# Secure Debugging for Microcontrollers

Modern microcontrollers have embedded flash memories that can be reprogramed in the field allowing for firmware upgrades of deployed systems.

Usually the initial firmware upload in the factory is done by dedicated tools connected to a dedicated debug or programming port providing access to the internal memory. Once programmed this port is disabled by issuing some commands that will disable the port permanently by blowing some fuses. In some other cases is possible to restore the port access by forcing a total flash erase. This security features are necessary to protect the system from somebody trying to get access to the content of the memory. The manufacturer may want to protect either sensitive information stored on the device like encryption keys, activity logs etc.., or they need to protect against an attempt to reading the firmware itself.

C:\devel\thinkos\docs\secure-remote-debug-case-2.emfC:\devel\thinkos\docs\secure-remote-debug.emfC:\devel\thinkos\docs\debug-monitor.emf