

M U N I
F I

Výzkumná spolupráce se společností **Honeywell v oblasti návrhu a analýzy bezpečnostně kritických leteckých systémů**

T. Vojnar (AVELAB FI MUNI), J. Pavela, J. Fiedor a řada dalších



Struktura přednášky

- Oblasti spolupráce:
 - Expertní systémy pro řízení kyberfyzikálních systémů („*cyber-physical systems*“ – CPS).
 - Analýza a generování testů z modelů CPS pomocí splnitelnosti formulí prvořádových teorií („*satisfiability modulo theories*“ – SMT).
 - Vysokoúrovňové specifikace a jejich analýza pomocí logického kalkulu událostí („*event calculus*“ – EC).
 - Nástroje pro editování, vizualizaci, nástroje pro propojení ostatních nástrojů, ...
- Formy spolupráce.
- Formy zapojení studentů.

Expertní systémy pro řízení CPS

- Tvorba řídicích programů založených na expertních systémech

- Podobné logickému programování:

- *databáze faktů* + *pravidla typu „pokud něco platí/neplatí, pak ...“*,
 - okolí (senzory, komunikace, ...) může ovlivňovat databázi.

- Vycházíme z jazyka CLIPS – vyvíjen NASA.

- Umožňuje vysokoúrovňové programování.

- Forma vysvětlitelné umělé inteligence.

```
(defrule accelerate
  (cruise_control (speed ?acc))
  (not (obstacle))
  ?s <- (speedometer
        (speed ?curr&(< ?curr ?acc)))
  => (modify ?s (speed (+ ?curr 1))))
```

- Aktuální implementace nevhodné pro programy kontinuálně běžící s omezenými zdroji

- Exponenciální časová složitost v počtu podmínek v pravidlech (RETE).

- Lineární, ale závislé na počtu vložení/odebrání faktů (LEAPS) – ten je ale neomezený!

- Nově navržený ECLEAPS – již nyní podporuje významnou podmnožinu CLIPS

- Bez exponenciální složitosti, nezávislý na délce běhu.

- V Honeywellu již prošel poměrně vysoko v interním hodnocení „*technology readiness level*“ (TRL).

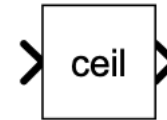
- Další výzkum: rozšiřování možností a zejména analýza ECLEAPS programů.

Analýza a generování testů pomocí SMT

- Generování testů nad Matlab/Simulink modely CPS, resp. jejich subsystémů
 - Honeywell vytvořil infrastrukturu BLADE/BALROG.
 - Poskytuje veřejné Simulink komponenty, modely nad nimi a převod do JSON a grafové reprezentace v Pythonu.
 - Honeywell rovněž vytvořil infrastrukturu SAMWISE pro použití SMT pro generování testů.

– SMT

- Splnitelnost formulí prvořádových formulí s různými teoriemi:
 - aritmetika, bitové vektory, neinterpretované funkce, ...
- Bohatá a neustále se lepšící nástrojová podpora: Microsoft Z3, CVC5, ...



$$(out_1 \geq in_1) \wedge (in_1 + 1 > out_1)$$

– Generování testů pomocí SMT

- Model se přeloží na formuli: včetně zohlednění časování apod.
 - Ptáme se, zda existují vstupy, které vedou na určité výstupy/vnitřní stavy.
 - Základ pro generování testů pro programy generované z modelů.
 - Nutný překlad různých komponent: od sčítaček po např. interpolační tabulky, řetězcové operace, ...
 - Uplatnění výzkumu FIT VUT v oblasti SMT pro řetězcové logiky (L. Holík & comp.) a FI MU v oblasti aritmetiky.
-
- Další výzkum: různé způsoby překladu a vyhodnocení, [goniometrické funkce](#), ...

Analýza vysokoúrovňových specifikací CPS

– Vysokoúrovňové specifikace CPS

- Často přirozený jazyk, případně nějakým způsobem šablonovaný (EARS, CLEAR, ...).
- Popisuje reaktivní hybridní systémy.
- Nalézt chyby na této úrovni je z hlediska nákladů nejlevnější.

While the **aircraft is on-ground**, **when** the **requested door position becomes open**, the door control system **shall** **change the state of the cargo door from closed to open** **within 10 secs**.

– Event Calculus

- Logický formalismus.
- Body v čase, události, „*fluents*“ – v čase proměnná fakta s připojenou kvantitativní informací, (spojité) trajektorie.
- Nástroje pro vyhodnocení založené na přístupech „*answer set programming*“ a „*constraint solving*“.

```
happens(pilot_requests_door_to_open, T) :- % Map change of state trigger to happens
    -holdsAt(door_requested_position(open), T1),
    holdsAt(door_requested_position(open), T2), T2 #=< T1+10, T1 #< T, T #=< T2.
```

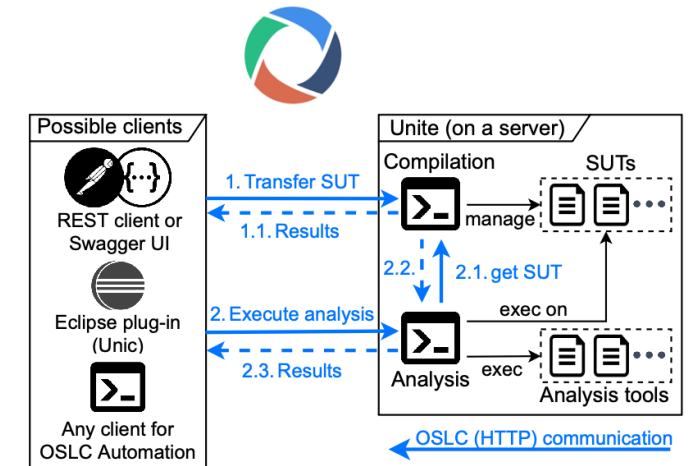
– Analýza specifikací CPS pomocí EC

- Malá sémantická mezera – překlad lze v budoucnu případně svěřit LLM, ale lidé mají šanci ho ověřit.
- Následně algoritmický „*machine reasoning*“.

– Další výzkum: zlepšování škálování přístupu, automatizace překladu.

Editace, vizualizace, interoperabilita, ...

- Interoperabilita pomocí OSLC („Open Services for Lifecycle Collaboration“)
 - Unite – podpora pro snadné zpřístupnění nástrojů pro analýzu s textovým rozhraním jako webových služeb.
 - Používáno Honeywell CZ, Indie, Čína.
 - UniC – návazná podpora pro zapojení analyzátorů s textovým rozhraním do IDE s GUI.



- Editování a vizualizace modelů mimo Matlab/Simulink (včetně výsledků analýz)
- Podpora pro zavádění doménově specifických jazyků do vývojových prostředí
- Podpora projektového řízení

Formy spolupráce

- Převážně založeno na studentských pracích
 - Od 2. ročníku bakaláře přes magisterské po doktorské studium.
 - Blíže další slajd.
- Projekty
 - Před časem TAČR a evropsko-národní projekty H2020 JU ECSEL.
 - Několik GAČR projektů – bez přímého zapojení Honeywell.
 - Nyní (snad) získán evropsko-národní projekt HE JU Chips.
 - Na FIT VUT nyní smluvní výzkum, na FI MU plánován.
- Zapojení mezi průmyslové partnery fakult s příslušným příspěvkem
- Společné publikace
 - Od testování (ISSTA – v dřívější době), přes softwarové inženýrství (ESEC/FSE), logické programování (ICLP), po programovací jazyky (aktuálně zasláno).

Formy zapojení studentů

- **Bakalářské a diplomové práce**
 - Aktuálně na FI MU: 4x BP, 7x DP.
 - Aktuálně na FIT VUT: 5x BP.
- **Studenti mimo bakalářské a diplomové práce**
 - FI MU – *soutěž o spolupráci s laboratorii a průmyslovým partnerem* – začíná od konce 1. ročníku Bc:
 - Několik soutěžních úloh na doma, následně pohovor, student i lab+firma si vybírají,
 - firma nabízí určitou odměnu (nízké tis. Kč měsíčně na rok), student cca 1 den práce týdně.
 - Aktuálně 3 studenti.
 - FI MU – laboratorní projektové předměty.
 - FIT VUT: *předmět tzv. projektové praxe* (bakalářský i magisterský):
 - Studenti se hlásí na vypsaná témata, vedoucí si vybírá,
 - semestrální prezentace + krátká technická zpráva, za kredity.
 - Aktuálně 5 studentů.
 - Na FI MU i FIT VUT samozřejmě možnost zapojení do grantových projektů/smluvního výzkumu.
- **Doktorští studenti**
 - V rámci společného výzkumu se školiteli: klíčoví ve všech zmíněných oblastech výzkumu.