# FutureHorizons

The Global Semiconductor Industry Analysts

# FH MONDAY

30 March 2020

## Smart and Secure Embedded Solutions for IoT Design

Microchip Technology Inc. has launched a range of IoT solutions for rapid prototyping by using cloud connectivity for all integrated microcontroller solutions.

read more

## Sinch Helps Ericsson 5G Customers Get the Message

Ericsson recently selected Sinch AB, a global cloud communications and software provider for mobile operators, to support its worldwide 5G rollout with messaging technology. Sinch's SMS Function (SMSF), a cloud-native 3GPP-specified messaging product, will be incorporated into the Ericsson core network offering.

read more

## Maxim Intros MCU with PUF Technology

Maxim Integrated introduced the MAX32520 ChipDNA Secure ARM Cortex-M4 Microcontroller, a device that integrates physically unclonable functionality (PUF) technology for multiple levels of protection in IoT, healthcare, industrial, and IT systems.

read more

FutureHorizons

**TALK TO US**

## 5G: Rollout Stalls as Standards Work Is Suspended

LONDON — The 5G rollout will grind to a slower pace with a decision by the 3GPP to suspend work on some crucial parts of the specification due to the impact of the novel coronavirus. The delay had been signaled a few weeks earlier when the association announced it would cease all face-to-face meetings for at least three months.

read more

## EVENTS

Silicon Chip Industry Seminar

-16 March 2020– London UK

Industry Forecast Briefing

– 15 Sept 2020 – London UK

DON'T MISS OUT.- BOOK NOW BY CALLING

+44 1732 740440

OR EMAIL

mail@futurehorizons.com

## Securing IoT With PUF Technology

More IC vendors are beginning to explore a device-level technology approach for safeguarding data called physically unclonable function, or PUF. Though silicon production processes are precise, this technology exploits the fact that there are still tiny variations in each circuit produced

read more

Future Horizons Ltd, • 44 Bethel Road • Sevenoaks • Kent TN13 3UE • England
Tel: +44 1732 740440 • Fax: +44 1732 740442
e-mail: mail@futurehorizons.com• http://www.futurehorizons.com/
Affiliates in Europe, India, Israel, Japan, Russian, San Jose California, USA

## Smart And Secure Embedded Solutions For Iot Design

Microchip Technology Inc. has launched a range of IoT solutions for rapid prototyping by using cloud connectivity for all integrated microcontroller solutions.

IoT design is characterized by pairing the appropriate microcontroller solutions with the ideal connection protocol for your application. Microchip Technology Inc. announced a line-up of full-stack, embedded development solutions that provide any number of such combinations. The line ranges from the smallest PIC and AVR microcontrollers (MCUs) for sensors and actuators, to 32-bit MCU gateway and microprocessor (MPU) solutions for edge computing. Connectivity options include Wi-Fi, Bluetooth or 5G narrowband technologies, all while maintaining a security foundation with support from its Trust Platform for the CryptoAuthentication family.

## Sinch Helps Ericsson 5G Customers Get The Message

Ericsson recently selected Sinch AB, a global cloud communications and software provider for mobile operators, to support its worldwide 5G rollout with messaging technology. Sinch's SMS Function (SMSF), a cloud-native 3GPP-specified messaging product, will be incorporated into the Ericsson core network offering.

Sinch's Jeff Hasen tells IndustryWeek, SMS can either be supported over an IP user plane or the control plane in 5G deployments. In the IP user plane, messages are IP-based and are sent over an IP-SM Gateway. On the control plane, messages do not require IP connectivity and are sent over the SMSF. Each method will be essential in 5G networks — and Sinch provides both as part of its 5G messaging portfolio.

## Maxim Intros MCU With PUF Technology

Maxim Integrated introduced the MAX32520 ChipDNA Secure ARM Cortex-M4 Microcontroller, a device that integrates physically unclonable functionality (PUF) technology for multiple levels of protection in IoT, healthcare, industrial, and IT systems.

IoT applications are continuously proliferating. On the bright side, we are able to do things never imagined before and improve our lives. But like any good thing, there is a downside to IoT: it is becoming an increasingly attractive target for cybercriminals, with far too many IoT devices vulnerable to cyber attacks.

Designers need solutions to ensure data protection for critical applications where exposure to secret keys could destroy networks, ruin businesses, and negatively affect people's lives. The new solution offered by Maxim integrates ChipDNA PUF technology, which allows all devices to be immune to invasive attacks because the primary cryptographic key produced by it is not stored in memory or by static values.

## 5G: Rollout Stalls as Standards Work Is Suspended

LONDON — The 5G rollout will grind to a slower pace with a decision by the 3GPP to suspend work on some crucial parts of the specification due to the impact of the novel coronavirus.

The delay had been signaled a few weeks earlier when the association announced it would cease all face-to-face meetings for at least three months.

The 3GPP — the global association responsible for standardizing the technology — has now confirmed that it would delay work on Stage 3 of Release 16, and, more worryingly, announced that Release 17 would also be delayed. Taken together, the moves mean stage 3 can not be frozen as a standard before September 2021. This, in practice, means no further functions can be added.

## Securing IoT With PUF Technology

More IC vendors are beginning to explore a device-level technology approach for safeguarding data called physically unclonable function, or PUF. Though silicon production processes are precise, this technology exploits the fact that there are still tiny variations in each circuit produced. The PUF uses these tiny differences to generate a unique digital value that can be used as a secret key. Secret keys are essential for digital security.

Security is increasingly becoming one of the big concerns for developers of connected, or internet of things (IoT), devices, especially with the huge risk they face from attacks by hackers, or compromises to information and security breaches.

One of the challenges for adding security in an IoT device is how to do so without adding silicon real estate or cost, given the resource constraints in terms of maintaing minimum power consumption and optimizing the processing resources on the devies.