Winbond Seminar

Date 14th November 2017
Venue The Westin Grand Munich, Arabellastrasse 6, 81925, Munich. Germany.
Language English

Summary of sessions

Winbond Session: Winbond SpiStack powers evolutionary IoT Networks

- Serial NOR Flash memory (typically used for storing code) and serial NAND Flash memory (typically used for data storage and as a back-up location for code) occupy a relatively large proportion of the total board real estate in many space-constrained, portable and handheld device designs.
- Winbond's Quad Serial Peripheral Interface (QSPI) innovation was an important step in the miniaturization of the memory system's board footprint, replacing high pin-count parallel Flash interfaces. QSPI Flash dramatically reduced the Flash memory pin count and board footprint.
- More recently, Winbond, the predominant serial Flash manufacturer has adopted an additional way to increase memory capacity while reducing footprint: stacking Flash memory dies inside a single package.
- Both homogeneous (NOR + NOR, NAND + NAND) and heterogeneous (NOR + NAND) stacked-die devices are being produced.
- The benefits of using a stacked die include reduced development time, because the designer can increase memory capacity instantly by replacing a single-die package with a stacked-die package that has the same footprint and pinout, and therefore avoid the need for a board re-spin.
- A stacked die also enables the designer to accommodate a greater Flash memory density without increasing the board footprint, thus saving space. In other words, instead of using multiple memory chips on a board, a single SpiStack chip will provide the same memory solution with a single package.
- The Winbond implementation of Flash memory die stacking has two unique advantages.
    - The first is a software Chip Select (CS) function operating over a single channel. This makes for a smaller and less complex board layout by comparison with competitors' devices, which implement the CS function in hardware, requiring a pin and a channel on the host controller for each die.
    - The second is support for concurrent operation, so that the host can perform Erase or Program operations on one die while reading from another die. This offers a valuable performance improvement over conventional Flash memory

ICs, avoiding the bottlenecks caused when the system tries to read and write to Flash at the same time.
    - Read While Write-RWW feature-set can improve system performance in targeted applications such as IoT Connectivity.
- Winbond has a detailed roadmap for the development of many SpiStack products with various homogeneous and heterogeneous stacked-die options.
    - NOR+NAND heterogeneous stacked-die devices is unique to Winbond's implementation.
    - NOR+NAND SpiStack lets the customer and/or Eco-system customized densities based on their Code-Storage usage model.
- Winbond' is uniquely positioned to help customer take advantage of Die-Stacking as they prefer to make Spiflash' more SUITED for critical code storage and OS such as Linux Kernel optimum partitioning of Serial-NOR and Serial-NAND.

Fujitsu Session: Creating Benefits for Automotive and Industrial Customers

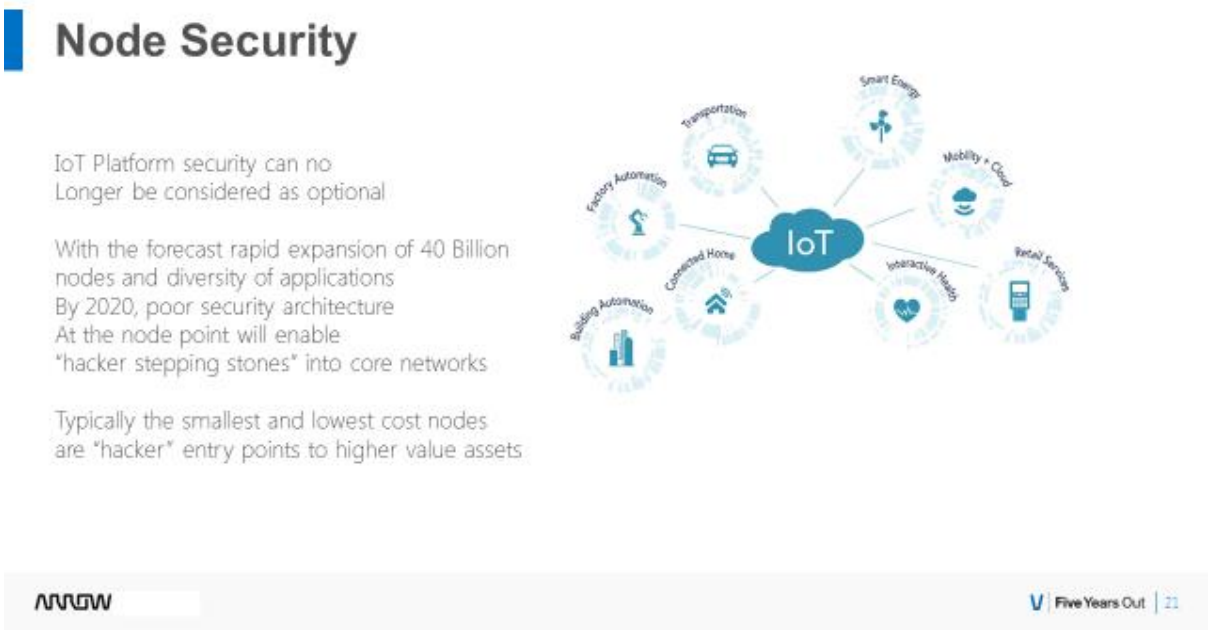
Fujitsu Electronics Europe (FEEU) is looking back to a long lasting relationship with its European automotive and industrial customer base. Applying the knowledge from the semiconductor business with the new end to end approach and the constant addition of new vendors fulfilling the requirements of the target industry, FEEU is in the unique position to support customers for automotive and industrial applications. From ASIC develop over standard components such as ASSP and sensor up a complete EMS service all options are available. These technical solutions are provided to our customers by a supply chain meeting all needs of the individual customer. Finally, having a worldwide footprint, FEEU can follow the customer wherever the production site may be.

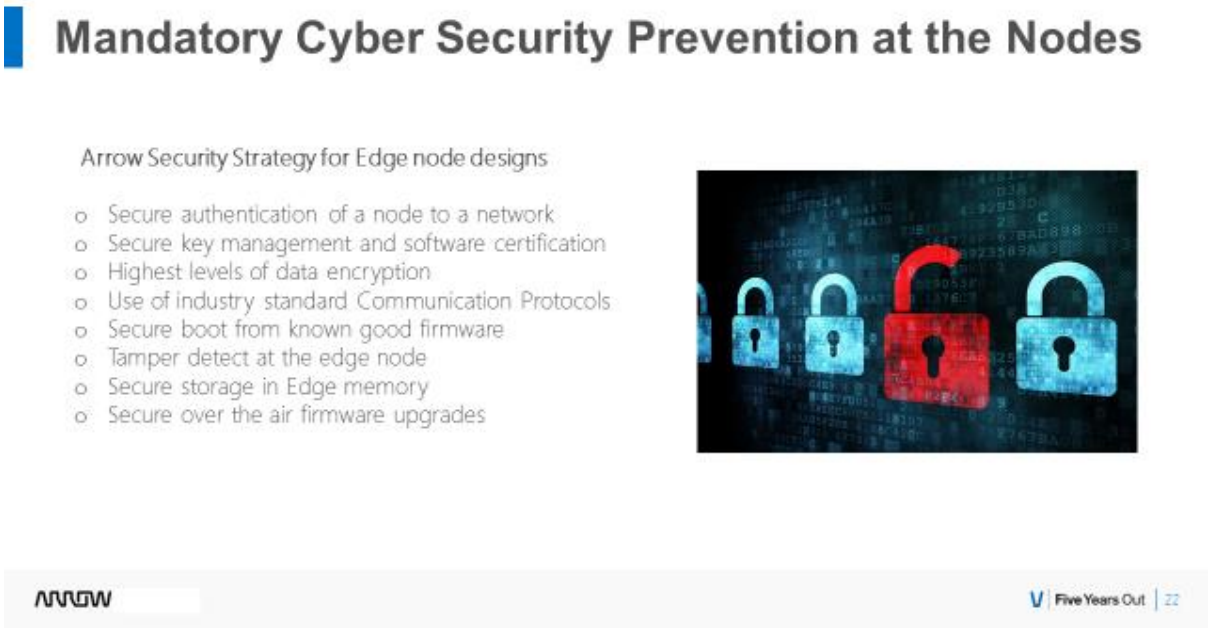
Winbond Session: How the Flash product can improve the IoT edge node power consumption

- Today, the circuitry on the board in mainstream industrial and consumer products operates from a wide range of supply voltages: the power rails are most commonly at 5V, 3V, 2.5V, 1.8V and various lower voltages.
- Designers of mobile and portable products in particular are constantly under pressure to reduce power consumption, and therefore are looking for IC manufacturers to standardise their devices' power rails at levels below 1.8V.
- The DRAM market offers a model for the way that standard voltages can be driven down, from DDR1 at 2.5V to the latest DDR4 generation at 1.2V.
- In the Flash market, standard devices today are available operating at 3V, 2.5V or 1.8V. With no option for operation at a level below 1.8V, the scope for power saving has been limited.

- This gap has now been filled by the new 1.2V W25QxxNE family (nominal voltage range 1.14V to 1.30V), and by the extended voltage range W25QxxND family operating from 1.14V to 1.6V.
    - Ideal for battery-operated applications
- The provision of devices at these operating voltages is aligned with broader trends in the semiconductor industry: its roadmap sees emerging support for 1.5V, 1.35V, and 1.2V as the next voltage levels after 1.8V, and eventual industry-wide standardisation at 1.2V.
- In the new Winbond devices, operation at 1.2V offers a 33% power saving in Active mode (50MHz clock speed) compared to the Active mode current of its 1.8V devices. Stand-by current of <0.5µA is half that of the equivalent 1.8V device.
- Over time, the availability of 1.2V devices also offers the potential to simplify the power circuit, eliminating the need for a dedicated 1.8V power rail and enabling both an SoC and external Flash to be supplied by a single 1.2V power rail.
- With these new extended 1.5V products from the W25QxxND family, it is very convenient to use a single 1.5V battery to supply power to many portable devices in the industry with IoT applications leading the way. Since the voltage range for these devices ranges from 1.6V to 1.14V, they are fully functional when the battery is new or full all the way till the battery drains out over time or over use. In contrast, today the same systems operating at 3V use two 1.5V AA, AAA or coin cell batteries in series to perform the same function.
- Winbond makes it easy for system developers to migrate their external memory provision from 1.8V to 1.2V, because it maintains pin compatibility and feature set compatibility across the families of 1.8V and 1.2V Flash products.

Arrow Session: Security at the Edge





Winbond Session: Flash Memory in Security World

- Security weaknesses in the companion Flash memory to a microcontroller or SoC expose OEMs to the commercially damaging risk of Intellectual Property (IP) theft, and to cloning of reverse-engineered PCB designs by unscrupulous electronics system assemblers.
- This is of critical importance to OEMs: while a product's hardware design can easily be cloned, its value is zero without the application code that runs on it. This application code is often stored in an external NOR Flash IC. If attackers can gain access to the code on this Flash IC, the OEM's most valuable IP is at risk.
- The security method most commonly used in Flash devices today, the unique ID, is inadequate to protect Flash memory from such attacks. The unique ID can easily be found by a competent hacker with a small amount of engineering effort.
- The weakness in this Flash security system is that the unique ID is not itself secure. It is a permanent, unchanging code number: once read out of memory, it can be used again by a non-authorised host.
- With its new W74M family of Authentication Flash ICs, Winbond has implemented symmetric crypto to generate a cryptographic and dynamic ID to protect it from attack.
- The method by which Winbond enables symmetric encryption operation to work, through the exchange of Hash-based Message Authentication Code (HMAC), uses hash technology meeting the US government as a FIPS (Federal Information Processing Standard).
- The W74M devices also implement a secondary barrier to attack, a non-volatile monotonic counter which protects the device from replay attack.

- The W74M also offers multi-channel authentication, to enable peripheral devices to access the legit Flash memory resources as well as the host MCU/SoC.
- Key provisioning is a crucial element of the security implementation process at the OEM, and Winbond can support the OEM's systems or implement key provisioning on the OEM's behalf.