Zastosowanie metod formalnych

Karol Kozlowski[1], Katarzyna Mielęcka [2], Piotr Głowacki [3], Jan Gawroński [4]
Politechnika Warszawska,
Wydzial Elektryczny

Politechnika Warszawska

Metody formalne

Metody formalne to matematyczne techniki wspomagające projektowanie i analizę systemów informatycznych. Główną zaletą metod formalnych są **matematyczne gwarancje poprawności**, szczególnie istotne w systemach krytycznych (medycznych, transportowych). Pozwalają one identyfikować złożone błędy, takie jak zakleszczenia czy warunki wyścigu, które często wymykają się tradycyjnym metodom testowania.

Kluczowe zalety metod formalnych

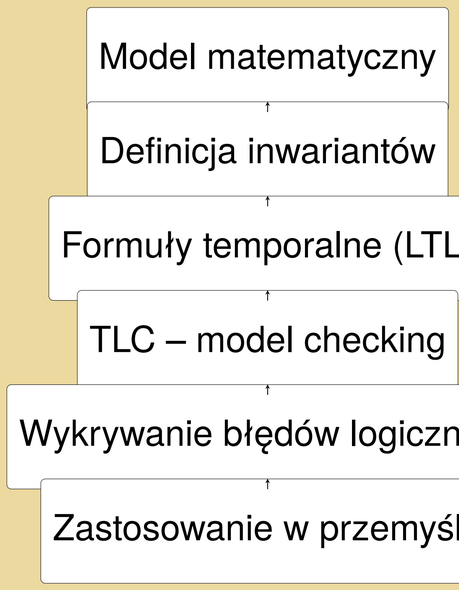
Some introduction of the list.

- Formalne gwarancje poprawności - zapewnienie matematycznie udowodnionej poprawności systemów, szczególnie w przypadku wymagań bezpieczeństwa.
- Precyzyjna specyfikacja wymagań - eliminacja niejednoznaczności dzięki matematycznym modelom i notacjom.
- Wykrywanie złożonych błędów - identyfikacja problemów takich jak zakleszczenia (deadlocks) czy warunki wyścigu (race conditions), które trudno wykryć tradycyjnymi metodami testowania.

System PVS w pigułce

pointer_env [P : TYPE, T : TYPE] : THEORY
BEGIN
pointer : TYPE = P + {nil}
env : TYPE = [pointer → (T + {undefined})]
END pointer_env

Zastosowanie metod formalnych – TLA+



Metody formalne pozwalają na matematyczne modelowanie i automatyczną weryfikację systemów. TLA+ wykorzystuje trzy główne podejścia:

- **Modelowanie systemu** – zmienne, akcje, przestrzeń stanów,
- **Inwarianty** – warunki poprawności w każdym stanie,
- **Własności temporalne** – analiza zachowania w czasie.

Weryfikacja odbywa się za pomocą narzędzia TLC i model checkingu. TLA+ stosowany jest w Amazonie, Microsoftcie i Google.

Metody formalne w kolejnictwie

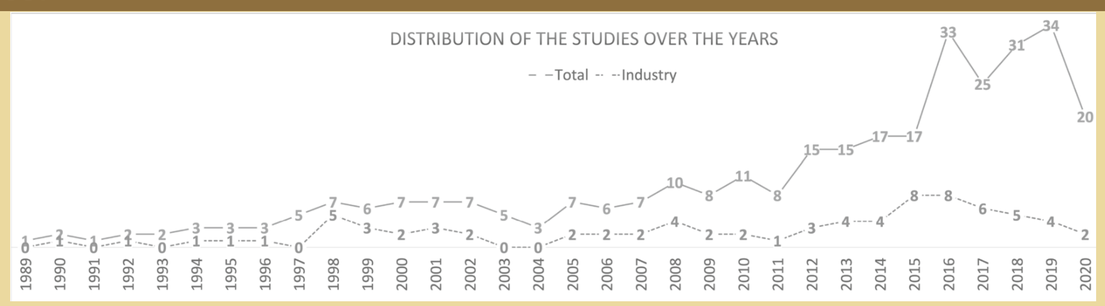
Użycie metod formalnych jest konieczne w branży tak nastawionej na bezpieczeństwo jak kolejnictwo. Zapewnia ono wykrywanie błędów na wczesnym etapie projektowania, minimalizację ludzkich pomyłek i pozwala na obniżenie sumarycznych kosztów. Ze względu na istotność metod formalnych w zapewnieniu prawidłowego działania systemu, ich użycie jest konieczne do spełnienia niektórych norm, takich jak **CENELEC EN 50128 (Safety Integrity Level 3/4)**.
Podstawowe metody używane w kolejnictwie to:

- Coq, Isabelle (dowodzenie twierdzeń)
- Metoda B (udoskonalanie oparte o stan)
- Sieci Petriego
- NuSMV, UPPAAL (sprawdzanie modeli)

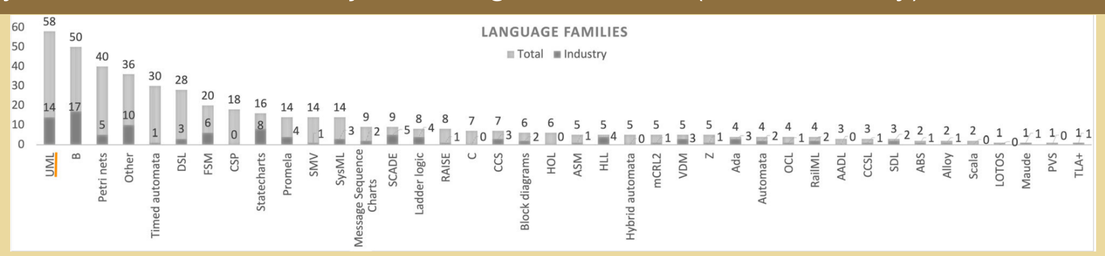
Sztandarowe przykłady użycia metod formalnych (metody B) w kolejnictwie:

- Metro paryskie (linia 14)
- Metro kopenhaskie

Ilość publikowanych badań na temat metod formalnych w kolejnictwie - wyraźny wzrost



Języki modelowania w kolejnictwie - głównie UML (semi-formalny) i B



Metoda B

- Specyfikacja (abstrakcyjne maszyny stanowe, wykorzystanie teorii zbiorów)
- Stopniowa udoskonalanie
- Generacja kodu z weryfikacją

Metody formalne w systemach wbudowanych

Metody formalne, takie jak RT-EFSM, Sieci Petriego z Czasem i Kolorami (TCPN) oraz metoda B, odgrywają kluczową rolę w projektowaniu, testowaniu i weryfikacji systemów wbudowanych działających w środowiskach krytycznych. Umożliwiają one precyzyjne modelowanie, analizę zachowań czasowych i współbieżnych oraz walidację zgodności z normami bezpieczeństwa, znacząco zwiększając niezawodność systemów.

Bibliografia

- Leslie Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley, 2002.
- Chris Newcombe et al., *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, 2015.
- Igor Konnov, Jure Kukovec, Thanh-Hai Tran, *TLA+ Model Checking Made Symbolic*, CAV 2019.
- Hillel Wayne, *Practical TLA+: Planning Driven Development*, Lospinato Books, 2018.
- S. Poreda, *Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych*, Uniwersytet Warszawski, 2023.
- Sławomir Lasota, *Weryfikacja protokołu Needhama-Schroedera przy użyciu narzędzi SPIN i UPPAAL*, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski, https://www.mimuw.edu.pl/~sl/teaching/03_04/WPKWK/PREZENTACJE-SPIN_UPPAAL/NS/.