

EBV Elektronik

SEARCH: What are you looking for? Recent Searches: EBV Solutions

Products Segments Services Suppliers About EBV Locations & Contact Events Media Center

New Products | Product Matrix | EBVtaps | Highlights | Product Finder

Home > Products > Highlights > The EBV IoT - Smart, Secure, Connected - Everywhere

The EBV IoT - Smart, Secure, Connected - Everywhere

For years, EBV has been supporting customers across EMEA with sensors, connectivity, low power microcontrollers and embedded processors. Many of the customers' end products (e.g. smart meters) are called today - the Internet of Things (IoT).

Based on this expertise and heritage, EBV is uniquely positioned to help companies in developing their IoT program and adding new functionalities such as security and access. Customers look for a best-in-class distribution partner that has in-depth market and technology expertise and the right ecosystem for complete design from hardware to software to manufacturing and distribution. The close cooperation between market and technology segments allows EBV to provide the best technologies and services for specific applications.

EBV IoT Industry 4.0 Customers

Committed to excellence

RUTRONIK EMBEDDED RUTRONIK SMART

Featured Internet of Things (IoT) applications:

Wearables

Whether it is a fitness tracker, a monitor the heart, a smart watch or smart headphones, ST's technology is embedded in many of today's most popular wearable devices.

ST's products are designed to meet the needs of the most demanding and innovative wearable devices, offering high precision sensing, low power consumption, tiny form factor and outstanding performance.

Smart Home

From electricity and gas metering, security and surveillance, to heating and energy control, the Internet of Things (IoT) brings your home devices together.

ST's products and solutions help create smart home appliances that can be interconnected to form a smart home ecosystem that offers its occupants a safer, more convenient and more enjoyable lifestyle.

ST's unique portfolio for IoT applications

- Analog & Mixed Signal components
- Connectivity
- Microcontrollers
- Power & Energy Management
- Sensors

Internet of Things (IoT)

Overview SOC IoT Applications IoT Products Resources

Discover solutions for today's IoT

Silicon Labs is making electronics smart, connected and energy friendly

Learn More

Featured IoT Applications

Connected Home

Reduce the complexity of connecting devices (e.g. lights, dimmer switches, contact sensors) in a connected home network.

Learn More

Wearables

Whether you are going for a run or monitoring your daily activity levels, our technology is embedded in today's top wearables.

Learn More

Industrial

The IoT is changing communication between industrial devices and operators.

Learn More

Smart Metering

Smart metering provides accurate, real-time data for utilities and consumers.

Find Out More

MICROCHIP CLOUD ENABLED TECHNOLOGY LETS

DEVICES UNITE!

EASIER CONNECTIVITY, RELIABLE PERFORMANCE

AWS IoT

The Internet of Things takes advantage of Cloud Connected Embedded Systems. Cloud Connected Embedded Systems can be found in products all around you. Products such as wearable fitness monitors, home security systems, home automation systems, garage door openers, industrial controls and more.

Microchip is proud to be a development partner of the new Amazon AWS IoT enablement platform. This revolutionary IoT methodology was recently launched by Amazon at the 2015 re:Invent Conference. With Microchip's new AWS IoT enabled IoT Wi-Fi AWS IoT Starter Kit you can easily Cloud Connect your Embedded Devices.

A Cloud Connected Embedded System connects either directly or indirectly to the Internet and utilizes cloud-computing resources.

- Remote Command and Control
- Remote Diagnostics and Field Re-programmability
- Remote Data Storage and Processing
- Profile and Status
- Push Notifications
- Order Fulfillment
- Consumer Insight and Advertising

powered by amazon web services

NXP IoT Truck - SMARTER WORLD TOUR

Register Now

Virtual Intelligence

Related Pages: Consumer Healthcare Automotive

Associated Products: ACNT-HSGL TRENCHTOP™ 5 SS IGBT XMC1400

New Products: ACNT-HSGL TRENCHTOP™ 5 SS IGBT BT5300T7

Recently Viewed Pages: Locations & Contact Search

Other Visitors also looked at: EBVun EBViv Event Filter

EBV Elektronik and NXP would like to invite you to the SMARTER WORLD TOUR driving the Internet of Things experience close to you. NXP's mobile Smarter World Tour highlights everything from the smallest microcontrollers to the most complex networking infrastructure through the most advanced NFC solutions. See technology, products, sensors, chips and software driving the Internet of Things today and your connected products tomorrow.

Experience more than 130 live demonstrations targeting the following applications:

- Smart Cities & Energy
- Smart Home & Building
- Secure Mobile, Medical & Wearables
- Smart Kitchens
- Smart Networks
- Secure Connected Vehicle

IoT Seminar

October 13th - 14th, 2015 | Warsaw

Enter Security. Your Everything

Atmel has you covered

Device Spoofing | Network On-Boarding | Device Identification | Remote Updates | Brand/IP Counterfeiting

Intelligent Security for Connected Device Ecosystems

The Internet of Things (IoT) is your new frontier. You're empowering your customers and creating new and innovative products. But there are dangers in any new frontier, and the IoT introduces vulnerabilities throughout the network. Whether it's the connected appliances in your home, or a vast network of devices accessed by cloud services over the Internet, you want to be able to control what and who can gain access to your network ecosystem. But how do you know which devices are authorized to be a part of your ecosystem and access the benefits of your network? How do you know if a network node is a device at all and not someone pretending to be a device so they can enter your network? Your home, your car, your office building, your product and its branded accessories are all ecosystems where you need explicit control over membership for security and a consistently positive user experience.

So how can you protect your customers—and your business? Controlling membership of an ecosystem is no trivial task especially

Next Steps: Order Samples Download Datasheets

Atmel COMMUNITY

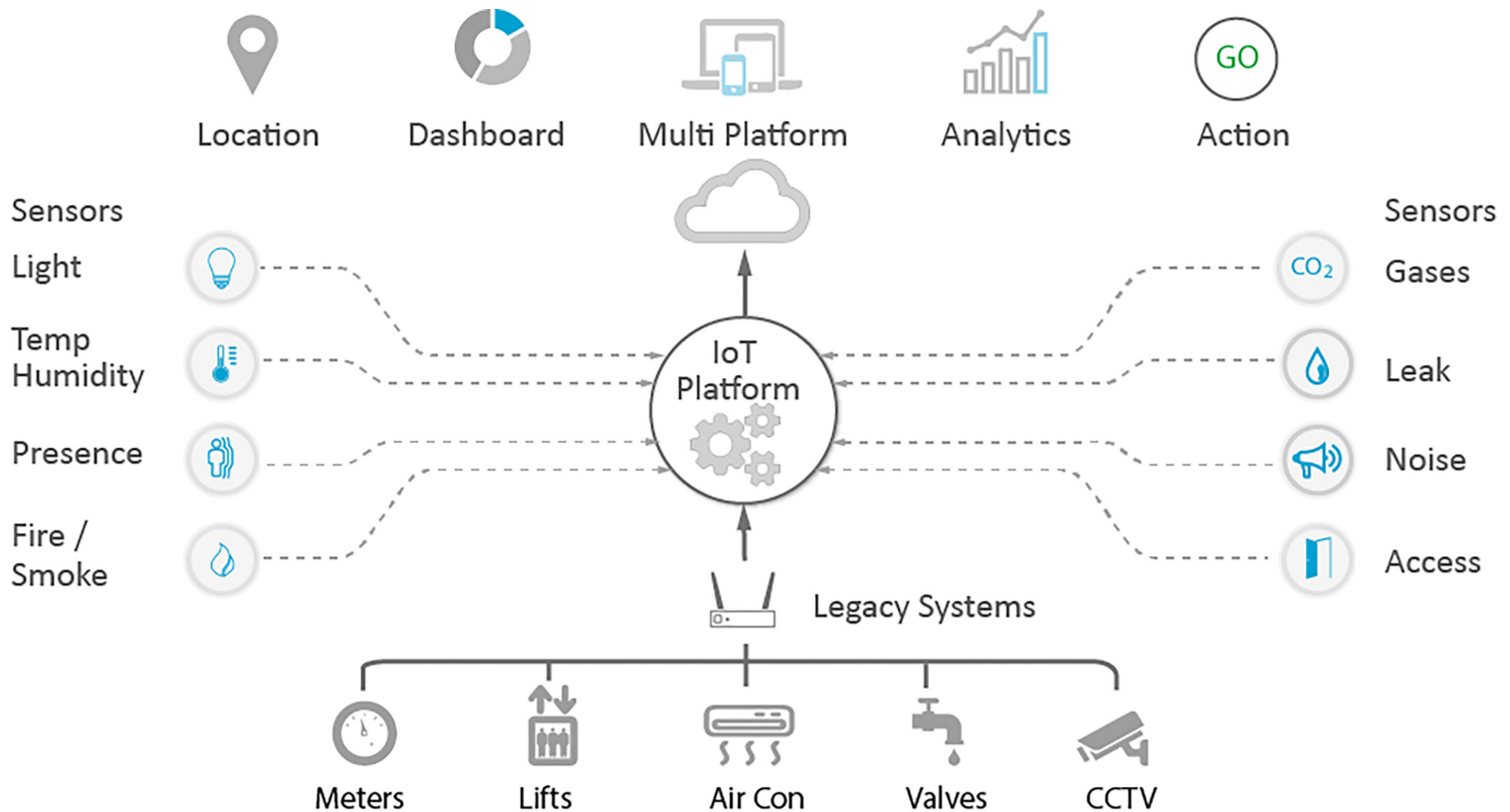
Visit Security Forum

IoT czyli...?

Idea Internetu Rzeczy – IoT – od dwóch lat przyciąga uwagę konstruktorów urządzeń elektronicznych. Nie da się jej nie zauważyć, bowiem wykorzystując jej marketingową nośność, próbują na niej zarobić wszyscy potencjalni uczestnicy rynku, w tym nawet producenci „specjalnych” złączy do aplikacji IoT. Czym tak naprawdę jest IoT?

Odpowiedzi na to pytanie łatwiej jest udzielić dziś niż choćby kwartał temu, bowiem szybko ewoluująca w stronę konkretnych rozwiązań idea IoT u swego zarania była bardzo ogólnym hasłem, obejmującym zasięgiem wszelkiego rodzaju urządzenia, które były wyposażone w techniczną możliwość dołączenia się do Internetu. Nie bardzo było wtedy wiadomo, po co te urządzenia miałyby być do Internetu dołączone, a co więcej, tej pewności w wielu przypadkach nie ma do dzisiaj. Efektownie opakowywana idea ma natomiast niebagatelną zaletę: poszerza potencjalne zapotrzebowanie na urządzenia nowej generacji, z których część nie konkuruje z dotychczasowymi rozwiązaniami, co stwarza nadzieję na to, że rynek urośnie, dając szansę na kolejne zyski.

Niedawny brak konkretyzacji idei IoT nie hamował inwencji specjalistów od marketingu poszukujących nowych pomysłów na zarabianie, czego przykładem jest oryginalne rozwinięcie akronimu IoT ogłoszone w lutym 2015 roku podczas norymberskich targów Embedded przez firmę Freescale: *Internet of Tomorrow*. Marketingowcy tej firmy twierdzili, że *Internet of Things* był „wczoraj”, a oni mają już podzespoły i pomysły aplikacyjne dla nadchodzącego *Internet of Tomorrow*. Buńczuczne stwierdzenie wywołało konsternację wśród dziennikarzy zgromadzonych na konferencji prasowej podczas targów, zwłaszcza że poza oryginalnym rozwinięciem akronimu, firma nie pokazała niczego specjalnego ani dla *Internetu Rzeczy* ani dla *Internetu Jutra*. Dajmy więc spokój nie zawsze udolnym zabiegom



Schemat blokowy oddający ideę systemów IoT pierwszej generacji

marketingowym, w dalszej części artykułu skupimy się na konkretnych związanych z IoT, a tych jest na szczęście coraz więcej.

Najważniejszą, konkretną informacją jest to, że podjęto już kroki w kierunku standaryzacji komunikacji urządzeń IoT, przy czym – jak to miało miejsce w przypadku ZigBee, Bluetooth 4.x czy USB – na rynku jest kilka konsorcjów SIG (Special Interest Group), które pracują nad własnymi standardami IoT. W ich ramach powstają m.in.: specyfikacje grup aplikacyjnych urządzeń, protokołów komunikacyjnych, metod ochrony przesyłanych danych przed ich nieuprawnionym przechwyceniem, definicje klas urządzeń wykorzystujących różne pasma radiowe itp.

Jednym z najsilniejszych konsorcjów standaryzujących zaangażowanych w przygotowanie specyfikacji IoT jest komitet IEEE, który utworzył Global Standards Initiative on Internet of Things (IoT-GSI). W prace tej grupy są zaangażowane niebagatelne postaci ze świata Internetu – m.in. Vinton G. Cerf (współtwórca protokołu TCP/IP

oraz Latif Ladid (jeden z inicjatorów poszerzenia obszaru adresowego w Internecie – standard IPv6) – co spowodowało, że pierwotnie nieco naiwne spojrzenie na IoT jako „świata odkurzaczy i ekspresów do kawy dołączonych do sieci” mocno zmodyfikowano. W ramach grupy IEEE P2413 (Standard for an Architectural Framework for the Internet of Things) od końca 2014 roku wypracowywane są elastyczne standardy dla wszelkiego rodzaju urządzeń, które mogą być przyłączane do Internetu, przy czym szczególna uwaga jest poświęcana integracji pojęć IoT i SmartCity, które także cieszą się rosnącą popularnością. Z tego powodu członkowie IEEE P2413 współpracują przy tworzeniu standardu z członkami innych grup roboczych, szczególnie z IEEE Communications Society – Power Line Communications (COM/PLC) oraz IEEE Consumer Electronics Society – Standards Committee (CES/SC). Ponieważ integracja wymiany danych przez urządzenia IoT ma się odbywać w chmurach obliczeniowych, członkowie IEEE P2413 blisko współpracują także z grupą roboczą

Komitet IEEE uruchomił konferencję o nazwie *World Forum on Internet of Things* (WF-IoT), która ma się odbywać co roku. Celem konferencji jest wsparcie tworzonego standardu oraz wypracowywanie rozwiązań i pomysłów alternatywnych do realizowanych w ramach grupy roboczej IEEE P2413. W roku 2015 konferencja odbyła się w połowie grudnia w Mediolanie.



IEEE Computer Society – Cloud Computing Standards Committee (C/CCSC). Jak widać, początkowe pustosłowie marketingowe przyjęło poważny kierunek rozwoju, czego dodatkowym potwierdzeniem jest zajęcie się tematyką IoT przez członków Parlamentu Europejskiego, w ramach którego działa od lutego 2015 pod kierownictwem holenderskiego posła Lamberta van Nistelrooija European Internet Forum (EIF). Specyfikacja standardu przygotowywana przez IEEE odwołuje się do niektórych wcześniejszych „przymiarek” do IoT, jak na przykład opracowana pod koniec 2012 roku przez agendę ONZ – International Telecommunication Union – rekomendacja ITU-T Y.2060, która zawiera jedną z pierwszych definicji tego, czym ma być IoT.

Obecnie trwają prace także nad alternatywnymi dla IEEE P2413 standardami IoT, czego przykładami mogą być m.in.: standard IIoT – Industrial Internet of Things – rozwijany przez Object Management Group pod kątem aplikacji przemysłowych (pomysł zmierza w kierunku Industry 4.0 i niewiele ma wspólnego z pierwotną ideą IoT) czy open-source’owy standard IoT opracowywany przez organizację Weightless, która skupia się na wykorzystaniu w aplikacjach IoT pasm radiowych poniżej 1 GHz.

Standaryzacja ma szansę zaprowadzić porządek na rynku urządzeń IoT, co ma o tyle znaczenie, że w już w 2020 roku na rynku ma funkcjonować od ponad 20 mld (wg danych analityków firmy Gartner) do blisko 40 mld (wg analityków firmy Juniper Research) urządzeń

IoT. Żeby uzyskać wysoką funkcjonalność, muszą być one przystosowane do pracy w ramach jednego systemu komunikacyjnego, muszą także zapewniać wysoki poziom ochrony danych, zwłaszcza w aplikacjach przemysłowych i SmartCity. Prace SIG komitetu IEEE zmierzają w tym kierunku, więc nie ma specjalnych obaw o przyszłość systemu IoT, zwłaszcza od strony funkcjonalnej. Obawy budzi natomiast ochrona danych przesyłanych do i z urządzeń IoT, bowiem nawet najdoskonalsze systemy kryptograficzne są możliwe do pokonania, czego przykłady obserwujemy na co dzień.

IoT niesie jeszcze jedno poważne niebezpieczeństwo: wdrażanie tego systemu jest jednoznaczne z oplataniem wszystkich dziedzin życia systemami monitorującymi, na których działanie nie będziemy mieli wielkiego wpływu. Dane gromadzone przez informatyczną chmurę mogą posłużyć nie tylko do zwiększenia wygody życia czy intensyfikacji sprzedaży i optymalizacji wykorzystania dóbr, ale także monitorowania i być może kontroli zachowania użytkowników urządzeń, czyli totalitaryzm w czystej postaci. Obawy nie są bezpodstawne, jeśli wziąć pod uwagę nie zawsze zgodne z oficjalnymi deklaracjami przypadki użycia danych gromadzonych obecnie przez banki za pomocą elektronicznych środków płatniczych czy danych gromadzonych przez operatorów sieci telekomunikacyjnych i dostawców usług sieciowych. Dzięki IoT Wielki Brat jeszcze bardziej urośnie...

Piotr Zbysiński, EP