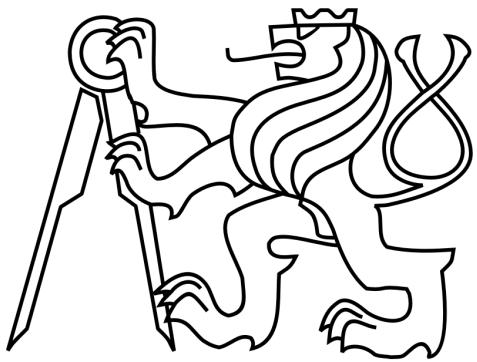
Formální Metody a Specifikace (LS 2011)
Přednáška 1: Úvod

Stefan Ratschan

Katedra číslicového návrhu
Fakulta informačních technologií
Ceské vysoké učení technické v Praze

18. únor 2010



Kontaktní údaje

Vždzy:

- Stefan Ratschan
- `http://www.cs.cas.cz/~ratschan`
- `stefan.ratschan@cs.cas.cz`

Čas okolo MI-FME:

- FIT, Kolejní 550/2, místnost 319

Jindy:

- Ústav Informatiky Akademie Věd
- Pod Vodárenskou věží 2
- Metro stanice Ládví

Pravidla hry

Prosím přerušit!

- (aspoň v České republice) jsem blbé otázky ještě nezažil,
- ale hodně blbého mlčení!

Přednáška vs. cvičení:

- V přednášce se učíme nový materiál,
- v cvičení ho cvičíme.

Z toho plyne:

- V cvičení nebudu vysvětlovat materiál z přednášky ještě jednou.
- Kdo nechodí do přednášek nebude rozumět tomu co děláme v cvičení!

Zdroje

Nebudu sledovat určitou učebnici.

Na slajdách každé přednášce budu uvádět zdroje (v angličtině)

Pokud návštěvujete přednášky, nebudete je potřebovat.

Pokud nenávštěvujete přednášky, budete potřebovat další zdroje

Slajdy budou obsahovat informaci jen částečně,
příklady, obrázky atd. budu kreslit na tabuli

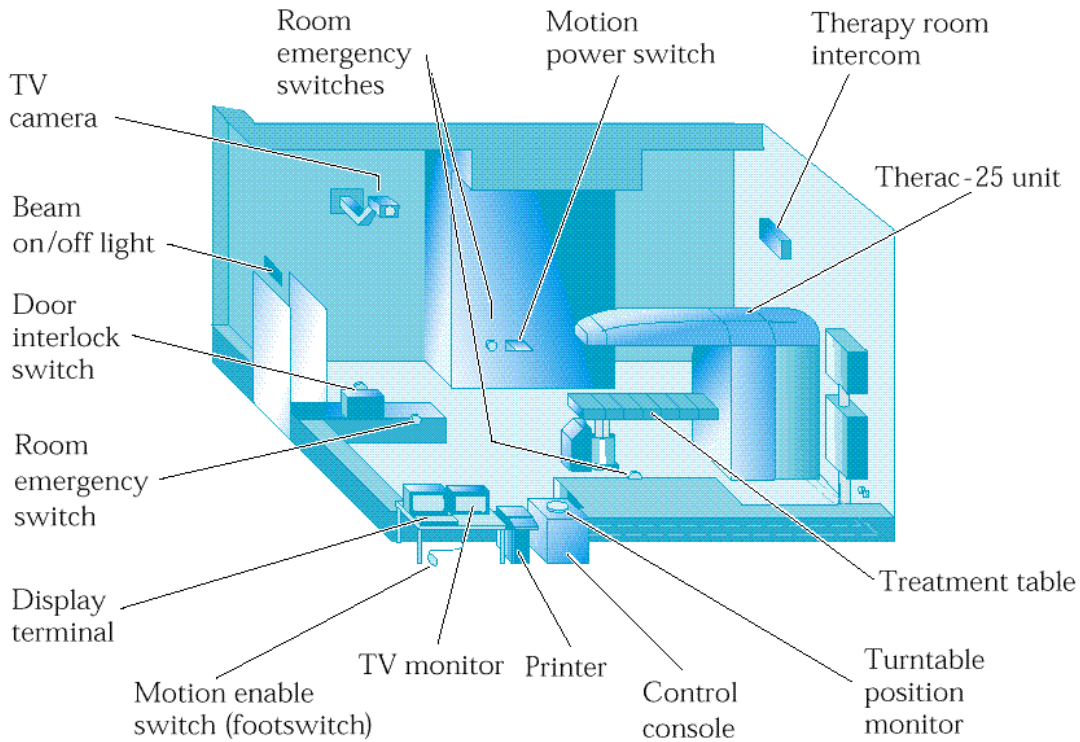
Pozor s wikipedií!

- Velká část obsahu přednášky tam není.
- Pokud je, často obsahuje chyby, špatné vysvětlení atd.

Wikipedie nemůže nahradit pochopení materiálu.

Teď: Katastrofický začátek.

Therac-25

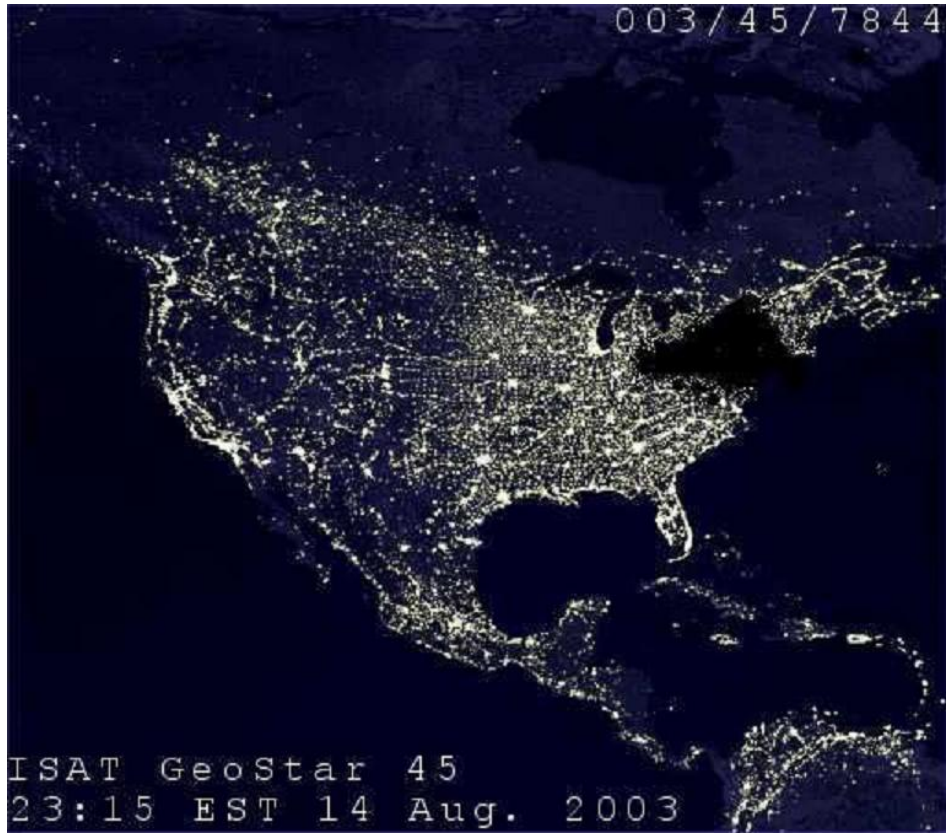


- Zařízení pro radioterapii
- Aspoň 6 havarií s nadměrnou dávkou radiace, částečně smrtelné

Ariane 5 raketa 501

- Start skončil několik desítek sekund po startu explozí
- Škoda: 290 M€
- Odklad programu jeden rok

Northeast Blackout of 2003



- Výpadek proudu ve velké části spojených státu 14.-16.8.2003
- Víc než 10 přimých úmrtí
- Obrovské finanční škody

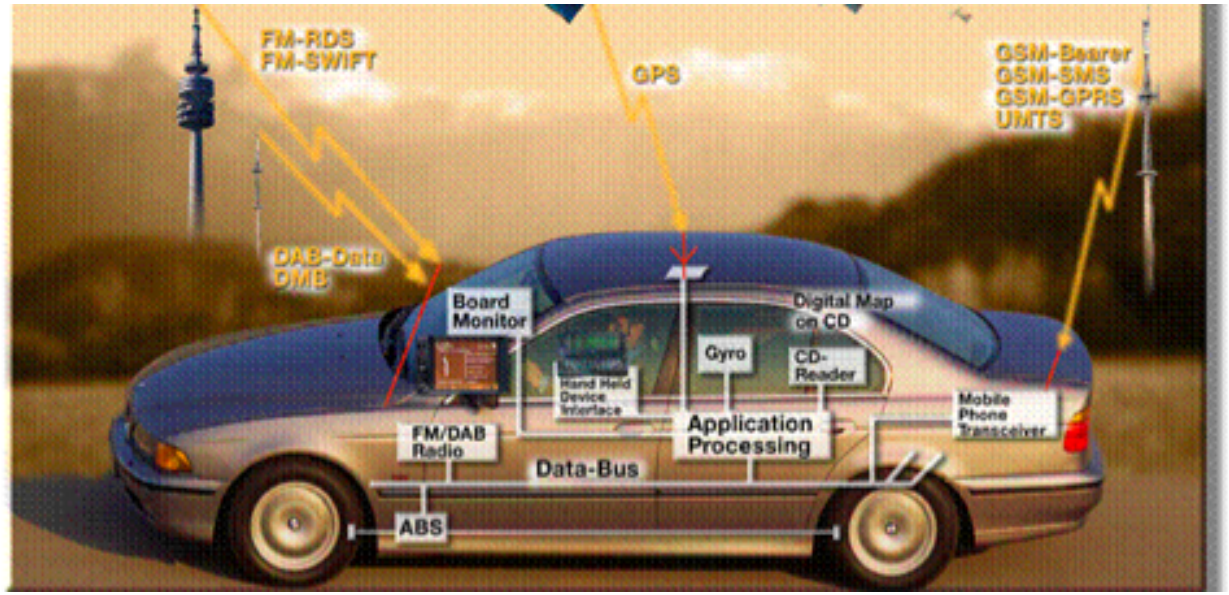
Souvislost

Co to má společného s informatikou a tímto předmětem?

- Každá nadměrná dávka v Therac-25 výsledek chyby v řidícím softwaru
- Explose Ariane 5 byl výsledkem
  chybné konverze z čísla s pohyblivou čárou do celého čísla
- Výpadek proudu výsledkem pozdní reakce na menší problém kvůli chybě v softwareu poplachového zařízení.

Cyber-Physical Systems (CPS)

Čím dál větši integrace digitalní elektronika/software a fyzikálních systémů



"Cost of electronics in cars expected to move beyond 50% soon" [Emb, 2005].

Dnes: většina výpočetní kapacity už se nenachází v stolních počitačích

Safety Critical System

Nejen,

čím dál větši integrace

digitalní elektronika/software a fyzikálních systémů,

ale i

integrace do každodenního lidského života

Poruchy můžou ohrožovat lidský život

Správnost nezbytná

Tato přednáška chce tomu přispívat.

Předmět přednášky

Formální Metody a Specifikace

Formální: Matematická preciznost

při

- specifikaci chování softwaru
- vytvoření softwaru který splňuje specifikaci

Ale: Není to jen teoretické cvičení, které se v praxi nepoužívá?

První přínos přednášky: Mozkový Upgrade

Lidský mozek vznikl před několika tisíci lety, a tentokrát měl jiný účel

Kvůli tomu historickému účelu,
ve moderním (a zejména informatickým) životě
ten modul je strašně náchylný k chybám

Tím, že cvičíme matematickou preciznost,
se vylepšujeme mozek pro informatický život!

Konkretní přínos pro Vás: budete spolehlivějšími vývojáři softwaru.

Druhý přínos přednášky: Nástroje z praxe

V průmyslu se čím dál víc prosazují formální nástroje
(hlavně v tzv. safety-critical aplikacích)

Přednáška Vám pomáha pochopit a používat nástroje
s kterými se budete potkat v praxi.

Automatické formální metody v průmyslu

Poloautomatické důkazy částečné správnosti počítačových čipů se běžně používají v hardwarovém průmyslu [Kropf, 1999]

Software: Důkaz "malých" vlastností [D'Silva et al., 2008]

- správnost transformací v kompilátoru
- žádná divize nulou
- žádné psaní mimo hranice polí
- ...

Příklady:

- Airbus používá automatické metody pro formální verifikaci programů `http://www.absint.de/astree/`
- Microsoft: "Windows Driver Kit" obsahuje "Driver Verifier"
- Automatická formální verifikace protokolů

Současní výzkum stále zvyšuje použitelnost,
v blízké budoucnost se budou běžně vyskytovat.

Co není obsahem přednášky

Dlouhá tradice výzkumu úplné formalizace vývojového procesu softwaru, např.:

- B-method
- Z-notation

Přes desetiletí výzkumů se stále
jen používají ve velmi specializovaných aplikacích.

Nebudeme se s nimi zabývat.

Ale: Přednáška přispívá i k pochopení takových metod.

Předběžný plán přednášek

1. Úvod
2. Specifikace programů a základy praktické logiky 1
3. Specifikace programů a základy praktické logiky 2
4. Formální modelování datových struktur
5. Aserce, správnost bezcyklových programů
6. Parciální správnost programů s cycly: invarianty
7. Správnost volání funkce
8. Terminace, totální správnost programů
9. Správnost objekt-orientovaných programů
10. Automatizace 1: Rozhodovací procedury
11. Automatizace 2: Ověřování modelů
12. Alternativní metody (operacionální, denotacionalní semantika)

Literature I

Study of worldwide trends and R&D programmes in embedded systems in view of maximising the impact of a technology platform in the area. Report for the European Commission, 2005.

V. D'Silva, D. Kroening, and G. Weissenbacher. A survey of automated techniques for formal software verification. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 27(7): 1165–1178, July 2008.

Thomas Kropf. *Introduction to Formal Hardware Verification*. Springer, 1999.