EBV Elektronik, ready for the Internet of Things

Thomas Stauding, VP Vertical Segments at EBV

With the Internet-of-Things there are opportunities for companies in the consumer goods, industrial, medical and automobile electronics sectors to participate in the fast growing internet market and to develop totally new markets with new systems.

At the beginning there was the mainframe computer, and then the PC brought in a real revolution in our lives. In a second wave, the internet and smart phones made completely new forms of communication possible with permanent connection to all computers worldwide. At present the Internet of Things is starting the third wave of the technical data revolution. This has resulted in a further fundamental reorganisation of our professional, every day and leisure worlds, the full opportunities and consequences of which we often do not recognise or foresee.

Definition

What is actually meant by the Internet of Things? In simple terms, almost all everyday objects will get an internet connection as well as a clear, worldwide individual internet address, by means of which it can be reached from everywhere or from any device in the world. Up to now 'only' computers, PCs, smartphones, tablets and some complex machines were connected to the internet but the trend is progressing so that all light switches, lights, sensors, air conditioning systems, cars, stereo equipment, washing machines etc., indeed almost all devices, will have an internet connection. Such an internet connected device, independent of its size and its function, will have the designation 'Internet Device' in English.

Wikipedia gives a very concise definition: 'The Internet of Things denotes the connection of clearly identifiable physical objects (things) with a virtual representation in a structure similar to the internet. There are no longer just human participants but also things'.

As part of the Internet of Things the marketing experts, according to a Cisco Study, mention 50 billion connected devices by 2020. About half of these will no longer be conventional nodes; conventional nodes include devices such as mainframe computers, PCs and smartphones. The other 25 billion network nodes are integrated into 'Things' and this area is particularly interesting for European companies.

Completely new potential for the industry

First came connectivity in the form of PCs, then came smartphones and consumer devices for example, TV sets with internet connection. In these markets it is mainly companies in North America and Asia that are active, but aspects such as Industry 4.0, Connected-Cars etc. also belong to the Internet of Things so that this subject is much more interesting for Europe than the conventional internet of the past. The Internet of Things is mainly about products for which European companies are world leaders.

Since the field of industrial automation and car industry suppliers is occupied to a large extent by medium sized companies, the distribution for the Internet of Things has a very special role. Even firms in the home automation field, which make or develop switches, lights, thermostats and similar products, must ask themselves whether and to what extent it is sensible to connect their products to networks or the internet. The same goes for applications around the smart grid, the intelligent controlled power supply.
In the past the internet subjects were rather under-represented in Europe, because the market leaders who were developing products in the internet area were working in the USA and in Asia. With the Internet of Things it is no longer a question of the connection of PCs and small portable personal devices to the internet, but rather of connecting devices and machines to the internet so that the European firms can play a leading, or even a dominant role on the world market.
With the Internet of Things the internet again becomes the focus of European companies.
Thus, there is a big opportunity for Europe to play an extremely active role in the Internet of Things. The car manufacturing, mechanical engineering and electrical engineering sectors stand to gain most from the Industry 4.0 theme, which is a part of the Internet of Things. This opportunity should make the companies involved take notice so that they do not run the risk of being shut out of the market by perhaps previously non-existent-competitors.

Examples of new applications
There are smart devices but also new approaches. In a smart device the connection formed by the Internet of Things is actually an additional connectivity function which is added to an existing device. So it is, for example, possible to install a controller in a thermostat as well as a connectivity function. Another solution might be to install, for example, about 100 temperature sensors in a house, which make their measurements available to an internal network in the house. Thus, the heating system can use the measurements of these temperature sensors to control the temperature, but the heating system would be only one possible assessor of the temperature sensor data from perhaps several. With these temperature sensors other systems, for example, movements or the temperature distribution in the room can be recorded. All sensor data from the house can be put into a system and then the individual systems can be separately assessed as part of a data analysis. Thus there is, for example, the possibility of recognising certain patterns and deriving corresponding service models. Depending on which company is working on this subject there is a completely different approach to the problem; then finally in order to stay with the example a manufacturer of heating control systems may have other preferences to a maker of lighting controls.
While previously just a single light or a few lights were controlled, it is now also possible in the Internet of Things to control a large number of lights. In this way movement sensors can determine the position of a person in a long corridor for example and arrange that the area around the person is always well lit while the lighting in the rest of the corridor is dimmed:The light practically moves along with the person who is walking down the corridor. Such functionality is at present unusual, but would result in a considerable energy saving.

Internet connection
A device that is part of the Internet of Things always has a microprocessor, as well as either a sensor or an actuator or both, and in addition a communication interface which produces the connection with the internet. In addition there is a power supply. Only very few

semiconductor manufacturers have the complete portfolio which is necessary to install such a device as part of the Internet of Things and thus there is a special role for distribution, for the distribution can in many cases help to bring these subjects together.
This always raises the question of whether the internet connection should be by means of a cable connection or wireless. In particular with the popular wireless connection it is necessary to comply with many specifications in order to provide an effective low power design. The distributor can also offer valuable support here. The connection of sensors often only produces relatively small quantities of data which can generally be very well transmitted by a narrow band transmission process to a concentrator which then has a faster data connection.
There are also, as part of Industry 4.0, various new instruments which function as a hub in order to collect several narrow band sensor signals and then take them further over LAN or data mobile wireless to a server or into the cloud. On the narrow band side there are at present various transmission standards of Bluetooth and Bluetooth Low Energy (BLE) over ZigBee to ZWave, the communication interface of which the data concentrators/hubs/router must control.
That is why for designs which form part of the Internet of Things it is generally necessary to have a know-how-mix in the areas of high frequency technology, CMOS sensors, Low Power Design, microcontroller/microprocessor and data safety (security).
EBV stands out in the distribution market in particular due to its intensive support in two areas: One of these is the wireless and high frequency technologies, which play a key part in many designs. The other area is data security in which many European industry customers have so far not had to collect any specific expertise, because questions regarding security problems before the connection to the Internet of Things have not yet been raised.
An important element of each system is the microcontroller or the microprocessor, but these aspects already comprehensively cover the conventional technology segments of manufacturers such as Atmel, Infineon, STMicroelectronics, Texas Instruments etc. from the Internet of Things point of view.

Security

Standards are also an important subject in this area because they are essential to guarantee interoperability. By the connection of previously autonomous systems the subject of data security of networked devices and data protection becomes much more important than before. Meanwhile, security is a central and essential subject which unfortunately is neglected much too often. In order to protect the private sphere and operating secrets, it is very important to decide suitable safety measures right at the start of the design. For smart meters (intelligent energy measuring instruments) there are very specific requirements of the BSI (*Bundesamt für Sicherheit in der Informationstechnik*) [Federal Office for Information Security], which the safety criteria of such an instrument must meet. Although there is no legal requirement on the handling of data within the domestic environment, these types of systems handle all their safety relevant data on a suitably high safety level in order to prevent bugging or manipulation of this data.
A further important aspect is also the protection of know-how and the IPs of the development team, as nobody wants another company to copy painstakingly produced hardware and software designs. Many market leaders have already recognised the importance of IP protection and built corresponding protection mechanisms into their design. For this reason it is possible to use, for example, the free programmable circuits available in FPGAs or special security chips in order to achieve a corresponding security level.

Smart-Grid

In the Smart Grid (intelligent power supply) and with Smart Meters the safety of the data is very important. What can happen, if hackers manipulate the power supply, is not only explained in the best-selling novel 'Blackout' by Marc Elsberg, but also in an investigation by the Federal Government (http://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf) which shows very clearly how important a permanent properly functioning power supply is, not only for the economy, but also for society.

A Smart Grid in the form of an intelligent power supply makes the flexible control of energy flow possible. In this the integration of the energy user plays an important role as Smart Grids will in future also be able to manage consumers. Although this is, in most cases, at present just wishful thinking, plans go quite clearly in this direction - and the communication runs strongly through the Internet of Things. A gateway with internet access serves as an interface to the consumer and to their home network or home automation system. Washing machines, air conditioning systems, freezers, mini-engine based co-generation systems, photovoltaic systems, roller blinds and many other devices will get their own internet address as part of the Internet of Things and thus can be controlled with corresponding authorisation by the worldwide data network.

If, for example, there is a surplus of generating capacity at night and power is therefore very cheap at this time, the energy suppliers (ESs) who are part of the Smart Grid can send a suitable electronic message over the Internet of Things to the consumers. If a freezer cabinet is so programmed that it mainly cools at night (so that the contents are a few degrees cooler, for example -25°C instead of the target value specified for foodstuffs of -18°C), the consumer can save money while the ESs can find a customer for their surplus power. In the same way the ESs can arrange that when there are load peaks, only those power users who have a very high priority are connected to whom the ESs sell power at peak times at a very high price.

Smart-Grids use many different technologies which are also used in the area of industrial automation, so that in both directions similar (or indeed the same) micro-controller and wireless interfaces play a significant role. Many communication applications may well fall back on the FPGA solutions or SoCs (Systems on a Chip) from Altera, because these FPGAs with integrated controllers enable a simple and nevertheless variable or flexible adjustable solution to be achieved, while at the same time adequate safety functionalities are integrated with these semiconductors.

Since the corresponding standards in the Smart-Grid area are in some cases generated by the software, the software plays an even bigger role. By means of suitable software partnerships those companies whose strengths do not lie in the programming of this type of software also get access to the necessary software.

The Smart Meter (intelligent energy measuring devices, intelligent electricity meters) represents the first step in bringing the necessary communication into the house as part of Smart Grids. Within the European Union, 80% of all household connections in total should have a smart meter installed by 2020; however from today’s perspective, it is unlikely that this schedule will be achieved. So, for example, Germany is likely to reach the 80% mark only in the year 2022. 2022 is, therefore, likely to measure 80% of energy consumed through smart meters which in current values accounts for merely 15% of installed meters. This, therefore, is a very long-term project, which offers many business opportunities. Suitable Smart-Meter products, which enable a clever data connection over the Internet of Things with high consumer benefits, consequently open a gigantic market.

Interdisciplinary work

EBV has for some time been building up relevant Internet of Things know-how in individual areas. A good example for this inter-disciplinary work is the lighting sector where already today there are lights with communication connections. It is then possible over interfaces such as ZigBee Light-Link, to switch the lights on/off, dim them, change the colour temperature, etc. With the matching App the user can control these functionalities even by means of his smart phone or a router. EBV Elektronik has already been actively involved in the design of these types of products.

Since EBV, with its organisational structure, offers a very broad spectrum over its many market and technology segments, developers can quickly get a suitable solution for their design requirements as part of the Internet of Things. There are many synergies here, which benefit the respective customer's design. By the connection of market and technology segments it has been possible for EBV Elektronik to offer its customers suitable expertise and support, to develop their products in working order and ready for market as part of the Internet of Things. A glance at the micro-sites of EBV's website clearly shows how this matrix structure enables targeted support to be given to the market orientated segments automotive, consumer, healthcare, high-rel and renewable energies which are just as clearly defined in detail as the technology driven segments FPGA, identification, LightSpeed (lighting technology) and RF & wireless.

In these segments there is no competitive organisation to the Sales Department. In fact the opposite is the case, for the segments are directly linked with the Sales Department, so that the corresponding EBV employee can talk to the developers, if necessary, as part of a team to put forward suitable made-to-measure technology packages for the respective applications.

EBV has consciously not set up a dedicated Internet of Things team because the distributor supports their customers over the segments in the solution of their design problems. For example, a lighting manufacturer contacts the EBV-LightSpeed team for their design questions, as they have always done, and the light team get in touch with the necessary technical segment supports, for example, in the area RF & wireless, to get them on board. EBV supplies support as part of the design process and for the design definition.

There is always the question of which segment a certain application belongs to. A good example of this is the LED lights for a sports car which on one hand belong to the automotive segment and on the other belong to the LightSpeed segment. In this case EBV experts from both segments work together with the developers to find the best solution for the respective application, in order to get a fast implementation of the design.

Reaching targets faster with partners

In the area of Internet of Things the developing companies look for partners who can help them not only with information but also to provide the necessary support so that the expertise obtained can be converted into a competitive advantage in products that are different. Since practically all development departments struggle with the time to market and limited development resources, the basic conditions are clearly defined. For this reason the relevant development board, reference design, module and partner protect the decisive competitive advantage of a product to be developed. If, for example, a potential partner already offers a non-competitive part of their own application, this can lead to a considerable shortening of the time to market, because it is not necessary to 'reinvent the wheel'.

A good example of this is the subject of safety. If an EBV customer needs a corresponding safety idea for their design, then EBV cannot actually supply this idea, but EBV can, as part

of its wide ranging, tightly knit partner network, provide a contact to suitable specialists. Even companies which want to connect their factory automation systems safely to the Internet are pleased to use this EBV contact, for finally they must ensure that nobody hacks into and manipulates the manufacturing plant.