Formal verification of the NASA runway safety monitor

Tomáš Janoušek
veden Pavlínou Vařekovou

seminář ParaDiSe
17. března 2008

Runway safety monitor

- součást výzkumu RIPS (systém prevence střetů na ranveji)
- zabudován do IDS (integrovaný zobrazovací systém)
- cílem RSM není *zabránit* střetu/vniknutí, ale *detekovat* a *varovat*

Definice

Vniknutí na ranvej je „událost na letišti zahrnující letadlo, vozidlo, osobu nebo objekt na zemi, který způsobuje riziko kolize anebo ztrátu bezpečné vzdálenosti s letadlem, které vzlétá, plánuje odletět, přistává, anebo plánuje přistát.“

Design

- běží na zařízení v kokpitu
- aktivováno před započetím přistání/odletu

Definice

Ownship je „letadlo, na kterém systém běží.“

Targets (cíle) jsou „ostatní letadla, vozidla, objekty.“

Cyklus o třech fázích, zhruba každou půlsekundu:

- získání informací z radaru, identifikace cílů a uložení jejich souřadnic
- přiřazení stavů (taxi, odlet, přistání, . . .)
- detekce vniknutí, alarm

SMART

SMART ≡ Stochastic and model checking analyzer for reliability and timing.

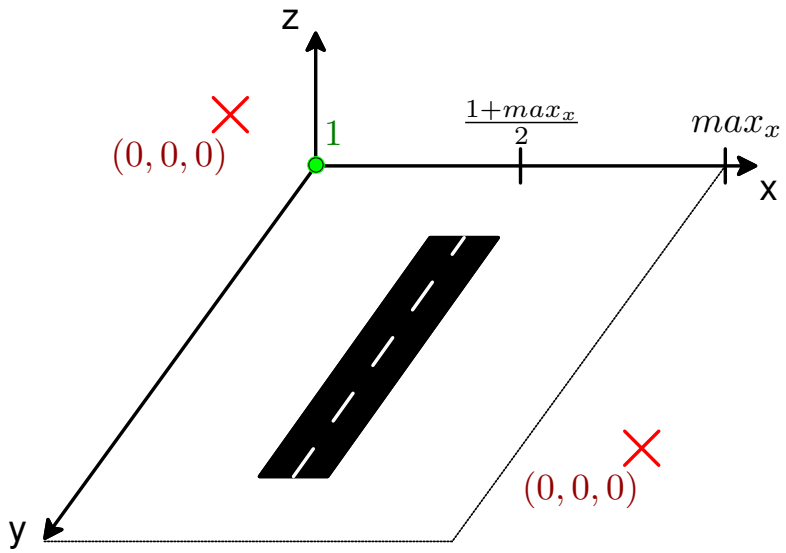
- vstupní jazyk – konečně stavové Petriho sítě s Turing-ekvivalentními rozšířeními
- algoritmy na symbolické procházení stavového prostoru
- efektivní uložení stavů pomocí MDD (multiway decision diagram)
- efektivní uložení přechodů pomocí Kroneckerových matic
- rychlé generování protipříkladů
- vyvíjen od roku 1994

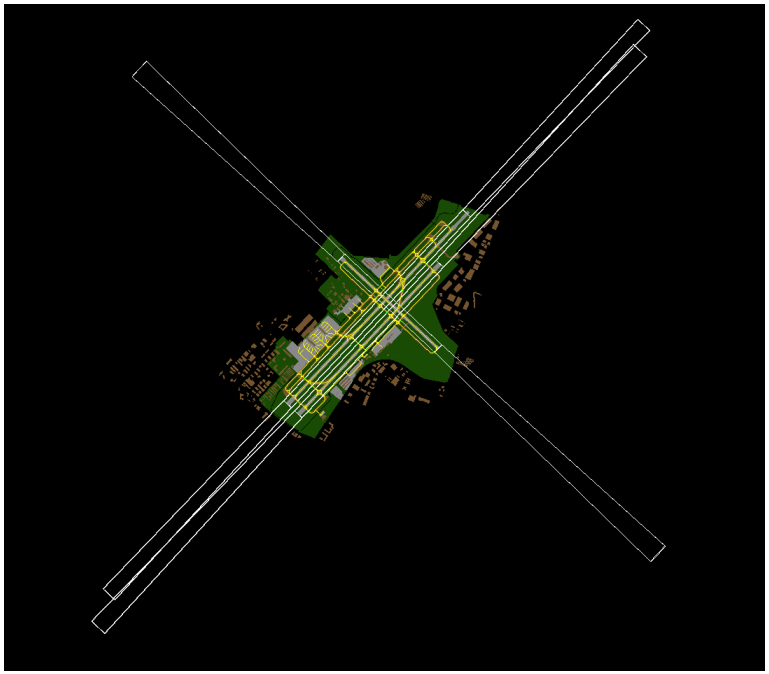
Model

- Atributy:
  - lokace: 3D vektor (x, y, z) (diskrétní)
  - rychlost a směr: 3D vektor (vx, vy, vz)
    (v Petriho síti jen kladná čísla)
  - akcelerace podél ranveje: ay (závislá na pohybu)
  - stav: enum *status*
    { vně, taxi, odlet, pojíždění, stoupání, přistání, přelet }
  - alarm: bool *alarm*
  - fáze: int *phase*
    { radar_update, set_status, detect }
- každé letadlo – podmodel
- model neuvažuje chyby při přenosu, radarové detekci, apod.

Monitorovaná zóna, souřadnice

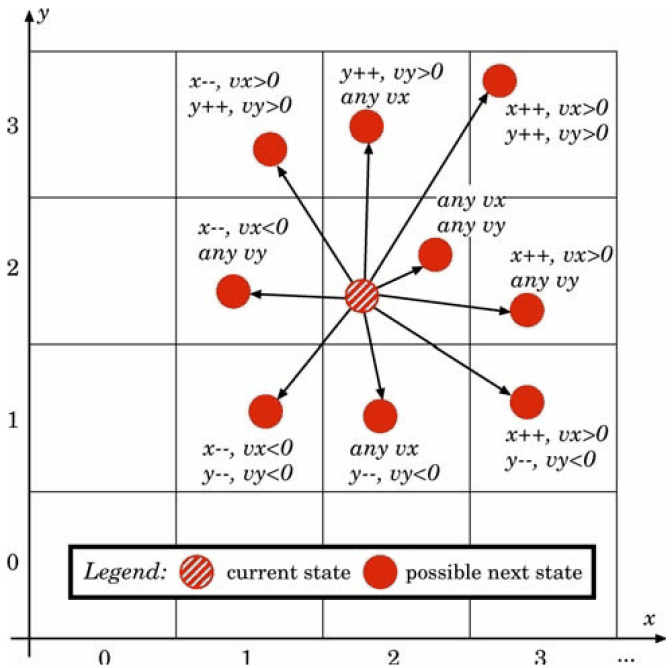
- Souřadnice
  - $(0, 0, 0)$ – nemonitorované objekty
  - $1 \ldots max_x$ – 3D síť uvnitř zóny
- Zóna
  - 67 m na každou stranu ranveje
  - 122 m na výšku
  - 2 km od každého konce ranveje

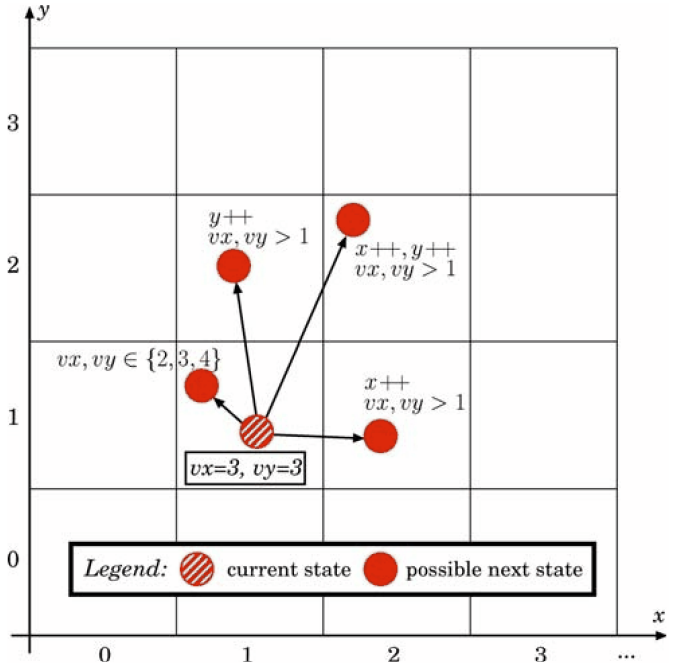


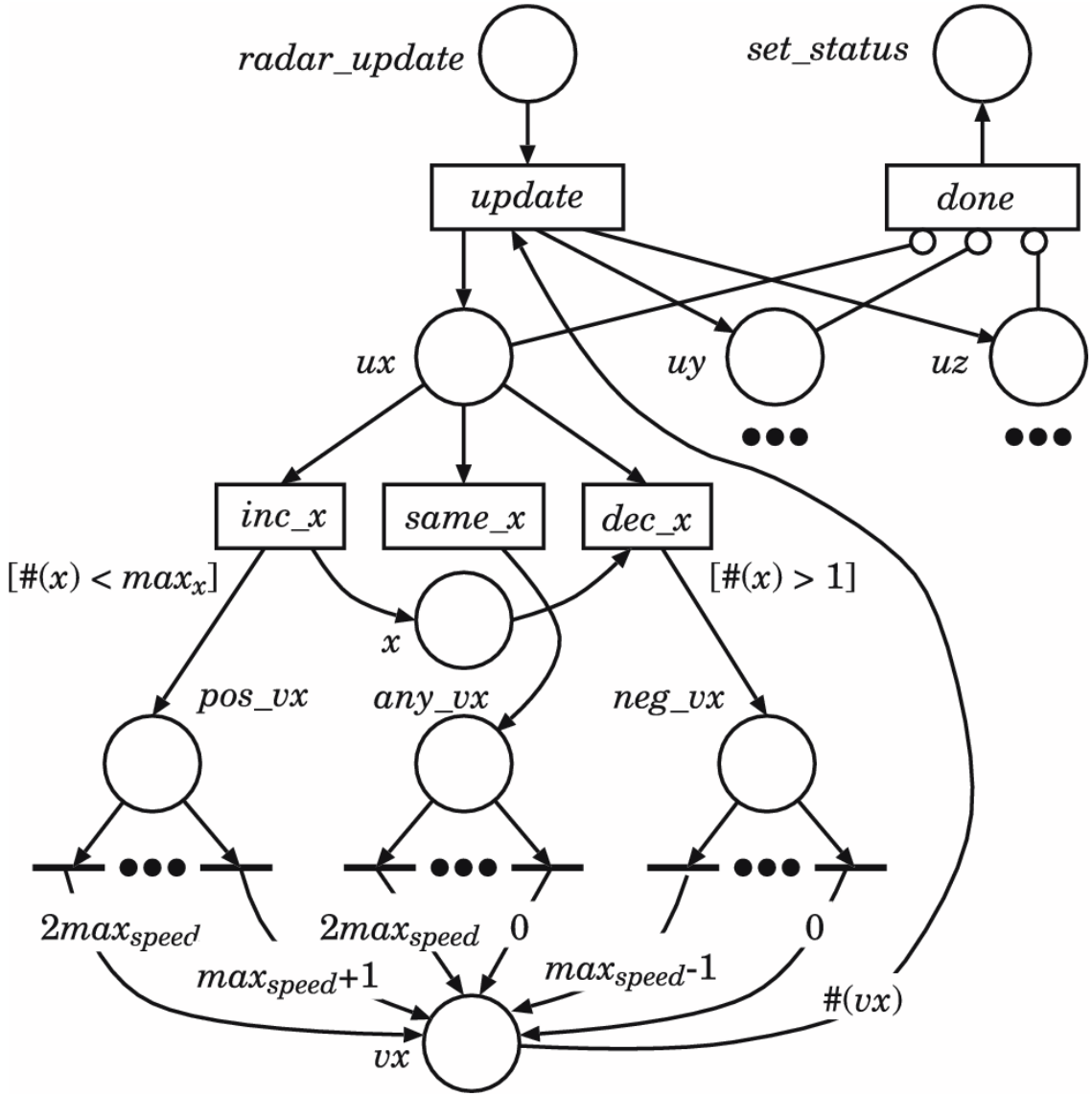


Pohyb

- volný pohyb
  - cíl může zůstat stát anebo se pohnout do jednoho z 26 sousedních políček
  - rychlost se dopočítá
- omezený pohyb
  - rychlosti se mohou měnit maximálně o 1
  - podle toho se mohou pohnout souřadnice







Obrázek: Podsíť pro aktualizaci proměnných x a vx

Stav letadel

vně mimo monitorovanou zónu

$$\equiv (x = 0) \wedge (y = 0) \wedge (z = 0)$$

taxi na zemi, pomalý anebo nerovnoběžný s ranvejí

$$\equiv (z = 1) \wedge ((|vx| \leq TS \wedge |vy| \leq TS) \vee (vx \neq 0))$$

odlet na zemi, rovnoběžný s ranvejí, akceleruje

$$\equiv (z = 1) \wedge (|vy| > TS \wedge (vx = 0) \wedge (a_y \geq 0)$$

pojíždění na zemi, rovnoběžný s ranvejí, deceleruje

$$\equiv (z = 1) \wedge (|vy| > TS \wedge (vx = 0) \wedge (a_y < 0)$$

stoupání ve vzduchu, rovnoběžný s ranvejí, ostře stoupá

$$\equiv (z > 1) \wedge (vx = 0) \wedge (vz > 0)$$

přistání ve vzduchu, rovnoběžný s ranvejí, klesá

$$\equiv (z > 1) \wedge (vx = 0) \wedge (vz \leq 0)$$

přelet ve vzduchu, není ve stavu *stoupání* ani *přistání*

$$\equiv (z > 1) \wedge (vx \neq 0)$$

Alarm

Ownship	Target *taxi*	*odlet*	*stoupání*	*přistání*	*pojíždění*	*přelet*
taxi	—	$a \wedge f$	$a \wedge f$	$a \wedge f$	$a \wedge c \wedge f$	—
odlet	$a \wedge f$	$d \vee e$	$d \vee e$	$d \vee e$	$a \vee d$	$b \wedge c$
stoupání	$a \wedge f$	$d \vee e$	$d \vee e$	$d \vee e$	$d \vee e$	$b \wedge c$
přistání	$a \wedge f$	$d \vee e$	$d \vee e$	$d \vee e$	$a \vee d$	$b \wedge c$
pojíždění	$a \wedge c \wedge f$	$a \vee d$	$a \vee d$	$a \vee d$	$d \vee e$	$b \wedge c$
přelet	—	$b \wedge c$	$b \wedge c$	$b \wedge c$	$b \wedge c$	—

$a \equiv$ zmenšuje se vzdálenost

$b \equiv$ v odletové/přistávací dráze

$c \equiv$ vzdálenost menší než bezpečná

$d \equiv$ odlet/přistání ve stejném směru, vzdálenost menší než bezpečná

$e \equiv$ odlet/přistání v opačném směru, zmenšuje se vzdálenost

$f \equiv$ taxi/stojící objekt na nebo blízko ranveje

Modelování podmínek pro alarm

- predikáty jako „zmenšuje se vzdálenost“ vyžadují geometrii a rovnice, složité v Petriho síti
- rozšíření stavu o staré proměnné
- využití toho, co víme ze stavu

Příklad (a – zmenšuje se vzdálenost)

$status_o = \text{taxi}$, $status_t = \text{odlet}$:

$z_o = z_t = 1,\ vx_o, vy_o \leq TS,\ vx_t = 0,\ |vy_t| > TS,\ vz_o = vz_t = 0$

$a \equiv (vy_t > 0 \wedge y_o > y_t) \vee (vy_y < 0 \wedge y_o < y_t)$

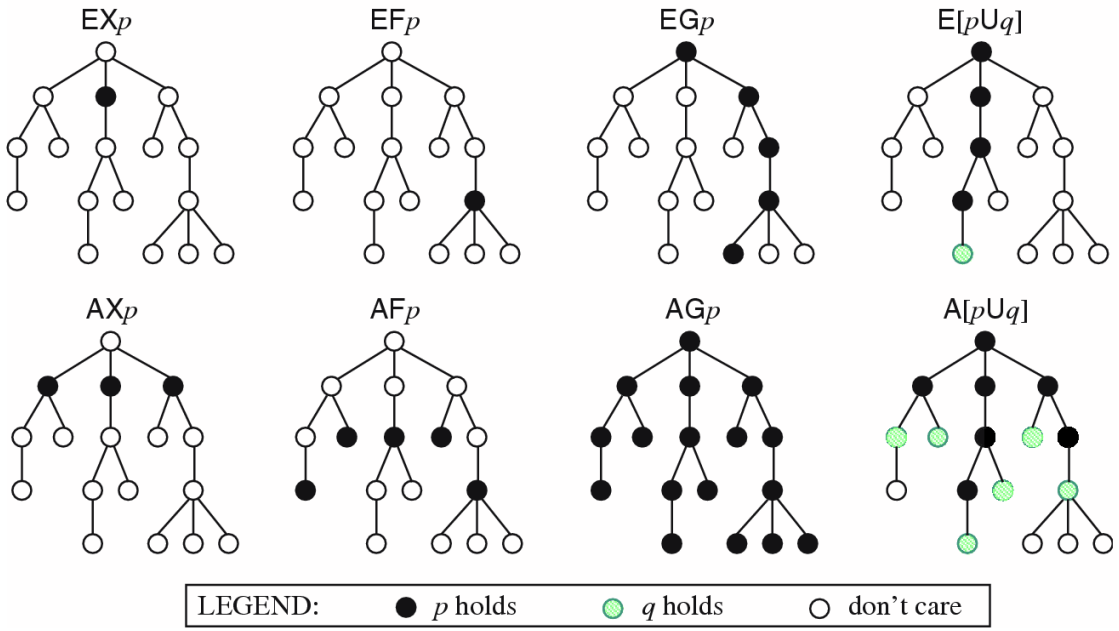
Příklad (f – taxi/stojící objekt na nebo blízko ranveje)

$f \equiv 1 < x_t < max_x$

Model checking, CTL

CTL operátory

- A na všech budoucích cestách
- E existuje cesta
- X další
- F v budoucnu, nakonec
- G globálně, obecně
- U dokud



Obrázek: Neformální semantika CTL

Safety property – pojmy

Definice

safety property – „nic špatného se nikdy nestane“

Situace, kdy se dvě letadla dostanou příliš blízko k sobě (tj. blíže než na bezpečnou vzdálenost 275 m) bez toho, aby se spustil alarm, se nazývá *zmeškaný alarm*.

Predikáty:

detect oba ve fázi detect
$\equiv phase_o = detect \wedge phase_t = detect$

sep nejsou příliš blízko
$\equiv distance(o, t) >$ min. sep.

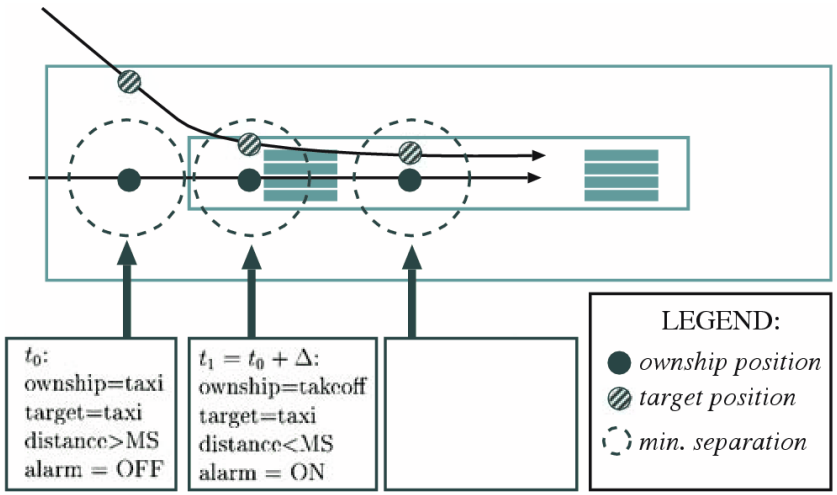
alarm je spuštěn alarm
$\equiv alarm_t = true$

track aspoň jedno odlétá n. přistává (RSM je aktivní)
$\equiv status_o \notin \{\text{taxi}, \text{přelet}\} \vee status_t \notin \{\text{taxi}, \text{přelet}\}$

Safety property 1

„Existuje stav, kde není udržena bezpečná vzdálenost a alarm není spuštěn?“

$$EF(detect \wedge track \wedge \neg sep \wedge \neg alarm)$$

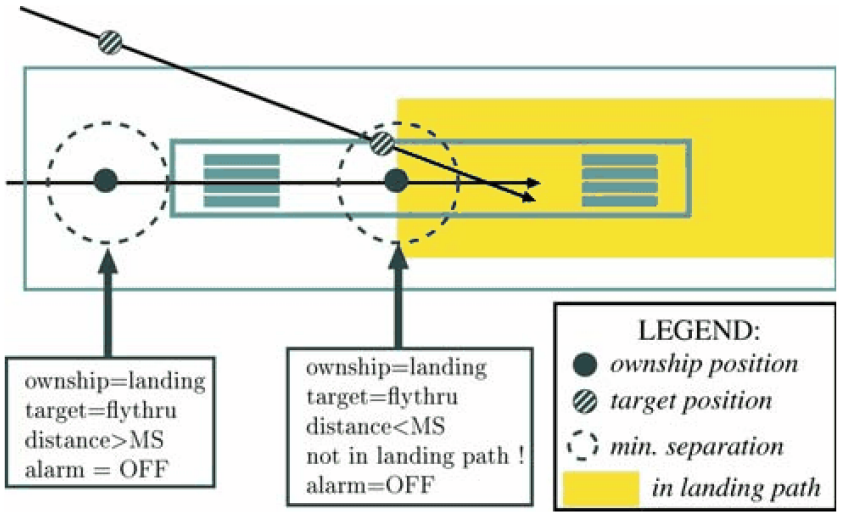


- vedle sebe na ranveji
- ale vzdálenost se nemění

Safety property 2

„Existuje stav, kde dojde ke ztrátě bezpečné vzdálenosti a alarm se nespustí?“

$$EF(detect \wedge track \wedge \neg sep \wedge E[(\neg detect)U(detect \wedge track \wedge \neg sep \wedge \neg alarm)])$$



- *ownship* přistává/stoupá, *target* přelétá
- podmínka: *v odletové/přistávací dráze* **a** vzdálenost menší než bezpečná

Závěr

- verifikace trvala 12 měsíců
- dělali na tom až 3 lidé

- chyby v případech, kdy jen jedno letadlo přistává/odlétá

- falešné alarmy
- chyby při přenosu

- generování *všech* protipříkladů

Diskuze

Děkuji za pozornost