-ups of other storage media or of manipulated operating systems are reliably prevented. Although TPM has existed as a specification by the Trusted Computing Group since 2003 already, it has thus far been applied only in relatively few, very safety-relevant applications such as banking and slot machines. Even the Moon Island software stack supports secure boot through the use of TPM modules. Any reservations associated with this subject are therefore more likely to be a thing of the past because all necessary components have already been suitably put together.

Anyone who speaks about embedded system security must not disregard the aspect of protection against plagiarism. Many companies put a lot of effort into implementing their application software. This is usually crucial to the range of functions and offers the greatest potential for unique features with respect to the competition. For that reason, it is more important than ever to protect specially developed software functions as well as the "profitable" licensing of individual product features. Secure mechanisms are needed to protect the investment and the competitive advantage. Software-based protective mechanisms usually constitute a suboptimal solution only. Protection is increased significantly if special security controllers such as the Sentinel HL by SafeNet are used, where individual, fully encrypted program code sequences of the application are processed in the external controller so that reverse engineering is virtually ruled out. Use of the security controller allows the completely secure implementation even of the secure license query of individual software features. The unauthorized execution of non-licensed software functions is thus impossible.

Several starter kits and software examples made by different software producers are available on the market for the security aspects outlined above. The embedded PC platform QSys by TQ offers a complete, embedded PC kit which consolidates all of the security features mentioned above in a solution that is ready to go into production. As a result, customized applications, BoxPCs and PanelPCs can be implemented quickly and inexpensively. Even full-custom designs are addressed by TQ. These can be reliably implemented completely from a single source from the concept stage to the finished product.

TQ Products are distributed and supported by Rugged Interconnect Systems throughout South Africa.

About the TQ-Group:

As an electronics service provider (E²MS supplier and CEM) TQ offers the complete range of services from development, through production and service right up to product life cycle management. The services cover assemblies, equipment and systems including hardware, software and mechanics. Customers can obtain all services from TQ on a modular basis as individual services and also as a complete package according to their individual requirements. Standard products such as finished microcontroller modules (minimodules) as well as solutions for drives and automation applications complete the range of services.

Through the combination of electronics services and finished system components, TQ offers customer-specific products as ODM products and thereby addresses customers who would like to receive finished products and at the same time benefit from the advantages of a customer-specific solution. ODM products are provided on time and economically using a comprehensive solution kit. The kit includes finished electronic, mechanical and software components including certification and licenses.

The TQ Group employs approx. 1,400 colleagues at their 13 sites (11 x Germany, 1 x Switzerland, 1 x China).

Further information on TQ can be found at www.tq-group.com

Rugged Interconnect Technologies

Rugged Interconnect Technologies focuses on offering rugged product solutions for industrial, mining, communications, defence and homeland security applications.

Working closely with our valued customers we can propose solutions based on application-ready computing platforms, customer specific requirements or a wide range of commercial off-the-shelf modules.

We represent best-of-breed suppliers with leading edge technologies consisting of rugged systems, processor, communication and multifunction I/O modules. Together we target applications such as sensor management and control, radar / sonar, digital signal processing, imaging, video tracking, situation awareness, recording and storage.

Rugged Interconnect Technologies prides itself in offering customers local sales and engineering support, product life cycle management and, when required assistance with next generation technology insertion. We have provided bus and board technologies to national and international customers for more than 30 years.

Contact details:
Rugged Interconnect Technologies
Email: sales@ri-tech.co.za
www.ri-tech.co.za