УДК 514.18;711.11

Мамедов Т.А., Меннанова С.Ш.,
Київський національний університет
ім. Тараса Шевченка

ФОРМАЛІЗАЦІЯ СИСТЕМИ МІСЬКОГО ТРАНСПОРТУ В-МЕТОДОМ НА ПРИКЛАДІ ПІДСИСТЕМИ “АВТОБУС”

Наводиться моделювання руху підсистеми “Автобус”, що включається в систему міського транспорту, формальним методом розробки програмного забезпечення B.

Ключові слова: абстрактна машина, специфікація, інваріант, імплементація, деталізація, контекст.

Вступ. Метод B – один із формальних методів розробки програмного забезпечення, завдяки яким запропоновані невірні проекти систем можуть бути переглянуті до того як буде зроблено основні витрати на власне саму реалізацію. Альтернативний підхід полягає в тому, аби, виконуючи кроки по уточненню специфікації, вірність яких можна довести, перетворити специфікацію на реалізацію, яка буде вірною через побудову. Отже, метод дозволяє істотно скоротити час тестування та підвищити надійність або показник безпеки, для захисту від помилок у процесі розробки.

B-Method – це набір математичних технологій для специфікації, проектування та реалізації компонент програмного забезпечення. Системи моделюються як сукупності незалежних Абстрактних Машин, для яких на всіх стадіях розробки застосовується об'єктно-орієнтований підхід.

В B-методі специфікації і коди написані в AMN (Abstract Machine Notation). Стандартна нотація використовується на всіх рівнях опису, від специфікації до реалізації. AMN — мова формальної специфікації, що базується на станах. Вона вийшла з тої ж школи що і VDM та Z. Абстрактна машина включає стан разом з операціями на тому стані. В специфікаціях та конструюванні Абстрактної Машини стани моделюються з використанням таких понять як множина, відношення, функції, послідовності і подібних. Оператори моделюються з використанням перед- та післяумов. В реалізації абстрактної машини стан знову моделюється з використанням теоретико-множинної моделі, але цього разу ми вже маємо реалізацію цієї моделі. Ця операція описується з використанням псевдокоду який є підмножиною AMN.

Також інший комерційний комплект інструментальних засобів розробки - Atelier-B був розроблений французькою групою дослідників. Недавно створили ще один метод, названий Event-B. Event-B розглядається як вдосконалення B

(відомого також як класичний B). Він має простіший синтаксис, що полегшує його вивчення та використання. Інструменти що його підтримують називаються платформою Rodin.

Формальна специфікація в B. Основними перевагами формальної специфікації в B є застосування процесу деталізації (уточнення) для представлення системи на різних рівнях абстракції і використання математичних доказів для перевірки логічності (послідовності) між рівнями деталізації.

В основі B лежить опис властивостей - інваріантів (invariants) системи і перевірка шляхом математичного доказу того, що виконання подій (в будь-яких допустимих станах) не порушить зазначені властивості. Таким чином, в процесі деталізації (refinement) створюється повна і несуперечлива специфікація системи.

Формальна специфікація в B являє собою сукупність контексту (context) і машини (machine) на кожному рівні деталізації. Контекст - необов'язковий, він містить константи, множини, а також аксіоми і теореми, які визначають типи і обмеження заданих констант і множин. Машина є обов'язковим елементом специфікації і, в загальному випадку, включає в себе список змінних, подій, які виконуються у відповідності з певними умовами, і інваріантів. Інваріанти визначають властивості змінних системи, які завжди виконуються.

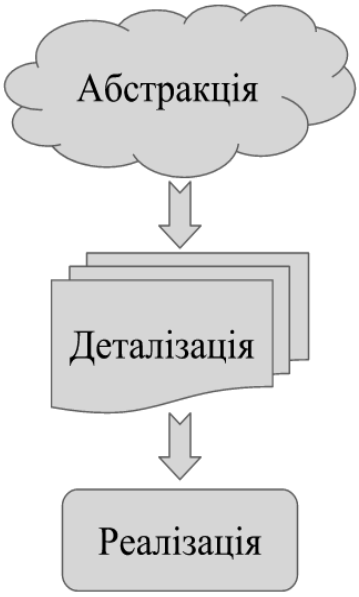

Рис. 1. Від абстракції до реалізації

Процес деталізації передбачає поступовий перехід від абстрактного опису до більш точного, з поступовим додаванням деталей системи.

При цьому зазначені на ранніх стадіях властивості системи зберігаються на всіх етапах деталізації. Сутність формалізації полягає в тому, що подіям

дається формальне математичне визначення і при додаванні властивостей системи здійснюється доказ їх відповідності інваріанта. Таким чином, гарантується коректна поведінка системи на всіх етапах її розробки.

Такий підхід знайшов широке застосування при розробці програмного забезпечення. У цьому випадку в B задається специфікація, а потім здійснюється одна або декілька проміжних деталізацій. Остання деталізація називається реалізацією. Ця реалізація може викликати операції інших машин (імпорт). Після повної перевірки розробленої реалізації B-методу можлива генерація коду програми на мові високого рівня.

Абстрактна машина. Для завдання специфікацій системи на програмованій логіці застосовується методика, першим кроком якої є створення абстрактної машини, яка описує поведінку системи в її оточенні.

Доведення. На наступному кроці деталізації задаються можливі стани системи і переходи між ними, а також проводиться аналіз деяких вхідних даних. Розробник доповнює специфікацію для того, щоб прояснити цілі розробки і зробити абстрактну машину більш конкретною. Це робиться шляхом додавання деталей про структури даних і алгоритми, що визначають, як цілі розробки мають бути досягнутими.

Реалізація. Після кількох послідовних кроків доведення, кожен з яких робить специфікацію більш конкретною, вона стає детерміністичною. Така її версія називається реалізацією. Кількість рівнів деталізації залежить від складності системи і вирішуваних завдань. На кожному наступному кроці додаються властивості системи, які уточнюють її поведінку в описаних раніше станах, а також нові події, необхідні для реалізації алгоритму управління.

Розробка ПС. В даній роботі формалізовано рух автобуса. Автобус повинен рухатись з зачиненими дверима, на зупинці автобус стоїть з відчиненими дверима. Також може виникнути надзвичайна ситуація, в цьому випадку відбувається екстрена зупинка та відкриваються всі двері.

Враховуючи дану інформацію було виділено наступні стани системи:

Стани автобуса:

- рухається;
- стоїть.

Стани дверей:

- зачинені;
- відкриті.

Положення автобуса відносно зупинки:

- на зупинці;
- між зупинками.

Надзвичайна ситуація:

- відсутня;
- виникла.

Вище описані стани системи “Автобус” в нотації B-методу задаються наступним чином:

```
BUS_STATE = {MOVES, STANDS};
DOORS_STATE = {OPENED, CLOSED};
BUS_POSITION = {AT_STOP, ON_ROAD};
EMERGENCY_STATE = {OCCURS, NONE};
```

Для забезпечення безпечної роботи в системі необхідно, щоб виконувалися наступні умови:

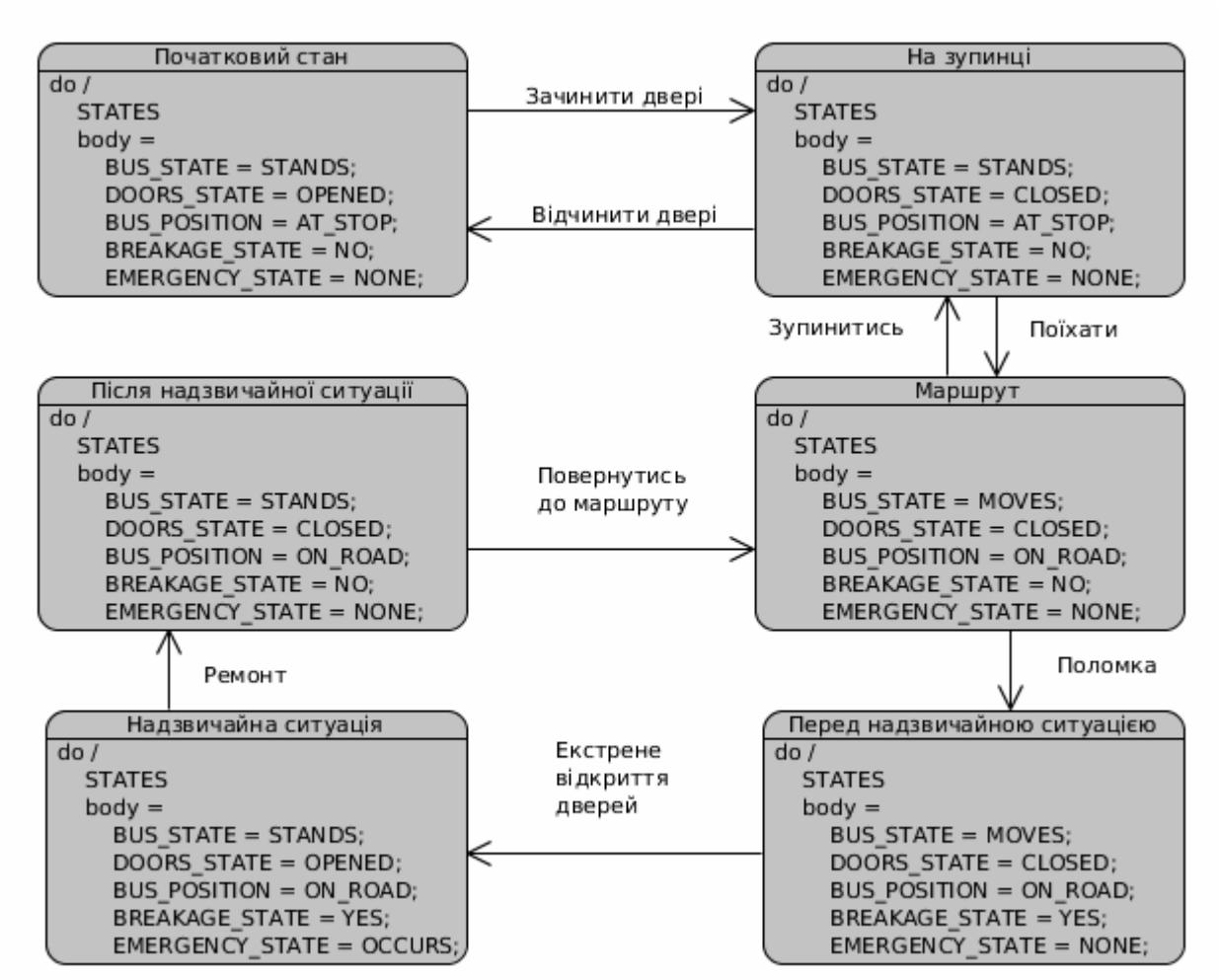

Рис. 2. Діаграма станів.

1. Двері повинні бути зачиненими під час руху автобусу.
2. Під час екстреної ситуації автобус зупиняється та двері відчиняються.
3. Прибувши на станцію автобус зупиняється.

```
((BUS_STATE = MOVES & BUS_POSITION = ON_ROAD) =>
(DOORS_STATE = CLOSED)) &
((EMERGENCY_STATE = OCCURS) => (BUS_STATE = STANDS &
```

```
DOORS_STATE = OPENED)) &
((BUS_POSITION = AT_STOP) => (BUS_STATE = STANDS))
```

Враховуючи вище описані вимоги для системи, її імплементацію було формально описано та верифіковано за допомогою системи Atelier-B. Внаслідок чого проводилися тести (наявність тупикових станів).

Нижче наведена діаграма станів системи “Автобус”, в якій описується її робота в звичайному та в надзвичайному режимах.

Висновки. Використання методів формальної специфікації та верифікації для створення системи на програмованій логіці веде до суттєвого зменшення часу тестування та верифікації кінцевого продукту.

Розроблена система ілюструє перевагу використання специфікацій в B, яке полягає в математичному доказі виконання тих чи інших властивостей і збереження їх на наступних кроках деталізації. Таким чином, результатом такого підходу є математично доведена реалізація системи, яка не потребує тестування.

Література

1. Abrial J.R. The B Book: Assigning Programs to Meanings. / J.R. Abrial. - Cambridge University Press, 1996.

2. Bert D. Adaptable Translator of B Specifications to Embedded C Programs/ D Bert, S. Boulmé, M.L. Potet, A. Requet, L. Voisin1 // FME 2003: Formal Methods. – 2003. – Vol. 2805. – P. 94-113.

3. Yang L. Automatic Translation from Combined B and CSP specification to Java Programs. / L. Yang, M.R. Poppleton // 7th International B Conference. - 17-19 January 2007. - Besancon, France.

4. Abrial J.R. / Event Driven Electronic Circuit Construction / J.R. Abrial. - 2001.

5. Seceleanu T. Systematic Design of Synchronous Digital Circuits / T. Seceleanu // TUCS Dissertations, Turku Centre of Computer Science. – May 2001. – No 32.

6. Boulanger J.L. Formalization of digital circuits using the B method /J.L. Boulanger, A. Aljer, G. Mariano // Eighth International Conference on Computers

7. Sørensen Ib Holm. Using B to specify, verify and design hardware circuits / Ib Holm Sørensen //ZUM '98: The Z Formal Specification Notation. Lecture Notes in Computer Science. – 1998. – Vol. 1493. – P. 60-65.

10. Lano K. The B Language and Method: A Guide to Practical Formal Development / K. Lano. - Springer-Verlag, FACIT series, 1996.

11. Atelier B. [Електронний ресурс] – Режим доступу: http://www.atelierb.eu.

12. Schneider S. The B-Method: An Introduction / S. Schneider // Palgrave, Cornerstones of Computing series, 2001.

Аннотация

Приводится моделирование движения подсистемы "Автобус", которая включается в систему городского транспорта, формальным методом разроботки програмного обеспечения B.

Ключевые слова: абстрактная машина, спецификация, интвариант, имлементация, детализация, контекст.

Abstract

The paper reviews "Bus" subsystem movement modelling, which is a part of urban traffic system, using formal software development method B.

Keywords: abstract machine, specification, invariant, implementation, detalization, context.