

RfM: A Radio Flashing Tool for Microcontrollers

1. Motivation: radio-controlled fitments

- low-performance (minimum functionality)
- hard to access
- development and maintenance (=reprogramming) requires unmounting and remounting



control module underneath a desk



disassembled control module



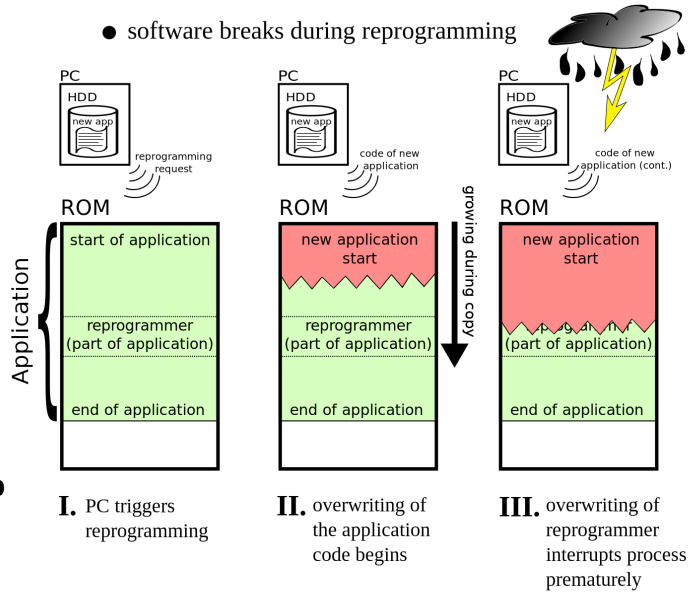
reprogramming station at a desk



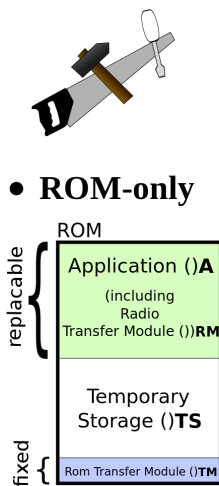
Reprogramming over radio

2. Problem: Self-overwriting

- software breaks during reprogramming



3. Approach: three-parted memory layout



• ROM&RAM

• ROM-only

• Algorithm:

1. receives request for reprogramming from PCA and transfers control to .RM
2. handles complete and correct reception of new RMA into and transfers control to .TSTM
3. transfers new from to final location (optionally, TMATS old is backed up in), and triggers reboot.ATS
4. New listens for reprogramming requests for three A seconds (bootloader fallback).
5. Optionally, if new crashes (detectable via watchdog), A TM restores old (ROM-only version).A
6. Execution of new .A

4. Results: infrastructure for radio-based reprogramming



- seamless integration into user application (minimal linking efforts, no linking scripts required)
- good portability/almost platform independent
- actual reprogrammer requires only little resources (< 2kB ROM)
- robust by bootloader-fallback, and optionally, predecessor restoring
- authors' implementation: CC1010 of Texas Instruments (8bit μ C, 2kB RAM, 32kB ROM), stable for 8 month now; heavily utilized for the development of distributed, self-organized evolutionary algorithm

Stefan Goldmann and Ralf Salomon

Faculty of Computer Science and Electrical Engineering
 Institute of Applied Microelectronics and Computer Engineering
 University of Rostock, Germany