boards & solutions + ECE

Combined Print Magazine for the European Embedded Market

November 05/17

Cover Story:

Combining flash storage and security meets industrial requirements

WIBU SYSTEMS

SPECIAL FEATURES:

- INDUSTRIAL COMPUTING & COMMUNICATION
- SAFETY & SECURITY
- COMPUTER-ON-MODULES

Combining flash storage and security meets industrial requirements

By Oliver Winzenried, Wibu-Systems

CodeMeter offers the protection, licensing, and security technology required nowadays in embedded solutions – ready for the Industrial IoT. The combination of flash storage and security in one device enables solutions never thought possible with separate devices.

Wibu-Systems is a leading vendor of sophisticated security and licensing software tools and hardware secure elements (CmDongle) for all common types of software. The flagship technology, CodeMeter, safeguards the integrity of data, applications, and digital communication, while adding versatile and granular licensing capabilities to pave the way for innovative business models. Both capabilities are combined in CmDongles with integrated flash memory for the strongest and most comprehensive production technology in the market. CodeMeter enables to meet the following trends in the Industrial Internet of Things. Connected systems are replacing closed infrastructures, software is replacing hardware, business models are evolving, the architectural landscape is diversifying, and new use cases and services are being released.

Illegal counterfeiting, re-engineering, and illicit copying are threatening the invaluable know-how of companies everywhere. This is not a new danger, as similar threats, such as sabotage, manipulation, or espionage via malware or wiretapping, have long become a sad, but all too familiar reality. The time of isolated solutions has long passed, as industry is moving towards the connected world of IIoT (Industrial Internet of Things). This opens new avenues for attacks, as machines have begun to communicate via TCP/IP networks that are open and inherently insecure. A soft underbelly has been exposed to new types of threats. Protection strategies are now required in many places where they were never needed before. Reports about hacked cars or medical devices accessed surreptitiously from simple laptops abound and demonstrate how important data security and integrity have become in our daily lives. Hackers cost the economy millions, as evidenced by the recall of 1.4 million Jeeps by Fiat Chrysler in the United States after a hacker attack.

CmDongles with integrated flash memory include the CodeMeter smart card chip with added space for more than 1,000 licenses and cryptographic keys and the full complement of CodeMeter security functions. The built-in flash memory can be accessed like any disk and includes different sized data partitions. Each CmDongle with flash memory comes with a CmPublic and CmSecure partition that can be read and written to through the CodeMeter API without being recognized as a disk by the host. The USB stick models include additional CmPrivate and CmCdRom partitions. The four partitions are unique to these highly integrated dongle designs and easily configured to accommodate new product or design strategies to match the user needs. CmDongle is available in USB stick, microSD card, SD card, CF card, and CFast card versions. Whatever the form factor, the full CodeMeter security feature set is always on board. This includes symmetric and asymmetric encryption, signatures, and the storage of X.509 certificates. The card versions are equipped with SLC flash memory, while the industrial-grade USB model has up to 8GB SLC (Single Level Cell) flash memory, compared to 2-bit MLC (Multi Level Cell) flash memory for its commercial-grade cousin. Selected CmDongle variants with flash memory can operate at temperatures from -40°C to +85°C. The SLC flash memory technology was chosen for its long lifespan, low power consumption, memory protection with AES encryption, and long availability in the market. In short: these CmDongles are ready for industry!

Why add flash memory if all CodeMeter security features are available on the non-flash CmDongles as well? Because of the many benefits of the combination product. The first is lower costs. In economic terms, any reduction in the number of components implies a reduction in administration costs. It also enables industrial-grade design. The devices promise a longer productive life of its components operating without breaks or faults. CmDongles with flash memory are designed, produced, and prepped for industrial applications. Their long life and long availability reduce the Total Cost of Ownership

Figure 1. The CodeMeter product porfolio is available in various form factors

Figure 2. All the security software is integrated in the CodeMeter ASIC

(TCO) and increase profits. The smaller form factor allows security functions to be included in very-small-scale devices. Combined devices consume less power than separate solutions. The combination product can be used with new software to upgrade the security of existing devices. Devices already in the field can be upgraded without any changes to their hardware, as the standard form factors USB stick, microSD card, SD card, CF card, or CFast card cover the entire range of common mobile flash memory solutions. Four special data partitions offer opportunities for new products and functions, such as secure storage of highly sensitive data on mobile devices, mobile software solutions, and greater security overall. The built-in combination of smart card chip and flash memory adds to the security of the design. Gambling machines, ATMs, or other devices that are popular targets for tampering and other cyberattacks can benefit from this unique quality.

How much revenue a manufacturer generates with a device can only be known once all costs incurred during the entire life of the device are deducted (commonly referred to as TCO). This includes the simple cost for the components as well as the spending on logistics, administration, certification, repairs and servicing, replacements, training, maintenance, or other lifecycle expenditures. For comparison, CmDongles with integrated flash memory disk come at a higher upfront price than consumer flash memory cards that typically employ MLC/TLC (Triple Level Cell) flash memory technology. Their economic advantage lies in the reduced need for logistics, administration, and certification: fewer parts mean simpler and cheaper provisioning. A single unit has to be procured, only one item introduced in the ERP system, and only one component stored, monitored, or replaced. Components for industrial applications are typically available for many years in identical formats. Firmware and internal electronics remain unchanged in order to work reliably in all OEM applications. Another advantage lies in greater equipment reliability. The CmDongle comes with a range of certifications to make full certification of the embedded device easier and less expensive. In a TCO calculation, the higher purchase price becomes a negligible factor.

Device availability and reliable operations are the prime directive for industrial applications. For integrated flash memory, this means that no data can be lost in case of power outages. Data integrity must be guaranteed even after many access cycles. Wibu-Systems uses only SLC and 2-bit MLC flash memory with high-end industrial flash memory controllers made by Hyperstone with its unique hymap flash firmware. Hyperstone, the only maker of flash memory controllers in Europe, specializes in industrial applications. Swissbit, the maker of CmCards for Wibu-Systems, is known for its industrial-grade memory products made in Germany. It uses Common-Criteria-certified smart card chips like Infineon SLM97 with EAL5+ certified hardware and Cryptolib. The electronic components and manufacturing partners were selected with long life, reliable operations, and the long-term availability of identical CmDongles with fixed bill of material (BOM) in mind. These CmDongles come with industrial-grade properties and can optionally be delivered with conformal coating. They achieve an unbeatable MTBF (Mean Time Between Failures). In commercial terms, the costs of machine stoppages or service repairs caused by faulty memory far exceed the upfront investment into long-life, high-reliability cards with SLC flash. There are certain applications with less stringent requirements and more emphasis on value-for-price which can benefit from 2-bit MLC flash and the excellent Hyperstone hymap firmware.

Product qualification is an expensive and time-consuming, but inevitable process for many industrial applications. CmDongles are qualified according to the following standards: compliance and regulatory tests, e.g. EMC (Emission, Immunity, ESD for CE, FCC, IC, VCCI, KCC, RCM) and registration of conformity (VCCI, KCC, UL), environmental tests (TC, UHAST, HTS, THB), robustness tests, e.g. hazardous gases, corrosion, free fall, shock, vibration, and lifetime tests. These tests are costly, as some require hundreds of samples and external labs need to be commissioned for tests and measurements according to the JEDEC, CISPR, UL, USB, MIL, IEC, EN standards. All of these tests guarantee reliability in industrial applications where use of consumer-grade products would be highly risky.

The life expectancy of a memory card depends on its internal design and technology. MLC flash memory technologies can distinguish more states of the cell compared to the regular two states, meaning that four or eight different charge states (in the case of the TLC) are identified when writing to or reading from the floating gate transistor. Each cell can hold more than one bit with this technology. Such MLCs are cheaper, because more bits are available per square inch, but they are also more susceptible to disruption, making bit errors and catastrophic failure more likely. In the end, the life expectancy of the memory is reduced. Processes to correct bit errors become increasingly complex when more than one bit is expressed in each

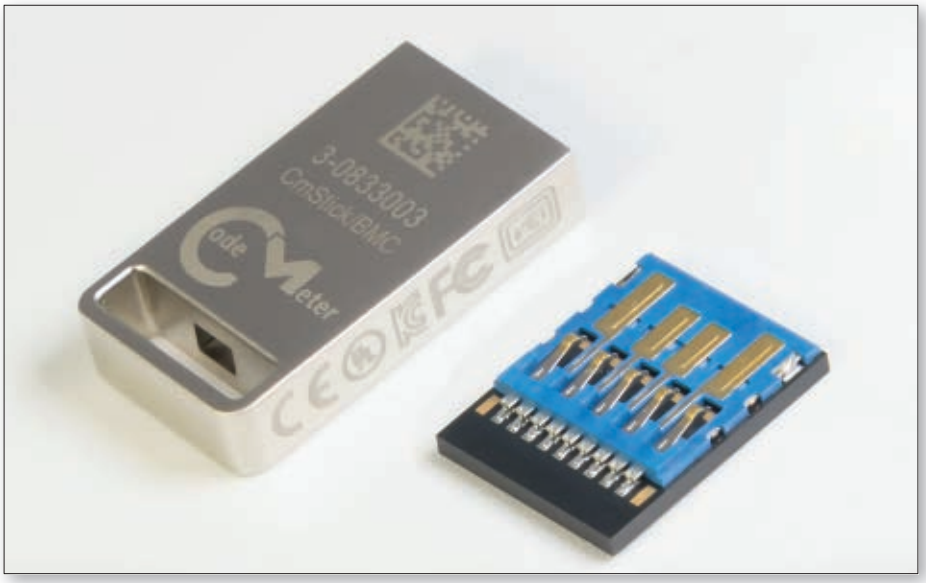

Figure 3. The new CmStick/BMC 16GB uses the latest SiP (System-in-Package) technologies with die stack in the SiP module

cell. 2-bit MLC flash with Hyperstone hymap firmware are a good compromise for some applications, whereas SLC flash offers the ultimate in reliability and life expectancy.

At the chip level, manufacturers need to know which objectives they are pursuing. If the goal is to save costs or achieve high write speeds, as in the case in most consumer-grade flash products, durability, MTBF, electric stability, or power consumption are not as important. Since Hyperstone has committed itself to industrial-grade designs, its goals are long-lasting availability, reliability, data integrity after power failures, and low power consumption. These attributes require additional resources and intelligent capabilities in the controller. The patented hymap firmware manages internal controller functionality, such as early acknowledgement, in an industry-ready manner to ensure that no data is lost when the power supply is disrupted.

Many embedded devices are tiny and use every last bit of available space. However, most embedded systems include flash memory storage for applications and other data. If this original flash memory card is replaced with a CmDongle with integrated flash memory, the same form factor and same number of interfaces now comes supercharged with maximum security. The smallest version of CmDongle with flash memory comes as a microSD card. At only 11mm × 15mm × 0.7mm in size, it fits even the tiniest devices – a great opportunity for making the controllers, sensors, and engines of the Industrie 4.0 world more secure. The new CmStick/BMC 16GB uses the latest SiP (System-in-Package) technologies with die stack in the SiP module to accommodate the smallest form factor with USB interfaces, highest reliability, humidity and shock resistance.

Industry and legislators are responding to the increasing threats of cybercrime with new regulations or changes to the old rulebooks. This is happening in Europe, Asia, the United States and the rest of the world. One recent example is the US Cybersecurity Improvement Act of 2017. Technical protection measures are already required by law for medical devices. New devices have begun to include security by design, but many legacy devices will remain in use until they are eventually replaced by newer machines. These devices can now benefit from the ability to retrofit security technology in an easy and streamlined manner. Security measures can be added whenever normal smart card connections are available. The existing hardware remains untouched, and only the software needs to be adjusted for the new security functions. Little effort is needed to bring old technology up to the newest standards of security. ■