Inside TRACK with Tim Morin,

Director of Marketing, Microsemi

Interview by JEAN-JACQUES DeLISLE

JJD: What are the largest technology challenges in fulfilling Internet of Things (IoT) market demand and growth?

TM: it's important to note that some semiconductor manufacturers focus on edge devices for the IoT and other hyperconnected applications. In contrast, companies like Microsemi are primarily focused on the associated communications infrastructures and how they are being impacted by growing security requirements—not just in the IoT, but also in the power grid, avionics, mobile networks, medical telemetry, transportation, and space systems, among others.

From our standpoint, there are several challenges in the IoT space—the first being availability of a proper Internet connection throughout the home or enterprise environment. Available connectivity drives the need for technologies like power-line communications (PLC). The second challenge relates to content and applications that can apply to in-car communications as easily as smart TVs and others. Once the connection, content, and applications are available, there also is the issue of ease of use and flexibility. Finally, security becomes important in a hyperconnected world. Communication must be secured against malicious monitoring and modification if connected machines are to be used safely and with confidence. This is most effectively achieved with machine-to-machine (M2M) authentication using Public Key Infrastructure (PKI), where the Private Key in the Public/Private Key scheme is derived from a physically unclonable function (PUF).

Additionally, a key challenge and common requirement for IoT and other infrastructure segments is "time." There is a need to discover how to harness time in order to synchronize secure communications systems, protocols, and applications so they all work together. Technologies for timing and synchronization solutions include ICs focused on timing for package networks and open-transport-network (OTN) systems. Otherwise, solutions are already available to tackle the challenges that arise across the rest of the IoT's security, power, reliability, and performance requirements. Examples include field-programmable gate arrays (FPGAs); RF and mixed-signal technology; and integrated circuits spanning applications including Power over Ethernet (PoE) and Reverse Power Feed (RPF), for next-generation power and data networking.

JJD: As the smart vehicle—specifically the electric car—becomes an integral part of our connected world, where does vehicle-to-grid (V2G) communications come into play?

TM: According to Navigant Research, V2G applications modulate the power flowing to (and in some cases, from) electric vehicles (EVs) to enable grid operators to match power supply and demand. This capability is expected to make the grid more energy efficient. The firm has reported that by 2022, demand response programs will be able to control nearly 640 MW of load from EVs. In the V2G infrastructure, however, privacy concerns will again be an issue. Plugging the vehicles in the recharging infrastructure may expose private information such as a user's locations and traveling habits.

JJD: How are the technologies developed for V2G communications also useful for RF applications for home automation, industrial IoT, and smart-grid solutions?

TM: In today's enterprise, telecommunications, and mobile-network infrastructures, a host of requirements is pushing semiconductor solutions to help implement, secure, and synchronize everything from X-band weather/radar systems and GPS solutions to medical telemetry and mobile backhaul equipment. One of these application examples is the power grid, which is moving to a two-way system that allows homes to generate their own electricity with solar energy. Such systems require secure and precise bidirectional communications between utilities and customers for more efficient power production and use.

JJD: As everything becomes connected and that information is readily available, what are some concerns for IoT security regarding home, automotive, and personal devices in particular?

TM: Security is a major concern for the remote, increasingly compact, and power-conscious advanced systems that support the IoT. These systems offer an ideal gateway for malevolent hackers. As a result, there is a critical need for security solutions that protect embedded intellectual property, system data, and the system itself by defending against the installation of malicious code, cloning, reverse-engineering, or tampering. FPGAs play a significant role in meeting these objectives.

JJD: As a recent component in all flexible radio devices, how are FPGAs enabling cutting-edge security features for IoT solutions?

TM: FPGAs are making base-level security easy to use and adopt by system architects. As FPGAs with embedded processors become the core of new systems, system-on-a-chip (SoC) FPGAs will ideally be provided with leading-edge embedded security features. Examples include physical unclonable functions, cryptographic accelerators, random number generators, and Differential Power Analysis (DPA). With such countermeasures in place, the system architect can layer in the security needed throughout the system.

> **"FPGAs are making base-level security easy to use and adopt by system architects."**

JJD: What are the additional costs and technology options for adding security to IoT solutions?

TM: The Internet of Things is essentially a collection of electronic networks that need end-to-end layered security that begins at the device level—and includes secure hardware, design security, and data security. Adding this security does come at a cost. These cost-related decisions begin with the choice between application-specific integrated circuits (ASICs), application-specific standard products (ASSPs) and FPGAs for IoT-system designs.

While FPGAs have traditionally been more costly than ASSPs or ASICs, they generally offer the fastest way to integrate a specific design into a single device. On top of that, they promise to support and facilitate field upgradability, design flexibility, and faster time-to-market. With the promise of significantly better overall total cost of ownership (TCO) compared to ASICs in many next-generation designs, FPGAs can play a pivotal role in improving security through the utilization of unique built-in features and differentiated capabilities.

However, it is essential that all FPGAs used in IoT and other hyperconnected system designs be protected from cloning, reverse engineering, and tampering in order to protect embedded intellectual property (IP). In addition, FPGAs need to include embedded-device security technology that makes base-level security easy to use and adopt. The best way to achieve this is to use flash memory rather than static random access memory (SRAM). The latter requires configuration from an external memory device each time it is turned on, which exposes the design to reverse engineering. Storing the configuration information in on-chip nonvolatile memory makes it impossible to capture the information. At the same time, it prevents reverse engineering and tampering.

JJD: How do FPGAs impact the power budget of low-power IoT systems?

TM: On the power front, FPGAs enable today's high-speed, DSP-intensive system designs by delivering not only the lowest possible static power, but the lowest total power as well—especially at lower frequencies and high temperatures. This requires a comprehensive approach encompassing process technology, architecture, and the design of configurable logic, as well as the inclusion of embedded features including SerDes, DDR2/3, and DSP blocks. MW