Diplomová práce

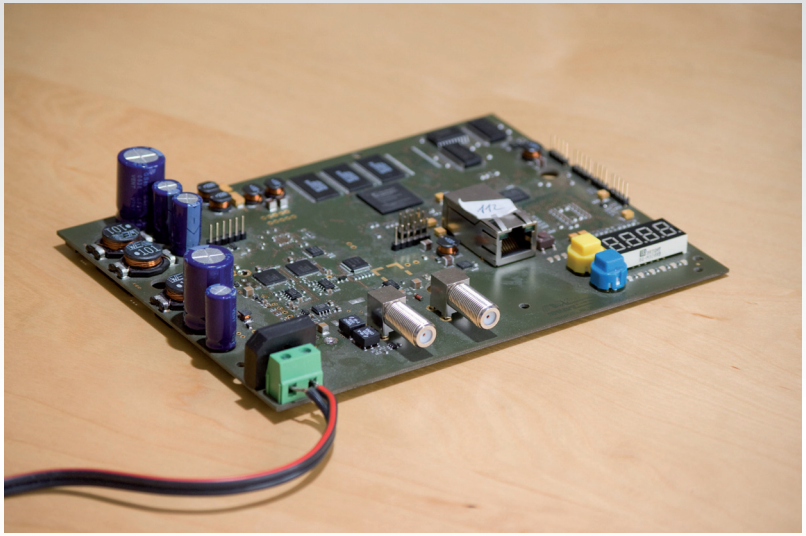
Pojítko SkyWire - Zabezpečení a ochrana před neoprávněnou manipulací

Bc. Martin Šmarda
ČVUT FIT
2013

svm
microwaves s.r.o.
www.svm.cz
svm
microwaves s.r.o.
www.svm.cz

DATOVÉ POJÍTKO

můžeme považovat za embeded počítač s velmi omezenými zdroji.



Parametry

- SH4 procesor na 200 MHz
- 16 MB flash
- 64 MB RAM

Projekt

- na půdě firmy SVM Microvaves s. r. o.
- spolupráce v teamu s rozdělenými odpovědnostmi
- spolupráce a konzultace s pracovníky firmy

Společný úkol

je osadit pojítko linuxovým systémem umožňujícím nastavení, monitorování a správu zařízení.

OBSAH MÉ PRÁCE

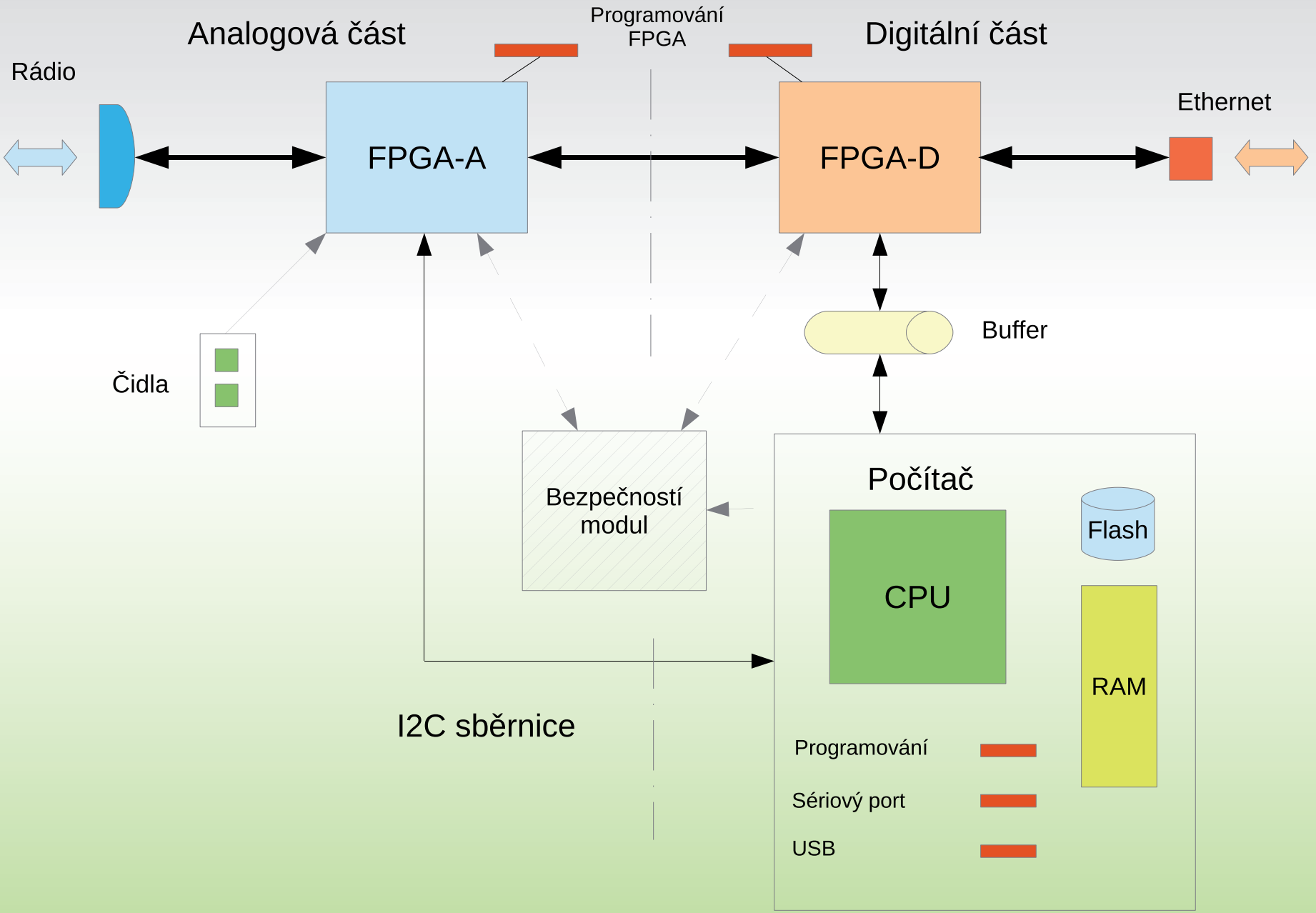
Systém

- identifikace způsobu nasazení a nároků na systém
- rozsáhlý průzkum a volba distribuce
- volba sestavovacího prostředí a komponent
- osazení distribuce potřebnými programy
- minimalizace a ladění

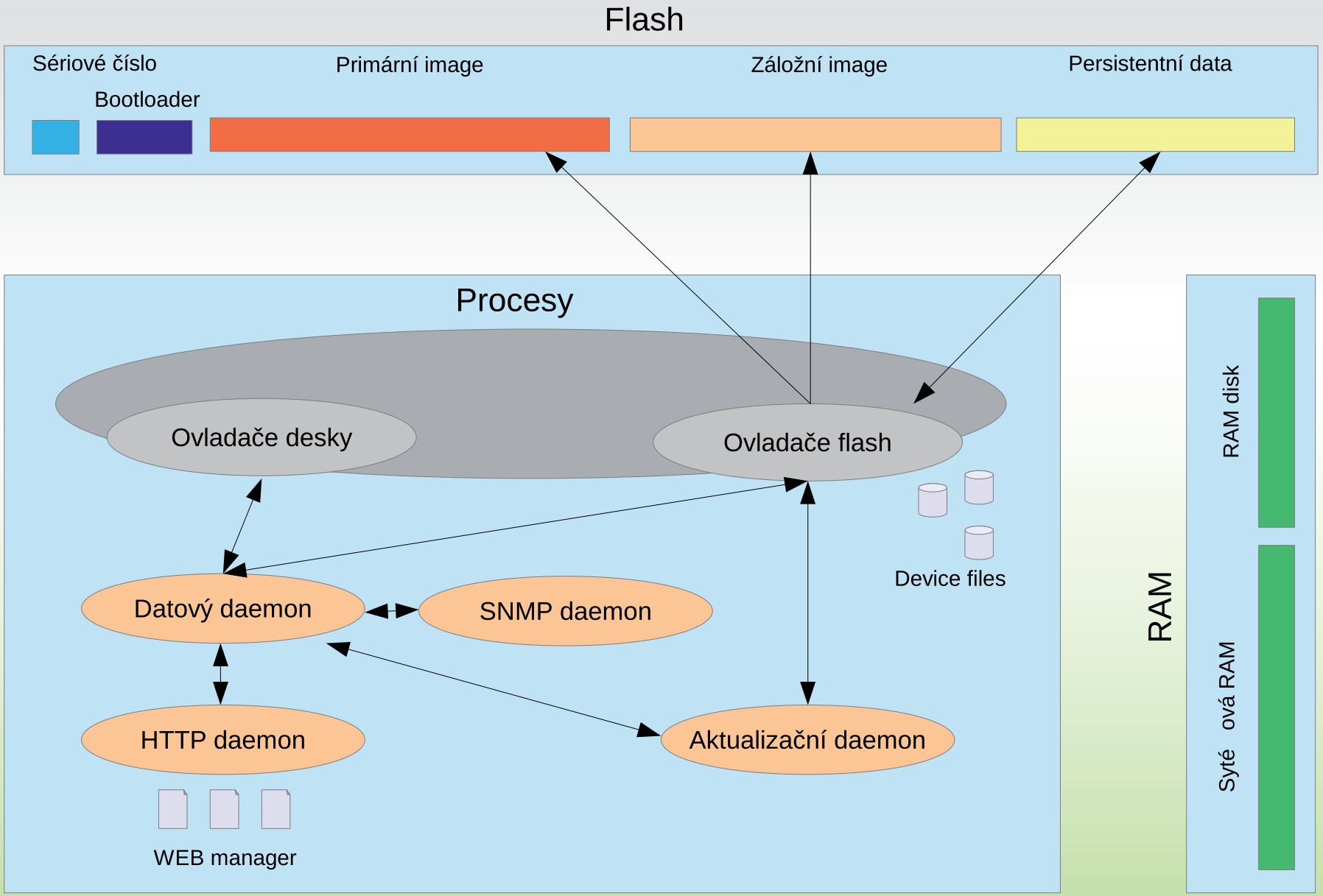
Zabezpečení

- analýza možností hardware a systému jako celku
- identifikace zranitelností
- analýza a návrh interních procesů
- aplikace některých bezpečnostních mechanizmů
- formulace doporučení

MODEL POJÍTKA



MODEL SYSTÉMU



ÚVAHA O KOMPONENTÁCH SYSTÉMU

Image systému může zabírat nejvýše třetinu paměti.
Jak jej zmenšit na minimum?

- použít minimalistickou libc (uClibc)
- použít minimalistický webový server (Lighttpd)

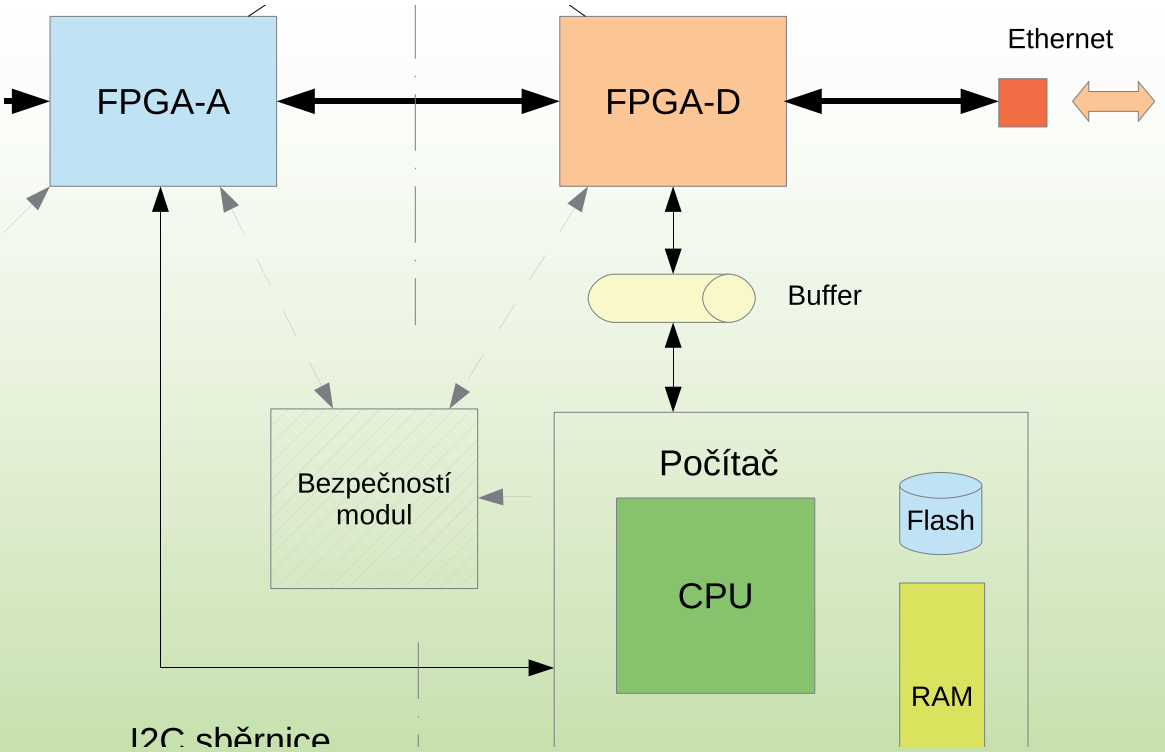
Co když to nestačí? Jak také zvýšit bezpečnost?
Odstranit nadbytečné a nežádoucí komponenty!

- ovladače hardware
- editory a nástroje pro vývoj
- nástroje pro správu uživatelů
- nástroje pro sledování běžících procesů
- SSH daemon

PROBLÉM ULOŽENÝCH HESEL A KLÍČŮ

Flash paměť není bezpečné médium.
Citlivá data nejsou bezpečná proti reverse engineeringu.

- algoritmické odvození v FPGA na základě sériového čísla
- uložení citlivých dat mimo flash



TESTOVÁNÍ

Automatizované testovaní je prakticky nemožné.
Manuální je zdlouhavé a náročné.

- rekompilace systému asi 30 minut
- manuální nahrání do spoje 5 minut

Použitý způsob testování

- zachování funkčnosti a integrity systému
- testování provedeného zásahu
- akceptační testování zda změny vyhovují potřebám

DOSAŽENÉ VÝSLEDKY

Výstupem je funkční operační systém a kompilační prostředí, jež se využívá v testování a dále se připravuje pro produkci.

Velikost celého balíčku systémů je zhruba 3,5 MB oproti původní verzi na 6,6 MB.

Firma SVM na základě mých analýz a doporučení začala řešit lepší podporu zabezpečení na úrovni hardware.

Podařilo se mi realizovat jednu z prvních prací ve spolupráci komerčního a akademického prostředí.

DĚKUJI ZA POZORNOST

prostor pro dotazy

ODPOVĚĎ NA OTÁZKU OPONENTA

Doporučuji pravidelně aktualizovat sestavovací balíčky a sledovat hlášení známých chyb.

Opravy a aktualizace sestavovacího prostředí vychází v tříměsíčním vývojovém cyklu.

Současně se hodí sledovat nějaké bezpečností listy pro aktuální informace o nových hrozbách.

Je třeba pravidelně vydávat aktualizace firmware s novými záplatami a motivovat zákazníka k jejich použití.

http://buildroot.uclibc.org/news.html