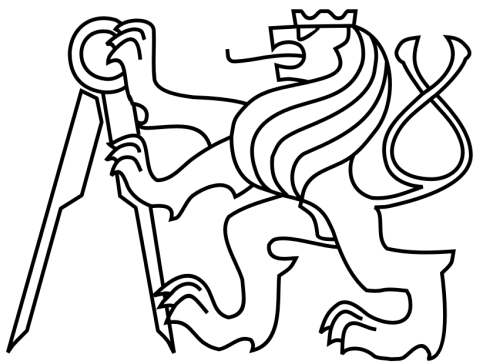
Formální Metody a Specifikace (LS 2011)
Přednáška 12:
Závěrečný souhrn a souvislosti

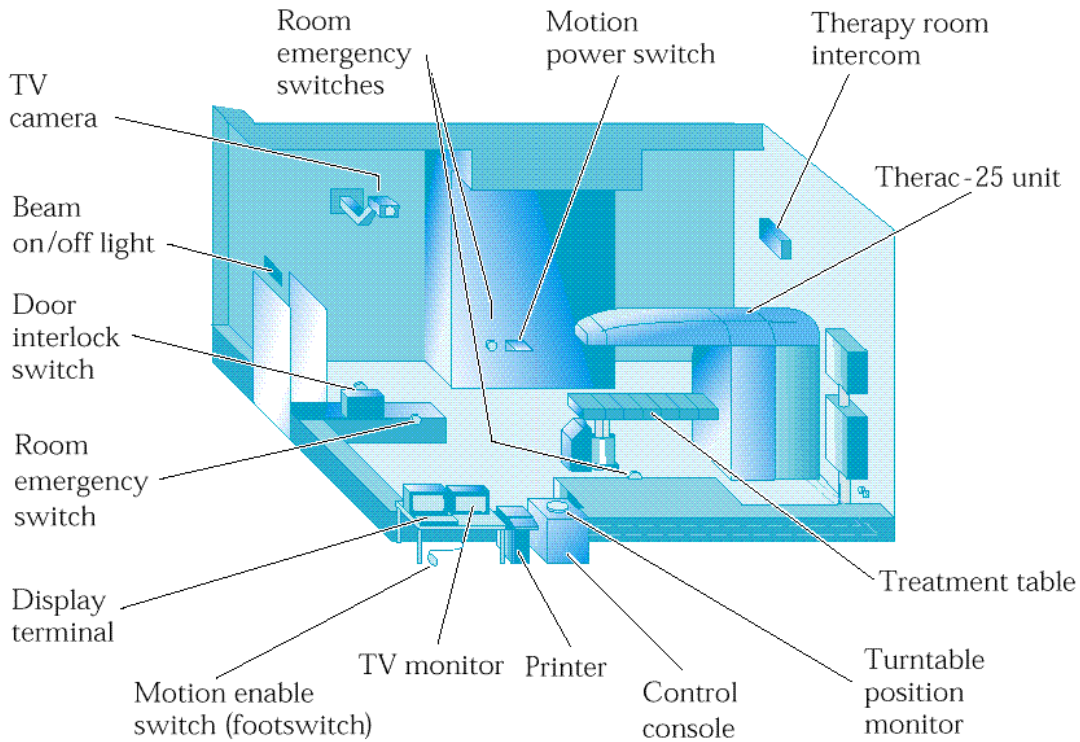
Stefan Ratschan

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

6. květen 2011



Therac-25

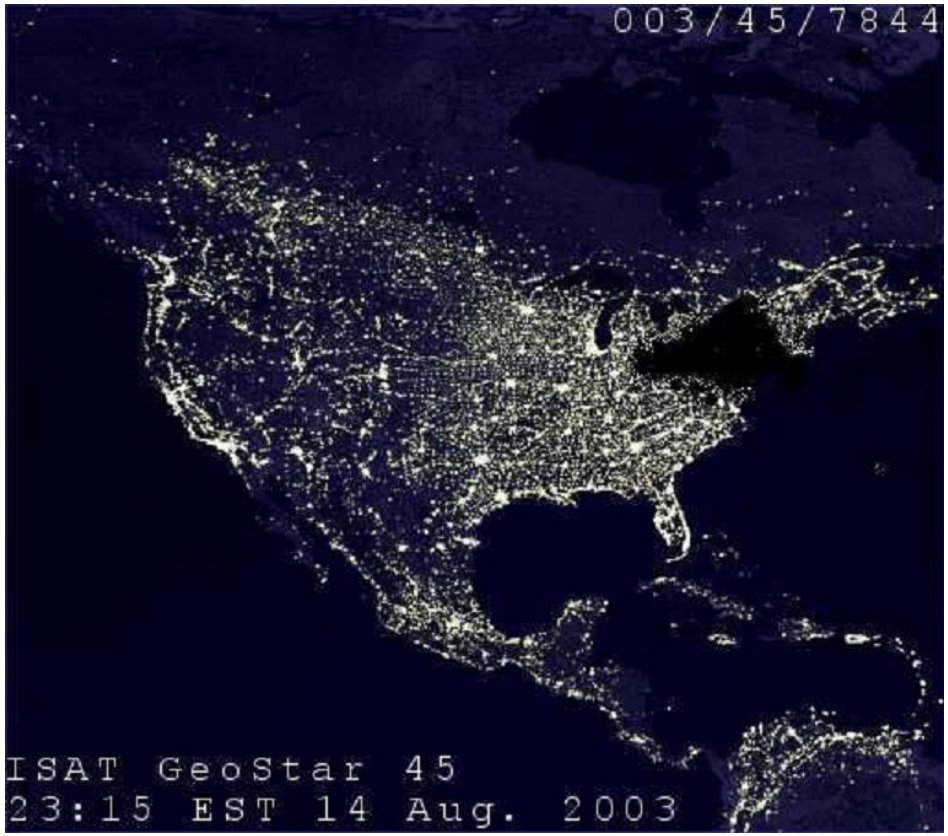


- Zařízení pro radioterapii
- Aspoň 6 havarií s nadměrnou dávkou radiace, částečně smrtelné

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

Cíl a metoda přednášky

Každá katastrofa byla výsledkem chyb v softwaru
(přestože byl důsledně testován)

Cíl přednášky: Aby informatici už nebyli viníky katastrof

Dva metody:

- Cvičení mozku: Lepší mozek, lepší software
  (sexy mozek pomáhá jen tradičním viníkům katastrof)
- Automatické ověřování správnosti softwaru

Ověřování správnosti softwaru

Krok 1: Formální specifikace

Jazyk: predikátová logika prvního řádu + logické teorie

Krok 2: Formule platí? Program splňuje specifikaci?

Problém: Nekonečnost (pro každý vstup . . .)

Řešení: Důkazy (konečný, objektivní doklad správnosti).

Důkazy

Důkaz správnosti formulí

Tím můžeme přímo ověřovat vlastnosti jednotlivých stavů

Programy dělají kroky! Formalizace: Přechodová podmínka

Důkaz omezené správnosti programů:

- Program splňuje specifikace během $k = 1, 2, \ldots$ kroků
- Každému k případu odpovídá formule $BMC(k)$ kterou musíme ověřit

Může zjistit nesprávnost každého nesprávného programu.

Může dokázat správnost jen pro programy s omezeným počtem kroku.

Důkaz neomezené správnosti programů

Používáme indukci, podmínky induktivity:

- $\models \forall r \,.\, I \Rightarrow V$
- $\models \forall r, r' \,.\, [V \wedge \Phi_P] \Rightarrow V[r \leftarrow r']$

pro V tak, že $\models \forall r \,.\, V \Rightarrow O$.

V odpovídá určitým asercím

Podmínky induktivity odpovídají ověřovacím podmínkám

- Pokud máme aserce které splňují ověřovací podmínky
  máme induktivný invariant.
- Pokud aserce navíc jsou dostatečně silně že splňuje specifikaci,
  pak víme že program je správný.

Ideální postup: Psaní asercí před psaním programem

Před psaním programu vědět co vlastně počítat.

a teď . . .

Vaše Role

Připravil jsem tento předmět úplně nově.

Navíc jsem předpoklady studentů moc neznal.

Tudíž jsem musel doladťovat hodně věci během semestru,
a to se podařilo jen částečně ...

Moje Role

. . . kvůli tomu, že týden bohužel má jen 7 dnů,
které jsem i (kromě velikonoc) opravdu používal.

Na druhé straně:

Nová přednáška, spojení s nejnovějším výzkumem

z toho plyne ...

Témata

Nabízím různá témata pro projekty, magisterské práce, doktorské práce.

Většinou v okruhu formálních metod pro složité vestavěné systémy
(software ve fyzikálním okolí)

Drobnosti zde: `http://www.cs.cas.cz/~ratschan/topics.html`

Ale nejlépe přímo ode mě, a ušité na míru.

Na konci

Hodně štěstí na zkoušce!