CS5470 Development of Trusted Software

Static Analysis in a Real World Project

Niusen Chen (PhD student)
Department of Computer Science

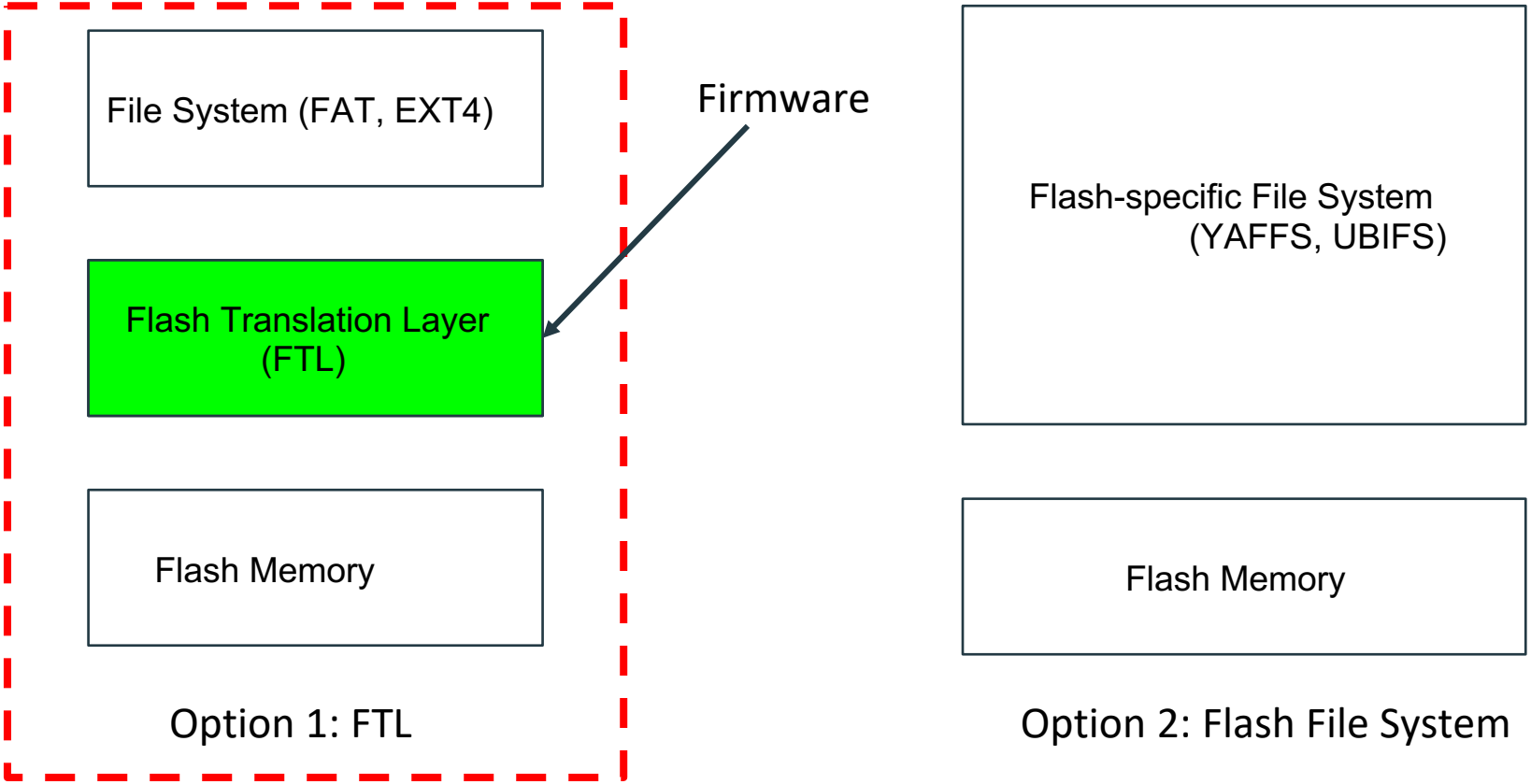
Flash Device

Cell Phone

SSD

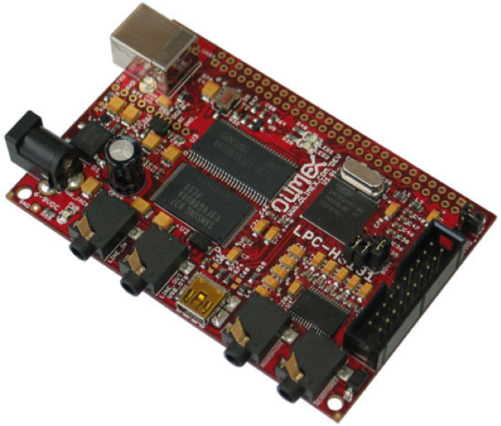
USB

How to Use Flash



Hardware & Firmware

Hardware:



Lpc H3131

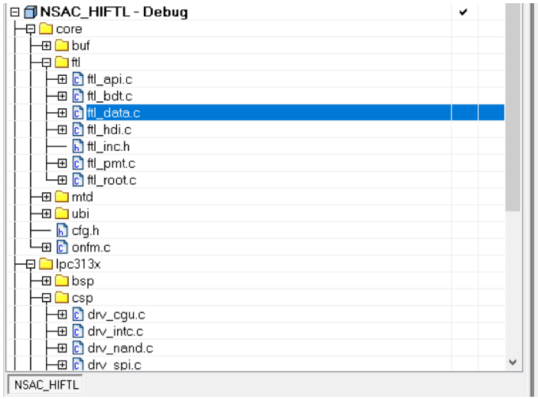
Firmware:

OpenNFM: An open source NAND flash controller framework

Github:
https://github.com/IMCG/opennfm

OpenNFM

ftl_api.c	upload codes.	9 years ago
ftl_bdt.c	upload codes.	9 years ago
ftl_data.c	upload codes.	9 years ago
ftl_hdi.c	upload codes.	9 years ago
ftl_inc.h	upload codes.	9 years ago
ftl_pmt.c	upload codes.	9 years ago
ftl_root.c	upload codes.	9 years ago




```
    }
  }
  return ret;
}

STATUS FTL_Read(PGADDR addr, void* buffer) {
  LOG_BLOCK block;
  PAGE_OFF page;
  STATUS ret;
  ret = PMT_Search(addr, &block, &page);
  if (ret == STATUS_SUCCESS) {
    ret = UBI_Read(block, page, buffer, NULL);
  }

  return ret;
}

STATUS FTL_Trim(PGADDR start, PGADDR end) {
```

CppCheck

Cppcheck is a static analysis tool for C/C++ code. It provides unique code analysis to detect bugs and focuses on detecting undefined behaviour and dangerous coding constructs

Link: http://cppcheck.sourceforge.net/

```
Example usage:
  # Recursively check the current folder. Print the progress on the screen and
  # write errors to a file:
  cppcheck . 2> err.txt

  # Recursively check ../myproject/ and don't print progress:
  cppcheck --quiet ../myproject/

  # Check test.cpp, enable all checks:
  cppcheck --enable=all --inconclusive --std=posix test.cpp

  # Check f.cpp and search include files from inc1/ and inc2/:
  cppcheck -I inc1/ -I inc2/ f.cpp
```

```
[mpt/dfu/dfu_main.c:63]: (error) Resource leak: nid
[mpt/dfu/dfu_main.c:63]: (error) Resource leak: boot_bin
[mpt/dfu/dfu_main.c:69]: (error) Resource leak: onfm_fw
[mpt/dfu/dfu_main.c:69]: (error) Resource leak: boot_bin
[mpt/dfu/dfu_main.c:78]: (error) Resource leak: onfm_fw
[mpt/dfu/dfu_main.c:78]: (error) Resource leak: nid
[mpt/dfu/dfu_main.c:78]: (error) Resource leak: boot_bin
[mpt/dfu/dfu_main.c:93]: (error) Resource leak: onfm_fw
[mpt/dfu/dfu_main.c:93]: (error) Resource leak: nid
[mpt/dfu/dfu_main.c:93]: (error) Resource leak: boot_bin
[mpt/dfu/dfu_main.c:121]: (error) Memory leak: nid_bin
[mpt/dfu/dfu_main.c:121]: (error) Resource leak: onfm_fw
[mpt/dfu/dfu_main.c:121]: (error) Resource leak: nid
[mpt/dfu/dfu_main.c:128]: (error) Memory leak: nid_bin
[mpt/dfu/dfu_main.c:128]: (error) Resource leak: onfm_fw
[mpt/dfu/dfu_main.c:128]: (error) Resource leak: nid
```

```
Checking onfm.c ...
[onfm.c:128]: (style) The scope of the variable 'i' can be reduced.
[onfm.c:168]: (style) The scope of the variable 'i' can be reduced.
Checking onfm.c: __ICCARM__...
[onfm.c:92]: (style) The function 'ONFM_Capacity' is never used.
[onfm.c:74]: (style) The function 'ONFM_Format' is never used.
[onfm.c:103]: (style) The function 'ONFM_Mount' is never used.
[onfm.c:124]: (style) The function 'ONFM_Read' is never used.
[onfm.c:214]: (style) The function 'ONFM_Unmount' is never used.
[onfm.c:164]: (style) The function 'ONFM_Write' is never used.
```

Demo