Integrating the Internet of Things

Necessary building blocks for broad market adoption

Authors:
Kaivan Karimi, VP and GM, Wireless Solutions, Atmel
Pierre Roux, Product Marketing Director - Wireless Solutions, Atmel
Andreas Eieland, Sr. Product Marketing Manager, Atmel
Espen Krangnes, Sr Product Marketing Manager / MCU Product Marketing, Atmel
Henrik Flodell, Sr. Product Marketing Manager, Development Tools, Atmel
Bill Boldt, Sr. Marketing Manager Crypto Products, Atmel

Getting connected

Forecast to have 50 billion connected devices by 2020, the Internet of Things (IoT) promises to connect all manner of industrial and consumer appliances to cloud service providers. The intention is that the data generated by, say, a personal fitness band can be automatically uploaded to the cloud. In this way we can keep track of and analyze our key body and performance measurements such as heart rate, calories burned, distance walked, and sleep duration.

Typically the data from a gadget—in this case a fitness band and more generally termed an "edge" device since it is on the very edge of the data collection path to the cloud—will upload its data via a smartphone application. The smartphone serves to visually present the data, if required in real time, and will also function as a gateway to further upload the data to the cloud-based service where historical trends and performance comparisons can be analyzed. In this example, and depending on its design, the data analysis might be performed in the fitness band, or in the smartphone. Not all data will end up in the cloud of course, it might be that the smartphone stores all the data and performs analysis. Whether the data is transferred to a cloud application will depend on the users and their own application preferences.

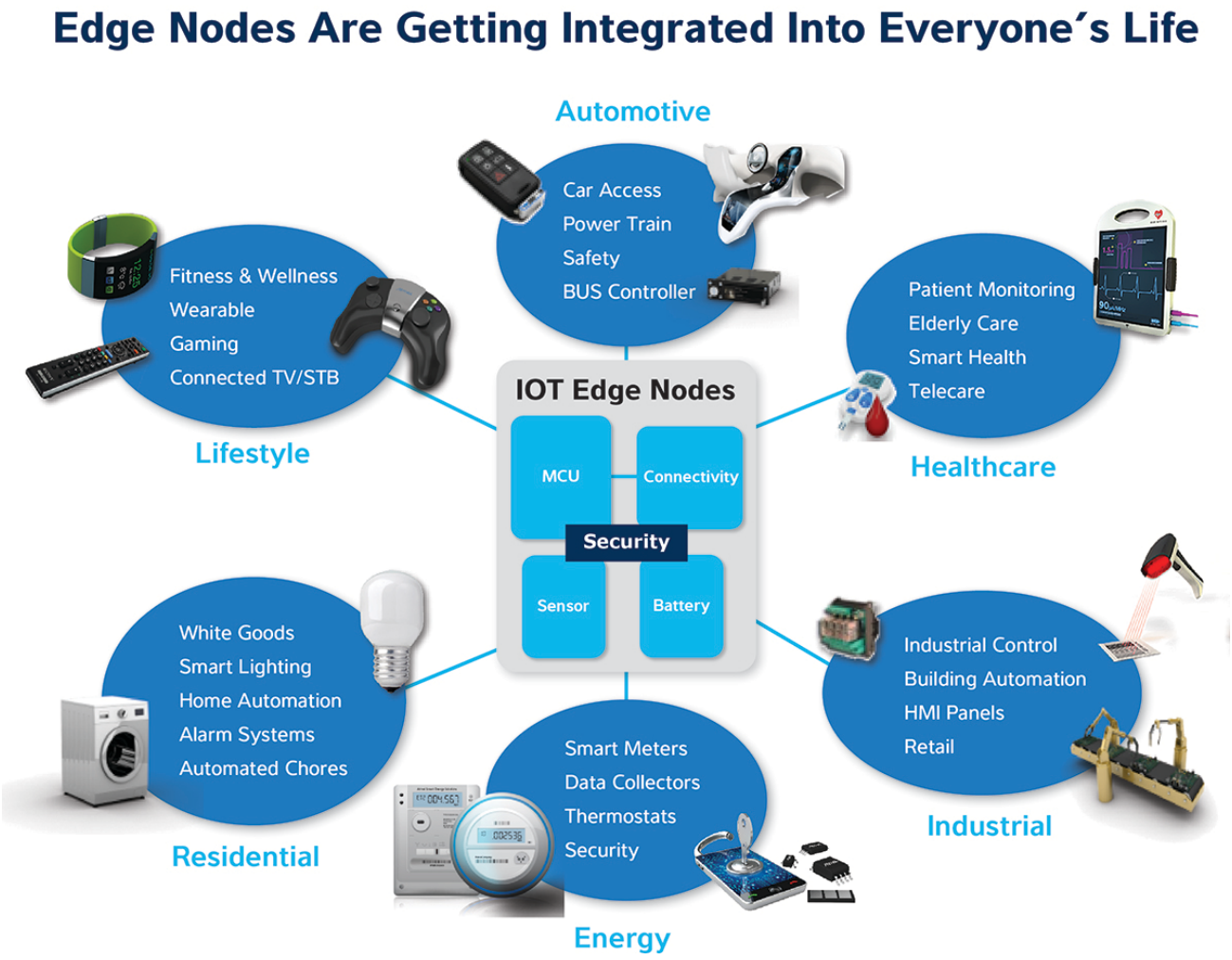

Figure 1 – IoT impacting every aspect of our lives

The fitness band is just one example of the growing trend to make all of our home appliances and personal technology devices connected. Figure 1 illustrates how the IoT is impacting every aspect of our lives—from wearable devices such as fitness bands and smart watches to personal health care monitors, IoT devices are making us connected. Our homes and white-goods appliances are also increasingly becoming IoT edge node candidates. The Smart Home concept, where energy consumption is carefully monitored by smart gateways at home and appliances can be remotely controlled, is fast gaining popularity. Appliances such as washing machines that negotiate a low-cost energy tariff during the night with the energy provider will soon be available. Smart thermostats, remote lighting controls and safety sensors such as smoke and carbon monoxide detectors are already becoming edge node devices in home automation systems. The edge node helps the user conserve power and increase comfort at the same time – because it is all done smarter. Needless to say, our cars, and the technology within them, are also becoming connected. Engine and power train monitoring, safety features and a host of traffic information initiatives such as the “C2C/C2X Connected Car” put in place by the European Commission promise to make our journeys much safer and easier.

While IoT will provide us with more data to monitor, trend and analyze than we have ever had before, it will also lay the path for exciting new business models. In the same way that the Internet brought major change to the retail sector—such as disintermediation, where consumers could buy directly from manufacturers—the IoT will allow manufacturers of products and services to take a completely different approach to the way they sell their products and services. Consider car insurance as an example. Traditionally, newly qualified young drivers have faced huge insurance policy costs. However, initiatives by a number of UK insurers have made it affordable by fitting a GPS-equipped “black box” into the vehicle that records and measures speed, braking pressure and cornering forces. Driving carefully and within the speed limit allows insurance companies to charge a fair rate to sensible and considerate young drivers. Other ideas yet to make it to market include charging for tires in a similar manner. Monitoring distance traveled, speed, acceleration and braking forces will allow tire companies to charge for tires based on a rental usage model rather than outright purchase.

There is no doubt that the IoT is enabling a far more informed life for us all. The IoT is also instigating major changes in the way industrial companies provide and charge for products and services. In consumer products, the IoT is allowing companies to custom-tailor the pricing for products and services on an individual basis.

Making the IoT work

On first inspection, the requirements of an IoT edge device appear to be much the same as any other microcontroller (MCU) based development project. You have one or more sensors that are read by an MCU, the data may then be processed locally prior to sending it off to another application or causing another event to occur such as turning on a motor. However, there are decisions to be made regarding how to communicate with these other applications. Wired, wireless, and power line communication (PLC) are the usual options. But, then you have to consider that many IoT devices are going to be battery powered, which means that their power consumption needs to be kept as low as possible to prolong battery life. The complexities deepen when you consider the security implications of a connected device as well. And that's not just security of data being transferred, but also ensuring your device can't be cloned and that it does not allow unauthorized applications to run on it.

Infrastructure of IoT

Edge nodes talking to a gateway, edge nodes talking to other edge nodes, and edge nodes talking direct to cloud-based service providers all create a number of challenges for developers. The first and foremost being time to market. With such commercial pressure on getting IoT-based products into the market, developers are looking at ways they can fast-track designs by using vendor-supplied reference designs that include most of the relevant software, as well as pre-certified wireless transceivers. Another aspect of this trend is that, according to several leading research organizations, by 2019 50% of IoT solutions will be provided by startups that are less than three years old. This means there will be many organizations designing IoT devices without the benefit of large, established engineering teams and resources.

For many of today's wearable designs, the smartphone has been the gateway of choice. Not only does this model provide the ability to provide longer-range connectivity to the cloud service providers but it also gives the user the ability to view and analyze the data. There are of course many other ways of communicating with the cloud such as the use of Fiber & DSL leveraging local ISP networks (usually the most cost effective way), power line communication, satellite, and other types of wide area networks (WAN) connectivity. In all cases hierarchy of new generation of smart gateways will be used to communicate with various types of edge node devices using short range connectivity technologies, and aggregate, analyze, provision services, and if needed send the data using WAN communication technologies to the cloud.

Cellular is still considered a viable long-range communication “pipe.” However, over time new generation of WAN connectivity that are better suited for IoT types of application will carry most of the IoT Traffic to the cloud. Also, in-building availability of a reliable cellular signal path can become a major issue for many IoT designs. For an increasing number of IoT applications, especially non-wearable and more industrial IoT applications where there is no need for local interpretation of the data generated, there is a growing need for a different type of gateway. The concept of a smart gateway will play a critical part of a secure service delivery infrastructure (see Figure 2) of edge node data through to the cloud service provider.

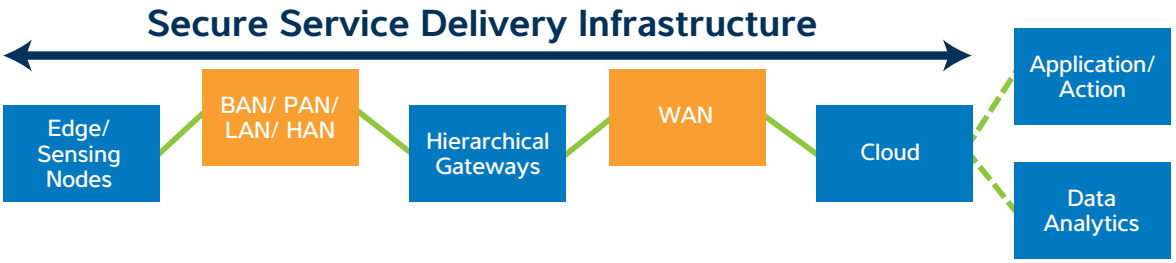

Figure 2 – Secure service delivery infrastructure

Such a smart gateway, or hierarchical gateway, will not only serve to provide short-range communication from the edge nodes through long-range WAN communication to cloud but it will also provide the ability to store, interpret and act on the data coming from the edge nodes. Short-range communications for most part will include 802.15.4 (ZigBee, 6LoWPAN, Wireless HART, ISA-100, etc.), Bluetooth/BLE, low power Wi-Fi. Many other evolving standards such as 802.11ah, which uses sub-GHz ISM frequencies, are gaining momentum so designers need to keep up to date with their adoption. Figure 3 shows an example of how such a smart hierarchical gateway might function.

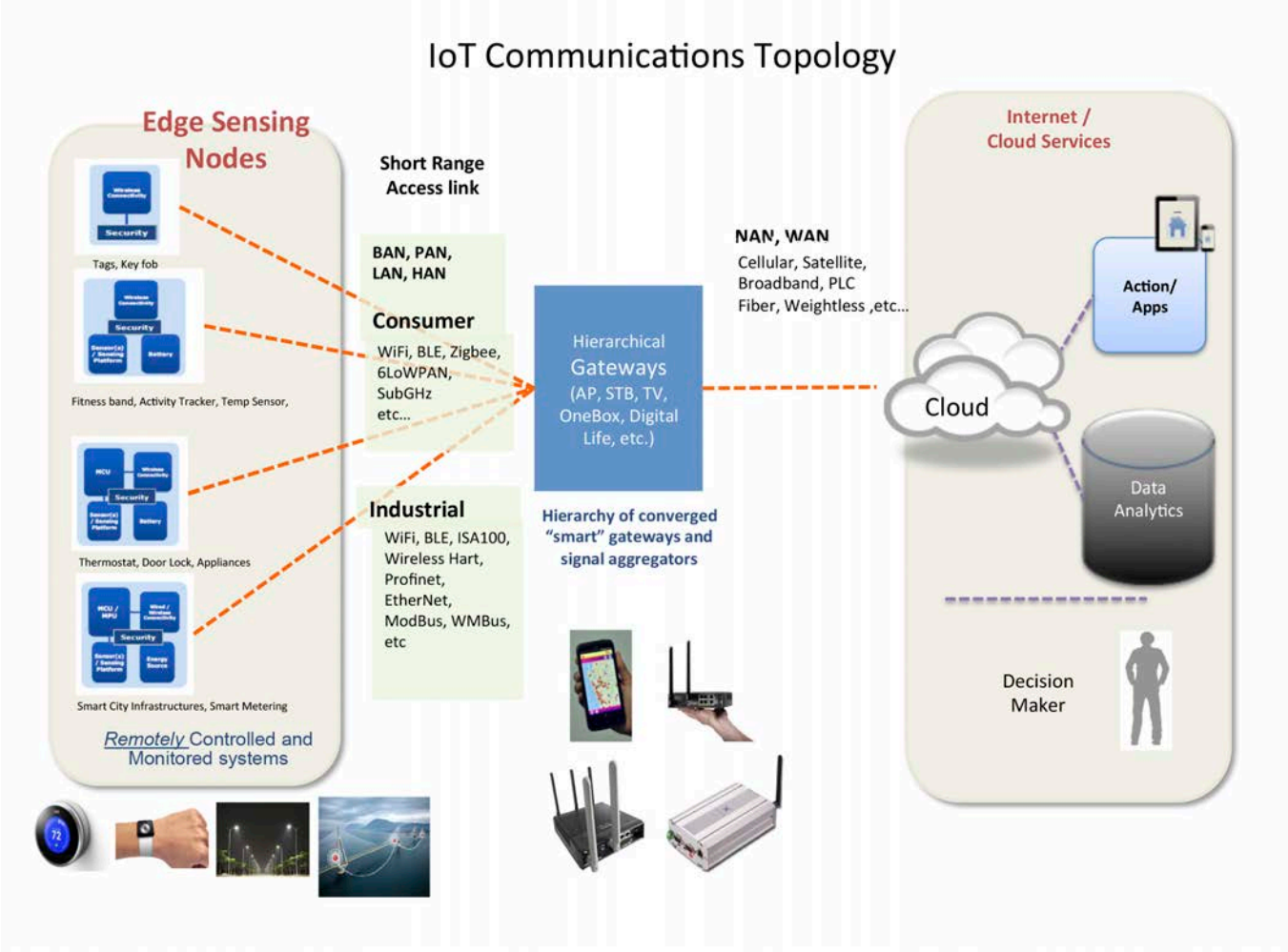

Figure 3 – Hierarchical gateway block diagram

The building blocks of IoT

No matter what type of IoT thing you might be looking at developing, fortunately the key building blocks are the same.

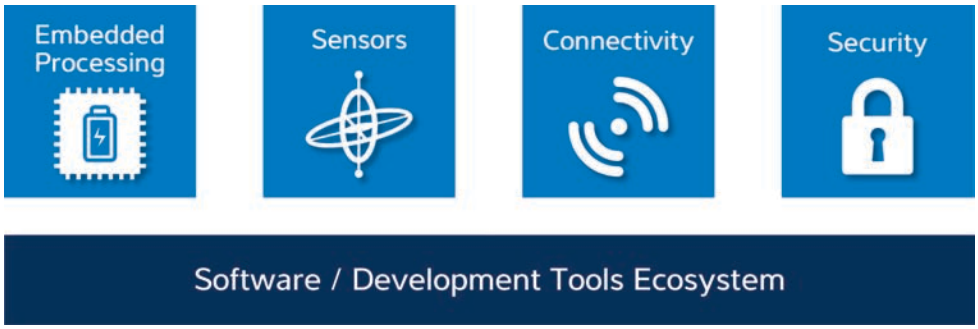

Figure 4 – Building blocks of the IoT

As Figure 4 illustrates, the core of any IoT design will incorporate an embedded processing device, potentially one or more sensors, connectivity that typically will be wireless-based, and finally, and possibly most importantly, device security. Underpinning all of these blocks will be a comprehensive and fully integrated tool chain ecosystem that will ease development and speed time-to-market. The degree of processing power and number of sensors will tend to be dictated by the type of edge node.

For the developer, there are a host of interrelated decisions that need to be considered at an early stage. For example, when looking at the requirements for a wearable item such as a fitness band, battery life will clearly be a prime consideration. Depending on the product specification, the band might require a display, while a higher-end device might have a need for touch controls for the user interface. Fitness bands typically would use a cell phone as the gateway, so Bluetooth Low Energy (BLE) (aka Bluetooth smart) connectivity would be adequate, whereas a more sophisticated smart watch could use both low power Wi-Fi as well as BLE. The way the device operates will also need attention. How often should data be read? How often should it transfer data to the gateway? For the most power-efficient use of the device, the question is how often to keep a wireless link active? Should data be processed only when it is about to be displayed rather when read? As in the rest of life, there are tradeoffs to make and all of these decisions will influence power consumption. For the developer faced with bringing an IoT product to market in the shortest period of time the need to select a vendor of the fundamental building blocks catering to the broadest range of IoT applications is the critical first step.

IoT design simplicity

With two decades of microcontroller, touch control, security, and wireless expertise, Atmel offers the broadest portfolio of devices that are ideal for incorporating into an IoT design—no matter how simple or complex it might be. Atmel microcontrollers (MCUs) and microprocessors (MPUs) can be found in thousands of consumer, industrial and automotive solutions today. The Maker community has also embraced Atmel technology with the Atmel® AVR® and SAM microcontroller devices being at the heart of several Arduino single-board computer platforms because of their ease of use. Popular with fashion designers, the Arduino Lilypad uses an Atmel ATmega168 microcontroller and was used in some of the first wearable and e-textile clothing.

Atmel offers the broadest portfolio of MCUs and MPUs based on the world's most popular 8- and 32-bit architectures—Atmel AVR and ARM. Both architectures are supported by the free-to-download Atmel Studio 6 ecosystem of embedded development tools and a powerful software library framework called Atmel Software Framework (ASF).

Both Atmel AVR and Atmel ARM®-based devices incorporate a number of Atmel IP, such as picoPower® and Sleepwalking. Atmel picoPower technology enables devices to be designed from scratch for the lowest possible power consumption. This includes low-leakage transistor design, process geometry, flexible clocking, and sleep modes. Atmel picoPower devices can operate down to 1.62 VDC, yet still maintain all functions. With short wake-up times and multiple wake-up sources from the deepest of sleep modes, picoPower ensures that your design is as energy efficient as possible. Sleepwalking adds peripheral intelligence to picoPower. It allows a peripheral to determine if incoming data required the use of the CPU or not. Sleepwalking defines wakeup events. It allows the microcontroller to be put into deep sleep and only wake up when a pre-defined event occurs. The CPU no longer needs to check whether a certain condition is present or an address match is true. With sleepwalking, the peripherals perform the checks and will only wake the CPU up from sleep when a valid condition is met.

Simply AVR

The Atmel AVR family of microcontrollers offers both 8-bit and 32-bit low power devices with a high degree of integration all based around the Atmel single-cycle RISC microcontroller core innovation. With 8-bit performance up to 1.0 MIPS/MHz and 32-bit performance up to 1.5 MIPS/MHz and clock speeds up to 66 MHz, the AVR family starts with the small yet powerful 6-pin Atmel tinyAVR® series of MCUs. Designed for high-level C code development, the AVR instruction set and CPU design are tuned for minimum code size and maximum execution speed. This combination of single-cycle instruction execution and high code density delivers an overall package of computing performance and low power consumption that is still leading in the industry.

There are three high-performance and power efficient Atmel 8-bit MCU families: the entry-level tinyAVR, the mid-range megaAVR®, and up to the most recent family, the AVR XMEGA®.

The tinyAVR devices are optimized for applications that require performance, power efficiency and ease of use in a small package. Capable of operating at just 0.7V, the devices integrate an

ADC, Flash, EEPROM and Brown Out detector, as well as on-chip debug for fast, secure and cost-effective in-circuit upgrades.

The mid-range megaAVR is more suited to applications requiring large amounts of code. Offering performance up to 20 MIPS, the range offers a wide selection in terms of memories, pin counts and peripherals, including specialized ones such as USB, LCD controllers, CAN, LIN and Power Stage Controllers.

The AVR XMEGA MCUs are composed of various fundamental blocks, including the AVR CPU, SRAM, Flash, EEPROM and a number of peripherals. The AVR XMEGA instruction set also supports 16-bit register access and ALU 32-bit arithmetics. A key feature of the family is the use of power-saving peripherals, achieved via the device's highly innovative Peripheral Event System (PES). This is a set of features that allows peripherals to interact without intervention from the CPU. It allows peripherals to send signals directly to other peripherals, ensuring a short and 100% predictable response time. When fully using the capabilities of the event system, it is possible to configure the chip to do complex operations, with very little intervention from the CPU, saving both valuable program memory and execution time.

All the Atmel 8-bit AVR devices use the proprietary Atmel picoPower technology, which includes an optimized balance of high performance and low-leakage transistors, low-voltage operation, various low-power/sleep modes with fast wake up, and the use of hardware DMA. In the case of the AVR XMEGA devices, an event system also offloads work from the CPU. Key performance characteristics include operation over 1.8 to 5.5V, consumption of 22µA per MIPS in active mode, 0.1µA in power-down mode, 0.6µA in power-saving mode (with a 32kHz crystal oscillator running), and less than 1us wake-up time.

Atmel | Smart

By incorporating Atmel microcontroller innovations such as picoPower, SleepWalking and the PES together with the extremely successful ARM core technology, Atmel has developed the Atmel | Smart™ line of ARM-based microcontrollers and microprocessors. Designed to keep up with the increasing need for high processing performance, low power and high-speed connectivity, the ARM-based devices are ideal for use in a broad range of IoT applications.

The Atmel | Smart family of Flash 32-bit MCUs include devices that use the ARM Cortex®-M0+ and ARM Cortex-M4 cores. For even more performance, and when an operating system such as

Linux or Android is required, the 32-bit MPU series is available with ARM9 or ARM Cortex-A5 cores.

The low power SAM D20/D21 series features an ARM Cortex M0+ core running at up to 48 MHz and is suited to low-end applications requiring limited display functionality such as an entry-level wearable fitness band. Available in a variety of pin-out packages with Flash memory from 16 KB to 256 KB and 2 KB to 32 KB SRAM the series also hosts configurable I^2C, USART and SPI serial communication ports (SERCOM), a 12-bit ADC and a 10-bit DAC and a self-calibrating capacitive peripheral touch controller (PTC) that supports buttons, wheels and slider controls. The enhanced SAM D21 series also features enhanced timers and counters, Full Speed USB and up to 52 GPIOs.

For space-constrained IoT designs, the low-pin-count SAM D10 and SAM D11 series is ideal. Available in 14-pin and 20-pin SOIC or 24-pin QFN packages, the devices host configurable SERCOM ports, ADC and DAC, PTC and up to 16 KB of Flash and 4 KB SRAM.

Suited to mid-range IoT applications, the ARM Cortex-M4 based SAM G series of MCUs is also equipped with a floating point unit (FPU). With its ultra-low power attributes, SAM G device power consumption goes as low as 7µA in sleep with SRAM retention with a wake-up time as little as 3 µs. Active power consumption can be 100 µA/MHz. Capable of operation up to 120 MHz and with up to 512 MB Flash and 96 MB SRAM, the series has a comprehensive and flexible set of peripherals, including I^2C Master and Slave, SPI, USART and UART. Packaged in a compact WLCSP 49-pin format, down to 2.84 x 2.84 mm, the SAM G family makes an ideal choice for IoT designs that might batch transfer a host of sensor data.

For high-performance computing applications, and those requiring Linux or Android support, the Atmel SAMA5D3 microprocessor series combines high performance, low power and ease of use. With an ARM Cortex-A5 application processor core running at up to 536 MHz coupled with an ARM FPU, the SAMA5D3 features a host of connectivity options, including Ethernet and CAN, a 64-bit internal bus and 32-bit DDR controller, ADC and 32-bit timers. The device is also equipped with an LCD controller with graphics accelerator, a camera interface and a state-of-the-art crypto engine for secure boot and advanced encryption standard (AES), triple encryption standard (DES), secure hash algorithm (SHA) and true random number generator (TRNG) functions. Figure 5 illustrates the comprehensive features of this device.

Another microcontroller that has been specifically designed for use in IoT applications is the Atmel SAM R21 MCU. This is a single-chip 32-bit ARM Cortex-M0+ based device that features an integrated ultra-low power 2.4 GHz transceiver for use in ZigBee and other 802.15.4 wireless applications. Capable of running up to 48 MHz and having up to 256 KB embedded flash, the SAM R21 offers the low power consumption that battery-powered designs required of less than 70 μA / MHz.

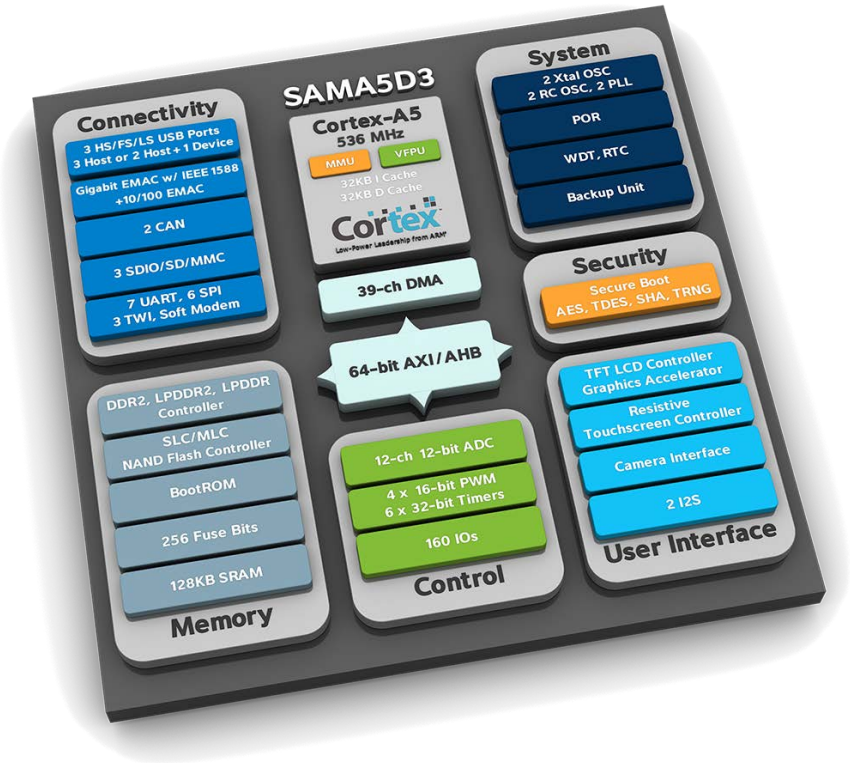

Figure 5 – The Atmel SAMA5D3 device block diagram

Despite its comprehensive list of features, the SAMA5D3 offers a low power solution suitable for battery-operated applications. The device consumes less that 150 mW when running a maximum speed and under 05 mW in low power mode.

Operating support for the SAMA5D3 includes Android Jelly Bean 4.2.2 and KitKat 4.4. Linux support includes Atmel distribution along with many from a list of certified partners.

Together, Atmel AVR and SMART microcontrollers and microprocessors provide the industry's most comprehensive, integrated and supported range of devices for any IoT application.

Sensing the world around us

Whatever the IoT application, it is highly likely to sense the world around it—including ourselves. Fitness bands, heating controllers, smart meters and smartphones all have more than one sensor that measures temperature, humidity, movement, and energy consumed. To make it as simple as possible to connect these to Atmel devices, the company has formed collaborative technical partnerships with the world's leading sensor manufacturers such as Bosch, AKM and Intersil to name a few. Whether you need to measure or detect environmental factors, acceleration and directional forces, or light and color you can be assured that Atmel and its partners have a sensor tested and ready to incorporate with an Atmel MCU or MPU in your application.

To speed your development even further, Atmel offers a number of evaluation boards and kits available for the controller devices mentioned above. For example, the SAMD21 Xplained Pro is an evaluation board for the SAMD21 series 32-bit ARM Cortex-M0+-based microcontroller. Figure 6 shows the SAMD21 together with a number of connected module additions. Atmel together with its partners provide an environment that delivers a rich selection of hardware, drivers, and example projects that will significantly speed up development, allow you to focus on your differentiating features, and get your product to market more quickly.

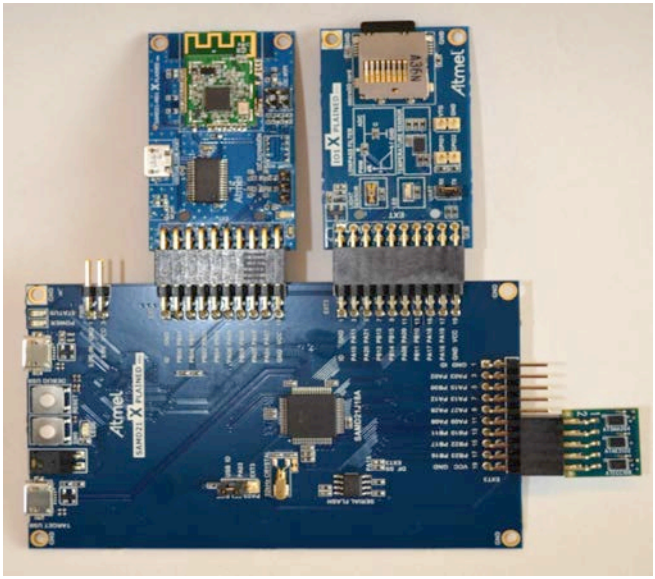

Figure 6 – SAM D21 Xplained Pro demo board with temp sensor, WiFi, and CryptoAuthentication modules connected

Connecting to the cloud

By its very definition, any IoT device requires connectivity to the Internet. Whether that happens via a gateway such as a smartphone, a smart gateway or direct to a cloud service provider by Wi-Fi or other standard, the embedded developer must create that connection.

Atmel has been providing single-chip wireless MCUs such as the ATmega64RFR2, a 2.4 GHz 802.15.4 / ZigBee transceiver for many years now, but a new range of wireless Atmel SmartConnect solutions aim at making IoT connectivity even easier. This new range complements and extends the range of sub-GHz, Bluetooth and Zigbee transceivers already available.

Traditionally, when faced with adding wireless connectivity to an MCU or MPU, a developer has had to deal with a number of challenges such as working with multiple software stacks from different suppliers, as well as antenna and coexistence issues, not to mention any regulatory compliance. The Atmel SmartConnect range of Wi-Fi network and link controllers aim to allow developers to add 'black-box' connectivity and simplicity to virtually any IoT design.

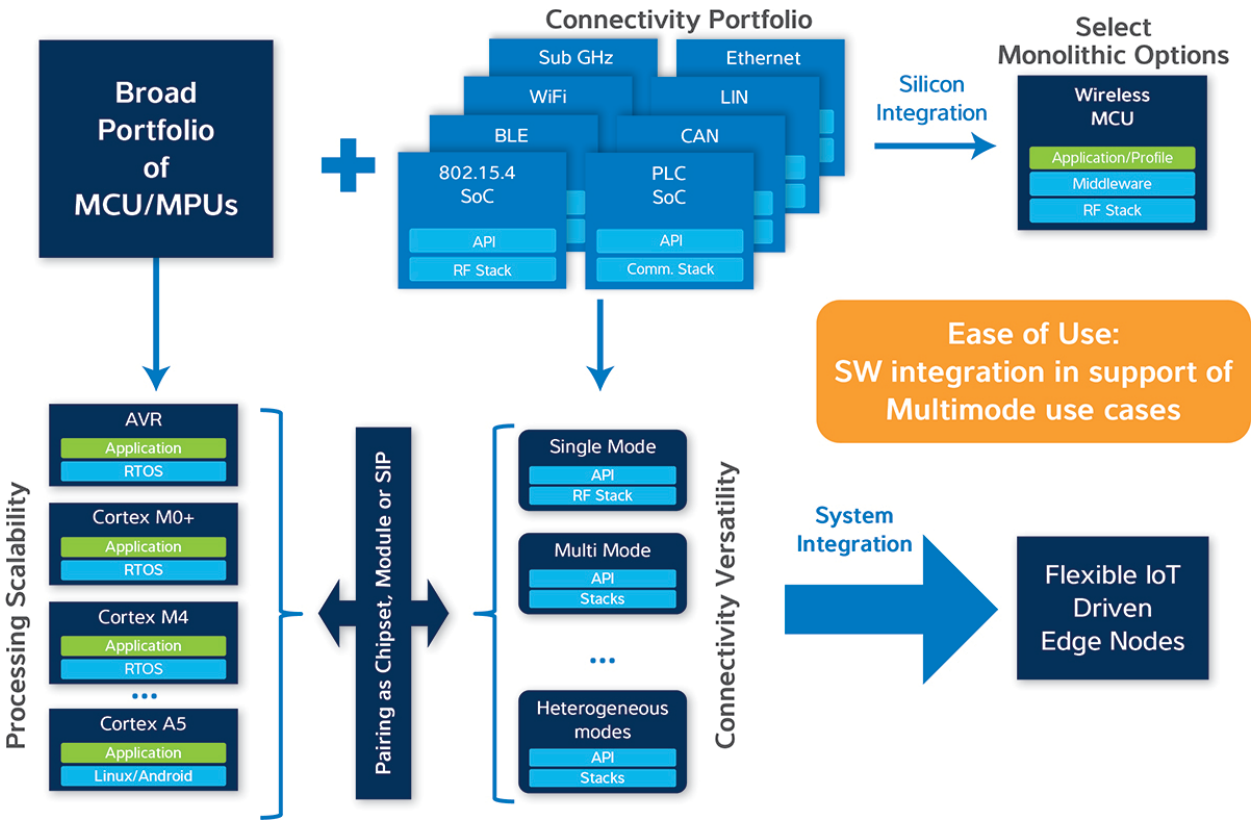

Figure 7 – The Atmel SmartConnect connectivity approach

Two SmartConnect Wi-Fi devices recently launched include the WILC1000 link controller and the WINC1500 network controller series. Giving design flexibility to a developer, the WILC1000 provides the wireless transceiver and the link control stack on a system-on-chip (SoC) device that can link to any Atmel MCU or MPU that is running the network stack. The WINC1500 adds the network stack capability to the WILC1000. Both controllers are certified and conform to the 802.11 b/g/n standard and have a maximum PHY rate of 72 Mbps. Figure 7 above illustrates the scope of connectivity options. They are targeted at high data rate and extended range Wi-Fi applications. Interface options to the host include SPI and UART for MCUs and SDIO for MPUs.

The WINC1500 package includes 4Mb of stacked Flash and a number of power-saving and fast boot options. Power sensitive IoT applications will benefit from the use of four states: Provision, Idle listen, Idle, and Suspend. Using this approach, available power budget can be preserved with the Suspend state consuming just 4 µA. Another extremely useful feature of the WINC1500 is the ability to upgrade its firmware over-the-air (OTA). This is ideal for designs that need to be updated during the applications lifetime.

Atmel has also launched a WINC1500 starter kit, see Figure 8 below, to help embedded developers fast track their designs. Including a SAM D21 Xplained Pro development board and a WINC1500 Xplained expansion board and an I/O prototyping board, developers will be able to quickly design and test their IoT design's capability. The Atmel CryptoAuth Xplained expansion board makes adding security very easy. Project examples already available within Atmel Studio make the task even easier.

Of interest to makers and professional engineers alike will be the recent launch of the Arduino Wi-Fi shield. The result of yet another joint collaboration between Atmel and Arduino, the stackable Wi-Fi 101 shield supports all Arduino platforms and also includes an Atmel Crypto-Authentication™ device, allowing experimentation with hardware authentication. Arduino has proved to be an extremely simple and reliable starting point of many IoT designs, so the Wi-Fi shield will make prototyping even easier.

Figure 8 - WINC1500 starter kit

Interacting with your IoT application

The type and complexity of an IoT application will determine whether any human interaction is required, and how much. A simple wall-mounted thermostat might need no interaction, whereas a more sophisticated programmable heating/air-conditioning controller might require a number of different interactions to set temperatures, zones, and times. Atmel has a superior offering of capacitive touch control solutions that can already be found in a wide range of industrial, automotive and smartphone products. Based around innovative Atmel maXTouch® technology, a number of touch sensing controller devices are available for simple button, wheel and slider controls through to large touchscreen applications. A variety of controller devices such as the mXT224T and mXT336T, are suitable for screen sizes up to 4.5 inches and passive stylus support together with single, dual or multiple touch detection. Capable of use with a gloved hand and with water immunity detection to reject water droplets, the controllers are ideally suitable for any high-end wearable IoT application.

For even more stylish product designs, Atmel XSense® touch sensors allow extremely narrow sensor node tracks, thin almost zero product borders, and use on a curved touch surface. Figure 9 below illustrates how XSense can bring an innovative approach to incorporating touch control surfaces into many consumer applications.

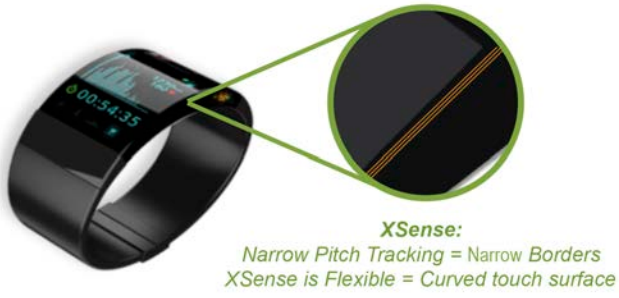

Figure 9 - An Atmel XSense-based wristwatch design example

Securing your IoT design

No discussion involving the Internet would be complete without mention of security, and that is because without security the IoT may likely not be widely adopted. Any IoT product requires the highest level of security possible. It is not just the data the IoT application generates that needs to be protected. Some designs such as wearable applications also store personal information, identities and log-in details for service provides that would certainly be a target for hackers. Likewise, being able to access an IoT application that is controlling other appliances such as a

heating and air conditioning systems would compromise system integrity and potentially have fatal consequences. Also, manufacturers need to protect their IoT devices from being cloned and being sold as counterfeit products in order to protect brand equity and preserve potential revenue streams. Security needs to have a layered approach as indicated in Figure 10.

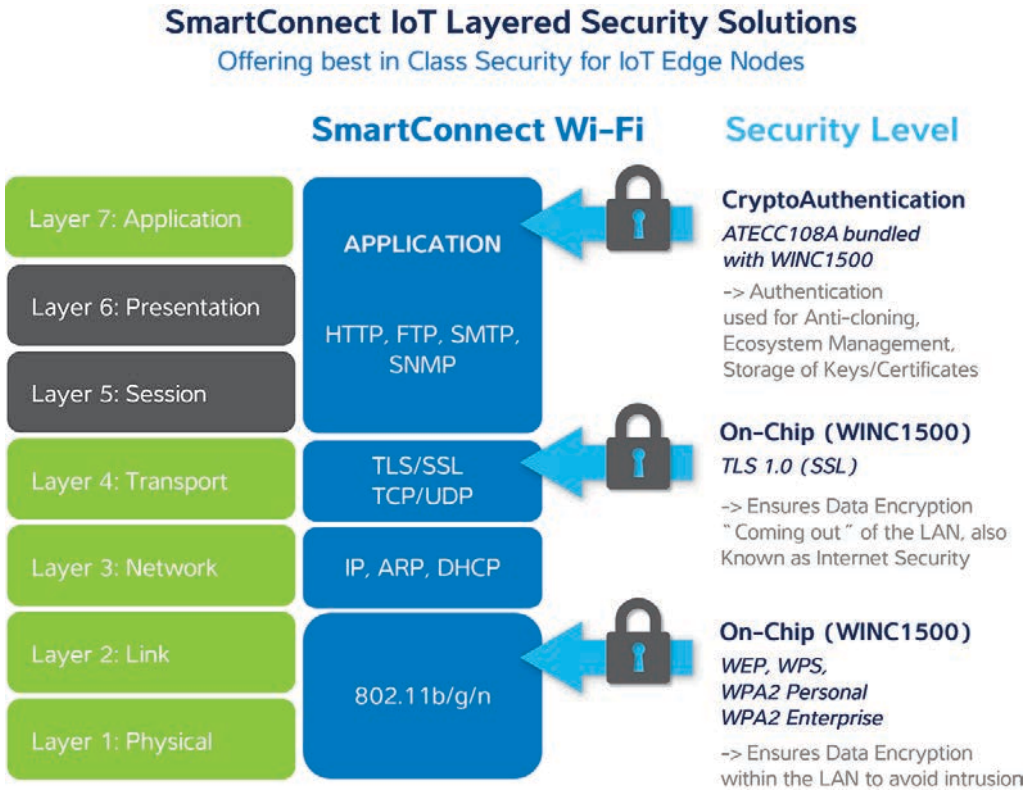

Figure 10 – Atmel SmartConnect IoT Layered Security Solutions

To achieve this security, Atmel offers one of the industry's widest ranges of hardware authentication and encryption devices containing proven methods of protecting secret keys that not only restricts access, but also provides key generation and management. When securing secret keys hardware key storage is stronger than software-only storage every time. Atmel crypto devices are available with SHA256, AES128 or ECC256/283 cryptography and provide cost-effective, optimized performance for the broadest spectrum of IoT designs and solutions. With a number of fully tested hardware evaluation kits available, and with the cryptography engineering being built-in by Atmel, developers do not need to be cryptography experts. Also, hardware countermeasures are employed on the devices to further protect security. These include a metal shield over the whole Crypto-Authentication device, no probe/test points and

tamper detection algorithms. In addition to discrete crypto authentication devices a number of Atmel microcontrollers such as the SAMA5D3 feature an on-chip crypto engine as well.

Create, configure and connect

The building blocks of creating and bringing an IoT design into market mentioned above are made complete by the ecosystem of software development tools available from Atmel. Reaching across the blocks of embedded processing, sensors, connectivity, touch controls and security is the Atmel Studio 6 integrated development environment. Providing device support for all of the Atmel AVR and SMART devices, evaluation/development kits and enabling seamless connection using Atmel in-system debugger products, Studio 6 provides the focal point for any embedded developer. Integrated within Studio 6 is the Atmel Software Framework (ASF). ASF provides a project wizard to create ready-to-run project examples on the comprehensive range of Atmel start-up kits, evaluation and development boards. ASF also provides peripheral drivers and communication stacks.

Complementing the software tools are the Xplained Pro range of evaluation boards that provide everything you need to start designing a new MCU-based applications in minutes. Easy to connect through an embedded debugger, they attach to a PC running the free Studio 6 development environment. A range of hardware extension boards provides easy access to all functionality of the MCU while ASF provides a large set of software drivers and components. With evaluation kits starting as low as $39 you can start developing your IoT design with Studio 6 today.

In addition to the hardware and software tools provided by Atmel, a wide range of forums will help you engage with fellow developers in order to help minimize design time or get support for your design activities. These include the popular AVRFreaks, an Atmel AT91 Community for ARM devices, not to mention a host of other forums and discussion groups.

Atmel solutions are also well supported by a range of partner and third-party design organizations. Whether you need a real-time operating system (RTOS) for your design or wish to employ a design consultant to help create your IoT design, plenty of help at on hand.

For those developers and makers that prefer to base their designs on the leading Arduino platform, there are also a huge range of extension shields, community sites, and IoT project ideas available.

Enabling unlimited possibilities

The IoT promises to connect us and our technology in ways never seen before. For consumers and companies it has the potential to deliver new and exciting ways of conducting business and providing services. For organizations wishing to architect these new products and services—many of which are start-ups—there is an urgent need to establish their offerings in the market in the shortest possible time. Needless to say, it is the engineering teams that feel this pressure to deliver against these time-to-market goals. Selecting a vendor that has a proven, trusted and integrated set of processors, connectivity and security devices is paramount.

Atmel solutions enable unlimited possibilities for customers to lead the markets they serve by creating products that are more powerful, smarter, more energy efficient, lower cost and more versatile than ever before. Atmel is at the heart of The Internet of Things, a highly intelligent, connected world where Internet-enabled devices will outnumber people. Atmel microcontrollers and supporting products are used in many IoT market segments, including industrial, consumer, communications, computing, automotive, and more.

Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**