Key Tips: PIC Microcontroller Code
Preventing PIC Microcontroller Code from being Duplicated
Preventing PIC Microcontroller Code from being Duplicated

If there is an electronic product that is strong or selling well, code copying is a hard reality that needs to be addressed.

Don't Ignore the Parrot: Use PIC Microcontroller Code Protection – Reading an unprotected firmware from a PIC microcontroller is simple. Ensure the microcontroller is connected to the programming header and the raw code can be extracted to a computer via the programming adapter.
Preventing PIC Microcontroller Code from being Duplicated

Want to Protect Your Code?

• **Enable Code Protection Bit**: In the PIC microcontroller, there is a code protection bit that will prevent read operation on the program memory when it is asserted.

• **Unique ID Authentication**: Instead of preventing the code from being read, this method requires the application to verify itself against a unique ID before launching the main program.

• **Epoxy Coated**: Where there is no need to update the firmware of the microcontroller, the epoxy coating can be used to physically prevent access to the microcontroller.

• **Self-Destructing Circuit**: It uses sensors to detect any illegal attempt to access the hardware and connect the microcontroller to a high voltage source. This is a drastic measure to take and the system may accidentally activate the self-destruct mode if the sensor malfunctions.
Key Serial-number Chips For PIC Microcontroller Code Protection
Key Serial-number Chips For PIC Microcontroller Code Protection

There are several good methods of microcontroller code protection that will keep your firmware safe from most hackers.

Count to Ten-Thousand: PIC Microcontroller Code Protection - Typically, processors are programmed by downloading the machine code into local memory.

The location of the program code is well-known by even inexperienced hackers, which makes it very insecure.
Key Serial-number Chips For PIC Microcontroller Code Protection

Hide and Seek for Your Code Security - The unique key must be in a location that can be read prior to executing the program.

• Flash Memory: This is the most common place for storing program code and keys that may be erased and rewritten. This is used during the debugging process and for in-circuit testing and development.

• Program Memory: This a usually a dedicated block of memory reserved for the program. It is a good place to hide the key, as well. Unless the encryption method for the key is known, it is difficult to separate actual program code from the key code.

• Microprocessor Memory (EEPROM): The key is hard-wired or burned into a ROM device and cannot be changed. This relies upon the system's ability to prevent read access from intruders.
Altium Designer 18

New to Altium Designer? Don’t be!

Try the latest release and get time saving workflows and enhanced team collaboration options today at:

www.Altium.com/free-trials
Thanks for your attention!