

A decorative horizontal bar with a complex, multi-colored pattern of overlapping lines and shapes in shades of green, purple, yellow, and blue.

System weryfikacyjny VERICS: stan obecny i perspektywy rozwoju

Wojciech Penczek

współautorzy

Piotr Dembiński, Agata Janowska, Paweł Janowski, Magdalena Kacprzak,
Agata Półrola, Maciej Szreter, Bożena Woźna, Andrzej Zbrzezny

IPI PAN, 2004



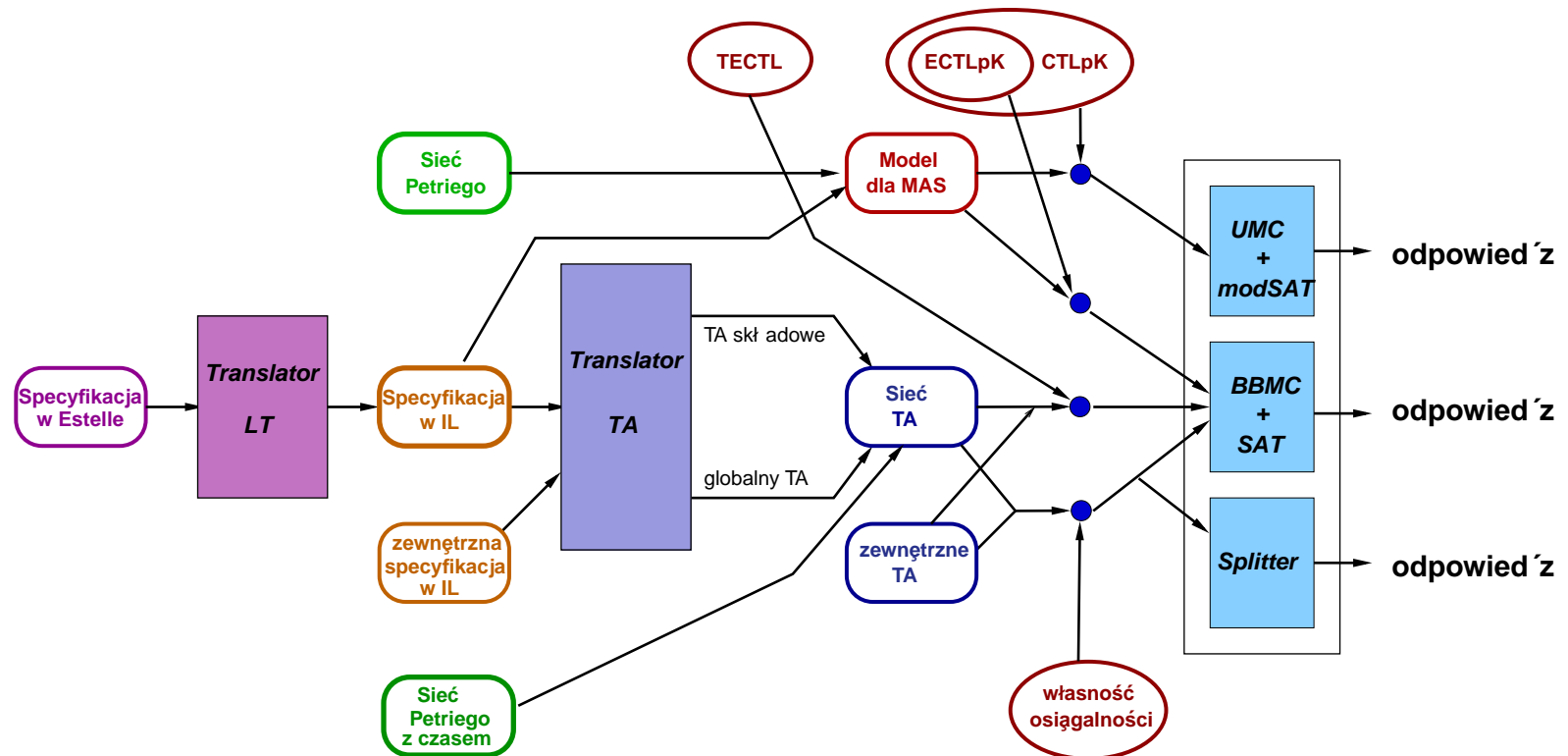
Katastrofa bezzałogowej rakiety "Ariane 5" 4 czerwca 1996 r.

- ✦ Weryfikacja programów i systemów,
- ✦ Architektura systemu Verics,
- ✦ Sieć automatów czasowych jako model systemów czasowych,
- ✦ Estelle - język specyfikacji wysokiego poziomu,
- ✦ Język bazowy,
- ✦ Problem osiągalności,
- ✦ Metoda OWM - szukanie kontrprzykładów,
- ✦ Metoda "splitting" - dowodzenie poprawności,
- ✦ Perspektywy rozwoju,
- ✦ Film - demo systemu Verics.

Ile kosztuje zaniechanie weryfikacji

- ✦ Błąd w module dzielenia procesora Pentium II - 475 mln dolarów,
- ✦ Błąd w systemie obsługi bagażu w Denver, który opóźnił otwarcie lotniska o 9 miesięcy - 1.1 mln dolarów DZIENNIE,
- ✦ 24-godzinna awaria systemu sprzedaży biletów spowoduje bankructwo każdego dużych linii lotniczych!
- ✦ Błąd w systemie obsługi aparatu do radioterapii THERAC-25 spowodował śmierć 6 pacjentów w latach 1985-87.
- ✦ Awaria sondy marsjańskiej Pathfinder i samolotów Airbus.

Architektura systemu Verics



Wejście: Estelle, język bazowy, sieć automatów czasowych, sieć Petriego, sieć Petriego z czasem

Sieć automatów czasowych - formalny model weryfikowanego systemu.

Weryfikacja: Ograniczona Weryfikacja Modelowa, Nieograniczona Weryfikacja Modelowa i "splitting".

Estelle - język specyfikacji wysokiego poziomu

- ✦ Język specyfikacji o standardzie ISO, zaprojektowany do opisu protokołów komunikacyjnych i systemów rozproszonych.
- ✦ Wykorzystuje model rozszerzonych maszyn skończonego-liczby stanów.
- ✦ Opisuje hierarchiczną strukturę niedeterministycznych komponentów, asynchroniczną wymianę informacji przekazywanych komunikatów przez dwukierunkowe kanały, i/lub poprzez współdzielenie pamięci.
- ✦ Umożliwia dynamiczną inicjalizację procesów.

Wejście dla systemu Verics:

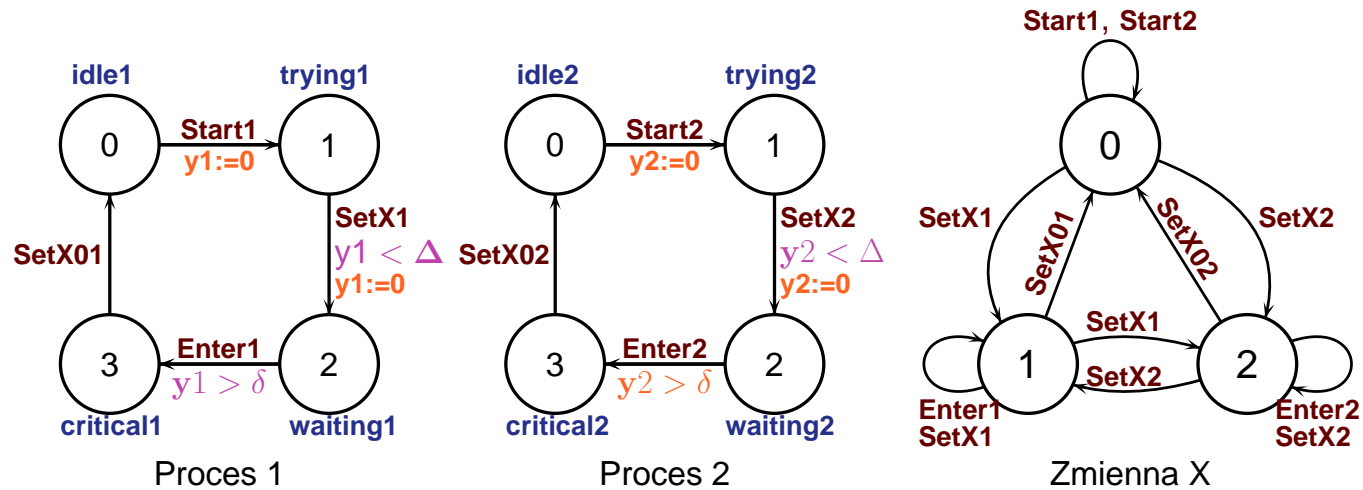
- ✦ podzbiór Estelle rozszerzony o specjalne komentarze rozpoznawane przez translator LT:
 - ✦ opisujące ograniczony rozmiar buforów
 - ✦ definiujące zmienne zdaniowe

Język bazowy (IL)

- ✦ Prawie bezpośrednia translacja z Estelle i podobnych języków wysokiego poziomu.
- ✦ Jednoznaczna semantyka IL ułatwia translację z IL do TA.
- ✦ Model komunikacji Estelle rozszerzony o globalne zmienne dzielone.
- ✦ Zachowuje model współbieżności z Estelle.

Sieć automatów czasowych jako model dla

MAS i systemów czasowych



Protokół wzajemnego wykluczenia (2 procesy)

Sieć automatów czasowych:

- lokacje
- relacja przejścia
- zmiennie zdaniowe
- akcje - umożliwiają synchronizację
- zegary, warunki umożliwienia
- niezmienniki, zerowanie zegarów

Problem:

Dana jest sieć automatów czasowych S i własność. Sprawdzić czy jest możliwe osiągnięcie stanu spełniającego rozważaną własność

Rozwiązanie:

1. Budowa modelu M_S dla systemu S .
2. Wyrażenie własności za pomocą formuły zdaniowej φ
3. Sprawdzenie automatycznie czy istnieje stan osiągalny ze stanu początkowego modelu M_S , który spełnia φ

Reprezentacja przestrzeni stanów



Symboliczna:

OWM



Bezpośrednia:

Splitting

OWM - poszukiwanie kontrprzykładów

✦ **OWM**: problem osiągalności zostaje sprowadzony do problemu badania spełnialności formuł y zdaniowej kodującej stany i relacje przejścia modelu.

✦ tylko fragment modelu jest wykorzystywany

✦ kodowane stany: regiony szczegól owe

✦ kodowana relacja przejścia:

✦ **projekcja czasowa**: przechodnie domknięcie następnika czasowego w grafie e regionów,

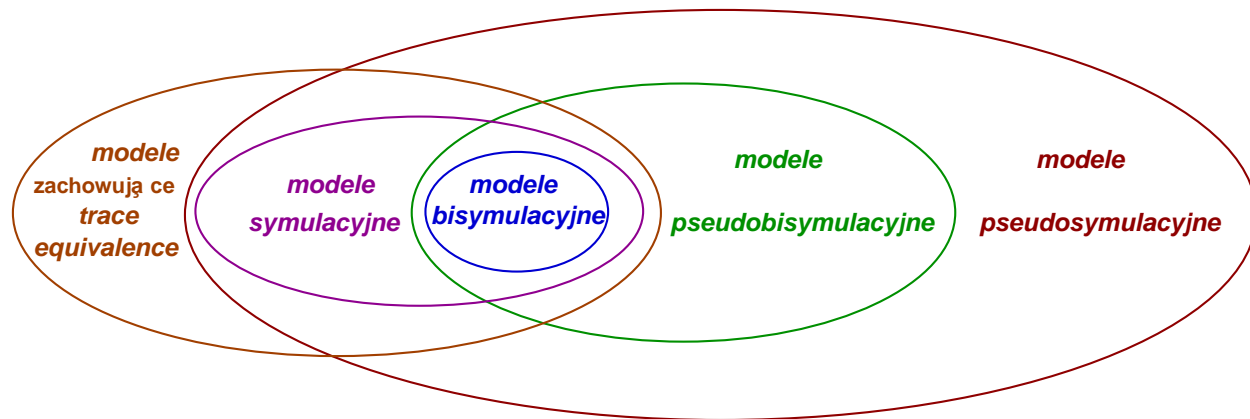
✦ **następnik akcyjny** w grafie e regionów.

✦ symboliczna ścieżka:



Splitting - dowodzenie poprawności

- metoda wyliczeniowa - generuje pewien model abstrakcyjny
- nowa relacja równoważności - **pseudo-(bi)symulacja**: mniej różni się niż (bi)symulacja, zachowuje właściwość osiągalności



- modele generowane przez algorytmy podziału
- stany to regiony (lokacja + strefa czasowa)
- weryfikacja "w locie" (on-the-fly)

Wyniki eksperymentalne - protokół alternującego bitu



Każda wiadomość jest reprezentowana przez parę (*dane*, *bit*), natomiast potwierdzenie jest reprezentowane przez *bit*.

Testowana własność C:

Jeżeli (nadawca wysłał potwierdzenie i bitS = 0), to bitR = 0

Formuła a (reprezentuje negację własności C)

$$\varphi_1 = \neg[(S_Sender_ack \wedge S_Sender_bit0) \Rightarrow R_Rec_bit0]$$

✗ (własność jest fałszywa)

Obecnie realizowane rozszerzenia systemu:

- ✦ **Interfejsy graficzne** wejście (projekt studencki), wizualizacja kontrprzykładów,
- ✦ **Komercyjny interfejs** do udostępniania systemu (praca magisterska),
- ✦ **Nowa metoda weryfikacji** nieograniczona weryfikacja modelowa dla systemów czasowych (badania własne),
- ✦ **Translator** z fragmentu języka **JAVA** do IL lub automatów czasowych (praca doktorska),

- ✦ Translator z języka **PROMELA** i **Timed-UML** do IL lub automatów czasowych (prace doktorskie),
- ✦ Opracowanie i implementacja współ bieżnej wersji modułów weryfikacyjnych (praca doktorska),
- ✦ Rozszerzenie metod weryfikacji do **automatów hybrydowych** (prace własne),
- ✦ **DOCELOWO**: profesjonalna weryfikacja komercyjnych programów i protokołów.



Demo systemu VERICS

Dziękuję za uwagę i zapraszam do testów naszego systemu dostępnego na stronie WWW:

<http://www.ipipan.waw.pl/~penczek/verics>