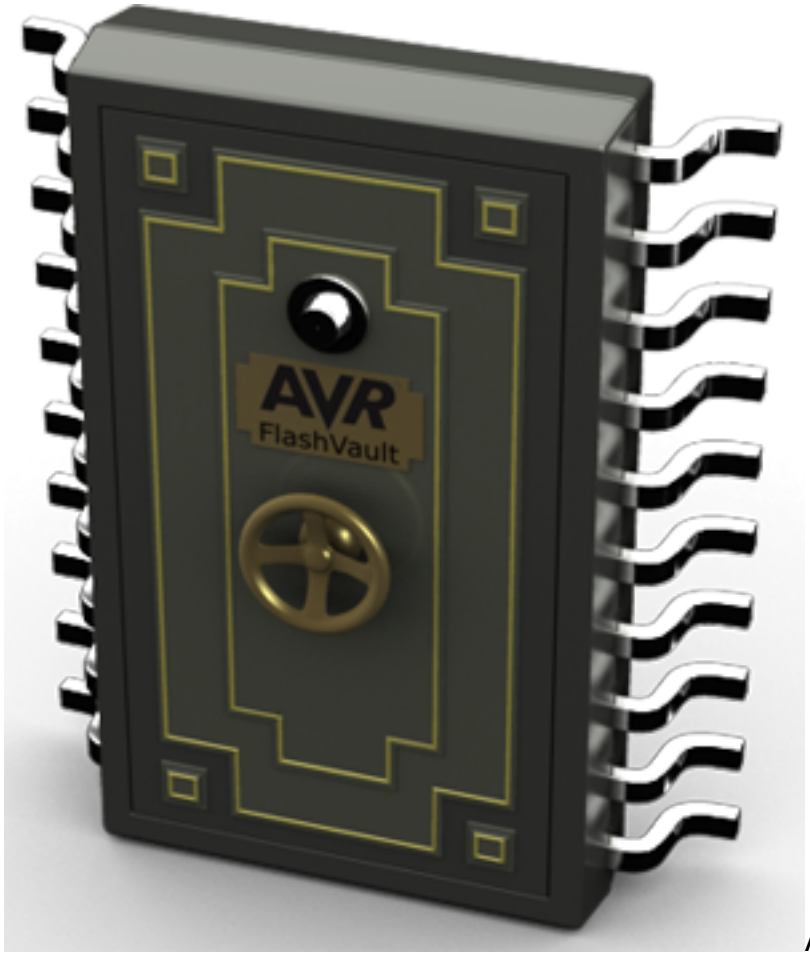
Securing Information in your Microcontroller Core

Oyvind Strom, Director, AVR Products, Atmel Corporation

For years, system designers have been trying to find a way to improve the microcontroller—the heart of their system designs. Improvements can range from increasing performance, lowering power consumption, increasing clock speeds and much more. However, security and flexibility to add different levels of security have surfaced over the recent years due to demanding customer applications.



Although many general microcontrollers come with a standard core and features, every design contains a software value that often comprises the real end customer value in the product. It is important for companies and their designers to be able to securely program and execute programs from the flash memory. At the same time, designers want to ensure the data is safe and can only be accessed by qualified devices. Understanding the system designer’s need for flexibility and security, Atmel developed a patented technology coined ‘FlashVault’ that addresses these concerns of the system designer. This technology was added to Atmel proprietary microcontroller AVR cores by adding on-chip Flash and SRAM memories to enable secure and fast access. In addition, the FlashVault technology allows libraries to be securely programmed into an Atmel AVR device and protects the value of the software library.

The FlashVault technology allows the program to be executed while the central

processing unit (CPU) is in a secure state and does not allow the flash in the microcontroller to be read by non-secure software in the device. This is useful for companies where the real value is in the software component of the system. Having safely programmed a part of the flash with the library, the customer can then ship the partially programmed system to an unsecure location where final application development can be done and the product can be programmed with the application code. Code from the secure library can be executed, without compromising the proprietary secure code.

With the security and flexibility of technologies such FlashVault, system engineers are now given the opportunity to customize a microcontroller core with the onboard flash without comprising security. In addition, it still allows the end customer the option to program their own code into the flash. This is useful for a long range of applications, including wireless stacks, applications relying on specific algorithms, and protection of patented software, such as audio systems and others that allow OEM and end customer system designers to easily embed software libraries without compromising security in the microcontroller.

Ultimately, technologies that allow partially programmed and locked flash, such as FlashVault, are only available in Atmel’s proprietary 32-bit AVR core. This will help system designers feel more confident that their software libraries are secure and will prohibit tampering of the flash memory.

As security continues to be a growing concern, more companies will benefit from technologies such as FlashVault to ensure that system designers and end customers can have their own customizable specifications and still allow the customers to add their own code.