

Anti-piracy protection for embedded systems

By Oliver Winzenried, Wibu-Systems

Anti-piracy protection is now available in form factors as small as μ SD cards. This smaller form factors versions of the CodeMeter software and IP protection platform are aimed at the specific needs of embedded systems manufacturers.



Figure 1. CmCard/ μ SD, CmCard/SD and CmCard/CF providing IP protection for the embedded industry

■ Embedded systems play an increasingly important role in industries as diverse as health-care, manufacturing, and retail. Products from pacemakers to household appliances, automobiles to industrial looms can contain embedded systems which house both microprocessors and custom software. Software in embedded systems can be the result of years of effort and represent a significant asset to the publisher. Unfortunately, along with the growth in embedded systems has come a growth in illegal piracy of software.

Just as Blackbeard the Pirate roamed the Atlantic hundreds of years ago, nowadays pirates roam the seas of cyberspace, looking for valuable cargo to steal. Piracy includes stealing and counterfeiting entire systems to compete with the legal manufacturer, as well as hijacking process and instruction manuals and copyrighted and trademarked designs. Pirates skip the expensive research and development stage of product development by copying existing systems. A recent study by VDMA (Verband Deutscher Maschinen- und Anlagenbauer e.V) put piracy-related losses to German machine manufacturer companies in 2009 in excess of €6.4 billion, with 45 percent of companies reporting piracy of entire systems. Because Germany is one of the leading countries in the world for the development and sale of embedded systems, such piracy is of serious concern

to both government and the private sector. To help find a solution to better protect embedded systems, Wibu-Systems teamed up with Hyperstone for their flash card controller and Swissbit for hardware assembly and testing. The partnership has produced the latest CodeMeter variants from Wibu-System: strong hardware-based security for software, intellectual property (IP), and data on CF (compact flash), SD (secure digital), and μ SD (micro SD) cards. The developer of the popular CodeMeter hardware- and software-based copy protection systems previously only offered hardware solutions with USB interfaces, which often did not meet the needs of embedded systems manufacturers. The hardware protection systems protect software, algorithms, and data through strong encryption. Only the CodeMeter stick (CmStick) can decrypt the information rendering it usable.

Aimed squarely at the tough requirements of embedded systems, the new CmCards provide equal security to their USB-based relatives (CmStick), with some additional features, including: ability to function from -25 to $+85^{\circ}\text{C}$; increased resistance to electro-static discharge (ESD); increased resistance to corrosive gases and improved contact durability through a galvanic hard coating; fixed BOM (bill of material) costs for the hardware and controlled firmware, all made in Germany; complete 100

percent compatibility with USB CodeMeter devices; improved read/write speed; better ECC (elliptic curve cryptography) error correction; wear leveling and bad-block handling via SLC flash memory and a 32-bit RISC controller; S.M.A.R.T. lifetime monitoring for flash memory; support for FAT32, NTFS, and EXT3 file systems.

With CodeMeter, embedded systems manufacturers gain some striking benefits. These cover prevention of piracy and illegal copying of systems for counterfeiting and protection of intellectual property (IP) including algorithms, processes, and trade secrets to avoid reverse-engineering by competitors. Using digital signatures for software components, the system's binary integrity can be guaranteed, reducing the risk of tampered software. Service manuals and production data including workflow descriptions and process diagrams can be encrypted and protected from falling into competitive hands.

New business models can be enabled such as pay per use and pay per feature. Systems can be more easily ported to multiple platforms such as Windows Embedded, Real Time Linux or VxWorks because of a complete cross-platform protection system. The need for a new memory controller brought Wibu-Systems to Hyperstone, a leading supplier of flash memory

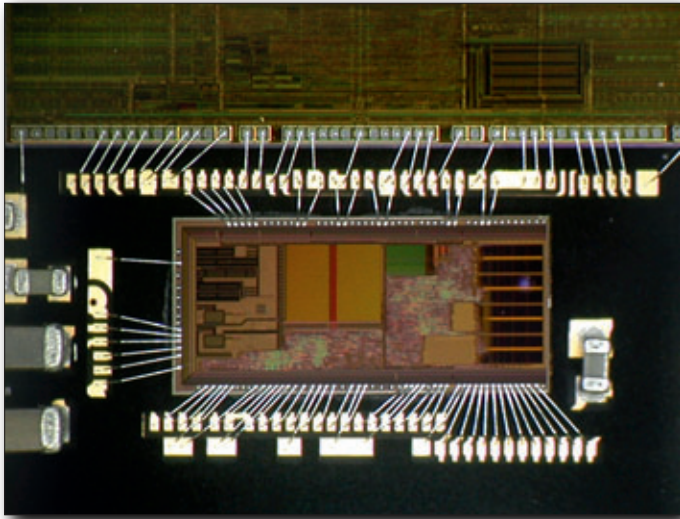


Figure 2. High technology inside the CmCard/ μ SD

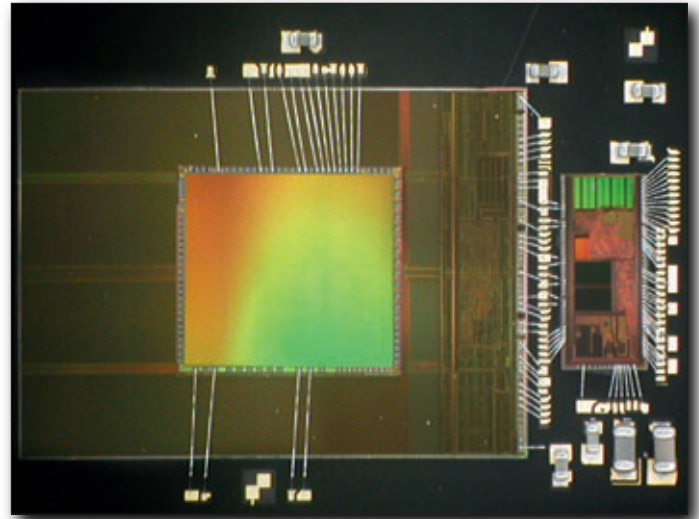


Figure 3. Details of the CmCard/ μ SD. This CmCard/SD allows the protection of IP for embedded systems.

controllers for SD and CF cards. This supplier serves a global base of customers from its headquarters in Konstanz, Germany, and subsidiaries in Taiwan and the USA. Hyperstone is an expert in fabless semiconductor and microprocessor design, and its products include the hyNet SoC for IP-cameras and real-time Ethernet as well as microcontrollers for solid state disks (SSD), disk-on-module (DoM), disk-on-board (DoB), embedded flash solutions such as eMMC, and flash cards such as CF, SD and μ SD. SwissBit, headquartered in Bronschhofen in Switzerland, manufactures

industrial memory products at its production site in Berlin, Germany. The company has a highly automated and top-quality production of COP and Die-Stack.

Previously, conventional software protection hardware was only available in much larger sizes. The new CodeMeter hardware will have an immediate effect in the growing smartphone software market and for mobile Internet use. The company had to overcome some significant engineering challenges in designing the CmCard/ μ SD. For example, it was difficult to find

a board manufacturing partner with technical expertise in miniature board fabrication. The overall design required a thickness of just 150 μ m, holes of 0.1 mm, circuit paths of 40 μ m widths and different gilding on the plug contacts and the bondpads, all of which presented significant technical challenges. Swissbit was chosen as production partner. The die-stack and ultra-miniature form factor was a difficult challenge, in addition to the requirements for testing with industrial parameters, a fixed bill of materials, and life-cycle management for flash-based products. ■