การทวนสอบแบบจำลองการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงานเชิงโครงสร้าง

นายสุวิช ถิระโคตร

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

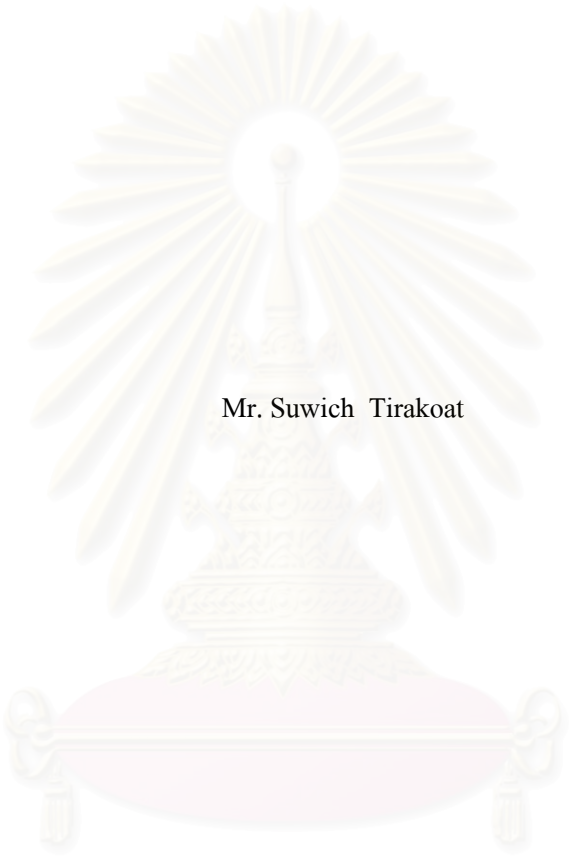
วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545

ISBN 974-030-279-3

ลิขสิทธิ์ของ จุฬาลงกรณ์มหาวิทยาลัย

VERIFICATION OF ANALYSIS MODELS FOR STRUCTURAL ACTIVE-OBJECT SYSTEM PROGRAMS

Mr. Suwich Tirakoat



สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

A Thesis Submitted in Partial Fulfillment of the Requirement
for the Degree of Master of Science in Computer Science

Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University

Academic Year 2002
ISBN 974-030-279-3

หัวข้อวิทยานิพนธ์	การทวนสอบแบบจำลองการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงานเชิงโครงสร้าง
โดย	นายสุวิช ถิระโคตร
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร. พรศิริ หมื่นไชยศรี

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร. สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ธาราทิพย์ สุวรรณศาสตร์)

..... อาจารย์ที่ปรึกษา
(ผู้ช่วยศาสตราจารย์ ดร. พรศิริ หมื่นไชยศรี)

..... กรรมการ
(อาจารย์ ดร. อาทิตย์ ทองทักษ์)

..... กรรมการ
(อาจารย์ ดร. วีระ เหมืองสิน)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สุวิช ถิระโคตร : การทวนสอบแบบจำลองการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงานเชิงโครงสร้าง (VERIFICATION OF ANALYSIS MODELS FOR STRUCTURAL ACTIVE-OBJECT SYSTEM PROGRAMS)
อ. ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร. พรศิริ หมื่นไชยศรี, 82 หน้า. ISBN 974-030-279-3

งานวิจัยนี้มีจุดมุ่งหมายเพื่อนำเสนอการทวนสอบแบบจำลองการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงาน ซึ่งเป็นระบบที่วัตถุต่างๆ ภายในระบบทำงานพร้อมๆ กัน โดยไม่ต้องรอรับคำร้องขอจากวัตถุอื่นๆ แบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงานประกอบด้วยแผนภาพยูสเคส แผนภาพคลาส และแผนภาพสเตทชาร์ตแบบเพิ่มเติม ในงานวิจัยนี้ผู้วิจัยได้สร้างระบบวัตถุพร้อมทำงานเชิงรูปนัย แอกเซียมสำหรับระบบวัตถุพร้อมทำงาน เพื่อใช้สำหรับทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน ผู้วิจัยได้ทดลองการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงานกับตัวอย่างระบบ 3 ตัวอย่างคือระบบเครื่องปรับอากาศ ระบบสัญญาณไฟจราจร และระบบการปรับระดับความดังเสียงโทรทัศน์ ผลที่ได้คือระบบตัวอย่างได้ผลการวิเคราะห์ระบบที่ถูกต้อง

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....
ปีการศึกษา 2545 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

4270626721 : MAJOR COMPUTER SCIENCE

KEY WORD : VERIFICATION / AXIOMATIC SYSTEM / ACTIVE-OBJECT SYSTEM

SUWICH TIRAKOAT : VERIFICATION OF ANALYSIS MODELS FOR STRUCTURAL ACTIVE-OBJECT SYSTEM PROGRAMS. THESIS ADVISOR : ASST. PROF. Dr. PORNSIRI MUENCHAISRI, 82 PP.

ISBN 974-030-279-3

The objective of this research is to present the verification of analysis models for Structural Active-Object System (SAOS). A SAOS program is an object-oriented program that is structurally and hierarchically constructed from a collection of active objects. The analysis models for modeling an active object system consist of a use case diagram, a class diagram and extended statechart diagrams. In this research, SAOS is formalized and axiom of analysis models for active object system is created. The researcher tests this verification of analysis models for SAOS by verifying three systems examples which are the air-condition system, the traffic light system and the television volume-adjusting system. The result of testing of all example analysis models are valid.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Department Computer Engineering Student's signature .....

Field of study Computer Science Advisor's signature .....

Academic year 2002 Co-advisor's signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงไปด้วยดี เพราะได้รับความช่วยเหลือแนะแนวทาง และแก้ไขข้อบกพร่องจาก ผู้ช่วยศาสตราจารย์ ดร. พรศิริ หมื่นไชยศรี ขอขอบพระคุณ อาจารย์ ดร. อรรถสิทธิ์ สุรฤกษ์ สำหรับตัวอย่างการพิสูจน์และคำแนะนำ รวมทั้งได้รับการตรวจสอบและแก้ไขเพื่อความสมบูรณ์และถูกต้องจากคณะกรรมการสอบวิทยานิพนธ์ ผู้วิจัยขอขอบพระคุณอาจารย์ทุกท่านเป็นอย่างสูง

ขอขอบพระคุณ บิดา มารดา ซึ่งให้ความรัก กำลังใจ และส่งเสริมให้ได้รับการศึกษาจนกระทั่งสำเร็จการศึกษาระดับปริญญามหาบัณฑิต

และขอขอบคุณเพื่อนๆ ในวิชาเอก และเพื่อนๆ ในห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ที่ให้คำปรึกษา และคำแนะนำอันเป็นประโยชน์ต่อการทำวิจัยนี้

สุวิช ถิระโคตร

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญ

หน้า

บทคัดย่อภาษาไทย…….. ง
บทคัดย่อภาษาอังกฤษ…….. จ
กิตติกรรมประกาศ…….. ฉ
สารบัญ…….. ช
สารบัญภาพ…….. ฌ
สารบัญตาราง…….. ฎ

บทที่

1. บทนำ…….. 1
    1.1 ความเป็นมาและความสำคัญของปัญหา…….. 1
    1.2 วัตถุประสงค์…….. 3
    1.3 ขอบเขตการวิจัย…….. 3
    1.4 ขั้นตอนและวิธีการดำเนินการวิจัย…….. 4
    1.5 ประโยชน์ที่คาดว่าจะได้รับ…….. 4
2. แนวคิดและทฤษฎีที่นำมาใช้ในการวิจัย…….. 5
    2.1 ระบบวัตถุพร้อมทำงาน…….. 5
    2.2 แบบจำลองการวิเคราะห์ของระบบวัตถุพร้อมทำงาน…….. 8
    2.3 การพิสูจน์ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์…….. 23
    2.4 สรุปขั้นตอนการทวนสอบแบบจำลองการวิเคราะห์เชิงวัตถุ…….. 35
3. นิยามและแอกเซียมของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน…….. 37
    3.1 นิยามแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน…….. 37
    3.2 แอกเซียมของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน…….. 40
4. ตัวอย่างการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน…….. 43
    4.1 ระบบเครื่องปรับอากาศ…….. 43
    4.2 ระบบสัญญาณไฟจราจร…….. 58
    4.3 ระบบการปรับระดับความดังเสียงโทรทัศน์…….. 69

สารบัญ(ต่อ)

บทที่ หน้า

5. สรุปผลการวิจัยและข้อเสนอแนะ……..79

5.1 สรุปผลการวิจัย……...79

5.2 ข้อเสนอแนะ……...80

รายการอ้างอิง……..81

ประวัติผู้เขียนวิทยานิพนธ์…….. 82

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญภาพ

รูปที่ หน้า

2.1 แอคเตอร์……...…9

2.2 ตัวอย่างความสัมพันธ์ของยูสเคส……10

2.3 ตัวอย่างแผนภาพยูสเคส……..10

2.4 ตัวอย่างการตั้งชื่อคลาส……..11

2.5 การกำหนดคุณลักษณะภายในแผนภาพคลาส……11

2.6 การกำหนดการทำงานในแผนภาพคลาส……12

2.7 การพึ่งพากันของคลาส……12

2.8 ความมีลักษณะทั่วไปของคลาส……..13

2.9 การกำหนดชื่อของการติดต่อกัน……14

2.10 การกำหนดบทบาทในการติดต่อกัน……...14

2.11 การกำหนดจำนวนของวัตถุ……....14

2.12 การรวมกันของคลาส……15

2.13 ตัวอย่างแผนภาพคลาส……...15

2.14 ตัวอย่างการแสดงสถานะ……17

2.15 การเปลี่ยนแปลงสถานะ……..17

2.16 กิจกรรมเมื่อเข้าและออกจากสถานะ และการเปลี่ยนแปลงภายใน……..18

2.17 ตัวอย่างสถานะย่อย……..19

2.18 สัญลักษณ์แสดงเหตุการณ์การเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน……...20

2.19 รูปแบบการกำหนดชื่อการเปลี่ยนแปลงสถานะ……..21

2.20 ตัวอย่างแผนภาพสเตทชาร์ตแบบเพิ่มเติม……...…22

2.21 รูปแบบการรวมแบบจำลอง…..……..26

2.22 ตัวควบคุม แผนภาพคลาส และแผนภาพวัตถุของระบบ……30

2.23 แผนภาพการเปลี่ยนแปลงสถานะของระบบเครื่องปรับอากาศขนาดเล็ก……31

3.1 แบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน……..……37

3.2 การเปลี่ยนแปลงสถานะของงวัตถุโดยเหตุการณ์ changeOf……...40

3.3 การกำหนดค่าล่วงหน้า..... 41

4.1 แผนภาพยูสเคสของระบบเครื่องปรับอากาศ.....……...43

4.2 แผนภาพคลาสของระบบเครื่องปรับอากาศ.....……44

4.3 แผนภาพแสดงวัตถุของระบบเครื่องปรับอากาศ.....……...……...44

สารบัญภาพ(ต่อ)

หน้า

4.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติมวัตถุ ctrl……..45
4.5 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ body…….46
4.6 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ room……46
4.7 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ thermo…….47
4.8 แผนภาพยูสเคสของระบบสัญญาณไฟจราจร…….59
4.9 แผนภาพคลาสของระบบสัญญาณไฟจราจร……..59
4.10 แผนภาพแสดงวัตถุของระบบสัญญาณไฟจราจร……60
4.11 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ ctrl……..60
4.12 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ light…….61
4.13 ส่วนประกอบของระบบการปรับความดังเสียงของโทรทัศน์…….....69
4.14 แผนภาพยูสเคสของระบบการปรับระดับความดังเสียงโทรทัศน์……...69
4.15 แผนภาพคลาสของระบบการปรับระดับความดังเสียงโทรทัศน์…….70
4.16 แผนภาพแสดงวัตถุของระบบการปรับระดับความดังเสียงโทรทัศน์……..70
4.17 แผนภาพสเตทซาร์ตแบบเพิ่มเติมของวัตถุ control…….71
4.18 แผนภาพสเตทซาร์ตแบบเพิ่มเติมของวัตถุ display…….71

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญตาราง

ตารางที่ หน้า

2.1 ความสัมพันธ์ในแผนภาพคลาส……9

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันแนวคิดเชิงวัตถุ (Object-Oriented Concepts) สำหรับพัฒนาซอฟต์แวร์ได้รับความนิยมเพิ่มมากขึ้น เนื่องจากการเขียนโปรแกรมเชิงวัตถุ (Object-Oriented Programming) มีคุณลักษณะต่างๆ ได้แก่ การสืบทอดคุณสมบัติ (Inheritance) การห่อหุ้ม (Encapsulation) และการมีหลายรูปแบบ (Polymorphism) จึงทำให้เหมาะสมสำหรับการนำเอาองค์ประกอบซอฟต์แวร์กลับมาใช้ใหม่ได้ (Reuse) ดังนั้นผลดีที่จะได้รับคือ ผู้พัฒนาซอฟต์แวร์สามารถนำเอาองค์ประกอบซอฟต์แวร์เก่ามาใช้กับงานที่พัฒนาได้เลยโดยไม่ต้องเริ่มเขียนองค์ประกอบนั้นใหม่ทั้งหมด อีกประการหนึ่งคือ ผู้พัฒนาสามารถไว้ใจได้ว่าสิ่งที่นำมาใช้ใหม่นั้นมีความถูกต้องแล้ว เนื่องจากองค์ประกอบเหล่านั้นถูกใช้มาแล้ว และมั่นใจได้ว่าองค์ประกอบที่นำมาใช้อีกนั้นถูกต้อง

เนื่องจากเหตุผลข้างต้น จึงทำให้เกิดวิธีการเชิงวัตถุ (Object-Oriented Methodology) สำหรับพัฒนาซอฟต์แวร์มากมาย เช่น Object Modeling Technique (OMT) Fusion Booch The Unified Modeling Language (UML) เป็นต้น ในวิธีการต่างๆ จะเริ่มต้นด้วยการวิเคราะห์ระบบก่อน จากนั้นจึงออกแบบและเขียนโปรแกรม ในขั้นตอนการวิเคราะห์ จะมีการสร้างแบบจำลอง (Model) ซึ่งจะแสดงถึงพฤติกรรมทางตรรกะ (Logical Behavior) ของระบบนั้น การสร้างแบบจำลองการวิเคราะห์จะต้องทำให้มีความถูกต้อง เพราะแบบจำลองการวิเคราะห์มีผลกระทบต่อการออกแบบการเขียนโปรแกรม รวมถึงการซ่อมบำรุงระบบ (Maintenance) ด้วย ดังนั้นผู้พัฒนาซอฟต์แวร์ควรจะต้องตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์

Toshiaki Aoki และ Takuya Katayama ได้เสนอ การรวมและการตรวจสอบความสอดคล้องของแบบจำลองการวิเคราะห์เชิงวัตถุ [1] โดยใช้แบบจำลอง OMT แสดงมุมมองด้านต่าง ๆ ของระบบ ได้แก่ โมเดลโครงสร้าง โมเดลพฤติกรรม และโมเดลฟังก์ชัน ซึ่งผู้พัฒนาสามารถออกแบบแต่ละโมเดลได้โดยอิสระ จากนั้นนำแบบจำลองทั้ง 3 มารวมเข้าด้วยกันเป็นแบบจำลองรวม โดยการใช้แผนร่างการรวม (Unification Mapping) และตรวจสอบความสอดคล้องของแบบจำลองทั้งสามโดยอาศัยระบบแอ็กเซียมเมติค (Axiomatic System) และกฎการอนุมาน (Inference Rules)

ต่อมา Toshiaki Aoki, Masaki Hanada และ Takuya Katayama เสนอ การใช้ตรรกะอันดับสูง (High Order Logic :HOL) สนับสนุนการตรวจสอบความสอดคล้องของแบบจำลองการวิเคราะห์เชิงวัตถุ [2] ในแนวความคิดการตรวจสอบที่เรียกว่า การตรวจสอบความสอดคล้องโดยใช้ค่าไม่เปลี่ยนแปลง (Consistency Verification Using Invariant) เพื่อตรวจสอบความสอดคล้องระหว่างแบบจำลองวัตถุพื้นฐาน (Basic Object Model) และแบบจำลองพลวัตพื้นฐาน (Basic Dynamic Model) โดยกำหนดค่าไม่เปลี่ยนแปลงเข้าไป แล้วทดสอบว่าในแต่ละคลาสของแบบจำลองยังมีค่าไม่เปลี่ยนแปลงอยู่ เมื่อสถานะของคลาสเปลี่ยนแปลงไป การสนับสนุนการตรวจสอบโดยใช้ตรรกะอันดับสูง เป็นการสร้างโปรแกรมคอมพิวเตอร์พิสูจน์ตามทฤษฎีและกฎเกณฑ์เข้ามาช่วยการตรวจสอบ เนื่องจากการตรวจสอบด้วยคนอาจจะมีความบกพร่องและความไม่เข้าใจผลลัพธ์ ดังนั้น ด้วยการสนับสนุนด้วยคอมพิวเตอร์นี้จะช่วยขจัดความผิดพลาดเนื่องจากความบกพร่องและความไม่เข้าใจผลลัพธ์ของคนได้

Takaaki Tateishi Toshiaki Aoki และ Takuya Katayama นำเสนอระบบแอ็กเซียมเมติคสำหรับการตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์เชิงวัตถุ [3] งานวิจัยนี้เสนอระบบแอ็กเซียมเมติค และการนิยามเพื่อการตรวจสอบ ที่ได้มาจากแบบจำลองการเปลี่ยนแปลงสถานะ (State Transition Diagram) ที่เป็นการเปลี่ยนแปลงสถานะวัตถุและการติดต่อสื่อสารกันระหว่างวัตถุ วิธีพิสูจน์เป็นการตรวจสอบแอตทริบิวต์ (Attribute) ที่มีอยู่ในแต่ละแบบจำลอง โดยใช้การพิสูจน์จากกรณีเฉพาะ (Induction) โดยเริ่มต้นจากแต่ละสถานะไปจนครบทุกสถานะทั้งหมดของวัตถุหนึ่ง ๆ รวมทั้งการสื่อสารกันระหว่างวัตถุด้วย จากงานวิจัยนี้ เราสามารถนำแนวทางการพิสูจน์นี้มาประยุกต์ใช้กับแบบจำลองการวิเคราะห์ที่สร้างขึ้นด้วยวิธีอื่น ๆ ได้

Toshimi Minoura และ Sungwoon Choi ได้นำเสนอวัตถุอีกรูปแบบหนึ่งที่มีลักษณะแตกต่างจากวัตถุแบบเดิม (Conventional Object-Oriented Programming) เรียกว่า วัตถุพร้อมทำงาน (Active Object) ระบบวัตถุพร้อมทำงานมีลักษณะเป็นองค์ประกอบเชิงโครงสร้างและลำดับชั้น (Structural and Hierarchical Composition) ของวัตถุพร้อมทำงาน จึงเรียกว่า ระบบวัตถุพร้อมทำงานเชิงโครงสร้าง (Structural Active-Object System : SAOS) [4] วัตถุพร้อมทำงานสามารถเริ่มการทำงานของตัวเองได้โดยไม่ต้องรอคำร้องขอ (Request) จากวัตถุอื่น เนื่องจากพฤติกรรมของวัตถุชนิดนี้ควบคุมด้วยกฎการเปลี่ยนแปลงและตัวควบคุม นอกจากนี้แล้วยังสามารถที่จะทำงานในเวลาเดียวกัน (Concurrent) ข้อดีสำหรับวัตถุพร้อมทำงานคือ สามารถแสดงรูปแบบการทำงานได้เช่นเดียวกับสิ่งต่างๆ ที่ปรากฏในโลก และสามารถนำมาใช้กับระบบเกิดขึ้นพร้อมกัน (Concurrent System) ได้ นอกจากนี้ระบบวัตถุพร้อมทำงานยังมีกรอบทำงาน (Framework) เพื่อให้ผู้พัฒนานำไปสร้างงานของตนเองได้อย่างสะดวก

วุฒิพงษ์ เรือนทอง และคณะ ได้ออกแบบแผนภาพสเตทชาร์ตเพิ่มเติม เพื่อสามารถอธิบายพฤติกรรมของวัตถุพร้อมทำงานได้อย่างเหมาะสม [7] การเพิ่มเติมแผนภาพสเตทชาร์ตมีดังนี้คือ เพิ่มสัญลักษณ์ของเหตุการณ์ที่เกิดขึ้นเนื่องจากการเปลี่ยนค่าของตัวแปรพร้อมทำงาน เพิ่มชื่อของสัญลักษณ์การเปลี่ยนแปลงสถานะและแก้ไขสัญลักษณ์ของเหตุการณ์ที่เกิดขึ้นตามเวลา และเพิ่มสัญลักษณ์ของเหตุการณ์กำหนดค่าล่วงหน้าและการเรียกใช้ฟังก์ชันล่วงหน้า

ในปัจจุบัน ระบบวัตถุพร้อมทำงานยังไม่มีการนิยามอย่างเป็นทางการ จึงยังไม่มีการตรวจสอบความถูกต้องของโปรแกรมประยุกต์ที่สร้างขึ้นโดยอาศัยพื้นฐานของระบบวัตถุพร้อมทำงาน ดังนั้นวิทยานิพนธ์นี้จึงมีจุดมุ่งหมายเพื่อสร้างระบบวัตถุพร้อมทำงานเชิงรูปนัย (Formal Notation) จากแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน และอธิบายความหมายของระบบวัตถุพร้อมทำงานเชิงรูปนัย และสร้างระบบตรวจสอบความถูกต้องสำหรับระบบวัตถุพร้อมทำงานที่สร้างขึ้นโดยอาศัยพื้นฐานของระบบวัตถุพร้อมทำงาน ผู้วิจัยทดสอบระบบตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงานด้วยการทวนสอบแบบจำลองการวิเคราะห์ของระบบวัตถุพร้อมทำงานด้วยตัวอย่าง 3 ตัวอย่าง คือ ระบบเครื่องปรับอากาศขนาดเล็ก ระบบสัญญาณไฟจราจร และระบบการปรับระดับความดังเสียงโทรทัศน์

1.2 วัตถุประสงค์

วิทยานิพนธ์นี้มีจุดประสงค์ดังนี้

1. สร้างระบบวัตถุพร้อมทำงานเชิงรูปนัย และอธิบายความหมายของระบบวัตถุพร้อมทำงานเชิงรูปนัย
2. สร้างระบบแอ็กเซียมเมติคสำหรับระบบวัตถุพร้อมทำงาน เพื่อใช้ในการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์

1.3 ขอบเขตของการวิจัย

1. แบบจำลองการวิเคราะห์ที่ใช้สำหรับการพิสูจน์ความถูกต้อง เป็นแบบจำลองการวิเคราะห์ ประกอบด้วย แผนภาพคลาส และแผนภาพแสดงพฤติกรรมของระบบที่สร้างโดยอาศัยพื้นฐานระบบวัตถุพร้อมทำงาน
2. การแสดงการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ระบบจะทำกับอย่างน้อย 1 โปรแกรมประยุกต์

3. แบบจำลองการวิเคราะห์ที่ใช้สำหรับการพิสูจน์ความถูกต้อง จะต้องประกอบด้วยตัวแปรพร้อมทำงานอย่างน้อย 1 ตัวแปร

1.4 ขั้นตอนและวิธีการดำเนินงานวิจัย

1. ศึกษาแนวคิดและการใช้งานระบบวัตถุพร้อมทำงาน
2. ศึกษาวิธีการตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์
3. ศึกษาแบบจำลองการวิเคราะห์ แสดงพฤติกรรมของระบบ ที่สร้างโดยอาศัยพื้นฐานของระบบวัตถุพร้อมทำงาน
4. สร้างรูปนัยของแบบจำลองการวิเคราะห์ของระบบ พร้อมอธิบายความหมาย
5. สร้างระบบแอ็กเซียมเมติคจากแบบจำลองการวิเคราะห์แสดงพฤติกรรมของวัตถุพร้อมทำงาน
6. แสดงการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ระบบกับอย่างน้อย 1 โปรแกรมประยุกต์
7. สรุป และจัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่จะได้รับ

1. สามารถตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์ที่สร้างด้วยระบบวัตถุพร้อมทำงาน
2. ใช้เป็นแนวทางสำหรับการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์โดยอัตโนมัติ

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 2

แนวคิดและทฤษฎีที่นำมาใช้ในการวิจัย

บทนี้จะอธิบายแนวคิดและทฤษฎีต่าง ๆ ที่ใช้ เพื่อความเข้าใจในการทวนสอบแบบจำลองการวิเคราะห์ของโปรแกรมระบบวัตถุพร้อมทำงาน โดยจะกล่าวถึงรายละเอียดของ 3 หัวข้อใหญ่ดังนี้

1. ระบบวัตถุพร้อมทำงาน
2. แบบจำลองการวิเคราะห์ของระบบวัตถุพร้อมทำงาน
3. การพิสูจน์ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์
4. สรุปขั้นตอนการทวนสอบแบบจำลองการวิเคราะห์เชิงวัตถุ

2.1 ระบบวัตถุพร้อมทำงาน

ในการเขียนโปรแกรมเชิงวัตถุ โดยทั่วไปแล้ว วัตถุจะประกอบด้วยข้อมูล (Data) และพฤติกรรม (Behavior) วัตถุหนึ่งจะทำงานก็ต่อเมื่อวัตถุอื่นๆ สั่งให้ทำงาน โดยการส่งคำขอ (Message) มาให้ ซึ่งจะเรียกวัตถุประเภทนี้ว่า พาสซีพออฟเจคต์ (Passive Object) นอกจากนี้ มีวัตถุอีกประเภทหนึ่ง คือ วัตถุพร้อมทำงาน (Active Object) วัตถุนี้มีคุณสมบัติพิเศษเพิ่มเติมเข้ามาอีกนอกเหนือจากข้อมูลและพฤติกรรม คือสามารถที่จะทำงานได้โดยตัวเอง โดยไม่ต้องรอรับคำขอจากวัตถุอื่น

2.1.1 ระบบวัตถุพร้อมทำงานแบบโครงสร้าง (Structural Active Object System)

แนวคิดของระบบพร้อมทำงานนี้เสนอโดย Toshimi Minoura และ Sungwoon Choi ระบบวัตถุพร้อมทำงานแบบโครงสร้างเป็นระบบที่ประกอบด้วยวัตถุพร้อมทำงานต่าง ๆ ที่ประกอบกันแบบโครงสร้างและลำดับชั้น (Structural-and-Hierarchical Object Composition : SHOC) [4] วัตถุพร้อมทำงานจะสามารถเริ่มต้นการทำงานได้โดยตัวเอง โดยไม่ต้องรอคำขอจากวัตถุอื่นๆ การเริ่มการทำงานของวัตถุชนิดนี้จะขึ้นอยู่กับการเปลี่ยนแปลงของค่าตัวแปรในวัตถุนั้นๆ การเขียนโปรแกรมเชิงวัตถุที่คอยตอบสนองคำร้องขอจะมีข้อบกพร่องบางประการ คือ วัตถุไม่มีส่วนควบคุม

ในตัวเอง (Encapsulation of Control) การเขียนโปรแกรมต้องสร้างส่วนควบคุมแยกไว้ต่างหาก จึงมีผลทำให้ไม่สะดวกต่อการนำวัตถุนั้น ๆ กลับมาใช้ใหม่ในงานอื่นๆ

ในความเป็นจริงของโลกมีระบบจำนวนมากที่เป็นลักษณะการทำงานเช่นเดียวกับการทำงานของระบบพร้อมทำงาน เช่น สัญญาณไฟจราจรในความเป็นจริงแล้วสัญญาณไฟจราจรจะใช้ตัวจับเวลาในตัวเอง เพื่อคอยจับเวลาที่จะเปลี่ยนสีของสัญญาณไฟเป็นสีแดง เหลือง หรือเขียว ตามเวลาที่กำหนดไว้ ถ้าต้องการเขียนโปรแกรมจำลองการทำงานของสัญญาณไฟจราจรนี้ในรูปแบบของวัตถุที่คอยตอบสนองคำร้องขอ เราจะต้องสร้างวัตถุ 2 วัตถุคือ วัตถุที่ 1 วัตถุที่เป็นสัญญาณไฟ วัตถุที่ 2 วัตถุที่คอยส่งคำร้องขอไปให้สัญญาณไฟเปลี่ยนสีตามเวลา ในขณะเดียวกันถ้านำระบบนี้มาเขียนด้วยโปรแกรมเชิงวัตถุพร้อมทำงาน จะสามารถสร้างสัญญาณไฟที่สมบูรณ์ และเหมือนในโลกความเป็นจริง นั่นคือการควบคุมการเปลี่ยนสัญญาณไฟจะอยู่ภายในตัววัตถุที่เป็นสัญญาณไฟและสามารถทำงานได้เองโดยไม่ต้องรอคำร้องขอจากวัตถุอื่นๆ

2.1.2 การกำหนดพฤติกรรม

พฤติกรรมของวัตถุพร้อมทำงานสามารถกำหนดได้โดยใช้ประโยคแสดงการเปลี่ยนแปลง (Transition Statement) ซึ่งแบ่งออกได้เป็น 3 แบบได้แก่

2.1.2.1 กฎการเปลี่ยนแปลง (Transition rules)

การกำหนดพฤติกรรมแบบนี้จะอยู่ในรูปของคู่เงื่อนไขและการกระทำ (Condition-Action Pair) ส่วนของการกระทำจะถูกทำงานเมื่อส่วนของเงื่อนไขมีค่าเป็นจริง กฎการเปลี่ยนแปลงเริ่มต้นทำงานทุกครั้งเมื่อค่าของตัวแปรเงื่อนไข (Condition Variable) ใดๆ หรือเรียกอีกอย่างหนึ่งว่าค่าพร้อมทำงาน (Active Value) ที่ถูกใช้ในส่วนของเงื่อนไขมีค่าเปลี่ยนแปลง กฎการเปลี่ยนแปลงนี้จะทำงานได้โดยอัตโนมัติ

ตัวอย่างเช่น การกำหนดกฎการเปลี่ยนแปลงสำหรับคลาส Processor ของระบบคิวจะใช้คำสำคัญ transition นำหน้า โดยมีเงื่อนไข *when(input->nJobs > 0 && state == Pidle)* และส่วนของการกระทำจะกำหนดดังนี้

```
{job = input->dequeue();
state = PBusy;
state = PComplete after maxProcessingTime * random();}
```

ส่วนของการกระทำของกฎการเปลี่ยนแปลงนี้ จะได้รับการประมวลผลก็ต่อเมื่อเมื่อใดก็ตามที่ตัวแปรพร้อมทำงาน *nJob* ของ *input* และ *state* เปลี่ยนแปลงค่า และทำให้เงื่อนไขเป็นจริง

2.1.2.2 สมการกำหนดค่า (Equational assignment)

เป็นการกำหนดพฤติกรรมคล้ายกับกฎการเปลี่ยนแปลง แต่รูปแบบแตกต่างออกไป สำหรับสมการกำหนดค่าตัวแปร จะประกอบด้วยส่วนที่อยู่ด้านซ้ายเครื่องหมายเท่ากับ (=) และส่วนที่อยู่ทางขวาของเครื่องหมาย การกำหนดค่าจะต้องมีตัวแปรพร้อมทำงานอยู่อย่างน้อย 1 ตัว เมื่อไรก็ตามที่ตัวแปรพร้อมทำงานในสมการมีการเปลี่ยนแปลงค่า ระบบจะทำการคำนวณค่าในส่วนของด้านขวา และกำหนดให้ค่าทางด้านซ้ายมีค่าเท่ากับผลที่ได้จากการคำนวณนั้น

ตัวอย่างเช่น การกำหนดพฤติกรรมของคลาส AND_Gate ที่สืบทอดคุณสมบัติมาจากคลาส *Gate* มีรายละเอียดดังต่อไปนี้

```
class Gate{
  public:
    bool output;
}
class AND_Gate{
  interface:
    Gate *input1, *input2;
  private:
     always output = (input1->output && input2->output);
}
```

จะเห็นว่าคลาส AND_Gate มีตัวแปรชนิดอินเตอร์เฟซ input1 และ input2 ซึ่งเป็นตัวอย่างของคลาส Gate และตัวแปรทั้งสองจะมีตัวแปร output ซึ่งเป็นคุณสมบัติของคลาส Gate

การกำหนดพฤติกรรมแบบสมการกำหนดค่า จะใช้คำสำคัญ *always* เช่น

```
always output = (input1->output && input2->output);
```

สำหรับประโยคข้างต้น ทุกครั้งที่ค่าของ *output* ของ *input1* และ *input2* เปลี่ยนแปลง จะทำให้สมการนี้ได้รับการประมวลผล

2.1.2.3 การกระทำตามเหตุการณ์ (event routines)

การกำหนดพฤติกรรมแบบนี้ จะอยู่ในรูปแบบของการเรียกฟังก์ชันล่วงหน้า (Future Call) และการกำหนดค่าล่วงหน้า (Future Assignment) การเรียกฟังก์ชันล่วงหน้าจะเป็นการ

เรียกฟังก์ชัน โดยมีการกำหนดเวลาหน่วงไว้ด้วย ฟังก์ชันดังกล่าวจะถูกประมวลผลก็ต่อเมื่อเวลาผ่านไปเท่ากับเวลาหน่วงที่กำหนดไว้ ส่วนการกำหนดค่าล่วงหน้าก็มีลักษณะเช่นเดียวกับการเรียกฟังก์ชันล่วงหน้าคือเมื่อผ่านเวลาที่กำหนดไว้จะมีการประมวลผล แต่การประมวลผลที่เกิดขึ้นคือการกำหนดค่าให้กับตัวแปร

จากงานวิจัยนี้จะเห็นได้ว่า วัตถุพร้อมทำงานมีการเปลี่ยนแปลงไปทั้งรูปแบบ และการสั่งให้ทำงาน สำหรับการเปลี่ยนแปลงสถานะของวัตถุพร้อมทำงานจะเปลี่ยนแปลงจากสถานะหนึ่งไปเป็นอีกสถานะหนึ่ง สิ่งที่จะทำให้เปลี่ยนได้ไม่มีเพียงแต่เหตุการณ์ (Event) เท่านั้นเช่นเดียวกับวัตถุที่ตอบสนองคำร้องขอ แต่จะใช้กฎการเปลี่ยนแปลงของแต่ละวัตถุนั้นๆ ด้วย

2.2 แบบจำลองการวิเคราะห์ของระบบวัตถุพร้อมทำงาน (Active object's Analysis Models)

สำหรับแบบจำลองการวิเคราะห์เชิงวัตถุพร้อมทำงาน จะแสดงด้วยแผนภาพในแบบต่างๆ เพื่อแสดงพฤติกรรมของระบบ คลาส และพฤติกรรมของวัตถุ จะแสดงได้โดยใช้แผนภาพยูสเคส (Use Case Diagram) แผนภาพคลาส (Class Diagram) และแผนภาพสเตทชาร์ตแบบเพิ่มเติม (Extended Statechart Diagarm) ตามลำดับ มีรายละเอียดดังนี้

2.2.1 แผนภาพยูสเคส

แผนภาพยูสเคส แสดงพฤติกรรมของระบบ (System) ระบบย่อย (Subsystem) หรือคลาส (Class) ในแผนภาพนี้จะประกอบด้วยแอคเตอร์ (Actor) และยูสเคส (Use Case)

2.2.1.1 แอคเตอร์

แอคเตอร์จะเป็นบุคคล กระบวนการ หรือสิ่งต่างๆ ภายนอกที่มีปฏิสัมพันธ์กับระบบ ระบบย่อย หรือคลาส ขณะที่ระบบกำลังทำงาน (Run Time) ผู้ใช้งาน (User) 1 คน อาจจะเป็นหลายๆ แอคเตอร์ภายในระบบก็ได้ หรือผู้ใช้หลายๆ คน อาจจะเป็นแอคเตอร์เดียวกันก็ได้ การสื่อสารกันระหว่างแอคเตอร์กับยูสเคสโดยใช้แมสเซส (Message) ลักษณะของแอคเตอร์อาจจะเป็นลำดับของแอคเตอร์ก็ได้ (Hierarchy) โดยมีแอคเตอร์ทั่วไป (Abstract Actor) อธิบายลักษณะที่ใช้ร่วมกัน เพื่อให้ผู้ใช้ลำดับขั้นต่อไปได้นำไปใช้ รูปที่ 2.1 แสดงแอคเตอร์ในแผนภาพยูสเคสจะใช้รูปตัวคนขนาดเล็ก และมีชื่อกำกับอยู่ใต้รูป

รูปที่ 2.1 แอคเตอร์ [6]

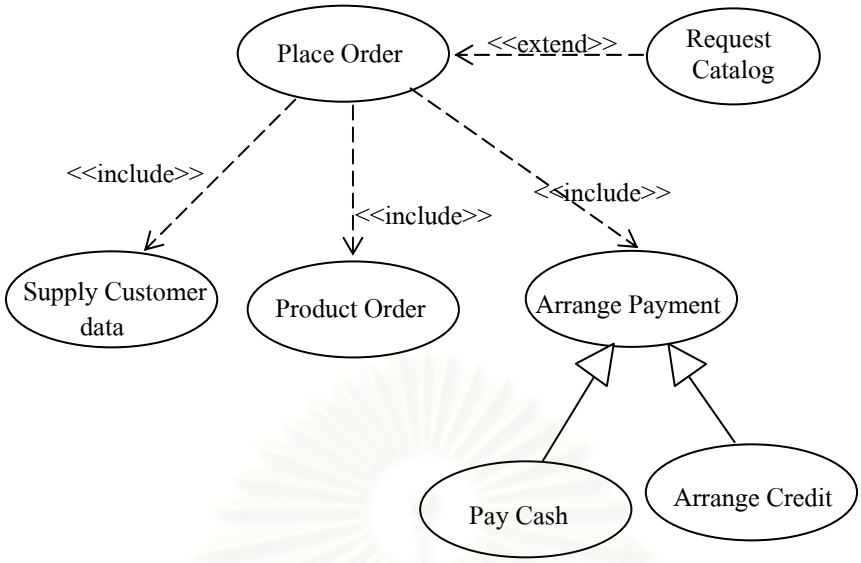
2.2.1.2 ยูสเคส

ยูสเคสเป็นกลุ่มของงานจริงๆ ที่ปรากฏอยู่ในระบบ ซึ่งจะถูกใช้โดยแอคเตอร์ จุดประสงค์ของยูสเคสคือ การอธิบายพฤติกรรมของระบบโดยที่ไม่ต้องอธิบายถึงโครงสร้างระบบ ยูสเคสและแอคเตอร์มีความสัมพันธ์กันได้หลายๆ รูปแบบ ดังแสดงในตารางที่ 2.1 ดังนี้

ตารางที่ 2.1 ความสัมพันธ์ในแผนภาพยูสเคส

ความสัมพันธ์	ลักษณะ	สัญลักษณ์
Association	เป็นการสื่อสารกันระหว่างผู้แสดงกับฟังก์ชันงาน	———
Extend	เป็นความสัมพันธ์จากยูสเคส A ไปยังยูสเคส B โดยที่ B อาจจะรวมเอาพฤติกรรมที่กำหนดไว้ใน A ด้วยก็ได้ (ใช้ความสัมพันธ์นี้ในกรณีพิเศษเท่านั้น)	A - - <<extend>> -> B
use case generalization	ความสัมพันธ์ระหว่างฟังก์ชันงานแม่ (General Use Case) กับฟังก์ชันงานลูก (Specific Use Case) โดยการสืบทอดคุณสมบัติ	——▷
Include	เป็นความสัมพันธ์จากยูสเคส A ไปยังยูสเคส B โดยที่พฤติกรรมส่วนหนึ่ง A จะเป็นพฤติกรรมที่กำหนดใน B (ใช้ความสัมพันธ์นี้ในกรณีพิเศษเท่านั้น)	A - - <<include>> -> B

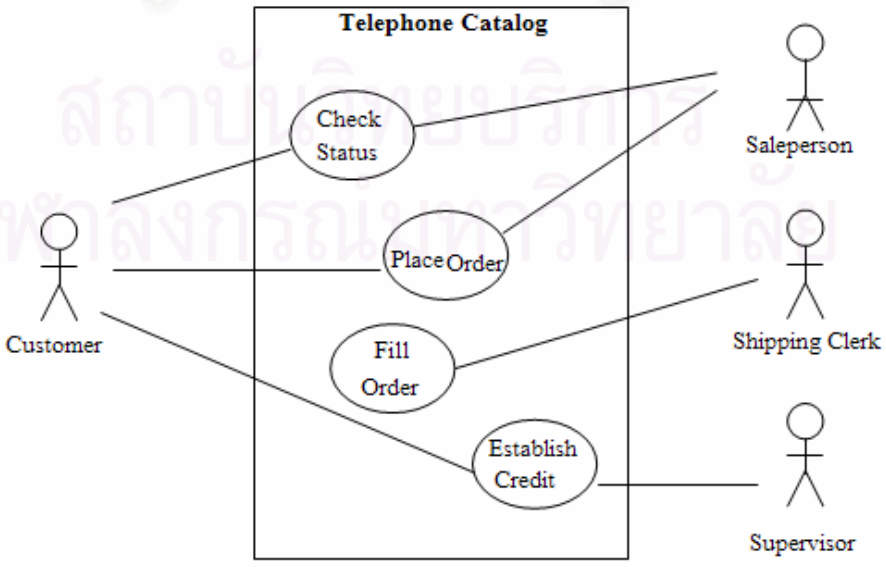
สัญลักษณ์ที่ใช้แทนยูสเคสคือ รูปวงรี ที่มีชื่องานเขียนกำกับไว้ภายในหรือใต้วงรี ดังรูปที่ 2.2



รูปที่ 2.2 ตัวอย่างความสัมพันธ์ของยูสเคส [6]

2.2.1.3 ตัวอย่างแผนภาพยูสเคส

ตัวอย่างแสดงในรูปที่ 2.3 ต่อไปนี้ เป็นตัวอย่างง่ายๆ ของแผนภาพยูสเคส ตัวอย่างนี้แสดงให้เห็นถึงการเขียนแผนภาพที่สมบูรณ์ของระบบ Telephone Catalog จากรูปที่ 2.3 จะเห็นว่าระบบ Telephone Catalog ประกอบด้วยแอคเตอร์ Customer Saleperson Shipping Clerk และ Supervisor และแต่ละแอคเตอร์มีความสัมพันธ์กับยูสเคสดังนี้ แอคเตอร์ Customer สัมพันธ์กับยูสเคส Check Status Place Order และ Establish Credit แอคเตอร์ Saleperson สัมพันธ์กับยูสเคส Check Status และ Place Order แอคเตอร์ Shipping Clerk สัมพันธ์กับยูสเคส Fill Order และแอคเตอร์ Supervisor สัมพันธ์กับยูสเคส Establish Credit



รูปที่ 2.3 ตัวอย่างแผนภาพยูสเคส [6]

2.2.2 แผนภาพคลาส

แผนภาพคลาส แสดงให้เห็นถึงกลุ่มของคลาส ส่วนเชื่อมต่อ (Interface) การทำงานร่วมกัน (Collaboration) และความสัมพันธ์ (Relationship) ของคลาส

2.2.2.1 คลาส

คลาสจะอธิบายกลุ่มของวัตถุที่ใช้คุณลักษณะ (Attribute) การทำงาน (Operation) ความสัมพันธ์ ร่วมกัน สัญลักษณ์ที่ใช้แทนคลาสในแผนภาพคลาสคือ รูปสี่เหลี่ยม

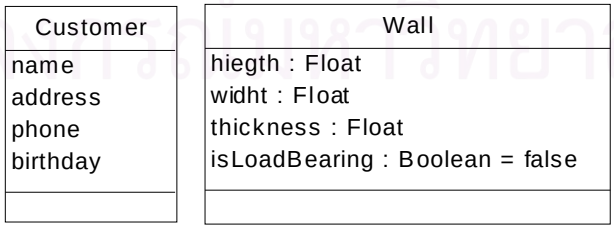
ชื่อ (Name)

ทุกๆ คลาสจะต้องมีชื่อเพื่อแสดงความแตกต่างกับคลาสอื่น ชื่ออาจจะเป็นข้อความเดี่ยว ชื่อเส้นทางที่คลาสอยู่ (Path Name) คลาสอาจจะมีแต่ชื่อคลาสเท่านั้นก็ได้ ดังแสดงในรูปที่ 2.4

รูปที่ 2.4 ตัวอย่างการตั้งชื่อคลาส [6]

คุณลักษณะ

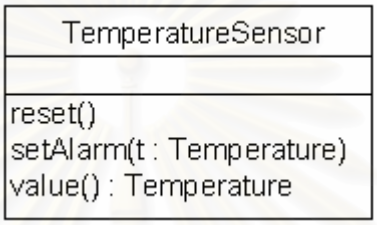
คุณลักษณะบ่งบอกถึงคุณสมบัติ (Properties) ที่มีอยู่ในคลาสภายในแบบจำลองที่สร้างขึ้น คลาสที่แสดงในแผนภาพคลาสอาจจะระบุหรือไม่ก็ได้ เนื่องจากคลาสสามารถสืบทอดคุณสมบัติมาจากคลาสอื่น การกำหนดคุณลักษณะของคลาส จะเขียนเป็นรายการของคุณลักษณะไว้ใต้ชื่อคลาส โดยมีเส้นแบ่งระหว่างชื่อกับรายการนี้ รายการของคุณลักษณะประกอบด้วยชื่อของลักษณะ โดยอาจจะมีชนิดและค่าเริ่มต้นของคุณลักษณะนั้นประกอบอยู่ด้วยก็ได้ รูปที่ 2.5 เป็นตัวอย่างการเขียนคุณลักษณะในแผนภาพคลาส



รูปที่ 2.5 การกำหนดคุณลักษณะภายในแผนภาพคลาส [6]

การทำงาน

การทำงานคือการกำหนดงานต่างๆ ซึ่งวัตถุของคลาสสามารถที่จะเรียกใช้งานได้เพื่อแสดงพฤติกรรมของตน หรือมองอีกแง่หนึ่งคือ จะบอกได้ว่าวัตถุสามารถทำงานอะไรได้ คลาสที่แสดงในแผนภาพคลาสอาจจะมีหรือไม่มีการทำงานนี้ก็ได้ เนื่องจากคลาสจะสามารถสืบทอดคุณสมบัติจากคลาสอื่น การเขียนรายการทำงานจะเขียนต่อจากรายการคุณลักษณะโดยมีเส้นตรงกั้นไว้ แต่ละรายการการทำงานอาจจะประกอบด้วยชื่อ ชนิดของค่าที่ส่งกลับ และพารามิเตอร์ (Parameter) ตัวอย่างการเขียนการทำงานภายในคลาส ดังแสดงในรูปที่ 2.6



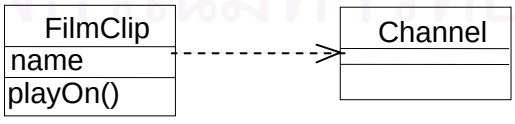
รูปที่ 2.6 การกำหนดการทำงานในแผนภาพคลาส [6]

2.2.2.2 ความสัมพันธ์ระหว่างคลาส

ความสัมพันธ์ระหว่างคลาส แสดงถึงการเชื่อมต่อหลายๆ คลาส ในแบบจำลองเชิงวัตถุจะมีความสัมพันธ์ที่สำคัญๆ อยู่ 3 แบบคือ การพึ่งพากัน (Dependency) ความมีลักษณะทั่วไป (Generalization) และการติดต่อกัน (Association)

การพึ่งพากัน

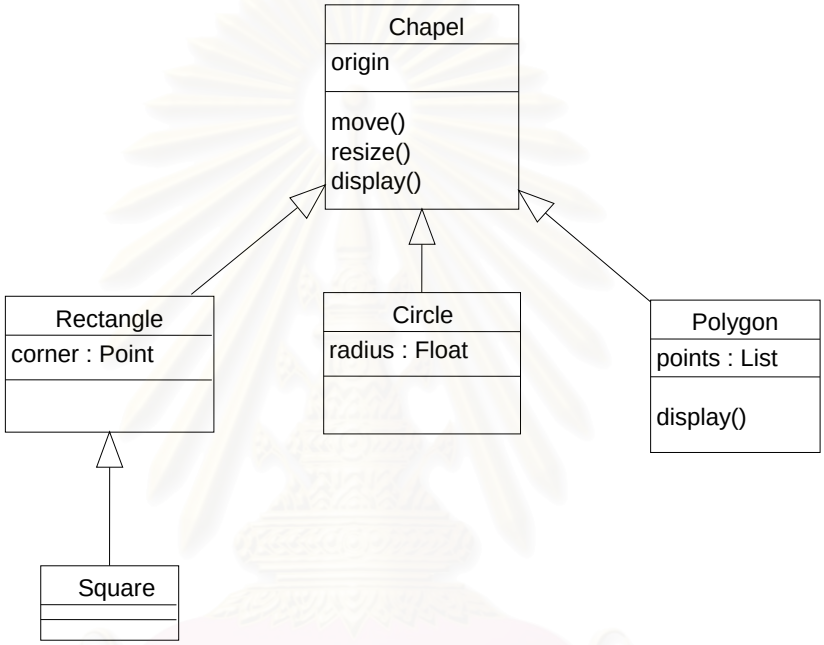
การพึ่งพากันคือการใช้ความสัมพันธ์ในลักษณะของการขึ้นต่อกัน ถ้าลักษณะของสิ่งหนึ่งเปลี่ยนไป อาจจะมีผลกระทบต่ออีกสิ่งหนึ่งที่ขึ้นตรงต่อสิ่งนั้นด้วย สัญลักษณ์ใช้แทนความสัมพันธ์ชนิดนี้คือ เส้นประมีหัวลูกศรชี้ไปยังคลาสที่พึ่งพาอยู่ ตัวอย่างในรูปที่ 2.7 คลาส FilmClip จะมีการทำงาน playOn() ซึ่งขึ้นอยู่กับคลาส Channel



รูปที่ 2.7 การพึ่งพากันของคลาส [6]

ความมีลักษณะทั่วไป

เป็นความสัมพันธ์ระหว่างคลาสที่มีความทั่วไปกว่า ซึ่งเรียกว่า ซูเปอร์คลาส หรือ คลาสแม่ (Super Class หรือ Parent) และคลาสที่มีความจำเพาะ หรือเรียกว่า สับคลาส หรือคลาสลูก (Subclass หรือ Child) ความสัมพันธ์ชนิดนี้จะเรียกว่า ความสัมพันธ์แบบเป็นชนิดของ (Is-a Relationship) คลาสลูกจะสืบทอดคุณลักษณะและการทำงานของคลาสแม่มาได้ทั้งหมด บางครั้งคลาสลูกจะเพิ่มคุณลักษณะและการทำงานของตนเองเข้าไปอีก หรือแก้ไขสิ่งที่สืบทอดมาจากคลาสแม่ให้เหมาะสม รูปที่ 2.8 เป็นตัวอย่างของความมีลักษณะทั่วไป



รูปที่ 2.8 ความมีลักษณะทั่วไปของคลาส [6]

สัญลักษณ์ที่ใช้แสดงความสัมพันธ์นี้คือ เส้นที่เริ่มเขียนจากคลาสลูก ไปยังคลาสแม่และมีหัวลูกศรขนาดใหญ่ชี้ไปที่คลาสแม่

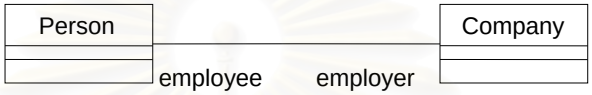
การติดต่อกัน

การติดต่อกันคือความสัมพันธ์เชิงโครงสร้างที่คลาสเชื่อมต่อกัน สัญลักษณ์ที่ใช้สำหรับแสดงคือ เส้นตรงที่ลากเชื่อมระหว่าง 2 วัตถุ ซึ่งอาจจะมีองค์ประกอบต่อไปนี้อยู่ด้วย

- **ชื่อ** เราสามารถที่จะกำหนดชื่อของการติดต่อกันได้ ซึ่งจะเป็นการอธิบายลักษณะของความสัมพันธ์ระหว่างสองคลาส และป้องกันการซ้ำกันของความหมายของความสัมพันธ์ จะเขียนชื่อของการติดต่อไว้บนเส้นและมีหัวลูกศรชี้บอกทิศทางของการอ่านชื่อ ตัวอย่างเช่นในรูปที่ 2.9 ชื่อของการติดต่อกันคือ Work for (ทำงานให้กับ) หมายความว่า Person ทำงานให้กับ Company

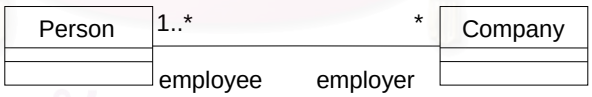
รูปที่ 2.9 การกำหนดชื่อของการติดต่อกัน [6]

- **บทบาท (Role)** เป็นการบอกบทบาทหน้าที่ของแต่ละคลาสในการติดต่อกัน ว่าเป็นอะไร ตัวอย่างเช่นในรูปที่ 2.10 หมายความว่า Person มีหน้าที่เป็นลูกจ้าง (Employee) และ Company มีหน้าที่เป็นนายจ้าง (Eemployer)



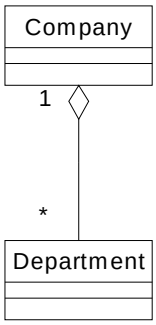
รูปที่ 2.10 การกำหนดบทบาทในการติดต่อกัน [6]

- **จำนวนของวัตถุ (Multiplicity)** เป็นการบอกจำนวนของวัตถุที่ติดต่อกัน การเขียนอาจจะระบุจำนวนเป็นนิพจน์ในกรณีที่ระบุจำนวนได้ไม่แน่นอน หรือระบุจำนวนที่แน่นอนเป็นตัวเลขได้ เช่น 1 แทนจำนวนวัตถุ 1 ชิ้น 0..1 แทนไม่มีวัตถุหรือมีแค่หนึ่งเท่านั้น 0..* แทนไม่มีวัตถุหรือมีได้มากกว่าหนึ่ง 1..* แทนมีมากกว่าหรือเท่ากับหนึ่ง เป็นต้น ตัวอย่างในรูปที่ 2.11 หมายถึงบริษัท (Company) หลายๆ บริษัท จะมีพนักงาน (Person) อยู่ตั้งแต่ 1 คนเป็นต้นไป



รูปที่ 2.11 การกำหนดจำนวนของวัตถุ [6]

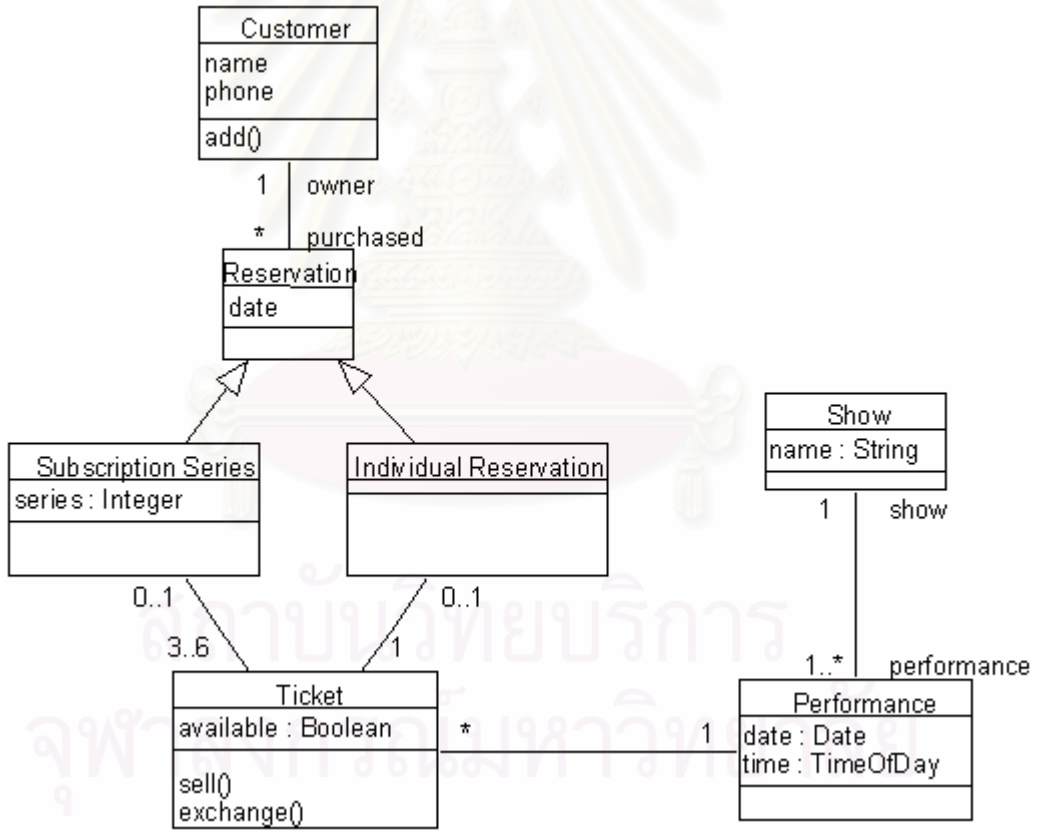
- **การรวมกัน (Aggregation)** ในบางครั้งการติดต่อกันของ 2 คลาสซึ่งอยู่ระดับเดียวกัน ไม่มีคลาสหนึ่งสำคัญกว่าอีกคลาสหนึ่ง แต่ถ้าเราต้องการที่จะจำลองความสัมพันธ์แบบ whole/part โดยที่คลาสหนึ่งจะใหญ่กว่า (คือ whole) อีกคลาสหนึ่งซึ่งเล็กกว่า (คือ part) ลักษณะความสัมพันธ์แบบนี้จะแสดงถึง ความสัมพันธ์แบบ has-a หมายถึง วัตถุที่เป็น whole จะประกอบด้วยวัตถุที่เป็น part ตัวอย่างในรูปที่ 2.12 หมายความว่า บริษัทหนึ่งบริษัทจะประกอบด้วยหลายๆ แผนก (Department)



รูปที่ 2.12 การรวมกันของคลาส [6]

2.2.2.3 ตัวอย่างแผนภาพคลาส

ตัวอย่างในรูปที่ 2.13 แสดงแผนภาพคลาสของโปรแกรม Box Office โดยแสดงแบบจำลองการขายตั๋วภาพยนตร์ ประกอบด้วยหลายๆ คลาสคือ Customer Reservation Ticket และ Performance



รูปที่ 2.13 ตัวอย่างแผนภาพคลาส [6]

2.2.3 แผนภาพสเตทชาร์ต

แผนภาพสเตทชาร์ตอธิบายพฤติกรรมของวัตถุ (Object) เหตุการณ์ (Event) แสดงชนิดของการเปลี่ยนแปลงที่วัตถุสามารถเปลี่ยนจากสถานะหนึ่งไปเป็นอีกสถานะหนึ่งได้ เหตุการณ์ดังกล่าวอาจจะเป็นเหตุการณ์การเปลี่ยนแปลงค่า หรือเหตุการณ์การผ่านช่วงเวลา

แผนภาพสเตทชาร์ตเป็นแผนภาพที่แสดงสถานะและการเปลี่ยนแปลงสถานะ (Transition) โดยปกติแล้วแผนภาพนี้จะเกี่ยวข้องกับตัวแทนคลาส (Instance of Class) หรือวัตถุ มีหน้าที่อธิบายเหตุการณ์ที่เกิดขึ้นกับวัตถุ และเหตุการณ์ที่วัตถุได้รับ

2.2.3.1 เหตุการณ์ (Event)

เป็นสิ่งที่เกิดขึ้นในช่วงเวลาหนึ่งๆ เหตุการณ์มีหลายประเภทดังนี้

1. เหตุการณ์ประเภทการเรียก (Call event) เป็นการเรียกใช้ระหว่างวัตถุ ไวยากรณ์สำหรับเหตุการณ์ประเภทนี้คือ op(a: T) โดยที่ op คือชื่อของโอเปอร์เรชัน a: T เป็นชื่อของแอตทริบิวต์ และชนิดของแอตทริบิวต์ ตามลำดับโดยมีเครื่องหมายโคลอน (:) คั่น

2. เหตุการณ์ประเภทการเปลี่ยนแปลง (Change event) เป็นเหตุการณ์ที่ตรวจสอบนิพจน์บูลีน (Boolean expression) โดยนิพจน์จะเป็นจริงหรือเท็จขึ้นอยู่กับค่าของคุณสมบัติของนิพจน์นั้นๆ ไวยากรณ์สำหรับเหตุการณ์ประเภทนี้นิยามดังนี้ *when(exp)*

3. เหตุการณ์ประเภทสัญญาณ (Signal event) เหตุการณ์ที่เกิดขึ้นเมื่อมีการส่งสัญญาณมาจากวัตถุอื่น หลังจากส่งสัญญาณเสร็จแล้ววัตถุที่ผู้ส่งสัญญาณสามารถทำงานอื่นต่อไปได้ทันทีโดยไม่ต้องคอยให้วัตถุผู้รับสัญญาณทำงานเสร็จก่อน ไวยากรณ์สำหรับเหตุการณ์ประเภทนี้คือ sname(a: T) โดยที่ sname เป็นชื่อของสัญญาณ

4. เหตุการณ์เกิดขึ้นตามเวลา (Time event) เป็นเหตุการณ์ที่เกิดขึ้นเมื่อเวลาที่กำหนดไว้มาถึง เวลาอาจจะกำหนดเป็นเวลาของวัน (time of day) หรือระยะเวลาที่กำหนด ไวยากรณ์สำหรับเหตุการณ์ประเภทนี้คือ *after(times)*

2.2.3.2 สถานะ (State)

เป็นสภาวะของวัตถุที่คอยการเกิดของเหตุการณ์บางอย่างเพื่อที่จะตอบสนองต่อเหตุการณ์นั้น เช่นคลาสเครื่องปรับอากาศ จะมีสถานะเป็นหยุดนิ่ง เริ่มทำงาน เป็นต้น สถานะจะประกอบด้วยส่วนต่าง ๆ ดังนี้

1. ชื่อ (Name) เป็นข้อความที่บ่งบอกถึงความหมายของสถานะนั้น ๆ เพื่อแสดงความแตกต่างกับสถานะอื่น

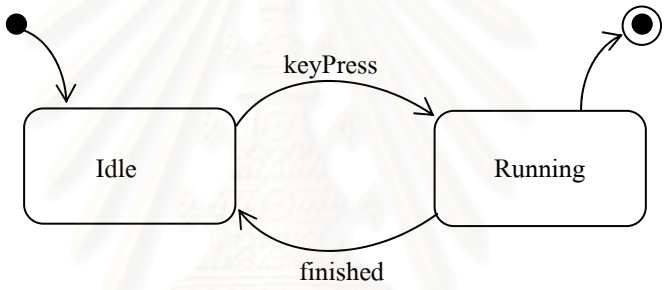
2. การกระทำเมื่อเข้าสู่สถานะและออกจากสถานะ (Entry/exit action) เป็นการกระทำที่ปฏิบัติได้ทันทีที่เข้าสู่สถานะและออกจากสถานะ

3. การเปลี่ยนแปลงภายใน (Internal transition) การเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ต้องมีการเปลี่ยนสถานะ

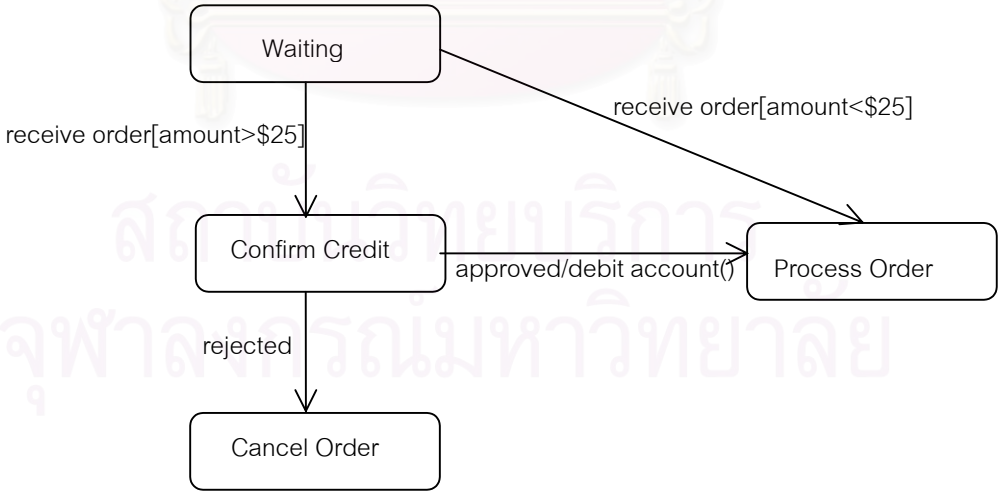
4. สถานะย่อย (Substate) เป็นโครงข่ายซ้อนของสถานะ

5. เหตุการณ์ถูกหน่วง (Deferred event) รายการของเหตุการณ์ที่ไม่ถูก ทำงานตามเหตุการณ์ในสถานะนั้นๆ แต่จะถูกเก็บเอาไว้เพื่อทำงานในสถานะอื่นๆ ของวัตถุอื่น

สถานะเริ่มต้นและสถานะสิ้นสุด (Initial and Final State) สถานะเริ่มต้นจะบอกจุดเริ่มต้นของการเปลี่ยนแปลงสถานะของวัตถุ จะแสดงด้วยวงกลมเล็กๆ ระบายทึบ แล้วมีหัวลูกศรชี้ไปยังสถานะแรกที่จะถูกทำงาน สถานะสิ้นสุดบ่งบอกถึงสถานะสุดท้ายของการเปลี่ยนแปลงในวัตถุ ซึ่งแสดงด้วยวงกลมทึบและซ้อนทับด้วยวงกลมอีกชั้นหนึ่ง สถานะแสดงด้วย สี่เหลี่ยมมุมมน ตัวอย่างการเขียนสถานะอย่างง่าย แสดงในรูปที่ 2.14



รูปที่ 2.14 ตัวอย่างการแสดงสถานะ [6]



รูปที่ 2.15 การเปลี่ยนแปลงสถานะ [6]

2.2.3.3 การเปลี่ยนแปลงสถานะ (Transition)

เป็นความสัมพันธ์ระหว่างสถานะ 2 สถานะ ที่แสดงให้เห็นวัตถุในสถานะแรกเปลี่ยนเป็นสถานะที่สอง เมื่อมีเหตุการณ์เกิดขึ้นและเงื่อนไขของเหตุการณ์นั้นถูกต้อง องค์ประกอบของการเปลี่ยนแปลงมีดังนี้

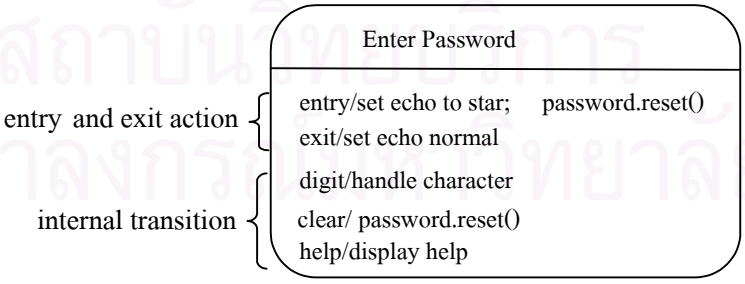
1. สถานะต้น (Source State) เป็นสถานะที่การเปลี่ยนแปลงเริ่มเกิดขึ้น โดยที่วัตถุจะรับเหตุการณ์และเงื่อนไขของเหตุการณ์

2. เหตุการณ์ เป็นเหตุการณ์ที่รับโดยสถานะต้น ถ้าเงื่อนไขของเหตุการณ์เป็นจริงจะทำให้เกิดการเปลี่ยนแปลงสถานะ บางครั้งเหตุการณ์อาจจะมีพารามิเตอร์ส่งมาพร้อมกับเหตุการณ์ก็ได้ ตัวอย่างของเหตุการณ์ในรูปที่ 2.15 ประกอบเหตุการณ์ receive order approved และ rejected

3. เงื่อนไข (Guard Condition) เป็นนิพจน์บูลีน จะถูกตรวจสอบเพียงครั้งเดียวเมื่อสถานะได้รับเหตุการณ์ ถ้าตรวจสอบแล้วเงื่อนไขเป็นจริงการเปลี่ยนแปลงสถานะก็จะเกิดขึ้น แต่ถ้าไม่เป็นจริง การเปลี่ยนแปลงสถานะก็ไม่เกิดขึ้น ตัวอย่างเช่น จากรูปที่ 2.15 ถ้าสถานะ Waiting ได้รับเหตุการณ์ receive order โดยที่มีเงื่อนไขคือ amount > $25 ถ้าเงื่อนไขนี้เป็นจริง จะเกิดการเปลี่ยนแปลงสถานะไปเป็นสถานะ Confirm Credit

4. การกระทำ (Action) เป็นกิจกรรมที่จะถูกทำงานเมื่อเกิดการเปลี่ยนแปลงสถานะขึ้น อาจจะเป็นการทำงานตามคำสั่ง (Operation) ของการเรียก (Call) การสร้างหรือการทำลายวัตถุ หรือการส่งสัญญาณไปยังวัตถุ จากรูปที่ 2.15 การกระทำที่เกิดขึ้นเมื่อวัตถุเปลี่ยนแปลงสถานะจากสถานะ Confirm Credit ไปเป็น Process Order คือการกระทำ debit account()

5. สถานะปลายทาง (Target state) เป็นสถานะที่เกิดภายหลังจากการเปลี่ยนแปลงเสร็จสมบูรณ์



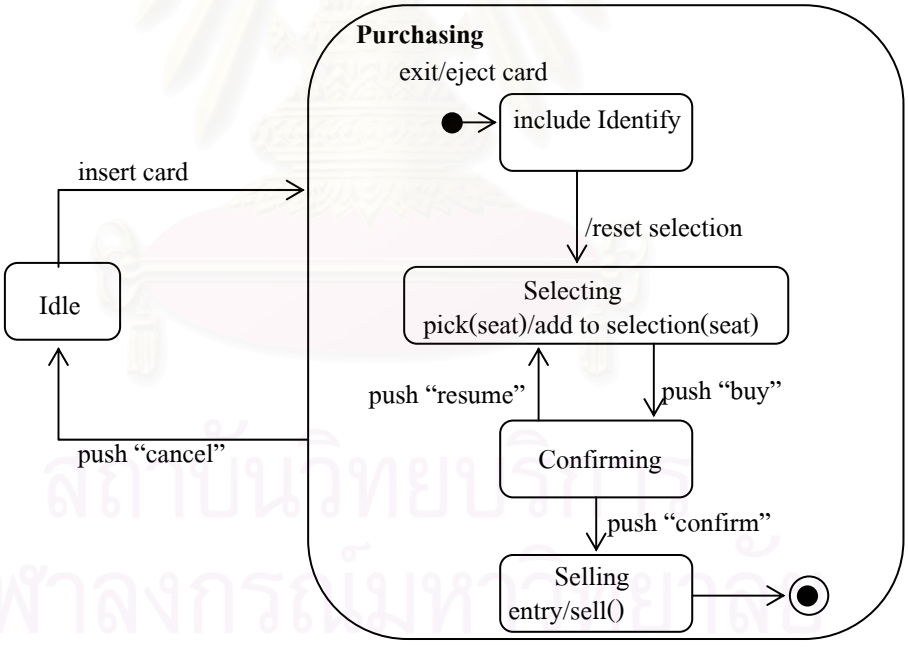
รูปที่ 2.16 การกระทำเมื่อเข้าและออกจากสถานะ และการเปลี่ยนแปลงภายใน [6]

การกระทำเมื่อเข้าสู่สถานะและออกจากสถานะ ในบางกรณีการออกแบบแบบจำลองต้องการให้เกิดการกระทำเมื่อเริ่มต้นเข้าสู่สถานะและออกจากสถานะ โดยไม่ต้องมีการเปลี่ยนแปลงใดๆ บอกให้ทำงาน การแสดงการกระทำเมื่อเข้าสู่สถานะและออกจากสถานะ จะเขียน

เป็นข้อความภายในสถานะ โดยการกระทำเมื่อเข้าสู่สถานะใช้ไวยากรณ์ *entry/action* สำหรับการกระทำเมื่อออกจากสถานะ จะใช้ไวยากรณ์ *exit/action* ตัวอย่างเช่นในรูปที่ 2.16 การกระทำเมื่อเข้าสู่สถานะคือ set echo to star; password.reset() และการกระทำเมื่อออกจากสถานะคือ set echo normal

การเปลี่ยนแปลงภายในสถานะ (Internal Transition) เป็นการเปลี่ยนแปลงภายในสถานะใด สถานะหนึ่งเท่านั้น ไม่มีสถานะปลาย การทำงานเหมือนกับการเปลี่ยนแปลงสถานะทั่วไป แต่จะไม่ทำให้สถานะเปลี่ยน การใช้งานการเปลี่ยนแปลงภายในจะเหมาะสำหรับการกระทำการขัดจังหวะการทำงาน (Interrupt) ตัวอย่างเช่น ในรูปที่ 2.16 มีการเปลี่ยนแปลงภายในสถานะ เช่น digit/handle character

สถานะย่อย เป็นสถานะที่อยู่ในสถานะใดๆ เพื่ออธิบายสถานะต่างๆ ที่เกิดขึ้นภายในสถานะหนึ่ง สถานะย่อยจะมีสถานะเริ่มต้นและสิ้นสุดของมันเอง และส่วนประกอบอื่นๆ เหมือนกับสถานะที่กล่าวมาแทบทั้งสิ้น ตัวอย่างเช่น ในรูปที่ 2.17 จะประกอบด้วยสถานะหลัก คือ Idle และ Purchasing ภายในสถานะ Purchasing จะประกอบด้วยสถานะย่อย ทั้งหมด 4 สถานะย่อย คือ include Identify Selection Confirming และ Selling



รูปที่ 2.17 ตัวอย่างสถานะย่อย [6]

สถานะประวัติ (History state) เป็นสถานะเทียม (Psudostate) ที่เก็บการทำงานครั้งหลังสุดภายในสถานะ จะแสดงด้วยสัญลักษณ์ Ⓗ

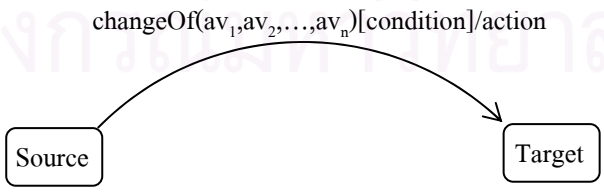
2.2.4 การเพิ่มเติมแผนภาพสเตทชาร์ตเพื่อให้เหมาะสำหรับแสดงพฤติกรรมของระบบวัตถุพร้อมทำงาน

ลักษณะของวัตถุพร้อมทำงานมีความแตกต่างจากวัตถุทั่วไป คือ (1) วัตถุพร้อมทำงานจะรวมข้อมูล (Data) พฤติกรรม (Behavior) และตัวควบคุม (Control) ไว้ในตัวเอง (2) การทำงานของวัตถุจะทำงานทุกครั้งเมื่อค่าของตัวแปรพร้อมทำงาน (Active Variable) เปลี่ยนแปลง แผนภาพสเตทชาร์ตของยูเอ็มแอล (UML statechart diagram) ใช้อธิบายพฤติกรรมของวัตถุแต่ไม่สามารถที่จะอธิบายพฤติกรรมของวัตถุพร้อมทำงานได้อย่างสมบูรณ์ [7] เนื่องจากไม่มีสัญลักษณ์ที่อธิบายเหตุการณ์การเปลี่ยนแปลงค่าแอตทริบิวต์ ซึ่งหมายถึงการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน สัญลักษณ์เกี่ยวกับเหตุการณ์เกิดขึ้นตามเวลา (Time Events) ที่มีอยู่เดิมไม่สามารถที่อธิบายพฤติกรรมของวัตถุพร้อมทำงานได้อย่างสมบูรณ์ และแผนภาพสเตทชาร์ตของยูเอ็มแอล ไม่สนับสนุนการกระทำที่เกิดขึ้นในอนาคต (Future Actions) ของวัตถุพร้อมทำงาน

วุฒิพงษ์ เรือนทอง และคณะ ได้นำเสนอแผนภาพสเตทชาร์ตที่เพิ่มเติมเพื่อให้เหมาะสมสำหรับแสดงพฤติกรรมของระบบวัตถุพร้อมทำงานว่า “แผนภาพสเตทชาร์ตแบบเพิ่มเติม” ดังรายละเอียดดังต่อไปนี้

2.2.4.1 สัญลักษณ์เกี่ยวกับเหตุการณ์การเปลี่ยนแปลง

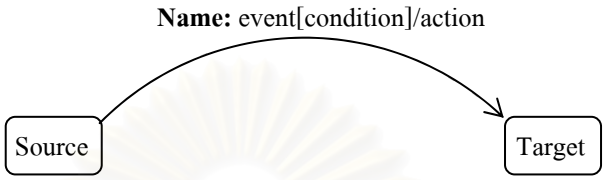
สำหรับแผนภาพสเตทชาร์ตของยูเอ็มแอลจะมี *when(Boolean expression)* เพื่อแสดงพฤติกรรมเหตุการณ์การเปลี่ยนแปลงสำหรับวัตถุประเภทพาสซีฟ แต่สำหรับวัตถุพร้อมทำงานจะทำงานเมื่อค่าของตัวแปรพร้อมทำงานเปลี่ยนแปลงค่า ดังนั้นจึงใช้สัญลักษณ์ *changeOf(av_1, av_2,...,av_n)* [7] แทน จากรูปที่ 2.18 เมื่อค่าของตัวแปรพร้อมทำงาน av_1,av_2,...,av_n ตัวใดตัวหนึ่งเปลี่ยนแปลงค่า และเงื่อนไข condition เป็นจริงสถานะของวัตถุนี้จะเปลี่ยนแปลงจากสถานะ Source เป็นสถานะ Target และการกระทำ action จะทำงานทันที



รูปที่ 2.18 สัญลักษณ์แสดงเหตุการณ์การเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน [7]

2.2.4.2 สัญลักษณ์เกี่ยวกับเหตุการณ์ที่เกิดขึ้นตามเวลา

ใช้เพื่อการอ้างอิงถึงการเปลี่ยนแปลงสถานะได้ง่ายขึ้น งานวิจัยของวุฒิพงษ์จึงเพิ่มเติมการกำหนดชื่อของการเปลี่ยนแปลง (Transition-name) เข้าไปในแผนภาพ ดังแสดงในรูปที่ 2.19 ซึ่งการกำหนดชื่อเปลี่ยนแปลงนี้จะมีหรือไม่มีก็ได้ และควรกำหนดชื่อให้กับการเปลี่ยนแปลงที่เป็นการเปลี่ยนแปลงขึ้นกับเวลา



รูปที่ 2.19 รูปแบบการกำหนดชื่อการเปลี่ยนแปลงสถานะ [7]

การเพิ่มเติมสัญลักษณ์เกี่ยวกับเหตุการณ์เกิดขึ้นตามเวลาคือ $after(\{t_1,t_2,...,t_n\}_{opt},time,\{r_1,r_2,...,r_n\}_{opt})$ [7] โดยที่ $\{t_1,t_2,...,t_n\}$ เป็นเซตของการเปลี่ยนแปลงทริกเกอร์ (trigger-transition) *time* คือเวลาที่กำหนดเพื่อให้เกิดการเปลี่ยนแปลง $\{r_1,r_2,..,r_n\}$ เป็นเซตของการเปลี่ยนแปลงที่ถูกยกเลิก

2.2.4.3 สัญลักษณ์ของกิจกรรมในอนาคต

การเรียกใช้ฟังก์ชันล่วงหน้า และการกำหนดค่าล่วงหน้า เป็นกิจกรรมที่เกิดขึ้นในอนาคต โดยที่การทำงานที่กำหนดให้เกิดขึ้นหลังจากที่เวลาหน่วงที่กำหนด (Delay Time) ผ่านไป สำหรับแผนภาพสเตทชาร์ตของยูเอ็มแอลจะไม่มีสัญลักษณ์ที่กำหนดพฤติกรรมเหล่านี้ ดังนั้น งานวิจัยของวุฒิพงษ์ จึงเพิ่มเติมสัญลักษณ์แสดงการเรียกใช้ล่วงหน้า และการกำหนดล่วงหน้าดังนี้

- การเรียกใช้ฟังก์ชันล่วงหน้า ใช้สัญลักษณ์

FCall(d,f)

โดยที่ d คือระยะเวลา

f คือฟังก์ชันที่ต้องการเรียกใช้

- การกำหนดค่าล่วงหน้า ใช้สัญลักษณ์

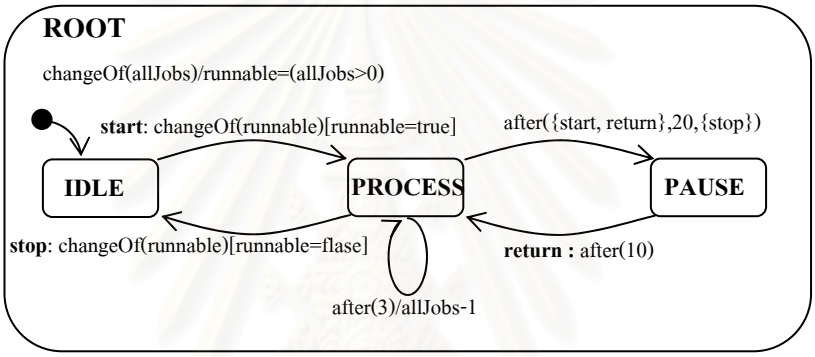
FAssign(d, var, val)

โดยที่ d คือระยะเวลา

var คือตัวแปรที่จะถูกกำหนดค่าให้

val คือค่าที่จะกำหนดให้กับตัวแปร

ตัวอย่างในรูปที่ 2.20 เป็นตัวอย่างการใช้แผนภาพสเตทชาร์ตแบบเพิ่มเติม การเปลี่ยนแปลง start เป็นการเปลี่ยนสถานะจากสถานะ IDLE เป็นสถานะ PROCESS จะขึ้นอยู่กับค่าของตัวแปรพร้อมทำงาน runnable ถ้าค่าของตัวแปรพร้อมทำงาน runnable เป็น true การเปลี่ยนแปลง stop เป็นการเปลี่ยนสถานะจากสถานะ PROCESS เป็นสถานะ IDLE ซึ่งขึ้นอยู่กับค่าของตัวแปรพร้อมทำงาน runnable ถ้าตัวแปรพร้อมทำงาน runnable มีค่าเป็น false การเปลี่ยนสถานะจากสถานะ PROCESS เป็นสถานะ PAUSE จะเกิดขึ้นเมื่อเกิดการเปลี่ยนแปลง start หรือ return แล้ว 20 หน่วยเวลา และจะมีผลให้ยกเลิกการเปลี่ยนแปลง stop ด้วย การเปลี่ยนแปลง return คือการเปลี่ยนสถานะจากสถานะ PAUSE ไปเป็นสถานะ PROCESS หมายถึงถ้าวัตถุอยู่ในสถานะ PAUSE 10 หน่วยเวลาแล้ว จะเกิดการเปลี่ยนแปลง return ทันที



รูปที่ 2.20 ตัวอย่างแผนภาพสเตทชาร์ตแบบเพิ่มเติม [7]

2.3 การพิสูจน์ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์

ในปัจจุบันมีวิธีการเชิงวัตถุ (Object-Oriented Methodology) สำหรับพัฒนาระบบที่มีขนาดใหญ่และมีความซับซ้อนจำนวนมาก ในวิธีการเหล่านั้น การวิเคราะห์เป็นกระบวนการแรกที่จะต้องทำ หลังจากนั้นจึงนำผลการวิเคราะห์ไปใช้ในขั้นตอนการออกแบบและการเขียนโปรแกรม ในกระบวนการวิเคราะห์ ผู้พัฒนาจะสร้างแบบจำลองการวิเคราะห์ขึ้นเพื่อแสดงภาพต่างๆ ของระบบ เช่น พฤติกรรมของระบบ เป็นต้น ถ้าผู้พัฒนาไม่มีการตรวจสอบและทำให้การวิเคราะห์นั้นถูกต้องก่อน จะมีผลกระทบต่อระบบที่สร้างขึ้นคืออาจจะมีข้อผิดพลาดแทรกอยู่ก็ได้ และทำให้ผู้พัฒนาอาจจะต้องวิเคราะห์และออกแบบหลาย ๆ รอบ เพื่อแก้ไขข้อผิดพลาดในการวิเคราะห์และการออกแบบนั้น ๆ ซึ่งทำให้เสียเวลาเพิ่มขึ้น ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องมีการตรวจสอบความถูกต้องของการวิเคราะห์ก่อนที่จะให้แบบจำลองการวิเคราะห์นั้นผ่านไปยังกระบวนการต่อ ๆ ไป

ในหัวข้อนี้จะอธิบายถึงรายละเอียดของระบบแอกเซียมและการพิสูจน์เชิงคณิตศาสตร์ และงานวิจัยที่เกี่ยวข้องกับการทวนสอบหรือตรวจสอบความถูกต้องแบบจำลองการวิเคราะห์ มีรายละเอียดดังต่อไปนี้

2.3.1 ระบบแอกเซียมเมติกและการพิสูจน์เชิงคณิตศาสตร์ [8]

ในหัวข้อนี้จะอธิบายแอกเซียม กฎการอนุมาน และการพิสูจน์ ดังนี้

2.3.1.1 แอกเซียม

แอกเซียม (axiom) เป็นความจริง กฎหรือสูตรที่แน่นอน ตัวอย่างเช่นทฤษฎีหนึ่งอาจจะประกอบด้วยแอกเซียม

A_0

$$\vdash 0 < 0'$$

ความหมายของ $'$ คือค่าตัวเลขถัดไปของจำนวนเต็มนั้นๆ (Successor Operation) ดังนั้น แอกเซียมข้างต้น จะหมายความว่าศูนย์ (0) มีค่าน้อยกว่าตัวเลขที่ถัดไป หรือหมายถึงเลข 1 นั่นเอง

2.3.1.2 กฎการอนุมาน

กฎการอนุมาน (Inference Rules) เป็นเครื่องมือสำหรับการพิสูจน์หรือการได้มาซึ่งทฤษฎีบทใหม่ (Theorem) จากทฤษฎีหรือความจริงอื่นๆ เราจะเขียนในรูปแบบดังนี้

$$\frac{f_1, f_2, ..., f_n}{f_0}$$

ความหมายของกฎอนุมานข้างต้นคือ ถ้า $f_1, f_2, ..., f_n$ เป็นจริงที่พิสูจน์ได้แล้ว f_0 เป็นจริงด้วย สูตรที่อยู่เหนือเส้นตรงแนวนอนนั้นเรียกว่า ข้อเสนอแรกของกฎ (Antecedent of Rule) และสูตรที่อยู่ใต้เส้นเรียกว่า ผลลัพธ์ (Consequent) ตัวอย่างของกฎการอนุมาน เช่น กฎการอนุมานโมดัสโพแนน (Modus Ponens)

MP

$$\frac{p,\ p \rightarrow q}{q}$$

กฎข้างต้นมีความหมายว่า ถ้า $p \rightarrow q$ เป็นจริง และ p เป็นจริง แล้วจะได้ว่า q เป็นจริงด้วย ซึ่งเราสามารถพิสูจน์กฎนี้โดยการใช้ตารางความจริง (Truth Table) ทางตรรกศาสตร์ได้

2.3.1.3 การพิสูจน์ทฤษฎี (Theorem Proving)

วิธีการสำหรับการได้มาซึ่งทฤษฎีใหม่จะเรียกว่า การพิสูจน์ ตามรูปแบบที่แน่นอน ถ้าการพิสูจน์ยึดถือตามรูปแบบอย่างเข้มงวดแล้ว การพิสูจน์นั้นจะสามารถตรวจสอบความถูกต้องได้อย่างมีประสิทธิภาพ

รูปแบบของการพิสูจน์ มีลำดับต่อไปนี้

1. การพิสูจน์ควรเป็นแบบเรียงลำดับทีละบรรทัด
2. กำหนดหมายเลขให้แต่ละบรรทัด (Number)
3. แต่ละบรรทัดประกอบด้วยสูตร (Formula) แอกเซียม หรือความจริงใดๆ ซึ่งสูตรนี้อาจจะเป็นสูตรที่อยู่หลังเครื่องหมาย $\vdash$
4. แต่ละบรรทัดจะบอกชื่อของแอกเซียม เหตุผล ที่มาของสูตร หรือรายการของหมายเลขอ้างอิงที่กำหนดไว้ให้แต่ละบรรทัดจากข้อที่ 2 (Justification)

ตัวอย่างการพิสูจน์ตามรูปแบบการพิสูจน์ข้างต้น กำหนดให้ แอกเซียม A_0 และ $A_{successor}$ และกฎการอนุมาน IND (กฎของการพิสูจน์โดยใช้กรณีเฉพาะ) ดังนี้

A_0

$$\vdash 0 < 0'$$

$A_{successor}$

$$\vdash m < n \rightarrow m' < n'$$

IND

$$\frac{\phi(0),\ \phi(n) \rightarrow \phi(n')}{\phi(n)}$$

จงพิสูจน์กฎต่อไปนี้

$$\vdash i < i'$$

หมายถึง “ทุกๆ จำนวนตัวเลขจะน้อยกว่าตัวถัดไปของตัวเลขนั้น”

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

พิสูจน์ได้ดังนี้

Number	Formula	Justification
M.1	$0 < 0^{'}$	A_0
M.2	$i < i^{'} \rightarrow i^{'} < i^{''}$	$A_{successor}$
M.3	$i < i^{'}$	M.1, M.2, IND

ในบรรทัด M.2 จะเห็นว่าเราให้ i แทน m และ $i^{'}$ แทน n และบรรทัด M.3 ที่เป็นกฎการอนุมานจะแทน $\phi(n)$ ด้วย $i < i^{'}$

2.3.2 การรวมและตรวจสอบความสอดคล้องของแบบจำลองการวิเคราะห์เชิงวัตถุ

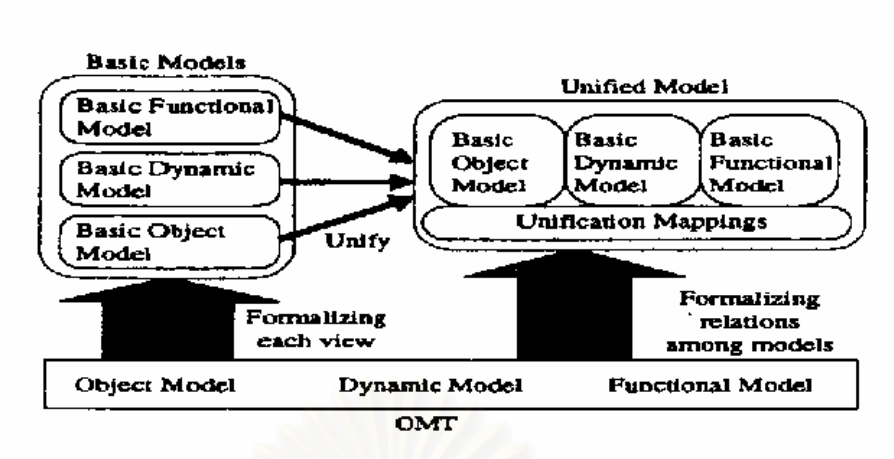
งานวิจัยนี้นำเสนอโดย Toshiaki Aoki และ Takuya Katayama มีจุดประสงค์เพื่อตรวจสอบความถูกต้องของแบบจำลองการวิเคราะห์เชิงวัตถุ [1] สำหรับงานวิจัยนี้ เริ่มจากการแสดงแบบจำลองการวิเคราะห์ด้วย OMT และสร้างแบบจำลองรวม (Unified Model) ขั้นตอนต่อไปคือ เสนอวิธีการพิสูจน์โดยใช้ระบบแอ็กเซียมเมติค โดยพิจารณาจากการไหลของข้อมูล (Dataflow)

2.3.2.1 การรวมแบบจำลองการวิเคราะห์

กระบวนการวิเคราะห์จะใช้แบบจำลอง OMT ซึ่งประกอบด้วย 3 แบบจำลองดังนี้ แบบจำลองวัตถุ (Object Model) แสดงความสัมพันธ์ของเอนทิตี (Entity) แบบจำลองพลวัต (Dynamic Model) แสดงการเปลี่ยนแปลงสถานะ และแบบจำลองฟังก์ชัน (Functional Mmodel) แสดงการไหลข้อมูล การรวมแบบจำลองมีแนวคิดดังแสดงในรูปที่ 2.20 ประกอบด้วย 2 ขั้นตอน คือ

ขั้นตอนที่ 1 สร้างแบบจำลองพื้นฐาน (Basic Model) ซึ่งประกอบด้วยแบบจำลองทั้ง 3 แบบดังกล่าวข้างต้น ซึ่งจะเรียกว่า แบบจำลองวัตถุพื้นฐาน แบบจำลองพลวัตพื้นฐาน และแบบจำลองฟังก์ชันพื้นฐาน (Basic Functional Model) แต่ละแบบจำลองจะประกอบด้วยตัวแปรที่แสดงให้เห็นถึงลักษณะการทำงานบางส่วนของระบบ ความหมายของตัวแปรต่าง ๆ จะถูกอธิบายไว้ในเอกสารของแต่ละแบบจำลอง และมีการใช้เซตอธิบายส่วนประกอบที่ปรากฏอยู่ในแบบจำลอง

ขั้นตอนที่ 2 รวมแบบจำลองพื้นฐานด้วยส่วนประกอบที่ใช้ร่วมกัน (Common Component) ให้เป็นแบบจำลองรวม (Unified Model) ซึ่งจะประกอบด้วยแบบจำลองพื้นฐานและแผนร่างการรวม (Unification Mapping) ที่สัมพันธ์กับส่วนประกอบที่มีอยู่ในแบบจำลองทั้งสาม



รูปที่ 2.21 รูปแบบการรวมแบบจำลอง [1]

2.3.2.2 การตรวจสอบความสอดคล้องระหว่างแบบจำลอง

วิธีตรวจสอบจะใช้แอ็กเซียม ที่ได้จากแบบจำลองพลวัตพื้นฐานที่แสดงการไหลข้อมูลตามระบบจริง และกฎการอนุมาน ซึ่งได้จากความหมายของแบบจำลองการไหลข้อมูล แบบจำลองมีความถูกต้องก็ต่อเมื่อสามารถพิสูจน์ได้ว่า การไหลของข้อมูลทั้งหมดปรากฏอยู่ในแบบจำลองฟังก์ชันพื้นฐานตามระบบแอ็กเซียมที่สร้างขึ้น ผลที่ได้รับจากงานวิจัยนี้คือ แบบจำลองการวิเคราะห์มีความน่าเชื่อถือเพิ่มขึ้น

2.3.3 ระบบแอ็กเซียมเมติคสำหรับการตรวจสอบแบบจำลองการวิเคราะห์เชิงวัตถุ

Takaaki Tateishi Toshiaki Aoki และ Takuya Katayama [3] เสนองานวิจัยนี้ โดยมีจุดประสงค์เพื่อเสนอวิธีการตรวจสอบความถูกต้องสำหรับตรวจสอบแอตทริบิวต์ว่ายังคงมีอยู่หรือยังถูกต้องอยู่ ในแบบจำลองการวิเคราะห์ และเสนอระบบแอ็กเซียมเมติค สำหรับตรวจสอบนี้ วิธีการตรวจสอบใช้การพิสูจน์ทางคณิตศาสตร์โดยใช้กรณีเฉพาะ กับแบบจำลองการเปลี่ยนแปลงสถานะ ตรวจสอบกับแอตทริบิวต์ที่อาจจะมีค่าไม่จำกัดได้

2.3.3.1 การนิยามแบบจำลองการวิเคราะห์และกลยุทธ์การพิสูจน์

1. การนิยามแบบจำลอง

ในการวิเคราะห์เชิงวัตถุ ระบบที่ต้องการวิเคราะห์จะถูกจำลองออกมาด้วยแผนภาพแสดงพฤติกรรมของวัตถุ โดยพฤติกรรมเหล่านี้จะนิยามไว้ในคลาส และวัตถุจะเป็นตัวอย่าง (Instance) ของคลาส สถานะที่เปลี่ยนแปลงไปของวัตถุถูกกำหนดในแบบจำลองการเปลี่ยนแปลงสถานะ

นิยามแบบจำลองการวิเคราะห์ (Analysis Model)

$$(C, O, STD, <, M_b)$$

โดยที่ C เป็นเซตของคลาส

O เป็นเซตของวัตถุ

STD เป็นเซตของแผนภาพการเปลี่ยนแปลงสถานะ

$<$ $= O \times C$

M_b $= C \rightarrow STD$

สัญลักษณ์ $<$ แสดงความสัมพันธ์ระหว่างวัตถุกับคลาส ซึ่งหมายถึงวัตถุเป็นตัวอย่างของคลาส M_b เป็นฟังก์ชันที่มีโดเมนเป็นเซตของคลาส และมีเรนจ์เป็นเซตของ STD แสดงถึงพฤติกรรมของคลาสที่กำหนดด้วย STD

นิยามแผนภาพการเปลี่ยนแปลงสถานะ std

$$std = (S, E_i, E_o, B, A, T, s_0)$$

โดยที่ S เป็นเซตของสถานะ

E_i เป็นเซตของเหตุการณ์ที่ std ส่งไป

E_o เป็นเซตของเหตุการณ์ที่ std รับเข้า

A เป็นเซตของการทำงาน

B เป็นเซตของเงื่อนไข

s_0 เป็นสถานะเริ่มต้น

T เป็นเซตของการเปลี่ยนแปลงสถานะ

วัตถุทำงานร่วมกันกับวัตถุอื่นโดยการสื่อสารกันด้วยการใช้เหตุการณ์ STD ได้นิยามการส่งและรับเหตุการณ์ โดย E_i และ E_o ตามลำดับ

เซตของการเปลี่ยนแปลงสถานะ : T ที่ปรากฏใน STD นิยามได้ดังนี้

$$T \subseteq (S \times E_i \times B \times P(E_o) \times A \times S)$$

โดยที่ $P(E_o)$ เป็นเซตกำลัง (power set) ของ E_o

2. กลยุทธ์การพิสูจน์

วิธีการพิสูจน์ใช้หลักการทางคณิตศาสตร์ คือ การพิสูจน์โดยใช้กรณีเฉพาะ ดังนี้ กำหนดค่าไม่เปลี่ยนแปลง (Invariant) เข้าไปในแต่ละสถานะ จากนั้นเริ่มต้นพิสูจน์จากแต่ละสถานะของวัตถุว่ายังคงมีแอตทริบิวต์หรือไม่ ซึ่งจะเรียกว่า โลคอลแอซเซิร์ทชัน (Local Assertion) โดยใช้การพิสูจน์โดยใช้กรณีเฉพาะ เมื่อแต่ละสถานะถูกยอมรับ จะสรุปได้ว่าทุกสถานะของวัตถุนั้นเป็นจริง เรียกว่าโกลบอลแอซเซิร์ทชัน (Global Assertion)

2.3.3.2 ระบบแอ็กเซียมเมติค

ระบบแอ็กเซียม ทั้งหมดประกอบด้วย นิยามของการเปลี่ยนแปลงสถานะของแต่ละสถานะของวัตถุ (Local Validity Definition : LVALID-DEF) โลคอลอินวาเรียนต์แอกเซียม (Local Invariant Axiom : LIV-AX) ได้จากแต่ละโลคอลแอซเซิร์ทชันที่ถูกต้อง โกลบอลอินวาเรียนต์แอกเซียม (Global Invariant Axiom : GINV-AX) ได้มาจากการพิสูจน์ได้ว่าทุกๆ สถานะของวัตถุยังมีค่าไม่เปลี่ยนแปลงอยู่ อีเว็นต์อินโทรดักชันแอ็กเซียม (Event Introduction Axiom : EINT-AX) แสดงเหตุการณ์ที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงเกิดขึ้น และอีเว็นต์คอมมูนิเคชันแอ็กเซียม (Event Communication Axiom : ECOM-AX) แสดงถึงเหตุการณ์ถูกส่งจากวัตถุหนึ่งและถูกรับโดยวัตถุอื่น

<u>นิยามที่ 1 (LVALID-DEF)</u>

$$\text{VALID obj } P_{s_1}\ P_{s_2}\ \ldots\ P_{s_n} = \bigwedge_i \nu_{t_i}$$

$$\nu_{t_0} = P_{s_1}(\text{initval}_1, \text{initval}_2,\ldots,\text{initval}_m)$$

$$\nu_{t_i} = P_{s_a}(obj.\text{attr}_1(s_a),\ldots,obj.\text{attr}_m(s_a)) \wedge (\text{TransCond}_{ti})$$

$$\Longrightarrow P_{s_b}(f_{i_1}(obj.\text{attr}_1(s_a)),\ldots,f_{i_m}(obj.\text{attr}_m(s_a)))$$

โดยที่ *obj*.attr(s) คือค่าของแอตทริบิวต์ attr ของวัตถุ obj ที่สถานะ s

t_i คือการเปลี่ยนแปลง

f_{i_m} คือการกระทำที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงที่ t_i ซึ่งเปลี่ยนค่า attr_m

s_a และ s_b คือสถานะก่อนและหลังการเปลี่ยนแปลง

TransCond_{ti} คือเงื่อนไข

แอกเซียมที่ 1 (LINV-AX)

$$\vdash \forall obj\ P_{s_1}\ P_{s_2}\ \ldots\ P_{s_n}\ .\ obj < \text{Class}$$
$$\Longrightarrow (\text{Class_VALID}\ obj\ P_{s_1}\ P_{s_2}\ \ldots\ P_{s_n}$$
$$\Longrightarrow (\underset{i=1,2,\ldots,n}{\wedge} P_{s_i}\ (obj.\text{attr}_1(s_i),\ldots,obj.\text{attr}_m(s_i))))$$

LINV-AX หมายถึง สำหรับทุกวัตถุ *obj* ที่เป็นตัวอย่างของคลาส *Class* ถ้า Class_VALID มีเป็นจริงแล้วเราสามารถเขียนในรูป $(\underset{i=1,2,\ldots,n}{\wedge} P_{s_i}\ (obj.\text{attr}_1(s_i),\ldots,obj.\text{attr}_m(s_i)))$ ได้

แอกเซียมที่ 2 (GINV-AX)

$$\vdash \forall obj\ .\ obj < \text{Class}$$
$$\Longrightarrow ((\underset{i=1,2,\ldots,n}{\wedge} G(obj.\text{attr}_1(s_i),\ldots,obj.\text{attr}_m(s_i)))$$
$$\Longrightarrow (\forall s.\ G(obj.\text{attr}_1(s),\ldots,obj.\text{attr}_m(s))))$$

GINV-AX หมายถึง สำหรับทุกวัตถุ *obj* ที่เป็นตัวอย่างของคลาส *Class* ถ้าทุกๆ การเปลี่ยนแปลง ของทุกสถานะในวัตถุนั้นเป็นจริงแล้ว เราสามารถเขียนในรูป $(\forall s.\ G(obj.\text{attr}_1(s),\ldots,obj.\text{attr}_m(s)))$ ได้

แอกเซียมที่ 3 (EINT-AX)

$$\vdash \forall obj\ .\ obj < \text{Class}$$
$$\Longrightarrow ((obj \downarrow_s e) \wedge \text{TransCond}$$
$$\Longrightarrow (obj \uparrow_{s'} e'_1 \ldots obj \uparrow_{s'} e'_n)))$$

โดยที่ $obj \downarrow_s e$ หมายถึงวัตถุ obj ได้รับเหตการณ์ e ที่สถานะ s

$obj \uparrow_{s'} e'_1 \ldots obj \uparrow_{s'} e'_n$ หมายถึงวัตถุ obj ส่งเหตุการณ์ $e'_1 \ldots e'_n$ ที่สถานะ s'

EINT-AX หมายถึง สำหรับทุกวัตถุ *obj* ที่เป็นตัวอย่างของคลาส *Class* แล้ว ถ้าวัตถุ *obj* ได้รับเหตุการณ์ *e* ที่สถานะ *s* และเงื่อนไข *TransCond* เป็นจริง แล้ววัตถุนั้นจะส่งเหตุการณ์ $e'_1 \ldots e'_n$ ออกไปจากสถานะ s'

แอกเซียมที่ 4 (ECOM-AX)

$$\vdash \forall obj_1\ obj_2\ .\ obj_1 \gtrless obj_2$$
$$\Longrightarrow (\forall P.\ (obj_1 \uparrow_s e) \wedge P(a_1,a_2,\ldots,a_n))$$
$$\Longrightarrow (obj_2 \downarrow_{s'} e) \wedge P(b_1,b_2,\ldots,b_n)))$$

โดยที่ $a_1,a_2,\ldots,a_n$ หมายถึงแอตทริบิวต์ที่ส่งออกไป

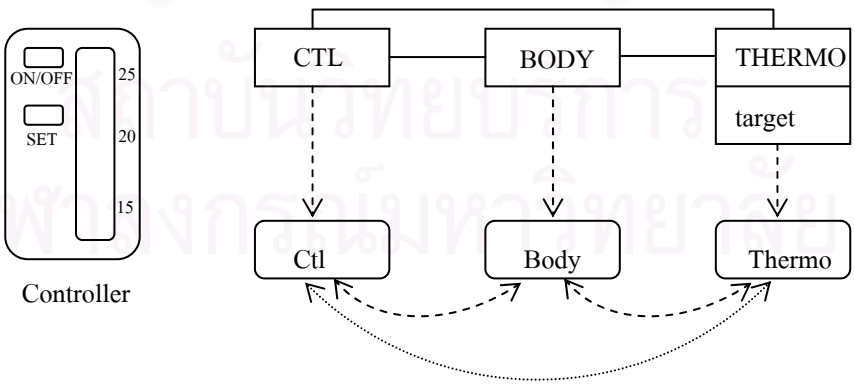
$b_1,b_2,\ldots,b_n$ หมายถึงแอตทริบิวต์ที่ถูกรับเข้า

ECOM-AX หมายถึง สำหรับทุกๆ วัตถุ obj_1 และ obj_2 ซึ่งทั้งสองวัตถุติดต่อกัน (><) ถ้าวัตถุ obj_1 ส่งเหตุการณ์ e ออกจากสถานะ s พร้อมด้วยแอตทริบิวต์ $a_1,a_2,\ldots,a_n$ แล้ววัตถุ obj_2 จะรับเหตุการณ์นั้นที่สถานะ s' ด้วยแอตทริบิวต์ $b_1,b_2,\ldots,b_n$

การตรวจสอบความถูกต้องโดยการใช้ระบบแอ็กเซียมเมติค จะเป็นการตรวจสอบแอตทริบิวต์ที่มีอยู่ในระบบเป้าหมาย ซึ่งแอตทริบิวต์เหล่านั้นจะปรากฏอยู่ในแบบจำลองการเปลี่ยนแปลงสถานะ การตรวจสอบจะเริ่มต้นด้วยการกำหนดค่าคงที่ให้กับแอตทริบิวต์ที่ต้องการตรวจสอบ ในทุกๆ สถานะของแบบจำลองการเปลี่ยนแปลงสถานะของวัตถุ จากนั้นก็นำข้อมูลที่อยู่ในแบบจำลองการแปลี่ยนแปลงสถานะมาสร้างการนิยาม และระบบแอ็กเซียมเมติค หลังจากนั้นก็พิสูจน์ความถูกต้องของโลคอลอินวาเรียนต์ก่อน ถ้าเป็นจริง ขั้นสุดท้ายคือ การพิสูจน์โกลบอลอินวาร์เรียนต์

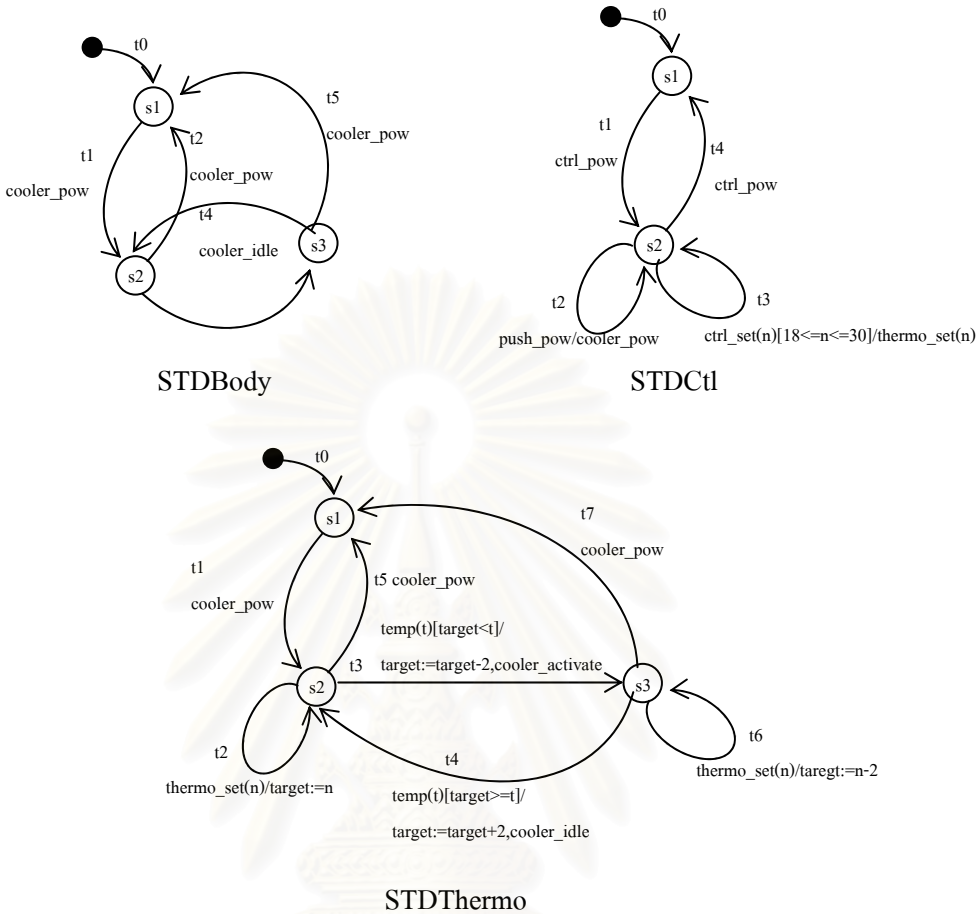
2.3.3.3 ตัวอย่างการทวนสอบแบบจำลองการวิเคราะห์

งานวิจัยของ Takaaki Tateishi Toshiaki Aoki และ Takuya Katayama ได้เสนอตัวอย่างการทวนสอบแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศขนาดเล็ก [3] ซึ่งระบบนี้ประกอบด้วยตัวควบคุม (Controller) เครื่องวัดอุณหภูมิ (Thermostat) และตัวเครื่องปรับอากาศ (Body) ผู้ใช้สามารถเปิดและปิดเครื่องปรับอากาศได้ และกำหนดอุณหภูมิที่ต้องการได้ จากรูปที่ 2.22 จะเห็นว่าระบบเครื่องปรับอากาศขนาดเล็กประกอบด้วยคลาส CTL BODY และ THERMO โดยที่คลาส THERMO มีแอตทริบิวต์ target วัตถุ Ctl Body และ Thermo เป็นตัวอย่างของคลาส CTL BODY และ THERMO ตามลำดับ ผู้ใช้สามารถเปิดและปิดเครื่องปรับอากาศ และกำหนดอุณหภูมิที่ต้องการได้โดยใช้ตัวควบคุม



รูปที่ 2.22 ตัวควบคุม แผนภาพคลาสและแผนภาพวัตถุของระบบ [3]

พฤติกรรมของวัตถุ Ctl Body และ Thermo แสดงด้วยแผนภาพการเปลี่ยนแปลงสถานะ STDCtl STDBody และ STDThermo ตามลำดับ ดังแสดงในรูปที่ 2.23



รูปที่ 2.23 แผนภาพการเปลี่ยนแปลงสถานะของระบบเครื่องปรับอากาศขนาดเล็ก [3]

จากรูปที่ 2.23 ถ้าผู้ใช้กดปุ่มเปิดเครื่องปรับอากาศ เหตุการณ์ ctl_pow จะถูกสร้างขึ้นในวัตถุ Ctl และวัตถุ Body จะรับเหตุการณ์ ctl_pow และเครื่องปรับอากาศจะเริ่มทำงาน ถ้าผู้ใช้กดปุ่มกำหนดอุณหภูมิของเครื่องปรับอากาศ เหตุการณ์ set_target พร้อมด้วยแอตทริบิวต์ n จะเกิดขึ้น ค่าของ n จะแสดงถึงอุณหภูมิที่ต้องการกำหนด เหตุการณ์ set_target จะถูกรับโดยวัตถุ Thermo และจะพยายามปรับอุณหภูมิให้เท่ากับอุณหภูมิที่ผู้ใช้กำหนด

การทวนสอบแบบจำลองการวิเคราะห์ของระบบเครื่องปรับอากาศขนาดเล็ก

การทวนสอบแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศขนาดเล็ก เริ่มต้นด้วยการกำหนดเป้าหมายของการทวนสอบคือ อุณหภูมิเป้าหมายต้องน้อยกว่า 30 องศาเสมอ หรือเขียนในรูปนิพจน์ได้ดังนี้

$$\forall s.\ \text{thermo.target}(s) \leq 30$$

กำหนดสมมติฐานของแบบจำลองการวิเคราะห์ของระบบเครื่องปรับอากาศขนาดเล็ก ดังนี้

ASSUMS = $\{a_1, a_2, a_3, a_4, a_5, a_6\}$

โดยที่ $a_1 = \forall$s. thermo $\downarrow$s temp หมายถึงทุกๆ สถานะของวัตถุ Thermo จะรับอุณหภูมิ temp

$a_2 = \forall$s. ctl $\downarrow$s push_pow หมายถึงทุกๆ สถานะของวัตถุ Ctl จะรับ push_pow

$a_3 = \forall$s. ctl $\downarrow$s ctrl_set หมายถึงทุกๆ สถานะของวัตถุ Ctl จะรับเหตุการณ์ ctrl_set

a_4 = Ctl >< Body หมายถึงวัตถุ Ctl เชื่อมต่อวัตถุ Body จริง

a_5 = Body >< Thermo หมายถึงวัตถุ Body เชื่อมต่อกับวัตถุ Thermo จริง

a_6 = Thermo >< Ctl หมายถึงวัตถุ Thermo เชื่อมต่อกับวัตถุ Ctl จริง

อันดับแรก กำหนดโลคอลแอซเซิร์ทชัน $P_{s_1}\ P_{s_2}\ P_{s_3}$ ให้กับสถานะ s_1 s_2 และ s_3 ตามลำดับ ดังนี้

$P_{s_1}(x) = x \leq 30$

$P_{s_2}(x) = x \leq 30$

$P_{s_3}(x) = x \leq 28$

ระบบแอกเซียมเมติคของระบบเครื่องปรับอากาศขนาดเล็กเป็นการนำข้อมูลของแบบจำลองการวิเคราะห์มาเขียนในแอกเซียมต่างๆ ที่อธิบายในหัวข้อที่ 2.3.3.2 ระบบแอกเซียมเมติคมีรายละเอียดดังแสดงใน A1, A2, A3, A4 และ D1

สำหรับการพิสูจน์ว่าคุณสมบัติที่สนใจ ยังมีค่าถูกต้องในสถานะใดๆ หรือไม่ การพิสูจน์ว่า $P_{s_1}\ P_{s_2}\ P_{s_3}$ เป็นโลคอลอินวาเรียนต์ จะแสดงด้วยการพิสูจน์ว่า $\nu_{t_0}, \nu_{t_1}, \ldots, \nu_{t_7}$ ถูกต้อง การพิสูจน์ ν_{t_3} และ ν_{t_6} แสดงด้วย P1 และ P2 ตามลำดับ จากนั้นจะพิสูจน์โกบอลอินวาเรียนต์ ซึ่งแสดงด้วย P3 สรุปได้ว่า P(thermo.target) มีค่าถูกต้องทุกๆ สถานะ หมายถึง ทุกๆ สถานะ อุณหภูมิเป้าหมายมีค่าน้อยกว่า 30 องศา จริง

A1 (LINV-AX)

$\forall obj\ .\ P_{s_1}\ P_{s_2}\ P_{s_3}\ .\ obj \lhd$ Thermo

$\Longrightarrow$ (Thermo_VALID $obj\ P_{s_1}\ P_{s_2}\ P_{s_3}$

$\Longrightarrow$ ($\underset{i=1,2,3}{\Lambda} P_{s_i\ i}(obj$.target(STDThermo.$s_i$))))

A1(LINV-AX) แสดงแอกเซียมโลคอลอินวาร์เรียนต์ ซึ่งมีความหมายคือ สำหรับทุกวัตถุ obj ที่เป็นตัวอย่างของคลาส THERMO ถ้า Thermo_VALID เป็นจริงแล้วจะสามารถเขียนให้อยู่ในรูป ($\underset{i=1,2,3}{\Lambda} P_{s_i}$ (*obj*.target(STDThermo.s_i)) ได้

D1 (VALID-DEF)

Thermo_VALID thermo $P_{s_1}\ P_{s_2}\ P_{s_3} = \underset{i=0,\ldots,7}{\Lambda} \upsilon_{ti}$

$\upsilon_{t4} = P_{s_3}$ (thermo.target(STDThermo.s_3)) $\wedge$ (thermo $\downarrow_{\text{STDThermo.s3}}$ temp)
$\wedge$((thermo.target(STDThermo.s_3)) $\geq$ (temp.t)
$\Longrightarrow P_{s_2}$ (thermo.target(STDThermo.s_3) + 2)

$\upsilon_{t6} = P_{s_3}$ (thermo.target(STDThermo.s_3)) $\wedge$ (thermo $\downarrow_{\text{STDThermo.s3}}$ thermo_set)
$\Longrightarrow P_{s_3}$ (thermo_set.n - 2)

D1(VALID-DEF) เป็นการตรวจสอบความถูกต้องของแต่ละการเปลี่ยนแปลงสถานะ จากตัวอย่างข้างต้น υ_{t4} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_4 ซึ่งเป็นการเปลี่ยนแปลงสถานะจากสถานะ s_3 ไปเป็นสถานะ s_2 และ υ_{t6} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_6 ซึ่งเป็นการเปลี่ยนแปลงภายในสถานะ s_3

ถ้าทุกการเปลี่ยนแปลงสถานะของวัตถุ thermo ถูกตรวจสอบความถูกต้อง และมีค่าเป็นจริงทั้งหมด จะสรุปได้ว่า Thermo_VALID เป็นจริง

A3 (EINT-AX)

[1] $\forall obj.obj \lhd$ Ctl $\Longrightarrow$ ((*obj* $\downarrow_{\text{STDCtl.s2}}$ push_pow)
$\Longrightarrow$ (*obj* $\uparrow_{\text{STDCtl.s2}}$ cooler_pow))

[2] $\forall obj.obj \lhd$ Ctl $\Longrightarrow$ ((*obj* $\downarrow_{\text{STDCtl.s2}}$ ctrl_set)
$\Longrightarrow$ (*obj* $\uparrow_{\text{STDCtl.s2}}$ thermo_set) $\wedge$ (18 $\leq$ thermo_set.n $\leq$ 30))

A3(EINT-AX) แสดงแอกเซียมอีเวนต์อินโทรดักชัน จากตัวอย่างข้างบน A3(EINT-AX)[1] แสดงให้เห็นว่า ถ้าวัตถุ *obj* ใดๆ ซึ่งเป็นตัวอย่างของคลาส Ctrl ที่สถานะ s_2 ได้รับเหตุการณ์ push_pow จะส่งเหตุการณ์ cooler_pow ออกมา และ A3(EINT-AX)[2] แสดงให้เห็นว่า ถ้าวัตถุ *obj* ใดๆ ซึ่งเป็นตัวอย่างของคลาส Ctrl ที่สถานะ s_2 ได้รับเหตุการณ์ ctrl_set จะส่งเหตุการณ์ thermo_set ออกมาพร้อมกับค่าพารามิเตอร์ n ซึ่งมีค่าอยู่ระหว่าง 18 ถึง 30

A4 (ECOM-AX)

[1] $\forall obj_1\ obj_2\ .\ obj_1 \bowtie obj_2$

$\Rightarrow ((\forall P.(obj_1 \uparrow_{\text{STDCtl.s2}} \text{thermo_set}) \wedge P(\text{thermo_set.n}))$

$\Rightarrow (obj_2 \downarrow_{\text{STDThermo.s3}} \text{thermo_set}) \wedge P(\text{thermo_set.n}))$

[2] $\forall obj_1\ obj_2\ .\ obj_1 \bowtie obj_2$

$\Rightarrow ((\forall P.(obj_1 \uparrow_{\text{STDThermo.s2}} \text{cooler_idle}))$

$\Rightarrow (obj_2 \downarrow_{\text{STDCooler.s3}} \text{cooler_idle}))$

A4(ECOM-AX) แสดงแอกเซียมอีเวนต์คอมมูนิเคชัน จากตัวอย่างข้างต้น A4(ECOM-AX)[1] ถ้าวัตถุ obj_1 และวัตถุ obj_2 มีการติดต่อกัน และวัตถุ obj_1 ที่สถานะ s_2 ส่งเหตุการณ์ thermo_set พร้อมพารามิเตอร์ n ออกมา แล้ววัตถุ obj_2 ที่สถานะ s_3 จะรับเหตุการณ์และพารามิเตอร์ที่ถูกส่งออกมา A4(ECOM-AX)[2] ถ้าวัตถุ obj_1 และวัตถุ obj_2 มีการติดต่อกัน และวัตถุ obj_1 ที่สถานะ s_2 ส่งเหตุการณ์ cooler_idle ออกไป แล้ววัตถุ obj_2 ที่สถานะ s_3 จะรับเหตุการณ์ cooler_idle

P1 เป็นการพิสูจน์ความถูกต้องของการเปลี่ยนแปลงสถานะ t_3

$$\frac{\text{ASSUMS} \vdash \text{T}}{\dfrac{\dfrac{\text{ASSUMS} \vdash ((\text{thermo.target}(\text{STDThermo.s}_1)) \leq 30)}{\Rightarrow ((\text{thermo.target}(\text{STDThermo.s}_2)) - 2 \leq 28)}}{\dfrac{\text{ASSUMS} \vdash P_{s2}(\text{thermo.target}(\text{STDThermo.s}_2))}{\Rightarrow P_{s3}(\text{thermo.target}(\text{STDThermo.s}_2) - 2)}}}{\text{ASSUMS} \vdash \upsilon_{t3}}$$

P2 เป็นการพิสูจน์ความถูกต้องของการเปลี่ยนแปลงสถานะ t_6

$$\frac{\dfrac{\dfrac{\text{ASSUMS} \vdash \text{ASSUMS}}{\text{ASSUMS} \vdash (\text{thermo} \uparrow_{\text{STDCtl.s2}} \text{thermo_set})}\ \text{EINT-AX}}{\wedge (18 \leq \text{thermo_set.n} \leq 30)}}{\dfrac{\text{ASSUMS} \vdash (\text{thermo} \downarrow_{\text{STDCtl.s2}} \text{thermo_set})}{\wedge (18 \leq \text{thermo_set.n} \leq 30)}\ \text{ECOM-AX}}}{\text{ASSUMS} \vdash \upsilon_{t6}}$$

P3 เป็นการพิสูจน์ความถูกต้องของทุกการเปลี่ยนแปลงสถานะของวัตถุ thermo

$$\dfrac{\dfrac{\dfrac{\text{ASSUMS} \vdash \text{T}}{\text{ASSUMS} \vdash \bigwedge_{i=0,\ldots,7} \upsilon_{ti}}}{\begin{array}{l}\text{ASSUMS} \vdash (\text{thermo.target}(\text{STDThermo.s}_1) \leq 30) \\ \qquad\qquad (\text{thermo.target}(\text{STDThermo.s}_2) \leq 30) \\ \qquad\qquad (\text{thermo.target}(\text{STDThermo.s}_3) \leq 28)\end{array}}\ \text{LINV-AX}}{\begin{array}{l}\text{ASSUMS} \vdash \text{thermo.target}(\text{STDThermo.s}_1) \leq 30) \\ \qquad\qquad \wedge (\text{thermo.target}(\text{STDThermo.s}_2) \leq 30) \\ \qquad\qquad \wedge (\text{thermo.target}(\text{STDThermo.s}_3) \leq 30)\end{array}}\ \text{GINV-AX}$$

$$\text{ASSUMS} \vdash \forall s.\text{thermo.target}(s) \leq 30$$

จากการพิสูจน์ข้างต้นจะเห็นว่า เป็นการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ของระบบซึ่งเป็นระบบวัตถุประเภทพาสซีพ สำหรับงานวิจัยนี้จะแสดงการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ระบบวัตถุพร้อมทำงาน ซึ่งมีพฤติกรรมซึ่งแตกต่างจากวัตถุประเภทพาสซีพ โดยบทที่ 3 จะกล่าวถึงรายละเอียดของนิยามและระบบแอกเซียมเมติคของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน บทที่ 4 จะแสดงตัวอย่างการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

2.4 สรุปขั้นตอนการทวนสอบแบบจำลองการวิเคราะห์เชิงวัตถุ

สำหรับขั้นตอนการทวนสอบแบบจำลองการวิเคราะห์เชิงวัตถุ หรือการพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์เชิงวัตถุ ทำตามขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 กำหนดสมมติฐานการพิสูจน์

เมื่อวิเคราะห์ระบบที่ต้องการแล้ว ผู้วิเคราะห์จะต้องนำระบบนั้นๆ มาแสดงรายละเอียดทั้งหมดในรูปแบบของแผนภาพ ซึ่งจะแสดงออกมาด้วยแผนภาพยูสเคส เพื่อแสดงภาพรวมของการทำงานของระบบ จะทำให้ผู้อ่านแผนภาพเข้าใจการทำงานของทั้งระบบได้ง่ายขึ้น แผนภาพคลาส เพื่อแสดงความสัมพันธ์ของคลาสทั้งหมดที่มีอยู่ในระบบ และแผนภาพแสดงพฤติกรรม เพื่อแสดงพฤติกรรมของแต่ละวัตถุพร้อมทำงานซึ่งเป็นตัวอย่างของคลาสในแผนภาพคลาส

เมื่อได้แผนภาพทั้งหมดแล้ว ก่อนการพิสูจน์ว่าระบบที่วิเคราะห์มานั้นถูกต้องหรือไม่ จะต้องกำหนดสมมติฐานของการพิสูจน์ก่อน ว่าจะพิสูจน์อะไร ตัวอย่างเช่น ระบบเครื่องปรับอากาศ อาจจะตั้งสมมติฐานว่า อุณหภูมิของเครื่องปรับอากาศจะต้องไม่เกิน 30 องศา ระบบลิฟต์ของตึก 20 ชั้น อาจจะตั้งสมมติฐานว่า ลิฟต์จะต้องเลื่อนขึ้นและลงได้อยู่ระหว่างชั้นที่ 1 ถึง 20 เท่านั้น หรือระบบคิว ที่กำหนดให้คิวเป็นสแตก (stack) จำนวน 20 สแตก สมมติฐานสำหรับพิสูจน์การออกแบบอาจจะเป็น ระบบคิวจะต้องมีจำนวนงานไม่เกิน 20 งานในคิว เป็นต้น

ขั้นตอนที่ 2 เพิ่มเติมพฤติกรรมของวัตถุ

หลังจากการกำหนดสมมติฐานการพิสูจน์แล้ว ผู้พิสูจน์อาจจะกำหนดกฎเกณฑ์อื่นๆ เพิ่มเติมเข้ามานอกเหนือจากพฤติกรรมของวัตถุที่กำหนดในแผนภาพแสดงพฤติกรรมก็ได้ ซึ่งจะกำหนดไว้ใน ASSUMS โดยที่ ASSUMS จะนิยามเป็นเซตของกิจกรรมต่างๆ ตัวอย่างเช่น

$$\mathbf{ASSUMS = \{a_1, a_2\}}$$

$$a_1 = obj_1 \uparrow_s event_1$$

$$a_2 = obj_1 \downarrow_s event_2$$

ถ้าแผนภาพแสดงพฤติกรรมไม่ได้ระบุการรับและส่งเหตุการณ์บางเหตุการณ์เอาไว้ อาจจะกำหนดเพิ่มเติมเพื่อให้เกิดความหมายที่ชัดเจนขึ้น

ขั้นตอนที่ 3 เขียนระบบแอกเซียมเมติคของระบบที่วิเคราะห์

จากแบบจำลองการวิเคราะห์ระบบในขั้นตอนที่ 1 เราจะนำข้อมูลจากแผนภาพแสดงพฤติกรรมของวัตถุมาเขียนลงในระบบแอกเซียมเมติที่มีอยู่

ขั้นตอนที่ 4 ทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

ก่อนการพิสูจน์ความถูกต้องของแต่ละการเปลี่ยนแปลงสถานะของวัตถุ จะกำหนดโลคอลแอซเซิร์ทชัน P_{s_i} ให้แต่ละสถานะของวัตถุที่เปลี่ยนแปลงแอตทริบิวต์ที่สนใจได้ เช่น กำหนดว่า ค่าของแอตทริบิวต์ที่สนใจ ในสถานะ s_1 จะมีค่าไม่เกิน 10 อาจจะเขียนได้ดังนี้

$$P_1(x) = x \leq 10$$

$P(x)$ หมายถึงการพิจารณาค่าของ x ในที่นี้ x จะหมายถึงแอตทริบิวต์ที่สนใจนั่นเอง แอซเซิร์ทชันข้างบน หมายถึงค่าของแอตทริบิวต์ที่สนใจในสถานะที่ s_1 มีค่าไม่เกิน 10

การทวนสอบแบบจำลองการวิเคราะห์เชิงวัตถุ จะใช้วิธีการพิสูจน์ทฤษฎี เพื่อสรุปให้ได้ว่าแต่ละการเปลี่ยนแปลงสถานะของทุกสถานะในวัตถุนั้นๆ ถูกต้องตามสมมติฐานหรือไม่

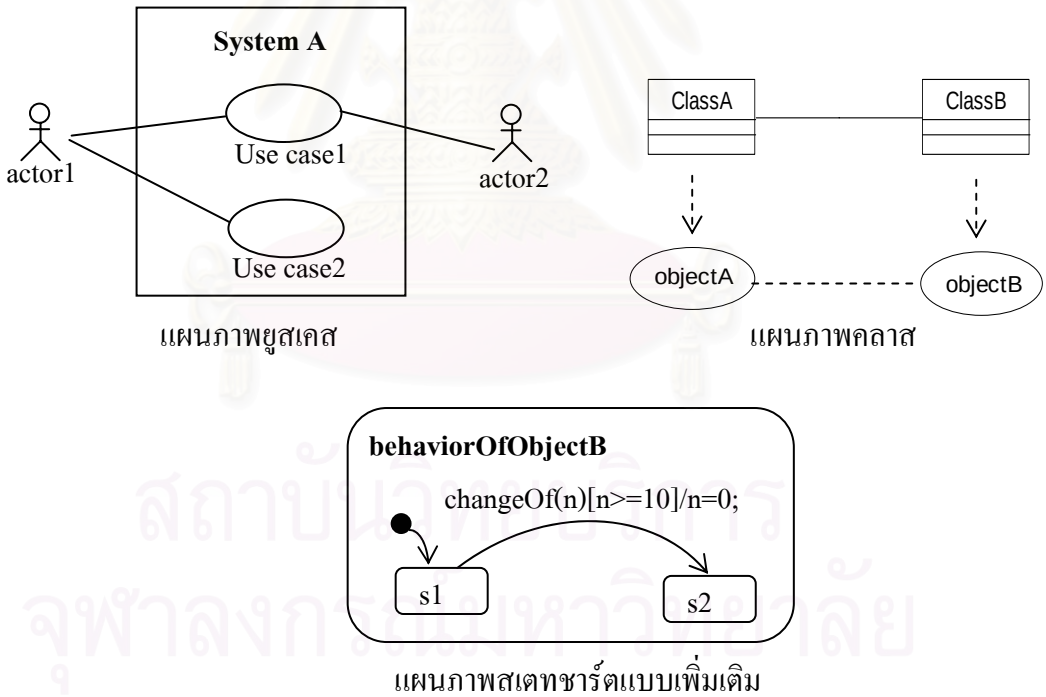
บทที่ 3

นิยามและแอกเซียมของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

บทนี้จะอธิบายนิยามของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน และแอกเซียมของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน ซึ่งทั้งนิยามและแอกเซียมนี้จะนำไปใช้ประโยชน์ในการทวนสอบความถูกต้องของแบบจำลองการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงานซึ่งจะกล่าวในบทที่ 4

3.1 นิยามแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

แผนภาพที่ใช้แสดงแบบจำลองการวิเคราะห์เชิงวัตถุ ได้แก่ แผนภาพยูสเคส แผนภาพคลาส แผนภาพสเตทชาร์ตแบบเพิ่มเติม ซึ่งแสดงดังตัวอย่างในรูปที่ 3.1



แผนภาพยูสเคส แผนภาพคลาส

แผนภาพสเตทชาร์ตแบบเพิ่มเติม

รูปที่ 3.1 แบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

จากรูปที่ 3.1 แสดงแผนภาพการวิเคราะห์ของระบบ System A จากแผนภาพยูสเคส จะมีแอคเตอร์คือ actor1 และ actor2 และยูสเคส 2 ยูสเคสคือ Use case 1 และ Use case 2 แผนภาพคลาสจะแสดงคลาสทั้งหมดภายในระบบ จากตัวอย่างคลาสจะประกอบด้วย ClassA และ ClassB ซึ่งทั้ง

สองคลาสนี้จะมีตัวอย่างเป็นวัตถุซึ่งแสดงในแผนภาพแสดงวัตถุ (Object Diagram) ประกอบด้วยวัตถุ objectA และ objectB การกำหนดพฤติกรรมของวัตถุแสดงในแผนภาพสเตทชาร์ต สำหรับวัตถุ objectB จะมีพฤติกรรมซึ่งแสดงด้วย behaviorOfObjectB วัตถุ objectB จะมีสถานะ 2 สถานะ คือสถานะ s1 และ s2 การเปลี่ยนแปลงสถานะจาก s1 ไปเป็น s2 จะเกิดขึ้นเมื่อวัตถุ objectB รับเหตุการณ์ changeOf(n) และเงื่อนไข n>=10 เป็นจริง เมื่อเกิดการเปลี่ยนแปลงสถานะการกระทำ n=0 จะทำงานด้วย

สำหรับการวิเคราะห์เชิงวัตถุ ระบบที่จะสร้างจะถูกจำลองออกมาในรูปของพฤติกรรมของวัตถุ ซึ่งวัตถุนั้นจะเป็นตัวอย่างของคลาส และพฤติกรรมของวัตถุจะถูกกำหนดด้วยแผนภาพสเตทชาร์ตแบบเพิ่มเติม เราสามารถเขียนนิยามของแบบจำลองการวิเคราะห์เชิงวัตถุ ได้ดังนี้

$$(C, O, SCD, <, M_b)$$

โดยที่ C คือเซตของคลาส

O คือเซตของวัตถุ

SCD คือเซตแผนภาพสเตทชาร์ตแบบเพิ่มเติม

$< \subseteq O \times C$

M_b คือ $C \rightarrow SCD$

$<$ หมายถึงความสัมพันธ์ระหว่างวัตถุและคลาส ซึ่งจะหมายถึงวัตถุเป็นตัวอย่าง (Instance) ของคลาสนั่นเอง ส่วน M_b เป็นฟังก์ชันซึ่งมีโดเมนเป็นเซตของคลาส และเรนจ์เป็นเซตของแผนภาพสเตทชาร์ตแบบเพิ่มเติม ซึ่งหมายความว่าพฤติกรรมของวัตถุซึ่งเป็นตัวอย่างของคลาสจะมีพฤติกรรมตามที่ระบุในแผนภาพสเตทชาร์ตแบบเพิ่มเติม (SCD) ดังนิยามได้ต่อไปนี้

$$SCD = (s_0, S, E, A, B, T, V_{av})$$

โดยที่ s_0 คือสถานะเริ่มต้น ($s_0 \in S$)

S คือเซตของของสถานะ

E คือเซตของเหตุการณ์

A คือเซตของกิจกรรม

B คือเซตของเงื่อนไข

T คือเซตของการเปลี่ยนแปลงสถานะ

V_{av} คือเซตของตัวแปรพร้อมทำงาน

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สำหรับวัตถุพร้อมทำงานจะทำงานด้วยตัวของวัตถุนั้นๆ เอง และการสื่อสารกันระหว่างวัตถุจะเป็นผลมาจากการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน ซึ่งแสดงด้วย V_{av} นอกจากนี้การทำงานก็ขึ้นอยู่กับเหตุการณ์ประเภทต่าง ๆ ที่เกิดขึ้น เหตุการณ์เหล่านั้นคือ เหตุการณ์ประเภทการเรียกใช้ เหตุการณ์ประเภทการเปลี่ยนแปลง (ได้แก่เหตุการณ์ changeOf(av_1,av_2,..av_n)) เหตุการณ์เกิดขึ้นตามเวลา (ได้แก่ Fcall(d,f) FAssign(d,var,val) เป็นต้น) และเหตุการณ์ประเภทสัญญาณ โดยแสดงเหตุการณ์ประเภทต่างๆ ด้วยเซต E

วัตถุพร้อมทำงาน สามารถเริ่มทำงานได้เอง เหตุการณ์ที่อธิบายการทำงานได้ด้วยตัวเองของวัตถุพร้อมทำงานคือ เหตุการณ์ประเภทการเปลี่ยนแปลง จะมีไวยากรณ์คือ changeOf(av_1,av_2,..av_n) [7] ทุกการเปลี่ยนแปลงของทุกวัตถุซึ่งนิยามด้วยเหตุการณ์นี้ เมื่อใดก็ตามที่ค่าของ av ใดๆ เปลี่ยนแปลงค่าจากเดิม เหตุการณ์ changeOf จะทำงานทันที ถ้าเงื่อนไขที่กำหนดในเหตุการณ์ถูกตรวจสอบแล้วว่าเป็นจริง สถานะของวัตถุนั้นๆ ก็จะเปลี่ยนแปลง จากตัวอย่างในรูปที่ 3.1 ตัวแปรพร้อมทำงานคือ n ดังนั้นถ้าค่าของตัวแปร n เปลี่ยน จะเกิดเหตุการณ์ changeOf ทันที และถ้าค่า n มากกว่าหรือเท่ากับ 10 แล้วสถานะของวัตถุ objectB จะเปลี่ยนจากสถานะ s1 เป็นสถานะ s2 และกำหนดค่า n เท่ากับ 0

ดังนั้นการเปลี่ยนแปลงสถานะของวัตถุจะประกอบด้วยสถานะก่อนการเปลี่ยนแปลง สถานะหลังการเปลี่ยนแปลง เหตุการณ์ที่เกิด เงื่อนไข และกิจกรรม จากตัวอย่างข้างต้นส่วนประกอบของการเปลี่ยนแปลงสถานะคือ “s1” “s2” “changeOf” “n>=10” และ “n=0” ตามลำดับ

เซตของการเปลี่ยนแปลงสถานะ T ที่ปรากฏในแผนภาพสเตทชาร์ตจะนิยามได้ดังนี้

$$T \subseteq (S_c \times E \times P(V_{av}) \times B \times A \times S_t)$$

โดยที่ S_c และ S_t คือสถานะก่อนการเปลี่ยนแปลง และสถานะหลังการเปลี่ยนแปลงตามลำดับ

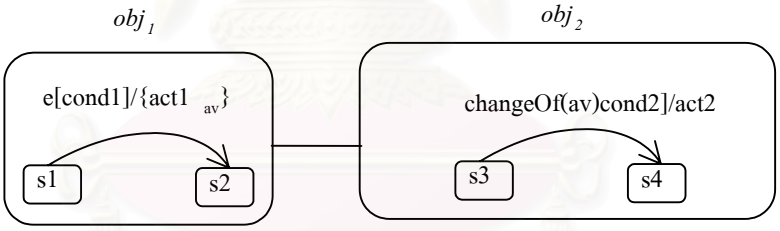
$P(V_{av})$ คือเซตกำลังของตัวแปรชนิดตัวแปรพร้อมทำงาน V_{av}

ฟังก์ชันของกิจกรรม A สามารถนิยามได้คือ $(S_c \times E \times B \rightarrow A)$ ซึ่งหมายความว่า ถ้า $S_c \times E \times B$ เป็นจริงแล้วจะเกิดกิจกรรม A ขึ้น จากตัวอย่างในรูปที่ 3.1 สามารถเขียนในรูปของนิพจน์ได้คือ s1, “changeOf”, “n>=10”, true $\rightarrow$ “n=0” และฟังก์ชันของการเปลี่ยนแปลงสถานะสามารถนิยามได้คือ $(S_c \times E \times B \rightarrow S_t)$ หมายความว่า ถ้า $S_c \times E \times B$ เป็นจริงแล้วจะเกิดการ

เปลี่ยนแปลงสถานะเป็น S_t จากตัวอย่างในรูปที่ 3.1 สามารถเขียนในรูปของนิพจน์ได้คือ s1, “changeOf”, “n>=10”, true $\rightarrow$ s2 เซตของตัวแปรพร้อมทำงานในเซตของการเปลี่ยนแปลงสถานะถูกกำหนดด้วยเซตกำลังของตัวแปรพร้อมทำงาน เนื่องจากบางการเปลี่ยนแปลงสถานะไม่เกี่ยวข้องกับตัวแปรพร้อมทำงาน

3.2 แอกเซียมของแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

สำหรับระบบวัตถุพร้อมทำงาน วัตถุสามารถที่จะทำงานได้ โดยไม่ต้องรอรับเหตุการณ์จากวัตถุอื่นๆ การทำงานได้ลักษณะนี้จะเป็นผลมาจากการเปลี่ยนแปลงของค่าตัวแปรพร้อมทำงาน ดังนั้น เมื่อค่าของตัวแปรพร้อมทำงานในวัตถุใดๆ เปลี่ยนแปลงและเงื่อนไขของการเปลี่ยนแปลงนั้นเป็นจริง จะเกิดการเปลี่ยนแปลงสถานะได้ทันที จากรูปที่ 3.2 แสดงให้เห็นถึงเมื่อสถานะ s1 ของวัตถุ obj_1 เปลี่ยนแปลงสถานะเป็น s2 และเกิดการกระทำ $act1_{av}$ ซึ่งหมายถึงกิจกรรมที่เปลี่ยนแปลงค่าของตัวแปรพร้อมทำงาน av สำหรับวัตถุ obj_2 เมื่อค่าของตัวแปรพร้อมทำงาน av เปลี่ยนแปลง จะเกิดเหตุการณ์ changeOf(av) ถ้าเงื่อนไข cond2 เป็นจริงจะเกิดการเปลี่ยนแปลงสถานะจาก s3 เป็น s4 ได้ และเกิดการกระทำ act2 การเปลี่ยนแปลงลักษณะอย่างนี้ วัตถุสองวัตถุมีการติดต่อกัน และวัตถุหนึ่งสามารถที่จะเข้าถึง (access) ข้อมูลของอีกวัตถุหนึ่งได้



รูปที่ 3.2 การเปลี่ยนแปลงสถานะของวัตถุโดยเหตุการณ์ changeOf

3.2.1 แอกเซียมของการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน

แอกเซียมของการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน (Active Variable Axiom : ACTV-AX) ของ 2 วัตถุ สามารถนิยามได้ดังนี้

แอกเซียมที่ 5 (ACTV-AX)

$$\vdash \forall obj_1\, obj_2.\ obj_1 \prec\!\succ obj_2$$
$$\Rightarrow ((obj_1 \downarrow_s e) \wedge \text{TransCond}$$
$$\Rightarrow (obj_2 \downarrow_{s'} \text{changeOf}(av_1, av_2, \ldots)))$$

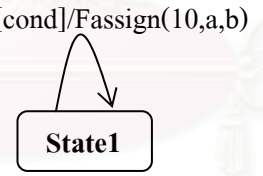
โดยที่ changeOf() หมายถึงเหตุการณ์ประเภทการเปลี่ยนแปลง

$av_1, av_2, \ldots$ คือตัวแปรพร้อมทำงาน

ความหมายของแอกเซียมนี้คือ ถ้าวัตถุ obj_1 ที่สถานะ s ได้รับเหตุการณ์ e และเงื่อนไข TransCond เป็นจริง จะทำให้เกิดกิจกรรมที่มีผลต่อการเปลี่ยนแปลงค่า $av_1, av_2, \ldots$ ตัวใดตัวหนึ่ง แล้ววัตถุ obj_2 จะได้รับเหตุการณ์ changeOf ทันที จากตัวอย่างในรูปที่ 3.2 ถ้าวัตถุ obj_1 ได้รับเหตุการณ์ e และเงื่อนไข cond1 เป็นจริง จะเกิดการกระทำ $act1_{av}$ แล้ววัตถุ obj_2 ที่สถานะ s_3 จะได้รับเหตุการณ์ changeOf

3.2.2 แอกเซียมสำหรับกิจกรรมในอนาคต

กิจกรรมในอนาคตประกอบด้วย 2 กิจกรรมคือ การเรียกใช้ล่วงหน้า และการกำหนดค่าล่วงหน้า ซึ่งรายละเอียดได้กล่าวในหัวข้อ 2.2.4.3 ในบทที่ 2 จากลักษณะของกิจกรรมในอนาคต จะถือว่า ระยะเวลาที่กำหนดให้ในแต่ละกิจกรรม เป็นตัวแปรพร้อมทำงาน เนื่องจากเมื่อกิจกรรมในอนาคตถูกสั่งให้ทำงาน เหตุการณ์ในกิจกรรมเหล่านั้นจะไม่ถูกประมวลผลทันที แต่จะรอให้ถึงเวลาที่กำหนดก่อน เหตุการณ์ที่กำหนดในกิจกรรมจึงจะถูกประมวลผล จากรูปที่ 3.3 เมื่อวัตถุอยู่ในสถานะ State1 ได้รับเหตุการณ์ e และเงื่อนไข cond ถูกตรวจสอบว่าเป็นจริง แล้วกิจกรรม Fassign(10, a, b) ถูกสั่งให้ทำงาน แต่เหตุการณ์การกำหนดค่าล่วงหน้า หมายถึงเหตุการณ์การกำหนดค่า a ให้มีค่าเท่ากับ b จะเกิดขึ้นเมื่อเวลาผ่านไปแล้ว 10 หน่วยเวลา



รูปที่ 3.3 การกำหนดค่าล่วงหน้า

การนิยามแอกเซียมสำหรับกิจกรรมในอนาคต (Future Action Axiom : FACT-AX) ทำได้ดังนี้

แอกเซียมที่ 6 (FACT-AX)

$$\vdash \forall obj\ .\ obj < \text{Class}$$
$$\Rightarrow (((obj \downarrow_s e) \wedge \text{TransCond} \wedge \text{d})$$
$$\Rightarrow (obj \uparrow_s e_f))$$

โดยที่ d คือการผ่านระยะเวลาที่กำหนดแล้ว

e_f คือเหตุการณ์ที่กำหนดในกิจกรรมในอนาคต

ความหมายของแอกเซียมนี้คือ สำหรับทุกวัตถุ *obj* ซึ่งเป็นตัวอย่างของคลาส *Class* ถ้าวัตถุ *obj* ที่สถานะ s รับเหตุการณ์ *e* และเงื่อนไข TransCond ถูกตรวจสอบว่าเป็นจริง และเมื่อระยะเวลาผ่านไป d หน่วยเวลาแล้ว วัตถุ *obj* ที่สถานะ s จะเกิดเหตุการณ์ e_f

ข้อกำหนดของ e_f ซึ่งเป็นเหตุการณ์ที่ถูกกำหนดในกิจกรรมในอนาคต ดังนี้ e_f สำหรับการเรียกใช้ล่วงหน้า [FCall(d,f)] จะแทนด้วย f และ e_f สำหรับการกำหนดค่าล่วงหน้า [FAssign(d,var,val)] จะแทนด้วย (var,val)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 4

ตัวอย่างการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน

ในบทนี้จะแสดงการทวนสอบแผนภาพการวิเคราะห์สำหรับโปรแกรมระบบวัตถุพร้อมทำงานด้วยวิธีการพิสูจน์ทฤษฎี ซึ่งจะต้องนำระบบแอกเซียมเมติคที่กล่าวมาแล้วในบทที่ 3 มาใช้แสดงด้วยตัวอย่างของโปรแกรม 3โปรแกรมดังนี้

1. ระบบเครื่องปรับอากาศ
2. ระบบสัญญาณไฟจราจร
3. ระบบการปรับระดับความดังเสียงโทรทัศน์

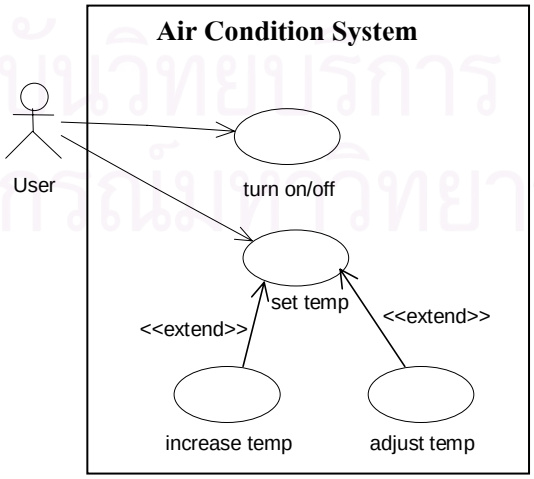
4.1 ระบบเครื่องปรับอากาศ

4.1.1 ลักษณะการทำงานของระบบเครื่องปรับอากาศ

ระบบเครื่องปรับอากาศที่นำเสนอเป็นระบบเครื่องปรับอากาศที่มีการทำงานอย่างง่ายๆ จะประกอบไปด้วยตัวควบคุม (Controller) เครื่องวัดอุณหภูมิ (Thermostat) และตัวเครื่องปรับอากาศ (Body) หลักการทำงานของระบบคือ ผู้ใช้สามารถที่จะเปิดและปิดเครื่องปรับอากาศได้ และผู้ใช้สามารถปรับอุณหภูมิของเครื่องปรับอากาศได้ตามที่ต้องการ

4.1.2 แผนภาพยูสเคสของระบบเครื่องปรับอากาศ

การทำงานของระบบเครื่องปรับอากาศ สามารถแสดงได้ตามรูปที่ 4.1

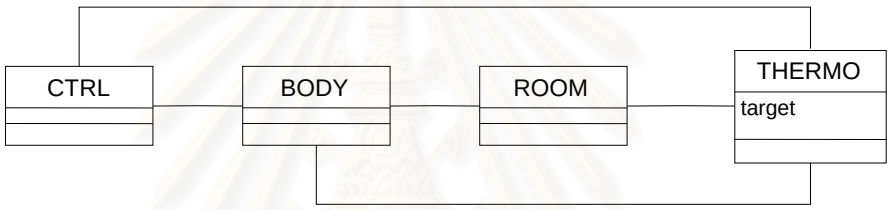


รูปที่ 4.1 แผนภาพยูสเคสของระบบเครื่องปรับอากาศ

จากรูปที่ 4.1 ระบบเครื่องปรับอากาศจะประกอบด้วยแอคเตอร์ *User* ซึ่งหมายถึงผู้ใช้เครื่องปรับอากาศ โดยที่ผู้ใช้ สามารถที่จะทำงานยูสเคส *turn on/off* และ *set temp* ซึ่งคือการเปิดปิดเครื่อง และการตั้งอุณหภูมิที่ต้องการได้ นอกจากนี้ระบบเครื่องปรับอากาศยังสามารถที่จะปรับอุณหภูมิให้ได้เท่ากับอุณหภูมิที่ผู้ใช้ตั้งไว้ โดยยูสเคส *adjust temp* และยูสเคส *increase temp* หมายถึงการทำให้อุณหภูมิภายในเพิ่มขึ้นได้ ซึ่งทั้งสองยูสเคสนี้จะมีความสัมพันธ์แบบ extend กับยูสเคส *set temp* ซึ่งหมายถึงทั้งสองยูสเคสใช้พฤติกรรมการเพิ่มอุณหภูมิและการปรับอุณหภูมิที่ถูกกำหนดไว้ในยูสเคส *set temp*

4.1.3 แผนภาพคลาสของระบบเครื่องปรับอากาศ

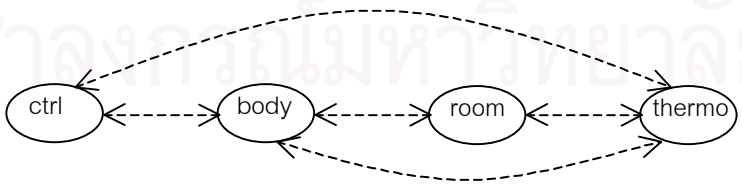
เราสามารถที่จะแสดงคลาสทั้งหมดที่เกี่ยวข้องในระบบเครื่องปรับอากาศได้ ดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพคลาสของระบบเครื่องปรับอากาศ

จากรูปที่ 4.2 จะเห็นว่า ระบบเครื่องปรับอากาศ จะประกอบด้วยคลาสต่างๆ คือ คลาส *CTRL* คลาส *BODY* คลาส *ROOM* และคลาส *THERMO* ความสัมพันธ์ของแต่ละคลาสจะเป็นจะแสดงให้เห็นโดยเส้นตรงที่เชื่อมระหว่างคลาส และคลาส *THERMO* จะประกอบแอตทริบิวต์ *target*

วัตถุเป็นตัวอย่าง (instance) ของคลาส ดังนั้นเราสามารถที่จะเขียนแผนภาพแสดงวัตถุซึ่งเป็นตัวอย่างของคลาสต่างๆ ดังแผนภาพคลาสของระบบเครื่องปรับอากาศได้ดังรูปที่ 4.3



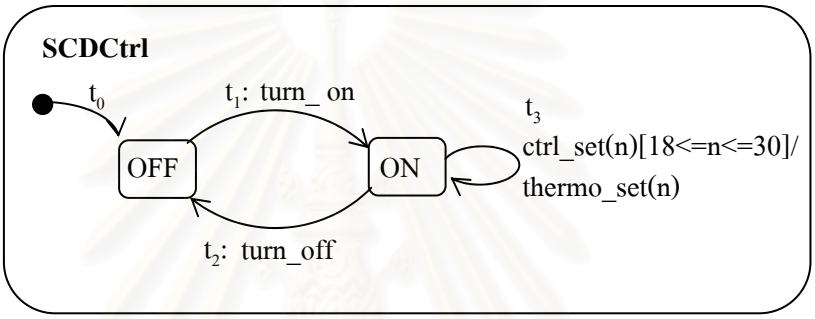
รูปที่ 4.3 แผนภาพแสดงวัตถุของระบบเครื่องปรับอากาศ

จากรูปที่ 4.3 จะเห็นว่าระบบเครื่องปรับอากาศประกอบด้วยวัตถุ *ctrl* วัตถุ *body* วัตถุ *room* และวัตถุ *thermo* ซึ่งเป็นตัวอย่างของคลาส *CTRL* คลาส *BODY* คลาส *ROOM* และคลาส *THERMO* ตามลำดับ

4.1.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของระบบเครื่องปรับอากาศ

แผนภาพสเตทชาร์ตแบบเพิ่มเติมจะเป็นภาพที่แสดงพฤติกรรมของวัตถุต่างๆ ที่เป็นตัวอย่างของคลาสในแผนภาพคลาส พฤติกรรมของวัตถุในคลาสระบบเครื่องปรับอากาศสามารถแสดงได้ ดังรูปที่ 4.4 4.5 4.6 และ 4.7

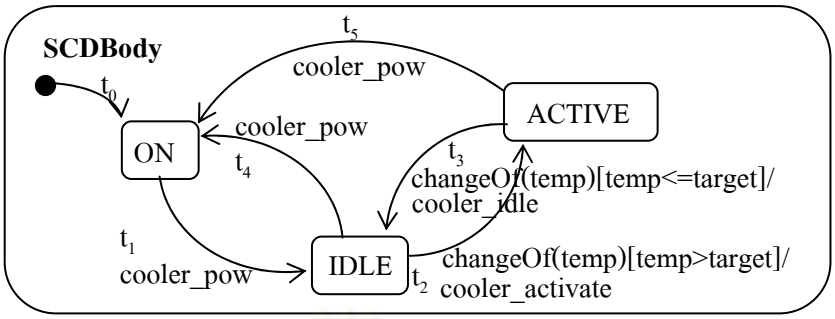
4.1.4.1 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDCtrl



รูปที่ 4.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ ctrl

จากรูปที่ 4.4 แสดงพฤติกรรมของวัตถุ ctrl ซึ่งแสดงโดยใช้แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDCtrl จะเห็นว่าวัตถุ ctrl มีสถานะ 2 สถานะคือ สถานะ *OFF* และสถานะ *ON* ซึ่งเป็นสถานะเมื่อปิดและเปิดเครื่องปรับอากาศ ตามลำดับ การเปลี่ยนแปลงสถานะ t_1 เป็นการเปลี่ยนสถานะ *OFF* เป็น *ON* เกิดขึ้นเมื่อมีเหตุการณ์ *turn_on* และการเปลี่ยนแปลงสถานะ t_2 เป็นการเปลี่ยนสถานะ *ON* เป็น *OFF* เกิดขึ้นเมื่อมีเหตุการณ์ *turn_off* เกิดขึ้น (เหตุการณ์ทั้งสองนี้ เป็นผลจากการเปิดและปิดเครื่องของผู้ใช้) และการเปลี่ยนแปลงสถานะ t_3 เกิดขึ้นเมื่อวัตถุ ctrl อยู่ในสถานะ *ON* ผู้ใช้กำหนดอุณหภูมิที่ต้องการ เหตุการณ์ที่เกิดขึ้นกับสถานะ *ON* คือเหตุการณ์ *ctrl_set(n)* โดยที่ *n* คือค่าอุณหภูมิที่ต้องการตั้ง และเงื่อนไขของเหตุการณ์นี้คือ ค่าที่ตั้งต้องอยู่ระหว่าง 18 ถึง 30 เท่านั้น ถ้าเงื่อนไขนี้เป็นจริง การกระทำ *thermo_set(n)* จะเกิดขึ้น

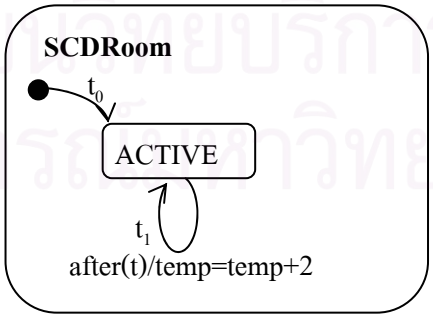
4.1.4.2 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDBody



รูปที่ 4.5 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ body

รูปที่ 4.5 แสดงพฤติกรรมของวัตถุ body ซึ่งประกอบด้วย 3 สถานะ คือสถานะ *ON* สถานะ *IDLE* และสถานะ *ACTIVE* ซึ่งหมายความว่าตัวเครื่องปรับอากาศจะถูกเปิด หยุดนิ่ง และเครื่องทำงาน ตามลำดับ การเปลี่ยนแปลงสถานะ t_1 t_4 และ t_5 ไม่ว่าวัตถุนี้จะอยู่ที่สถานะใดๆ สามารถที่เปลี่ยนเป็นสถานะ *ON* ได้โดยเหตุการณ์ *cooler_pow* ซึ่งหมายถึงการที่เครื่องยังคงเปิดและมีการให้ความเย็นอยู่ และการเปลี่ยนแปลงสถานะ t_2 และ t_3 เป็นการเปลี่ยนแปลงสถานะระหว่างสถานะ *IDLE* และสถานะ *ACTIVE* ซึ่งเปลี่ยนแปลงได้ทันทีเมื่ออุณหภูมิ *temp* ซึ่งหมายถึงอุณหภูมิที่เครื่องตรวจได้เปลี่ยนแปลงค่าและถ้าค่า *temp* มากกว่าค่า *target* (อุณหภูมิที่ผู้ใช้กำหนด) วัตถุ body จะเปลี่ยนแปลงสถานะ t_2 คือเปลี่ยนสถานะจาก *IDLE* เป็น *ACTIVE* ซึ่งหมายถึงการเร่งความเย็นขึ้น แต่ถ้าค่า *temp* น้อยกว่าหรือเท่ากับค่า *target* จะเกิดการเปลี่ยนแปลงสถานะ t_3 คือเปลี่ยนสถานะจาก *ACTIVE* เป็น *IDLE* ซึ่งหมายถึงเครื่องปรับอากาศหยุดนิ่ง ในที่นี้ *temp* คือตัวแปรพร้อมทำงาน

4.1.4.3 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDRoom

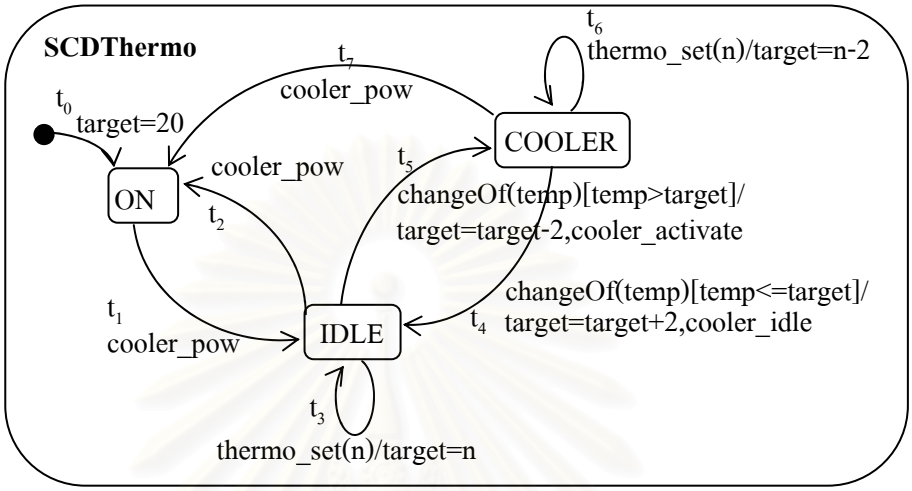


รูปที่ 4.6 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ room

จากรูปที่ 4.6 เป็นแผนภาพสเตทชาร์ทแบบเพิ่มเติมซึ่งแสดงพฤติกรรมของวัตถุ room มีสถานะ *ACTIVE* วัตถุ room สามารถที่จะเพิ่มอุณหภูมิของตัวเองเข้าไปได้โดยการ

เปลี่ยนแปลงสถานะ t_1 ซึ่งเป็นเหตุการณ์ *after(t)* โดยที่ *t* คือระยะเวลาที่กำหนด การเพิ่มอุณหภูมิจะทำได้โดยหลังจากเวลา *t* ให้เพิ่มอุณหภูมิ *temp* เข้าไปอีก 2 องศา

4.1.4.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDThermo



รูปที่ 4.7 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ thermo

จากรูปที่ 4.7 แสดงพฤติกรรมของวัตถุ thermo ซึ่งประกอบด้วย 3 สถานะคือ สถานะ *ON* สถานะ *IDLE* และสถานะ *COOLER* หมายถึงวัตถุ thermo นั้นอยู่ในสภาพที่ถูกเปิดให้ทำงาน หยุดนิ่ง และเร่งความเย็น ตามลำดับ การเปลี่ยนแปลงสถานะ t_0 เป็นการกำหนดค่าเริ่มต้น target = 20 ให้กับสถานะ *ON* การเปลี่ยนแปลงสถานะ t_1 t_2 และ t_7 เป็นการเปลี่ยนแปลงสถานะจากสถานะ *IDLE* และสถานะ *COOLER* มาเป็นสถานะ *ON* โดยเหตุการณ์ *cooler_pow* การเปลี่ยนแปลงสถานะ t_3 เกิดที่สถานะ *IDLE* โดยที่สถานะนี้เมื่อได้รับเหตุการณ์ *thermo_set(n)* ซึ่งเป็นการกระทำที่ถูกส่งออกมาจากวัตถุ ctrl จะกำหนดค่าของ *target* เท่ากับ *n* ซึ่งเป็นพารามิเตอร์ที่มาพร้อมกับเหตุการณ์ *thermo_set(n)* เนื่องจากสถานะนี้เป็นสถานะที่เครื่องปรับอากาศกำลังหยุดนิ่ง การเปลี่ยนแปลงสถานะ t_4 เป็นการเปลี่ยนสถานะจาก *COOLER* เป็น *IDLE* เกิดขึ้นเมื่อค่า *temp* เปลี่ยน และเงื่อนไขคือค่า *temp* น้อยกว่าหรือเท่ากับค่า *target* เป็นจริง จะเกิดการกระทำ *target=target+2* และ *cooloer_idle* การเปลี่ยนแปลงสถานะ t_5 เป็นการเปลี่ยนสถานะจาก *IDLE* เป็น *COOLER* เกิดขึ้นเมื่อค่า *temp* เปลี่ยน และเงื่อนไขคือ *temp* มากกว่าค่า *target* เป็นจริง จะเกิดการกระทำ *target=target-2* และ *cooloer_activate* และการเปลี่ยนแปลงสถานะ t_6 เกิดขึ้นที่สถานะ *COOLER* เกิดขึ้นเมื่อได้รับเหตุการณ์ *thermo_set(n)* และเกิดการกระทำ *target=n-2* เนื่องจากเหตุการณ์เกิดขึ้นขณะที่เครื่องปรับอากาศกำลังเร่งความเย็น

4.1.5 การทวนสอบแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศ

ขั้นตอนที่ 1 กำหนดสมมติฐานการพิสูจน์

จากแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศ เพื่อการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทงาน เราจะตั้งสมมติฐานของการพิสูจน์ดังนี้ *อุณหภูมิเป้าหมายของระบบจะต้องมีค่าไม่เกิน 30 องศาเสมอ* ซึ่งเขียนในรูปนิพจน์ได้คือ

$$\forall s \,.\, \text{thermo.target}(s) \leq 30$$

ขั้นตอนที่ 2 เพิ่มเติมพฤติกรรมของวัตถุในระบบเครื่องปรับอากาศ

ก่อนการพิสูจน์เราจะกำหนดสมมติฐานของแผนภาพดังต่อไปนี้

$$\text{ASSUMS} = \{a_1, a_2, a_3, a_4, a_5, a_6\}$$

$$a_1 = \forall s \,.\, \text{thermo} \downarrow_s \text{changeOf}$$

$$a_2 = \forall s \,.\, \text{ctrl} \downarrow_s \text{changeOf}$$

$$a_3 = \forall s \,.\, \text{body} \downarrow_s \text{changeOf}$$

$$a_4 = \forall s \,.\, \text{room} \downarrow_s \text{changeOf}$$

$$a_5 = \forall s \,.\, \text{ctrl} \downarrow_s \text{turn_on, turn_off}$$

$$a_6 = \forall s \,.\, \text{ctrl} \downarrow_s \text{ctrl_set}$$

สมมติฐาน a_1 จะหมายถึงทุกๆ สถานะของวัตถุ thermo รับเหตุการณ์ changeOf ความหมายของสมมติฐาน a_2 a_3 และ a_4 จะเป็นเช่นเดียวกับสมมติฐาน a_1 ของวัตถุ thermo แต่จะเกิดขึ้นกับวัตถุ ctrl body และ room ตามลำดับ a_5 และ a_6 หมายถึงวัตถุ ctrl ได้รับเหตุการณ์ turn on turn off และ ctrl_set ในทุกๆ สถานะ

กำหนดให้ s_1 ของวัตถุ thermo แทน สถานะ ON

s_2 ของวัตถุ thermo แทน สถานะ IDLE

s_3 ของวัตถุ thermo แทน สถานะ COOLER

s_1 ของวัตถุ ctrl แทน สถานะ OFF

s_2 ของวัตถุ ctrl แทน สถานะ ON

s_1 ของวัตถุ body แทน สถานะ ON

s_2 ของวัตถุ body แทน สถานะ IDLE

s_3 ของวัตถุ body แทน สถานะ ACTIVE

s_1 ของวัตถุ room แทน สถานะ ACTIVE

ขั้นตอนที่ 3 เขียนระบบแอกเซียมเมติคของระบบเครื่องปรับอากาศ

สามารถนำข้อมูลจากแบบจำลองการวิเคราะห์สำหรับวัตถุพร้อมทำงานของระบบเครื่องปรับอากาศมาเขียนเป็นระบบแอกเซียมเมติค ดังต่อไปนี้

D1(LVALID-DEF)

$$\text{Thermo_VALID thermo } P_{s_1}\ P_{s_2}\ P_{s_3} = \bigwedge_{i=0,1,2,\ldots,7} \nu_{t_i}$$

$$\nu_{t_0} = P_{s_1}(20)$$

$$\nu_{t_1} = P_{s_1}(\text{thermo.target(SCDThermo.s}_1\text{)})$$
$$\Rightarrow P_{s_2}(\text{thermo.target(SCDThermo.s}_1\text{)})$$

$$\nu_{t_2} = P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{)})$$
$$\Rightarrow P_{s_1}(\text{thermo.target(SCDThermo.s}_2\text{)})$$

$$\nu_{t_3} = P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{)})$$
$$\wedge (\text{thermo} \downarrow \text{SCDThermo.s}_2\ \text{thermo_set})$$
$$\Rightarrow P_{s_2}(\text{thermo_set.n})$$

$$\nu_{t_4} = P_{s_3}(\text{thermo.target(SCDThermo.s}_3\text{)})$$
$$\wedge (\text{thermo} \downarrow \text{SCDThermo.s}_3\ \text{changeOf})$$
$$\wedge (\text{thermo.target(SCDThermo.s}_3\text{)} \leq \text{temp})$$
$$\Rightarrow P_{s_2}(\text{thermo.target(SCDThermo.s}_3\text{)} + 2)$$

$$\nu_{t_5} = P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{)})$$
$$\wedge (\text{thermo} \downarrow \text{SCDThermo.s}_2\ \text{changeOf})$$
$$\wedge (\text{thermo.target(SCDThermo.s}_2\text{)} \leq \text{temp})$$
$$\Rightarrow P_{s_3}(\text{thermo.target(SCDThermo.s}_3\text{)} - 2)$$

$$\nu_{t_6} = P_{s_3}(\text{thermo.target(SCDThermo.s}_3\text{)})$$
$$\wedge (\text{thermo} \downarrow \text{SCDThermo.s}_3\ \text{thermo_set})$$
$$\Rightarrow P_{s_3}(\text{thermo_set.n} - 2)$$

$$\nu_{t_7} = P_{s_3}(\text{thermo.target(SCDThermo.s}_3\text{)})$$
$$\Rightarrow P_{s_1}(\text{thermo.target(SCDThermo.s}_3\text{)})$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ความหมายของการนิยามแต่ละการเปลี่ยนแปลงสถานะ มีดังนี้

ν_{t_0} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_0 ค่าของแอตทริบิวต์ target มีค่าเท่ากับ 20 ซึ่งน้อยกว่า 30 ซึ่งกำหนดไว้ในโลคอลแอซเซิร์ทชัน P_{s_1} ดังนั้นสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_0 ถูกต้อง

ν_{t_1} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะที่ t_1 ซึ่งจะเปลี่ยนจากสถานะ s_1 ไปเป็น s_2 เมื่อได้รับเหตุการณ์ cooler_pow ดังนั้นค่าของ target ยังคงเท่ากับ 20 เหมือนเดิม ซึ่งเป็นค่าที่น้อยกว่า 30 ซึ่งกำหนดไว้ในโลคอลแอซเซิร์ทชัน P_{s_2} ฉะนั้น การเปลี่ยนแปลงสถานะ t_1 จึงถูกต้อง

ν_{t_2} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_2 จะเปลี่ยนแปลงสถานะจาก s_2 เป็น s_1 เมื่อได้รับเหตุการณ์ cooler_pow แต่เนื่องจากเหตุการณ์นี้ไม่มีการกระทำที่สามารถเปลี่ยนแปลงค่า target ได้จึงทำให้การเปลี่ยนแปลงสถานะนี้ ถูกต้อง ตามสมมติฐานที่ตั้งไว้

ν_{t_3} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_3 ซึ่งเป็นการเปลี่ยนแปลงของสถานะ s_2 เมื่อได้รับเหตุการณ์ thermo_set พร้อมทั้งค่าแอตทริบิวต์ n เหตุการณ์นี้ถูกส่งมาจากวัตถุ ctrl กำหนดค่า n ไว้ในช่วง 18 ถึง 30 เท่านั้น ดังนั้นการกระทำที่กำหนดค่า target ของสถานะนี้จะมีค่าเป็น 18 ถึง 30 เท่านั้น ซึ่งมีค่าน้อยกว่าหรือเท่ากับ 30 ตามโลคอลแอซเซิร์ทชัน P_{s_2} จึงสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_3 ถูกต้อง

ν_{t_4} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_4 ทุกๆ ครั้งที่ค่าของ temp เปลี่ยนแปลงค่า การเปลี่ยนแปลงสถานะนี้จะเกิดขึ้นเมื่อเงื่อนไขที่กำหนดไว้เป็นจริง ที่สถานะ s_3 ค่าของ target จะมีค่าอยู่ระหว่าง 16 ถึง 28 เท่านั้น เพราะว่าสถานะ s_3 จะได้รับเหตุการณ์ thermo_set จากวัตถุ ctrl แล้วนำค่าแอตทริบิวต์ n ที่รับมานั้นมาลบออก 2 ดังนั้น เมื่อเกิดการเปลี่ยนแปลง t4 ขึ้นค่าของ target จะเพิ่มขึ้น 2 ซึ่งค่าของ tareget จะเป็น 18 ถึง 30 ซึ่งมีค่าน้อยกว่าหรือเท่ากับค่าที่กำหนดไว้ในโลคอลแอซเซิร์ชัน P_{s_2} จึงสามารถสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_4 ถูกต้อง

ν_{t_5} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_5 ซึ่งจะเปลี่ยนแปลงสถานะจาก s_2 เป็น s_3 เมื่อค่าของตัวแปร temp เปลี่ยนแปลงและเงื่อนไขที่กำหนดไว้เป็นจริง ที่สถานะ s_2 ค่าของแอตทริบิวต์ target จะมีค่าอยู่ระหว่าง 18 ถึง 30 ซึ่งเป็นการกำหนดค่าจากเหตุการณ์ thermo_set ซึ่งส่งออกมาจากวัตถุ ctrl เมื่อเกิดการเปลี่ยนแปลงสถานะจะเกิดการกระทำที่เปลี่ยนแปลงค่าของ target โดยการลดค่า target ลง 2 ดังนั้น จึงทำให้ค่า target อยู่ในช่วง 16 ถึง 28 ดังนั้นจะมีค่าน้อยกว่าหรือเท่ากับ 28 ตามที่กำหนดในโลคอลแอซเซิร์ทชัน P_{s_3} จึงสรุปได้ว่า การเปลี่ยนแปลง t_5 ถูกต้อง

ν_{t_6} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_6 ซึ่งเป็นการเปลี่ยนแปลงของสถานะ s_3 เมื่อได้รับเหตุการณ์ thermo_set ซึ่งส่งมาจากวัตถุ ctrl พร้อมกับค่าแอตทริบิวต์ n มีค่าอยู่ระหว่าง 18 ถึง 30 ดังนั้นเมื่อเกิดการเปลี่ยนแปลงนี้ ค่าแอตทริบิวต์ target จะเกิดการเปลี่ยนแปลง

ค่าโดยจะมีค่าเท่ากับค่า n – 2 ดังนั้นค่า target จะมีค่าอยู่ระหว่าง 16 ถึง 28 เท่านั้น ซึ่งมีค่าน้อยกว่าหรือเท่ากับ 28 ซึ่งกำหนดไว้ในโลคอลแอซเซิร์ทชัน P_{s_3} จึงสรุปได้ว่า การเปลี่ยนแปลง t_6 ถูกต้อง

v_{t_7} เป็นการตรวจสอบความถูกต้องของการเปลี่ยนแปลงสถานะ t_7 ซึ่งเป็นการเปลี่ยนแปลงจากสถานะ s_3 เป็น s_1 ที่สถานะ s_3 ค่าแอตทริบิวต์ target จะมีค่าอยู่ระหว่าง 16 ถึง 28 เท่านั้น ซึ่งน้อยกว่า 30 ตามที่กำหนดไว้ในโลคอลแอซเซิร์ทชัน P_{s_1} จึงสรุปได้ว่า การเปลี่ยนแปลง t_7 ถูกต้อง

สรุปได้ว่า Thermo_VALID มีค่าเป็นจริง

A1(LINV-AX)

$$\forall obj\ P_{s_1}\ P_{s_2}\ P_s\ .\ obj < \text{THERMO}$$
$$\Rightarrow (\text{Thermo_VALID}\ obj\ P_{s_1}\ P_{s_2}\ P_s$$
$$\Rightarrow (\underset{i=1,2,3}{\wedge} P_{s_i}\ (obj.\text{target}(\text{SCDThermo.s}_i))))$$

ความหมายของแอกเซียม A1 คือ ทุกวัตถุที่เป็นตัวอย่างของคลาส THERMO ถ้าโลคอลแอซเซิร์ทชัน $P_{s_1}\ P_{s_2}\ P_s$ ถูกต้องแล้วจะสรุปได้ว่าเป็นโลคอลอินวาเรียนต์

จากการตรวจสอบความถูกต้องของทุกการเปลี่ยนแปลงสถานะใน D1 แล้วเราสามารถสรุปได้ว่า Thermo_VALID ถูกต้องเนื่องจากทุกๆ การเปลี่ยนแปลงไม่ทำให้ค่า target มากกว่าค่าที่ตั้งไว้ในแต่ละโลคอลแอซเซิร์ทชัน ดังนั้นจะสรุปได้ว่าทุกโลคอลแอซเซิร์ทชันของวัตถุ thermo ถูกต้องด้วย

A2(GINV-AX)

$$\forall obj\ .\ obj < \text{THERMO}$$
$$\Rightarrow ((\underset{i=1,2,3}{\wedge} G(obj.\text{target}(\text{SCDThermo.s}_i)))$$
$$\Rightarrow (\forall \text{s}.\ G(obj.\text{target}(\text{SCDThermo.s}))))$$

ความหมายของแอกเซียม A2 คือ ทุกวัตถุที่เป็นตัวอย่างของคลาส THERMO ถ้าโกลบอลแอซเซิร์ทชันของทุกสถานะถูกต้องแล้ว จะสรุปได้ว่าเป็นโกลบอลอินวาเรียนต์

สำหรับแต่ละโกลบอลแอซเซิร์ทชันจะได้มาจากความถูกต้องของแต่ละโลคอลแอซเซิร์ทชันนั่นเอง

A3(EINT-AX)

$$\forall \text{obj} \,.\, \text{obj} < \text{Ctrl}$$
$$\Rightarrow ((\text{obj} \downarrow \text{SCDCtrl.s}_2 \text{ ctrl_set})$$
$$\Rightarrow (\text{obj} \uparrow \text{SCDCtrl.s}_2 \text{ thermo_set}) \wedge (18 \leq \text{thermo.n} \leq 30)$$

ความหมายของแอกเซียม A3 คือเมื่อวัตถุรับเหตุการณ์ใดๆ ที่สถานะหนึ่ง แล้วจะส่งอีกเหตุการณ์ออกไปจากสถานะนั้น

จากแอกเซียมข้างบน หมายความว่า ทุกๆ วัตถุที่เป็นตัวอย่างของคลาส Ctrl วัตถุรับเหตุการณ์ ctrl_set ที่สถานะ s_2 และส่งเหตุการณ์ thermo_set ออกไปจากสถานะ s_2 พร้อมกับแอตทริบิวต์ n ซึ่งกำหนดค่าให้อยู่ระหว่าง 18 ถึง 30

A4(ECOM-AX)

[1] $\forall obj_1\, obj_2 \,.\, obj_1 \prec\succ obj_2$
$$\Rightarrow ((\forall P.(obj_1 \uparrow \text{SCDCtrl.s}_2 \text{ thermo_set}) \wedge P(\text{thermo_set.n}))$$
$$\Rightarrow (obj_2 \downarrow \text{SCDThermo.s}_2 \text{ thermo_set}) \wedge P(\text{thermo_set.n})$$

[2] $\forall obj_1\, obj_2 \,.\, obj_1 \prec\succ obj_2$
$$\Rightarrow ((\forall P.(obj_1 \uparrow \text{SCDCtrl.s}_2 \text{ thermo_set}) \wedge P(\text{thermo_set.n}))$$
$$\Rightarrow (obj_2 \downarrow \text{SCDThermo.s}_3 \text{ thermo_set}) \wedge P(\text{thermo_set.n})$$

ความหมายของแอกเซียม A4 คือทุก 2 วัตถุใดๆ ที่มีการติดต่อกัน ถ้าวัตถุ obj_1 ส่งเหตุการณ์ออกไปจากสถานะใดๆ พร้อมกับพารามิเตอร์แล้ว วัตถุที่สองจะสามารถรับเหตุการณ์พร้อมกับพารามิเตอร์นั้นที่สถานะใดๆ

จากแอกเซียมข้างบน วัตถุ obj_1 และวัตถุ obj_2 มีการติดต่อกัน ถ้าวัตถุ obj_1 ส่งเหตุการณ์ thermo_set พร้อมกับพารามิเตอร์ n ออกไปจากสถานะ s_2 แล้ววัตถุ obj_2 จะรับเหตุการณ์พร้อมกับพารามิเตอร์ n ที่สถานะ s_2 และ s_3 ดังแสดงในแอกเซียม A4[1] และ A4[2] ตามลำดับ

A5(ACTV-AX)

[1] $\forall obj_1\, obj_2 .\, obj_1 \prec\succ obj_2$
$$\Rightarrow ((\, obj_1 \downarrow \text{SCDRoom.s}_1 \text{ after})$$
$$\Rightarrow (obj_2 \downarrow \text{SCDThermo.s}_2 \text{ changeOf(temp)}))$$

[2] $\forall obj_1\ obj_2.\ obj_1 \prec\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDRoom.s}_1\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDThermo.s}_3\ \text{changeOf(temp)}))$

ความหมายของแอกเซียม A5 คือ ถ้าวัตถุ room รับเหตุการณ์ after แล้ว จะเกิดการกระทำเปลี่ยนแปลงค่าของ temp ซึ่งเป็นตัวแปรพร้อมทำงาน ดังนั้น วัตถุ thermo จะได้รับเหตุการณ์ changeOf โดยทันที ที่สถานะ s_2 และ s_3 ซึ่งแสดงในแอกเซียม A5[1] และ A5[2] ตามลำดับ

ขั้นตอนที่ 4 ทวนสอบแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศ

ขั้นตอนที่ 4.1 กำหนดโลคอลแอซเซิร์ทชัน P_1 P_2 P_3 ให้กับสถานะ ON IDLE และ COOLER ตามลำดับ ดังนี้

$P_1(x) = x \leq 30$
$P_2(x) = x \leq 30$
$P_3(x) = x \leq 28$

โดยที่ x คือแอตทริบิวต์ที่สนใจ ในที่นี้ x คือค่าของตัวแปร target

ขั้นตอนที่ 4.2 การพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ระบบเครื่องปรับอากาศ จะทำได้ตามลำดับต่อไปนี้

P1

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{thermo.target(SCDThermo.s}_1)) = 20$ initial value

[3] $\text{ASSUMS} \vdash P_{s_1}(20)$ D1(ν_{t_0})

[4] $\text{ASSUMS} \vdash \nu_{t_0}$

บรรทัด [1] เป็นข้อเสนอสำหรับการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] กำหนดให้แอตทริบิวต์ target ของวัตถุ thermo มีค่าเป็น 20 ดังนั้น ค่าของ target ของวัตถุ thermo ที่สถานะที่ s_1 จึงมีค่าน้อยกว่า 30 จริง

บรรทัด [3] ถ้าค่าของแอตทริบิวต์ target ของวัตถุ thermo มีค่าเป็น 20 สามารถสรุปได้ $P_{s_1}(20)$ เป็นจริงตามสมมติฐาน ($P_1(x) = x \leq 30$) ซึ่งเป็นความจริงตามนิยามที่ D1(ν_{t_0})

บรรทัด [4] สรุปว่าการเปลี่ยนแปลงสถานะ t_0 ถูกต้องตามสมมติฐาน

P2

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash P_{s_1}(\text{thermo.target(SCDThermo.s}_1\text{))}$ P1

[3] $\text{ASSUMS} \vdash P_{s_1}(\text{thermo.target(SCDThermo.s}_1\text{))} \Rightarrow P_{s_2}(\text{thermo.target(SCDThermo.s}_1\text{))}$ D1(ν_{t_1})

[4] $\text{ASSUMS} \vdash \nu_{t_1}$

บรรทัด [1] แสดงถึงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] นำผลการพิสูจน์จาก P1 ซึ่งสรุปว่าเป็นจริงแล้ว มาใช้

บรรทัด [3] ถ้าเกิดการเปลี่ยนแปลงสถานะจากสถานะ s_1 เป็นสถานะ s_2 ซึ่งไม่มีผลต่อการเปลี่ยนค่าแอตทริบิวต์ target ของวัตถุ thermo จะทำให้ข้อเสนอในบรรทัดนี้ถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1(ν_{t_1})

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_1 ถูกต้องตามสมมติฐาน

P3

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{))}$ P2

[3] $\text{ASSUMS} \vdash P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{))} \Rightarrow P_{s_1}(\text{thermo.target(SCDThermo.s}_2\text{))}$ D1(ν_{t_2})

[4] $\text{ASSUMS} \vdash \nu_{t_2}$

บรรทัด [1] แสดงถึงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] การพิสูจน์ P2 ซึ่งสรุปได้ว่า แอตทริบิวต์ target ของวัตถุ thermo ที่สถานะ s_2 มีค่าไม่เกิน 30 จริง ดังนั้นสามารถเขียน $P_{s_2}(\text{thermo.target(SCDThermo.s}_2\text{))}$

บรรทัด [3] ถ้าเกิดการเปลี่ยนแปลงสถานะจากสถานะ s_2 เป็นสถานะ s_1 ซึ่งไม่มีผลต่อการเปลี่ยนค่าแอตทริบิวต์ target จะทำให้ข้อเสนอในบรรทัดนี้ถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1(ν_{t_2})

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_2 ถูกต้องตามสมมติฐาน

P4

[1] $\text{ASSUMS} \vdash \text{ASSUMS}$

[2] $\text{ASSUMS} \vdash (\text{ctrl} \uparrow \text{SCDCtrl.s}_2\ \text{thermo_set}) \wedge (18 \leq \text{thermo_set.n} \leq 30)$ A3

[3] $\text{ASSUMS} \vdash (\text{thermo} \downarrow \text{SCDThermo.s}_2\ \text{thermo_set}) \wedge (18 \leq \text{thermo_set.n} \leq 30)$ A4

[4] $\text{ASSUMS} \vdash \nu_{t_3}$ [2], [3], D1(ν_{t_3})

บรรทัด [1] เป็นข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ ที่มีการติดต่อระหว่าง 2 วัตถุ คือ วัตถุ ctrl และวัตถุ thermo

บรรทัด [2] ถ้าวัตถุ ctrl ส่งเหตุการณ์ thermo_set พร้อมกับพารามิเตอร์ n ออกมาจากสถานะ s_2 และค่าของ n มีค่าอยู่ระหว่าง 18 ถึง 30 ซึ่งเป็นจริงตามแอกเซียม A3(EINT-AX) โดยการแทนที่ *obj* ด้วยวัตถุ ctrl

บรรทัด [3] วัตถุ thermo จะรับเหตุการณ์ thermo_set ที่ส่งออกมา ที่สถานะ s_2 และค่าพารามิเตอร์ n ที่รับมานั้นมีค่าอยู่ระหว่าง 18 ถึง 30 ซึ่งมีค่าที่ยังคงถูกต้องตามสมมติฐานการพิสูจน์ บรรทัดนี้เป็นจริงตามแอกเซียม A4(ECOM-AX) โดยการแทนที่ obj_1 และ obj_2 ด้วยวัตถุ ctrl และวัตถุ thermo ตามลำดับ

บรรทัด [4] สามารถจะสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_3 ถูกต้อง

P5

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{thermo.target}(\text{SCDThermo.s}_3)) \leq 28 \Rightarrow ((\text{thermo.target}(\text{SCDThermo.s}_3)) + 2) \leq 30$ Arithmetic fact

[3] $\text{ASSUMS} \vdash P_{s_3}\ (\text{thermo.target}(\text{SCDThermo.s}_3)) \Rightarrow P_{s_2}\ ((\text{thermo.target}(\text{SCDThermo.s}_3)) + 2)$ D1(ν_{t_4})

[4] $\text{ASSUMS} \vdash \nu_{t_4}$ [2], [3]

บรรทัด [1] เป็นข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้ากำหนดค่าแอตทริบิวต์ target ของวัตถุ thermo ในสถานะ s_3 มีค่าน้อยกว่าหรือเท่ากับ 28 แล้วเพิ่มเข้าอีก 2 จะมีค่าน้อยกว่าหรือเท่ากับ 30 เป็นจริงตามหลักการทางคณิตศาสตร์

บรรทัด [3] จากความจริงในบรรทัด [2] ถ้ากำหนดการพิจารณาค่าแอตทริบิวต์ target ของวัตถุ thermo เข้าไป จะเห็นว่าค่าของแอตทริบิวต์นี้ยังคงถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1(ν_{t_4})

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_4 ถูกต้อง

P6

[1] ASSUMS $\vdash$ T

---

[2] ASSUMS $\vdash$ (thermo.target(SCDThermo.s_2)) $\leq$ 30 $\Rightarrow$ ((thermo.target(SCDThermo.s_2)) - 2) $\leq$ 28 — Arithmetic fact

---

[3] ASSUMS $\vdash P_{s_2}$ (thermo.target(SCDThermo.s_2)) $\Rightarrow P_{s_3}$ ((thermo.target(SCDThermo.s_2)) - 2) — D1(ν_{t_5})

---

[4] ASSUMS $\vdash \nu_{t_5}$

บรรทัด [1] เป็นข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้ากำหนดค่าแอตทริบิวต์ target ของวัตถุ thermo ในสถานะ s_2 มีค่าน้อยกว่าหรือเท่ากับ 30 แล้วลดค่าลง 2 จะมีค่าน้อยกว่าหรือเท่ากับ 28 เป็นจริงตามหลักการทางคณิตศาสตร์

บรรทัด [3] จากความจริงในบรรทัด [2] ถ้ากำหนดการพิจารณาค่าแอตทริบิวต์ target ของวัตถุ thermo เข้าไป จะเห็นว่าค่าของแอตทริบิวต์นี้ยังคงถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1(ν_{t_5})

บรรทัด [4] สรุปว่าการเปลี่ยนแปลงสถานะ t_5 ถูกต้อง

P7

[1] ASSUMS $\vdash$ ASSUMS

---

[2] ASSUMS $\vdash$ (ctrl $\uparrow$ SCDCtrl.s_2 thermo_set) $\wedge$ (18 $\leq$ thermo_set.n $\leq$ 30) — A3

---

[3] ASSUMS $\vdash$ (thermo $\downarrow$ SCDThermo.s_3 thermo_set) $\wedge$ (18 $\leq$ thermo_set.n $\leq$ 30) — A4

---

[4] ASSUMS $\vdash \nu_{t_6}$ — [2], [3], D1(ν_{t_6})

บรรทัด [1] เป็นข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ ที่มีการติดต่อระหว่าง 2 วัตถุ คือวัตถุ ctrl และวัตถุ thermo

บรรทัด [2] ถ้าวัตถุ ctrl ส่งเหตุการณ์ thermo_set พร้อมพารามิเตอร์ n ออกมาจากสถานะ s_2 และค่าของ n มีค่าอยู่ระหว่าง 18 ถึง 30 ซึ่งเป็นจริงตามแอกเซียม A3(EINT-AX) โดยการแทนที่ *obj* ด้วยวัตถุ ctrl

บรรทัด [3] วัตถุ thermo จะรับเหตุการณ์ thermo_set ที่ส่งออกมา ที่สถานะ s_2 และค่าพารามิเตอร์ n ที่รับมานั้นมีค่าอยู่ระหว่าง 18 ถึง 30 ซึ่งมีค่าที่ยังคงถูกต้องตามสมมติฐานการพิสูจน์ บรรทัดนี้เป็นจริงตามแอกเซียม A4(ECOM-AX) โดยการแทนที่ obj_1 และ obj_2 ด้วยวัตถุ ctrl และวัตถุ thermo ตามลำดับ

บรรทัด [4] สามารถจะสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_6 ถูกต้อง

P8

[1] $\text{ASSUMS} \vdash \text{T}$

---

[2] $\text{ASSUMS} \vdash P_{s_3}\ (\text{thermo.target(SCDThermo.s}_3\text{))}$ P6

---

[3] $\text{ASSUMS} \vdash P_{s_3}\ (\text{thermo.target(SCDThermo.s}_3\text{))}$ D1(ν_{t_7})

$\Rightarrow P_{s_1}\ (\text{thermo.target(SCDThermo.s}_3\text{))}$

---

[4] $\text{ASSUMS} \vdash \nu_{t_7}$

บรรทัด [1] เป็นข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้าโลคอลแอซเซิร์ทชัน P_{s_3} (thermo.target(SCDThermo.s_3)) เป็นจริงตามการพิสูจน์ที่ P6

บรรทัด [3] ถ้าวัตถุ thermo เกิดการเปลี่ยนแปลงสถานะจากสถานะ s_3 เป็นสถานะ s_1 และเนื่องจากการเปลี่ยนแปลงสถานะนั้นไม่มีผลต่อการเปลี่ยนค่าแอตทริบิวต์ target ของวัตถุ thermo จึงทำให้ค่าของแอตทริบิวต์ target ยังคงถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1(ν_{t_7})

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_7 ถูกต้อง

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

P9

[1] $ASSUMS \vdash T$

---

[2] $ASSUMS \vdash \bigwedge_{i=0,1,...,7} \nu_{t_i}$ P1,P2,…,P8

---

[3] $ASSUMS \vdash (thermo.target(SCDThermo.s_1) \leq 30)$ A2

$(thermo.target(SCDThermo.s_2) \leq 30)$

$(thermo.target(SCDThermo.s_3) \leq 28)$

---

[4] $ASSUMS \vdash (thermo.target(SCDThermo.s_1) \leq 30)$ A2

$\wedge (thermo.target(SCDThermo.s_2) \leq 30)$

$\wedge (thermo.target(SCDThermo.s_3) \leq 30)$

---

[5] $ASSUMS \vdash \forall s.thermo.target(s) \leq 30$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] สรุปทุกๆ การเปลี่ยนแปลงสถานะถูกต้อง เป็นผลมาจากการพิสูจน์ที่ผ่านมาใน P1 ถึง P8

บรรทัด [3] ทุกๆ การเปลี่ยนแปลงสถานะถูกต้องตามบรรทัด [2] จะสรุปได้ว่าแอกเซียมโลคอลอินวาเรียนต์เป็จริง

บรรทัด [4] แสดงแอกเซียมโกลบอลอินวาเรียนต์

บรรทัด [5] สรุปได้ว่าทุกๆ สถานะ แอตทริบิวต์ target ของวัตถุ thermo มีค่าน้อยกว่าหรือเท่ากับ 30 ตามสมมติฐานการพิสูจน์ที่ตั้งไว้

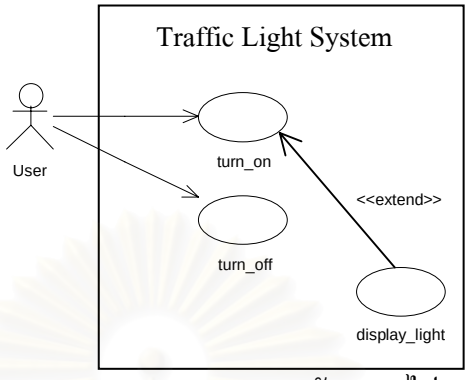
4.2 ระบบสัญญาณไฟจราจร

4.2.1 ลักษณะการทำงานระบบสัญญาณไฟจราจร

ระบบไฟสัญญาจราจร ที่จะยกตัวอย่างต่อไปนี้ เป็นสัญญาณไฟจราจรอย่างง่าย คือ มีไฟจราจรเพียง 1 จุดเท่านั้น การเริ่มทำงานของระบบสัญญาณไฟจราจร คือ ผู้ใช้มีหน้าที่เปิดและปิดการทำงานของสัญญาณไฟจราจร เมื่อเปิดสัญญาณไฟแล้ว ระบบจะทำงานเองอัตโนมัติ โดยเริ่มจากสัญญาไฟแดง แล้วเปลี่ยนเป็นสัญญาณไฟเหลือง และสัญญาณไฟเขียว ตามลำดับ

4.2.2 แผนภาพยูสเคสระบบสัญญาณไฟจราจร

แผนภาพยูสเคส ในรูปที่ 4.8 แสดงการทำงานของระบบสัญญาณไฟจราจร



รูปที่ 4.8 แผนภาพยูสเคสของระบบสัญญาณไฟจราจร

จากรูปที่ 4.8 แสดงแผนภาพยูสเคสของระบบสัญญาณไฟจราจร จะเห็นว่ามีแอคเตอร์คือ *User* สามารถที่จะเปิดและปิดสัญญาณไฟจราจรได้ ซึ่งแสดงด้วยยูสเคส *turno_on* และ *turn_off* ตามลำดับ ยูสเคส *display_light* มีความสัมพันธ์แบบ extend กับยูสเคส *turn_on* โดยการใช้พฤติกรรมการแสดงสีของสัญญาณไฟจราจร

4.2.3 แผนภาพคลาสของระบบสัญญาณไฟจราจร

คลาสในระบบสัญญาณไฟจราจร แสดงในรูปที่ 4.9 ดังนี้

รูปที่ 4.9 แผนภาพคลาสของระบบสัญญาณไฟจราจร

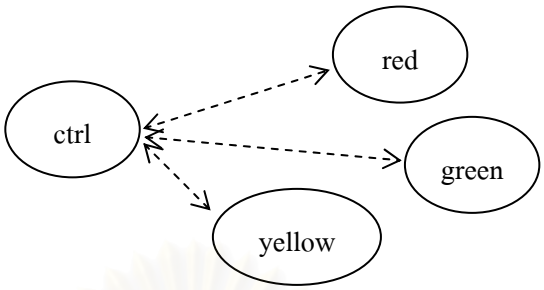
จากแผนภาพคลาส ในรูปที่ 4.9 จะเห็นว่า ระบบสัญญาณไฟจราจร ประกอบด้วยคลาส *CTRL* ซึ่งมีหน้าที่สั่งให้เริ่มต้นและหยุดการทำงานงานของระบบสัญญาณไฟจราจร และคลาส *LIGHT* เป็นคลาสที่มีหน้าที่แสดงสัญญาณไฟ โดยมีแอตทริบิวต์ *switch* ซึ่งเป็นค่าที่บอกให้รู้ว่าไฟจราจรแต่ละสีจะถูกเปิดหรือปิด

กำหนดให้ switch มีค่าและความหมายดังนี้

switch = on แสดงสัญญาณไฟถูกเปิด

switch = off แสดงสัญญาณไฟถูกปิด

จากแผนภาพคลาสในรูปที่ 4.9 จะสามารถแสดงแผนภาพวัตถุ และความสัมพันธ์ของวัตถุ ซึ่งเป็นตัวอย่างของคลาสในแผนภาพคลาส ได้ดังรูปที่ 4.10



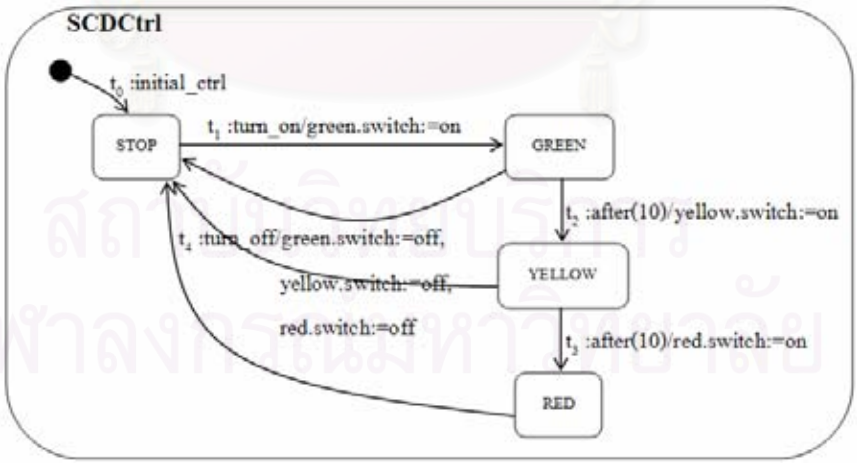
รูปที่ 4.10 แผนภาพแสดงวัตถุของระบบสัญญาณไฟจราจร

จากแผนภาพในรูปที่ 4.10 วัตถุ *ctrl* เป็นตัวอย่างของคลาส CTRL และวัตถุ *red green* และ *yellow* เป็นตัวอย่างของคลาส LIGHT

4.2.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของระบบสัญญาณไฟจราจร

แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDCtrl แสดงพฤติกรรมของวัตถุ ctrl และแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDLight แสดงพฤติกรรมของวัตถุ red green และ yellow แสดงในรูปที่ 4.11 และ 4.12 ตามลำดับ

4.2.4.1 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDCtrl

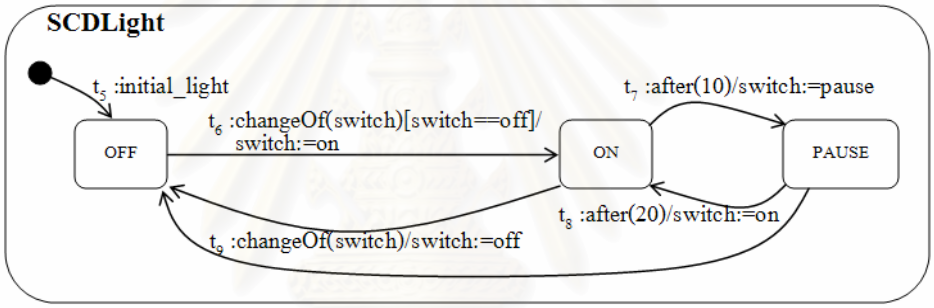


รูปที่ 4.11 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ ctrl

จากรูปที่ 4.11 แสดงแผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ ctrl จะเห็นว่าวัตถุ ctrl จะประกอบด้วยสถานะ 4 สถานะคือ *STOP GREEN YELLOW* และ *RED* หมายความว่าการหยุดการทำงานของสัญญาณไฟจราจรและการเปลี่ยนสีของสัญญาณไฟจราจร ตามการเปลี่ยนแปลง

สถานะดังต่อไปนี้ การเปลี่ยนแปลงสถานะเริ่มต้นของวัตถุคือ t_0 การเปลี่ยนแปลงสถานะ t_1 แสดงการเปลี่ยนแปลงสถานะจาก *STOP* เป็น *GREEN* โดยเมื่อรับเหตุการณ์ *turn_on* แล้วจะเกิดการกระทำ *green.switch:=on* ซึ่งหมายถึงกำหนดให้หลอดสัญญาณไฟจราจรสีเขียวถูกเปิด การเปลี่ยนแปลงสถานะ t_2 เป็นการเปลี่ยนแปลงสถานะจาก *GREEN* เป็น *YELLOW* โดยเมื่อเกิดการเปลี่ยนแปลงสถานะจะเกิดเหตุการณ์ *after()* ซึ่งกำหนดเวลาไว้ 10 หน่วยเวลา เมื่อเวลาล่วงไปแล้วจะเกิดการกระทำ *yellow.switch:=on* ซึ่งหมายถึงการเปิดไฟสัญญาณสีเหลือง การเปลี่ยนแปลงสถานะ t_3 เป็นการเปลี่ยนสถานะจาก *YELLOW* เป็น *RED* โดยเมื่อเกิดการเปลี่ยนแปลงสถานะจะเกิดเหตุการณ์ *after()* ซึ่งกำหนดเวลาไว้ 10 หน่วยเวลา เมื่อเวลาล่วงไปแล้วจะเกิดการกระทำ *red.switch:=on* ซึ่งหมายถึงการเปิดไฟสัญญาณสีแดง การเปลี่ยนแปลงสถานะ t_4 เกิดเมื่อได้รับเหตุการณ์ *turn_off* แล้วจะเกิดการกระทำต่อไปนี้ *green.switch:=off* *yellow.switch:=off* และ *red.switch:=off* ซึ่งหมายถึงการปิดหลอดไฟสัญญาณทุกสี

4.2.4.2 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDLight



รูปที่ 4.12 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ red green และ yellow

จากรูปที่ 4.12 แสดงแผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ red green และ yellow วัตถุนี้ประกอบด้วยสถานะ 3 สถานะคือ *OFF* *ON* และ *PAUSE* มีการเปลี่ยนแปลงสถานะดังนี้ การเปลี่ยนแปลงสถานะ t_6 เป็นการเปลี่ยนแปลงสถานะจาก *OFF* เป็น *ON* เมื่อมีการเปลี่ยนแปลงค่า switch และค่าของ switch เป็น off ให้เกิดการกระทำคือกำหนดค่า *switch:=on* การเปลี่ยนแปลงสถานะ t_7 เมื่ออยู่ที่สถานะ *ON* เป็นเวลา 10 หน่วยเวลา จะเกิดการกระทำกำหนดค่า *switch:=pause* การเปลี่ยนแปลงสถานะ t_8 เมื่ออยู่ในสถานะ *PAUSE* เท่ากับ 20 หน่วยเวลาแล้ว จะเกิดการกระทำ *switch:=on* การเปลี่ยนแปลงสถานะ t_9 ไม่ว่าจะอยู่ที่สถานะ ON หรือ PAUSE เมื่อมีการเปลี่ยนแปลงค่าของ switch จะเกิดการกระทำ *switch:=off*

4.2.5 การทวนสอบแบบจำลองการวิเคราะห์ระบบสัญญาณไฟจราจร

ขั้นตอนที่ 1 กำหนดสมมติฐานการพิสูจน์

ระบบสัญญาณไฟจราจร ประกอบด้วย 3 สัญญาณสี คือ แดง เหลือง และเขียว ดังนั้น สมมติฐานการพิสูจน์ คือ *การเปิดปิดสัญญาณไฟจราจร จะถูกเปิดครั้งละ 1 สีเท่านั้น* หรือในกรณีที่ตั้งสมมติฐานตามแผนภาพการวิเคราะห์ จะเขียนได้ดังนี้ *การกำหนดค่า switch เป็น on จะต้องกำหนดให้กับวัตถุ red หรือ yellow หรือ green เท่านั้น* เขียนในรูปของนิพจน์ดังนี้

$$\forall s \ \text{red.switch} == \text{on} \vee \text{yellow.switch} == \text{on} \vee \text{green.switch} == \text{on}$$

กำหนดชื่อสถานะของแต่ละวัตถุดังนี้

สถานะ s_1 ของวัตถุ ctrl หมายถึง STOP

สถานะ s_2 ของวัตถุ ctrl หมายถึง GREEN

สถานะ s_3 ของวัตถุ ctrl หมายถึง YELLOW

สถานะ s_4 ของวัตถุ ctrl หมายถึง RED

สถานะ s_1 ของวัตถุ light หมายถึง OFF

สถานะ s_2 ของวัตถุ light หมายถึง ON

สถานะ s_3 ของวัตถุ light หมายถึง PAUSE

ขั้นตอนที่ 2 เพิ่มเติมพฤติกรรมของวัตถุ

เนื่องจากแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDCtrl และSCDLight อธิบายพฤติกรรมได้ครบแล้ว จึงไม่ต้องกำหนดพฤติกรรมเพิ่มเติมให้กับวัตถุทั้งสอง

ขั้นตอนที่ 3 เขียนระบบแอกเซียมเมติคของระบบสัญญาณไฟจราจร

การเขียนระบบแอกเซียมเมติคของระบบสัญญาณไฟจราจรคือ การนำข้อมูลจากแบบจำลองการวิเคราะห์ระบบสัญญาณไฟจราจร มาเขียนลงในระบบแอกเซียมเมติคที่ประกอบด้วยนิยามการเปลี่ยนแปลงสถานะและแอกเซียมต่างๆ ดังนี้

D1(LVALID-DEF)

$$\text{Ctrl_VALID ctrl } P_{s_1} P_{s_2} P_{s_3} P_{s_4} = \bigwedge_{i=0,1,2,3,4} \nu_{t_i}$$

[1] $\nu_{t_0} = P_{s_1}$ (switch=off)

[2] $\nu_{t_1} = P_{s_1}$ (switch(SCDCtrl.s_1)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_1 turn_on)
$\Rightarrow P_{s_2}$ (switch=on)

[3] $\nu_{t_2} = P_{s_2}$ (switch(SCDCtrl.s_2)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_2 aftrer)
$\Rightarrow P_{s_3}$ (switch=on)

[4] $\nu_{t_3} = P_{s_3}$ (switch(SCDCtrl.s_3)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_3 after)
$\Rightarrow P_{s_4}$ (switch=on)

[5] $\nu_{t_4} = (P_{s_2}$ (switch(SCDCtrl.s_2)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_2 turn_off)) $\vee$
$(P_{s_3}$ (switch(SCDCtrl.s_3)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_3 turn_off)) $\vee$
$(P_{s_4}$ (switch(SCDCtrl.s_3)) $\wedge$ (ctrl $\downarrow$SCDCtrl.s_3 turn_off))
$\Rightarrow P_{s_1}$ (switch=off)

คำอธิบายของแต่ละการนิยามการเปลี่ยนแปลงสถานะดังนี้

ν_{t_0} เป็นการเปลี่ยนแปลงสถานะเริ่มต้นของการทำงานในวัตถุ ctrl ค่าของ switch เท่ากับ off

ν_{t_1} เป็นการเปลี่ยนแปลงสถานะของวัตถุ ctrl จากสถานะ s_1 เป็นสถานะ s_2 เมื่อเหตุการณ์ turn_on เกิดขึ้น จะทำให้ค่า switch ของสถานะ s_2 เพิ่มขึ้นเป็น on ซึ่งมีค่าถูกต้องตามสมมติฐานการพิสูจน์

ν_{t_2} เป็นการเปลี่ยนแปลงสถานะจากสถานะ s_2 เป็นสถานะ s_3 ของวัตถุ ctrl เมื่อเหตุการณ์ aftrer เกิดขึ้นแล้ว จะให้ค่า switch ของสถานะ s_3 มีค่าเพิ่มขึ้นเป็น on ซึ่งถูกต้องตามสมมติฐานการพิสูจน์

ν_{t_3} เป็นการเปลี่ยนแปลงสถานะของวัตถุ ctrl จากสถานะ s_3 เป็นสถานะ s_4 เมื่อเหตุการณ์ after เกิดขึ้น ค่าของ switch มีค่าเป็น on ซึ่งถูกต้องตามสมมติฐานการพิสูจน์

A1(LINV-AX)

$\forall obj\ P_{s_1} P_{s_2} P_{s_3} P_{s_4} . obj <$ CTRL
$\Rightarrow$(Ctrl_VALID $obj\ P_{s_1} P_{s_2} P_{s_3} P_{s_4}$
$\Rightarrow$($\underset{i=1,2,3,4}{\wedge} P_{s_i}$ (obj.switch(SCDCtrl.s_i))))

ความหมายของแอกเซียม A1 คือ A1 เป็นแอกเซียมโลคอลอินวาเรียนต์ มีความหมายคือ ถ้าทุกๆ การเปลี่ยนแปลงสถานะของแต่ละสถานะในวัตถุ ถูกตรวจสอบว่าเป็นจริงแล้ว เราสามารถเขียนในรูปนิพจน์ได้คือ

P_{s_1} (*obj*.switch(SCDCtrl.s_1))$\wedge P_{s_2}$ (*obj*.switch(SCDCtrl.s_2))$\wedge P_{s_3}$ (*obj*.switch(SCDCtrl.s_3)) $\wedge P_{s_4}$ (*obj*.switch(SCDCtrl.s_4)) ได้

A2(GINV-AX)

$$\forall obj\ .\ obj < \text{CTRL}$$
$$\Rightarrow ((\underset{i=1,2,3,4}{\wedge} G(obj.\text{switch}(\text{SCDCtrl.s}_i)))$$
$$\Rightarrow (\forall \text{s}.G(obj.\text{switch}(\text{SCDCtrl.s}))))$$

ความหมายของแอกเซียม A2 คือ A2 เป็นแอกเซียมโกลบอลอินวาเรียนต์ หมายความว่า ถ้าทุกๆ สถานะของวัตถุถูกตรวจสอบว่ามีความถูกต้องแล้ว จะสรุปได้ว่า สมมติฐานของการพิสูจน์ที่กำหนดไว้นั้น ถูกต้อง

A5(ACTV-AX)

[1] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_1\ \text{turn_on})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_1\ \text{changeOf(switch)}))$

[2] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_1\ \text{turn_on})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_2\ \text{changeOf(switch)}))$

[3] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_1\ \text{turn_on})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_3\ \text{changeOf(switch)}))$

[4] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_2\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_1\ \text{changeOf(switch)}))$

[5] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_2\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_2\ \text{changeOf(switch)}))$

[6] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_2\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_3\ \text{changeOf(switch)}))$

[7] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_3\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_1\ \text{changeOf(switch)}))$

[8] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_3\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_2\ \text{changeOf(switch)}))$

[9] $\forall obj_1\ obj_2.\ obj_1 \prec\!\succ obj_2$
$\Rightarrow ((\ obj_1 \downarrow \text{SCDCtrl.s}_3\ \text{after})$
$\Rightarrow (obj_2 \downarrow \text{SCDLight.s}_3\ \text{changeOf(switch)}))$

ความหมายของแอกเซียม A5 คือ A5 เป็นแอกเซียมของตัวแปรพร้อมทำงาน มีความหมายคือ ถ้าวัตถุ obj_1 ได้รับเหตุการณ์ใดๆ แล้ว และเงื่อนไขของเหตุการณ์นั้นเป็นจริง จะเกิดการกระทำที่มีผลกระทบต่อการเปลี่ยนแปลงค่าวัตถุพร้อมทำงาน ในที่นี้หมายถึงตัวแปร switch วัตถุ obj_2 ได้รับเหตุการณ์ changeOf ทันทีที่ค่าตัวแปร switch เปลี่ยน สำหรับแอกเซียมข้างต้นเกิดขึ้นกับวัตถุ 2 วัตถุคือ วัตถุ ctrl กับวัตถุ green red และ yellow

ขั้นตอนที่ 4 ทวนสอบแบบจำลองการวิเคราะห์ระบบสัญญาณไฟจราจร

การพิสูจน์ความถูกต้องของแผนภาพการวิเคราะห์ระบบสัญญาณไฟจราจร แสดงได้ตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 4.1 กำหนดโลคอลแอซเซิร์ทชันสำหรับทุกสถานะของวัตถุ ctrl ดังนี้

P_1(x) = switch = off
P_2(x) = switch = on
P_3(x) = switch = on
P_4(x) = switch = on

โดยที่ switch คือแอตทริบิวต์ที่สนใจ

ขั้นตอนที่ 4.2 การพิสูจน์ความถูกต้องของแบบจำลองการวิเคราะห์ระบบสัญญาณไฟจราจร ซึ่งจะต้องตรวจสอบทุกๆ การเปลี่ยนแปลงสถานะที่มีผลกระทบต่อแอตทริบิวต์ที่สนใจ คือ switch โดยที่ P1 ถึง P5 แสดงการพิสูจน์ความถูกต้องของการเปลี่ยนแปลงสถานะ t_0 ถึง t_4 และ P6 แสดงการพิสูจน์สมมติฐานการพิสูจน์

P1

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{switch}(\text{SCDCtrl.s}_1)) = \text{off}$ Initial value

[3] $\text{ASSUMS} \vdash P_{s_1}\ (\text{switch}\ (\text{SCDCtrl.s}_1))$ D1[1]

[4] $\text{ASSUMS} \vdash \nu_{t_0}$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] เป็นการกำหนดค่าเริ่มต้นให้กับ switch มีค่าเท่ากับ off

บรรทัด [3] เมื่อค่าของ switch มีค่าเท่ากับ off ดังนั้นค่านี้จึงถูกต้องตามโลคอลแอซเซิร์ทชัน ที่แสดงใน D1[1]

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_0 ถูกต้อง

P2

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{ctrl} \downarrow \text{SCDCtrl.s}_1\ \text{turn_on})$

[3] $\text{ASSUMS} \vdash P_{s_1}\ (\text{switch}(\text{SCDCtrl.s}_1))$ D1[2]

$\Rightarrow P_{s_2}\ (\text{switch}(\text{SCDCtrl.s}_2)=\text{on})$

[4] $\text{ASSUMS} \vdash \nu_{t_1}$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้าวัตถุ ctrl ได้รับเหตุการณ์ turn_on ตามเหตุการณ์ที่เกิดขึ้นในแผนภาพ SCDCtrl การกระทำที่เกิดขึ้นคือ สั่งให้ green.switch มีค่าเป็น on

บรรทัด [3] จากสถานะ s1 ซึ่งค่า switch เป็น off แล้วเกิดเหตุการณ์ในบรรทัดที่ [2] แล้วผลที่เกิดคือ ไฟจราจรถูกสั่งเปิดขึ้น 1 สี ตามข้อสมมติฐานที่ตั้งไว้

บรรทัด [5] สรุปได้ว่า การเปลี่ยนแปลง t_1 ถูกต้องตามสมมติฐานการพิสูจน์

P3

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{light} \downarrow \text{SCDLight.s}_2\ \text{changeOf})$ A5[5]

[3] $\text{ASSUMS} \vdash P_{s_2}\ (\text{ctrl.switch}(\text{SCDCtrl.s}_2)=\text{off})$ D1[3]

$\Rightarrow P_{s_3}\ (\text{ctrl.switch}(\text{SCDCtrl.s}_3)=\text{on})$

[4] $\text{ASSUMS} \vdash \nu_{t_2}$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้าวัตถุ light ได้รับเหตุการณ์ changeOf ที่สถานะ s_2 ซึ่งตรงกับแอกเซียม A5[5] โดยการแทนที่ obj_1 และ obj_2 ด้วย ctrl และ light ตามลำดับ จะเกิดการกระทำกำหนดค่า switch เป็น off ซึ่งหมายถึง ขณะที่หลอดไฟจราจรสีใดๆ กำลังถูกเปิดอยู่ เมื่อเกิดการกระทำนี้แล้วหลอดไฟหลอดนั้นจะถูกปิด

บรรทัด [3] ในขณะที่หลอดไฟจราจรที่เปิดในสถานะ s_2 ของวัตถุ ctrl ถูกปิด หลอดไฟจราจรในสถานะ s_3 จะถูกเปิดตาม D1[3] ซึ่งถูกต้องตามข้อสมมติฐานที่ตั้งไว้

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลง t_2 ถูกต้องตามสมมติฐานการพิสูจน์

P4

[1] $\text{ASSUMS} \vdash \text{T}$

[2] $\text{ASSUMS} \vdash (\text{light} \downarrow \text{SCDLight.s}_2\ \text{changeOf})$ A5[5]

[3] $\text{ASSUMS} \vdash P_{s_3}\ (\text{ctrl.switch(SCDCtrl.s}_3\text{)=off}) \Rightarrow P_{s_4}\ (\text{ctrl.switch(SCDCtrl.s}_4\text{)=on})$ D1[4]

[4] $\text{ASSUMS} \vdash \nu_{t_3}$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้าวัตถุ light ได้รับเหตุการณ์ changeOf ที่สถานะ s_2 ซึ่งตรงกับแอกเซียม A5[5] โดยการแทนที่ obj_1 และ obj_2 ด้วย ctrl และ light ตามลำดับ จะเกิดการกระทำกำหนดค่า switch เป็น off ซึ่งหมายถึง ขณะที่หลอดไฟจราจรสีใดๆ กำลังถูกเปิดอยู่ เมื่อเกิดการกระทำนี้แล้วหลอดไฟหลอดนั้นจะถูกปิด

บรรทัด [3] ในขณะที่หลอดไฟจราจรที่เปิดในสถานะ s_3 ของวัตถุ ctrl ถูกปิด หลอดไฟจราจรในสถานะ s_4 จะถูกเปิดตาม D1[4] ซึ่งถูกต้องตามข้อสมมติฐานที่ตั้งไว้

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลง t_2 ถูกต้องตามสมมติฐานการพิสูจน์

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

P5

[1] ASSUMS $\vdash$ T

---

[2] ASSUMS $\vdash$ (ctrl $\downarrow$ SCDCtrl.s turn_off)

---

[3] ASSUMS $\vdash$ P_{s_2} (switch(SCDCtrl.s_2)) $\vee$ D1[5]

P_{s_3} (switch(SCDCtrl.s_3)) $\vee$

P_{s_4} (switch(SCDCtrl.s_4))

$\Rightarrow$ P_{s_1} (switch(SCDCtrl.s_1)=off)

---

[4] ASSUMS $\vdash$ ν_{t_4}

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] ถ้าวัตถุ ctrl ได้รับเหตุการณ์ turn_off ที่สถานะ s_2 s_3 และ s_4

บรรทัด [3] การกระทำเกิดขึ้นคือ หลอดไฟจราจรถูกปิด ซึ่งเป็นไปตามสมมติฐานที่ตั้งไว้ข้างต้น

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลง t_2 ถูกต้องตามสมมติฐานการพิสูจน์

P6

[1] ASSUMS $\vdash$ T

---

[2] ASSUMS $\vdash$ $\underset{i=0,1,2,3}{\wedge} \nu_{t_i}$ P1,P2,P3,P4,P5

---

[3] ASSUMS $\vdash$ (ctrl.switch(SCDCtrl.s_1) = off) A1

(ctrl.switch(SCDCtrl.s_2) = on)

(ctrl.switch(SCDCtrl.s_3) = on)

(ctrl.switch(SCDCtrl.s_4) = on)

---

[4] ASSUMS $\vdash$ (ctrl.switch(SCDCtrl.s_1) = off) A2

$\wedge$(ctrl.switch(SCDCtrl.s_2) = on)

$\wedge$(ctrl.switch(SCDCtrl.s_3) = on)

$\wedge$(ctrl.switch(SCDCtrl.s_4) = on)

---

[5] ASSUMS $\vdash$ $\forall$s. ctrl.switch (s)

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] แสดงให้เห็นว่าการการเปลี่ยนแปลงสถานะ t_0, t_1, t_2, t_3 และ t_4 ถูกต้องตามสมมติฐานการพิสูจน์ ซึ่งแสดงใน P1, P2, P3, P4 และ P5

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บรรทัด [3] เนื่องจากทุกๆ การเปลี่ยนแปลงสถานะให้ค่า switch ต่างๆ กัน ดังนั้นจึงเขียนแอกเซียมโลคอลอินวาเรียนต์ ได้ดังบรรทัด [3]

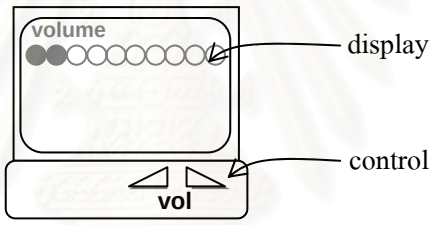
บรรทัด [4] จากบรรทัด [2] และบรรทัด [3] แสดงให้เห็นว่าทุกการเปลี่ยนแปลงสถานะถูกต้อง ดังนั้นจึงเขียนแอกเซียมโกลบอลอินวาเรียนต์ได้ดังบรรทัด [4]

บรรทัด [5] สรุปว่า ทุกๆ สถานะของวัตถุ ctrl มีค่าของ switch หนึ่งค่าเท่านั้น

4.3 ระบบการปรับระดับความดังเสียงโทรทัศน์

4.3.1 ลักษณะของระบบการปรับระดับความดังเสียงโทรทัศน์

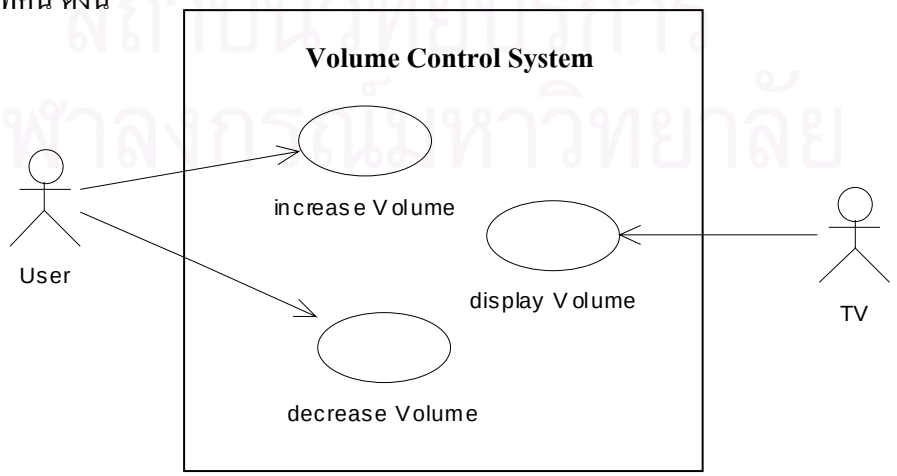
ระบบการปรับระดับความดังเสียงโทรทัศน์ มีลักษณะงานดังนี้คือ ผู้ใช้สามารถที่จะกดปุ่มเพิ่มเสียงหรือปุ่มลดเสียงได้ และเมื่อกดปุ่มดังกล่าวแล้ว ที่หน้าจอโทรทัศน์จะแสดงระดับความดังของเสียงด้วยจุดสีดำ ระดับความดังของเสียงจะกำหนดไว้ทั้งหมด 10 ระดับ ดังนั้นหน้าจอโทรทัศน์จะแสดงจุดทั้งหมดได้แค่ 10 จุดเท่านั้น ดังแสดงตัวอย่างในรูปที่ 4.13



รูปที่ 4.13 ส่วนประกอบของระบบการปรับระดับความดังเสียงโทรทัศน์

4.3.2 แผนภาพยูสเคสของระบบการปรับระดับความดังเสียงโทรทัศน์

แผนภาพยูสเคส ในรูปที่ 4.14 แสดงการทำงานของระบบการปรับระดับความดังเสียงโทรทัศน์ ดังนี้



รูปที่ 4.14 แผนภาพยูสเคสของระบบการปรับระดับความดังเสียงโทรทัศน์

จากรูปที่ 4.14 ระบบการปรับระดับความดังเสียงโทรทัศน์ ประกอบด้วยแอคเตอร์ คือ *User* และ *TV* แอคเตอร์ *User* สามารถกำหนดระดับความดังเสียงของโทรทัศน์ได้โดยการเพิ่มหรือลดเสียง ซึ่งแสดงโดยยูสเคส *increase Volume* และ *decrease Volume* ตามลำดับ ส่วนยูสเคส *display Volume* เป็นการแสดงระดับความดังเสียงบนจอโทรทัศน์

4.3.3 แผนภาพคลาสของระบบการปรับระดับความดังเสียงโทรทัศน์

คลาสทั้งหมดของระบบการปรับระดับความดังเสียงโทรทัศน์ แสดงในรูปที่ 4.15

รูปที่ 4.15 แผนภาพคลาสของระบบการปรับระดับความดังเสียงโทรทัศน์

จากรูปที่ 4.15 จะเห็นว่าระบบการปรับระดับความดังเสียงโทรทัศน์จะประกอบด้วยคลาส *CONTROL* และ *DISPLAY* ซึ่งแต่ละคลาสจะมีแอตทริบิวต์ cVol และ dVol ตามลำดับ จะเห็นว่า คลาสทั้งสองจะติดต่อกันได้ สามารถที่จะแสดงแผนภาพแสดงวัตถุที่เป็นตัวอย่างของคลาสในรูปที่ 4.15 ได้ดังแผนภาพในรูปที่ 4.16

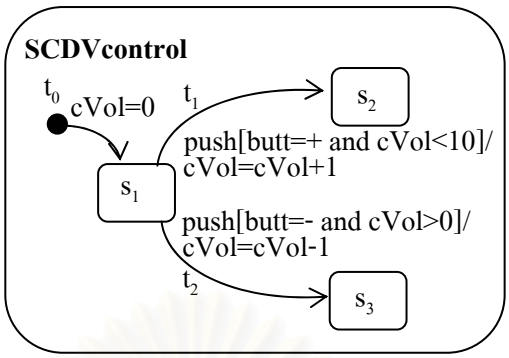
รูปที่ 4.16 แผนภาพแสดงวัตถุของระบบการปรับระดับความดังเสียงโทรทัศน์

จากรูปที่ 4.16 จะเห็นว่าแผนภาพประกอบด้วยวัตถุ *control* และ *display* ซึ่งเป็นตัวอย่างของคลาส CONTROL และคลาส DISPLAY ตามลำดับ

4.3.4 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของระบบการปรับระดับความดังเสียงโทรทัศน์

พฤติกรรมของวัตถุ control และวัตถุ display จะแสดงด้วยแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVcontrol และ SCDVdisplay ดังแสดงในรูปที่ 4.17 และ 4.18 ตามลำดับ

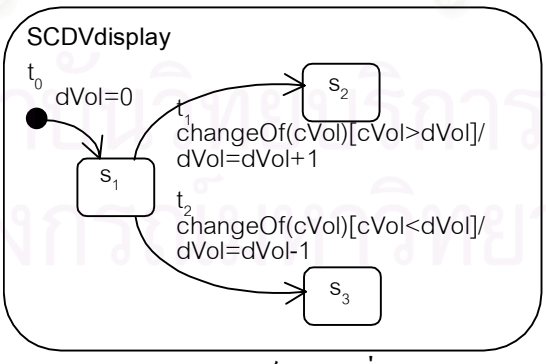
4.3.4.1 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVcontrol



รูปที่ 4.17 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ control

รูปที่ 4.17 แสดงแผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ control การเปลี่ยนแปลงสถานะ t_0 เป็นการกำหนดค่าเริ่มต้นของวัตถุ control ให้ค่าตัวแปร cVol มีค่าเป็น 0 การเปลี่ยนแปลงสถานะ t_1 เป็นการเปลี่ยนแปลงจากสถานะ s_1 เป็น s_2 การเปลี่ยนแปลงนี้เกิดขึ้นเมื่อผู้ใช้กดปุ่มเพิ่มระดับความดังเสียง วัตถุจะได้ที่สถานะ s_1 จะได้รับเหตุการณ์ push และเงื่อนไข butt=+ and vol<10 เป็นจริง จะเกิดการกระทำ cVol=cVol+1 และการเปลี่ยนแปลงสถานะ t_2 เป็นการเปลี่ยนสถานะจาก s_1 เป็น s_3 การเปลี่ยนแปลงนี้จะเกิดขึ้นเมื่อผู้ใช้กดปุ่มลดระดับความดังเสียงลง วัตถุที่สถานะ s_1 จะได้รับเหตุการณ์ push และเงื่อนไข butt=- and vol>0 เป็นจริง จะเกิดการกระทำ cVol=cVol-1

4.3.4.2 แผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVdisplay



รูปที่ 4.18 แผนภาพสเตทชาร์ตแบบเพิ่มเติมของวัตถุ display

รูปที่ 4.18 แสดงแผนภาพสเตทชาร์ตแบบเพิ่มเตมของวัตถุ display การเปลี่ยนแปลงสถานะ t_0 เป็นการกำหนดค่าเริ่มต้น dVol=0 และการเปลี่ยนแปลงสถานะ t_1 และ t_2 เป็นการเปลี่ยนแปลงสถานะจากสถานะ s_1 ไปเป็นสถานะ s_2 และ s_3 เมื่อใดก็ตามที่ค่าของแอตทริ

บิวต์ cVol ของวัตถุ control เปลี่ยนดังนั้นจะเรียก cVol ว่าตัวแปรพร้อมทำงาน การเปลี่ยนแปลงสถานะ t_1 เปลี่ยนจากสถานะ s_1 เป็นสถานะ s_2 เมื่อค่า cVol มีค่ามากกว่า dVol จริง (dVol จะแทนจำนวนจุดสีดำที่แสดงระดับความดังของเสียง ซึ่งแสดงบนหน้าจอโทรทัศน์) จะเกิดการกระทำ dVol=dVol+1 (หมายถึงการเพิ่มจุดสีดำแสดงระดับความดังเสียงขึ้น 1 จุด) และการเปลี่ยนแปลงจากสถานะ t_2 เปลี่ยนจากสถานะ s_1 ไปเป็นสถานะ s_3 เมื่อค่า cVol มีค่าน้อยกว่า dVol และเกิดการกระทำ dVol=dVol-1 (หมายถึงการลดจุดสีดำแสดงระดับเสียงลง 1 จุด)

4.3.5 การทวนสอบแผนภาพการวิเคราะห์ระบบการปรับระดับความดังเสียงโทรทัศน์

ขั้นตอนที่ 1 กำหนดสมมติฐานการพิสูจน์

สมมติฐานของการพิสูจน์คือ *การแสดงระดับความดังของเสียงบนหน้าจอโทรทัศน์จะต้องอยู่ไม่เกิน 10 ระดับ* เขียนเป็นนิพจน์ได้ดังนี้

$$\forall s.\ display.cVol(s) \leq 10$$

หมายความว่า ทุกๆ สถานะของวัตถุ display ค่าของแอตทริบิวต์ cVol จะต้องมีค่าน้อยกว่าหรือเท่ากับ 10

ขั้นตอนที่ 2 เพิ่มเติมพฤติกรรมของวัตถุ

เนื่องจากพฤติกรรมของวัตถุ control และ display ซึ่งแสดงด้วยแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVcontrol และ SCDVdisplay ตามลำดับ มีความสมบูรณ์แล้ว จึงไม่ต้องกำหนดพฤติกรรมเพิ่มเติมให้กับวัตถุทั้งสอง

ขั้นตอนที่ 3 เขียนระบบแอกเซียมเมติคของระบบการปรับระดับความดังเสียงโทรทัศน์

การเขียนระบบแอกเซียมเมติคของระบบการปรับระดับความดังเสียงโทรทัศน์กระทำได้โดยการนำข้อมูลจากแบบจำลองการวิเคราะห์ระบบ มาเขียนลงในระบบแอกเซียมเมติค ซึ่งประกอบด้วยนิยามการเปลี่ยนแปลงสถานะ และแอกเซียมต่างๆ ดังรายละเอียดต่อไปนี้

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

D1(LVALID-DEF)

$$\text{Display_VALID display } P_{s_1}\ P_{s_2}\ P_{s_3} = \underset{i=0,1,2}{\wedge} \nu_{t_i}$$

[1] $\nu_{t_0} = P_{s_1}(0)$

[2] $\nu_{t_1} = P_{s_1}(\text{display.dVol(SCDVdisplay.s}_1\text{))}$
$\wedge$ (display $\downarrow$SCDVdisplay.s_1 changeOf)
$\wedge$ (display.dVol(SCDVdisplay.s_1) < cVol)
$\Rightarrow P_{s_2}$ (display.dVol(SCDVdisplay.s_1) + 1)

[3] $\nu_{t_2} = P_{s_1}(\text{display.dVol(SCDVdisplay.s}_1\text{))}$
$\wedge$ (display $\downarrow$SCDVdisplay.s_1 changeOf)
$\wedge$ (display.dVol(SCDVdisplay.s_1) > cVol)
$\Rightarrow P_{s_3}$ (display.dVol(SCDVdisplay.s_1) - 1)

แต่ละการนิยามการเปลี่ยนแปลงมีความหมายดังนี้

ν_{t_0} เป็นการเปลี่ยนแปลงสถานะเริ่มต้นของแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVdisplay ซึ่งมีการกำหนดค่าให้กับแอตทริบิวต์ dVol ให้มีค่าเท่ากับ 0

ν_{t_1} เป็นการเปลี่ยนแปลงสถานะจาก s_1 เป็นสถานะ s_2 ซึ่งเมื่อค่าของแอต ทริบิวต์ cVol ของวัตถุ control เปลี่ยนค่า วัตถุ display จะได้รับเหตุการณ์ changeOf ที่สถานะ s_1 และค่าของแอตทริบิวต์ dVol น้อยกว่า cVol จริง จะเกิดการกระทำกำหนดค่า dVol ของสถานะ s_2 มีค่าเพิ่มขึ้นเป็น dVol + 1 ซึ่งค่าของ dVol ยังคงถูกต้องตามสมมติฐานการพิสูจน์

ν_{t_2} เป็นการเปลี่ยนแปลงสถานะจาก s_1 เป็นสถานะ s_3 เมื่อค่า cVol ของวัตถุ control เปลี่ยนค่า วัตถุ display จะได้รับเหตุการณ์ changeOf ที่สถานะ s_1 และค่าของ dVol มีค่ามากกว่า cVol จะเกิดการกระทำ dVol – 1 ซึ่งค่าของ dVol ของสถานะ s_3 ยังคงถูกต้องตามสมมติฐานการพิสูจน์

A1(LINV-AX)

$$\forall obj\ P_{s_1}\ P_{s_2}\ P_{s_3}.obj < \text{DISPLAY}$$
$$\Rightarrow (\text{Display_VALID obj } P_{s_1}\ P_{s_2}\ P_{s_3}$$
$$\Rightarrow (\underset{i=1,2,3}{\wedge} P_{s_i}(obj.\text{dVol(SCDVdisplay.s}_i\text{}))))$$

A2(GINV-AX)

$$\forall obj\ .obj < \text{DISPLAY}$$
$$\Rightarrow ((\underset{i=1,2,3}{\wedge} G(obj.\text{dVol}(\text{SCDVdisplay.s}_i)))$$
$$\Rightarrow (\forall \text{s}.G(obj.\text{dVol}(\text{SCDVdisplay.s}))))$$

A5(ACTV-AX)

[1] $\forall obj_1\ obj_2\ .obj_1 \gtrdot obj_2$
$\Rightarrow ((obj_1 \downarrow \text{SCDVcontrol.s}_1\ \text{push}) \wedge (\text{butt}=\text{"+"}) \wedge (\text{cVol}<10)$
$\Rightarrow (obj_2 \downarrow \text{SCDVdisplay.s}_1\ \text{changeOf(cVol)}))$

[2] $\forall obj_1\ obj_2\ .obj_1 \gtrdot obj_2$
$\Rightarrow ((obj_1 \downarrow \text{SCDVcontrol.s}_1\ \text{push}) \wedge (\text{butt}=\text{"-"}) \wedge (\text{cVol}>0)$
$\Rightarrow (obj_2 \downarrow \text{SCDVdisplay.s}_1\ \text{changeOf(cVol)}))$

ความหมายของแอกเซียม A1 A2 และ A5 คือ

A1 เป็นแอกเซียมโลคอลอินวาเรียนต์ ความหมายคือ ถ้าทุกๆ การเปลี่ยนแปลงสถานะของทุกสถานะในวัตถุถูกตรวจสอบความถูกต้องแล้ว หมายถึง โลคอลแอซเซิร์ทชัน $P_{s_1}\ P_{s_2}\ P_{s_3}$ เป็นจริง แล้วเราสามารถเขียนในรูปนิพจน์ $P_{s_1}(obj.\text{dVol}(\text{SCDVdisplay.s}_1)) \wedge P_{s_2}(obj.\text{dVol}(\text{SCDVdisplay.s}_2)) \wedge P_{s_3}(obj.\text{dVol}(\text{SCDVdisplay.s}_3))$ ได้

A2 เป็นแอกเซียมโกบอลอินวาเรียนต์ หมายถึง ถ้าทุกๆ สถานะของวัตถุถูกตรวจสอบแล้วว่าเป็นจริง แล้วจะสามารถสรุปได้ว่าสมมติฐานของการพิสูจน์ที่ตั้งไว้ถูกต้อง

A5 เป็นแอกเซียมของตัวแปรพร้อมทำงาน หมายถึง ถ้าวัตถุ obj_1 ได้รับเหตุการณ์ push และเงื่อนไขของการเปลี่ยนแปลงสถานะถูกตรวจสอบแล้วว่าเป็นจริง จะเกิดการกระทำที่มีผลกระทบต่อการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน แล้ววัตถุ obj_2 จะได้รับเหตุการณ์ changeOf โดยทันที

ขั้นตอนที่ 4 ทวนสอบแบบจำลองการวิเคราะห์ระบบการปรับระดับความดังเสียงโทรทัศน์

การทวนสอบแบบจำลองการวิเคราะห์ระบบการปรับระดับความดังเสียงโทรทัศน์แสดงได้ดังต่อไปนี้

ขั้นตอนที่ 4.1 กำหนดโลคอลแอซเซิร์ทชัน สำหรับแต่ละสถานะของวัตถุ display ดังนี้

$$P_1(x) = x \leq 10$$

$$P_2(x) = x \leq 10$$

$$P_3(x) = x \leq 9$$

โดยที่ x คือแอตทริบิวต์ที่สนใจ ในที่นี้ x คือตัวแปร dVol

ขั้นตอนที่ 4.2 การพิสูจน์ความถูกต้องของแต่ละการเปลี่ยนแปลงสถานะ t_0 t_1 และ t_2 ซึ่งแสดงใน P1 P2 และ P3 ตามลำดับ และการพิสูจน์ความถูกต้องของสมมติฐานการพิสูจน์แสดงด้วย P4 ดังรายละเอียดต่อไปนี้

P1

[1] $\text{ASSUMS} \vdash \text{T}$

---

[2] $\text{ASSUMS} \vdash (\text{display.dVol}(\text{SCDVdisplay.s}_1)) = 0$ Initial value

---

[3] $\text{ASSUMS} \vdash P_{s_1}(\text{display.dVol}(\text{SCDVdisplay.s}_1))$ D1[1]

---

[4] $\text{ASSUMS} \vdash \nu_{t_0}$

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] จากแผนภาพสเตทชาร์ตแบบเพิ่มเติม SCDVdisplay เป็นการกำหนดค่าเริ่มต้นให้กับตัวแปร dVol ของวัตถุ display ที่สถานะ s_1 มีค่าเท่ากับ 0

บรรทัด [3] เนื่องจาก dVol มีค่าเป็น 0 ดังนั้นโลคอลแอซเซิร์ทชันของสถานะ s_1 ถูกต้องตามสมมติฐาน

บรรทัด [4] สรุปได้ว่า การเปลี่ยนแปลง t_0 ถูกต้องตามสมมติฐานการพิสูจน์

P2

[1]	ASSUMS $\vdash$ T	
[2]	ASSUMS $\vdash$ (control $\downarrow$SCDVcontrol.s_1 push) $\wedge$ (control.butt="+") $\wedge$ (control.cVol<10) $\Rightarrow$ (display $\downarrow$SCDVdisplay.s_1 changeOf)	A5[1]
[3]	ASSUMS $\vdash$ display.dVol(SCDVdisplay.s_1) < 10 $\Rightarrow$ (display.dVol(SCDVdisplay.s_1) + 1) $\leq$ 10	Arithmetic fact
[4]	ASSUMS $\vdash$ P_{s_1} (display.dVol(SCDVdisplay.s_1)) $\Rightarrow$ P_{s_2} (display.dVol(SCDVdisplay.s_1) + 1)	D1[2]
[5]	ASSUMS $\vdash$ ν_{t_1}	

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] เป็นความจริงเนื่องจากตรงกับแอกเซียม A5[1] โดยการแทน obj_1 และ obj_2 ด้วย control และ display ตามลำดับ ซึ่งหมายถึงถ้าวัตถุ control ได้รับเหตุการณ์ push และเงื่อนไขที่กำหนดในเหตุการณ์นั้นเป็นจริงแล้ว วัตถุ display จะได้รับเหตุการณ์ changeOf และเกิดการกระทำขึ้นถ้าเงื่อนไขของเหตุการณ์เป็นจริง

บรรทัด [3] เป็นความจริงทางคณิตศาสตร์ ถ้าค่าของ cVol ของวัตถุ display ในสถานะ s_1 น้อยกว่า 10 แล้วเพิ่มค่า cVol เข้าไปอีกหนึ่งจะทำให้ค่า cVol มีค่าน้อยกว่าหรือเท่ากับ 10 ซึ่งตรงกับการกระทำที่เกิดขึ้นจากบรรทัด [2]

บรรทัด [4] พิจารณาค่าของ dVol เมื่อเกิดการเปลี่ยนสถานะจากสถานะ s_1 เป็นสถานะ s_2 ผลสืบเนื่องจากบรรทัด [3] จะเห็นว่าค่าของ dVol ยังคงถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1[2]

บรรทัด [5] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_1 ถูกต้อง

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

P3

[1]	ASSUMS $\vdash$ T	
[2]	ASSUMS $\vdash$ (control $\downarrow$SCDVcontrol.s_1 push) $\wedge$ (control.butt="-") $\wedge$ (control.cVol>0) $\Rightarrow$ (display $\downarrow$SCDVdisplay.s_1 changeOf)	A5[2]
[3]	ASSUMS $\vdash$ display.dVol(SCDVdisplay.s_1) $\leq$ 10 $\Rightarrow$ (display.dVol(SCDVdisplay.s_1) - 1) $\leq$ 9	Arithmetic fact
[4]	ASSUMS $\vdash$ P_{s_1} (display.dVol(SCDVdisplay.s_1)) $\Rightarrow$ P_{s_3} (display.dVol(SCDVdisplay.s_1) - 1)	D1[3]
[5]	ASSUMS $\vdash$ ν_{t_2}	

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] จะเป็นความจริงเนื่องจากตรงกับแอกเซียม A5[2] โดยการแทน obj_1 และ obj_2 ด้วย control และ display ตามลำดับ ซึ่งหมายถึงถ้าวัตถุ control ได้รับเหตุการณ์ push และเงื่อนไขที่กำหนดในเหตุการณ์นั้นเป็นจริงแล้ว วัตถุ display จะได้รับเหตุการณ์ changeOf และเกิดการกระทำขึ้นถ้าเงื่อนไขของเหตุการณ์เป็นจริง

บรรทัด [3] เป็นความจริงทางคณิตศาสตร์ ถ้าค่าของ dVol ของวัตถุ display ในสถานะ s_1 น้อยกว่าหรือเท่ากับ 10 แล้วลดค่า dVol ลงหนึ่งจะทำให้ค่า dVol มีค่าน้อยกว่าหรือเท่ากับ 9

บรรทัด [4] พิจารณาค่าของ dVol เมื่อเกิดการเปลี่ยนสถานะจากสถานะ s_1 เป็นสถานะ s_3 ผลสืบเนื่องจากบรรทัด [3] จะเห็นว่าค่าของ dVol ยังคงถูกต้องตามนิยามการเปลี่ยนแปลงสถานะ D1[3]

บรรทัด [5] สรุปได้ว่า การเปลี่ยนแปลงสถานะ t_2 ถูกต้อง

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

P4

[1]	ASSUMS $\vdash$ T	
[2]	ASSUMS $\vdash \bigwedge_{i=0,1,2} \nu_{t_i}$	P1, P2, P3
[3]	ASSUMS $\vdash$ (display.dVol(SCDVdisplay.s_1) $\leq$ 10) (display.dVol(SCDVdisplay.s_2) $\leq$ 10) (display.dVol(SCDVdisplay.s_3) $\leq$ 9)	A1
[4]	ASSUMS $\vdash$ (display.dVol(SCDVdisplay.s_1) $\leq$ 10) $\wedge$(display.dVol(SCDVdisplay.s_2) $\leq$ 10) $\wedge$(display.dVol(SCDVdisplay.s_3) $\leq$ 9)	A2
[5]	ASSUMS $\vdash \forall$s. display.dVol(s) $\leq$ 10	

บรรทัด [1] แสดงข้อเสนอการพิสูจน์การเปลี่ยนแปลงสถานะ

บรรทัด [2] จาก P1 P2 และ P3 จะสรุปได้ว่า การเปลี่ยนแปลงสถานะ t_0 t_1 และ t_2 ยังคงทำให้ค่าแอตทริบิวต์ cVol ถูกต้องตามสมมติฐานการพิสูจน์

บรรทัด [3] แสดงแอกเซียมโลคอลอินวาเรียนต์ ซึ่งแสดงถึงการเปลี่ยนแปลงสถานะของวัตถุถูกตรวจสอบและสรุปว่าถูกต้องตามสมมติฐาน

บรรทัด [4] แสดงแอกเซียมโกลบอลอินวาเรียนต์ ซึ่งแสดงว่าทุกๆ การเปลี่ยนแปลงสถานะมีความถูกต้อง ดังแสดงในบรรทัด [2]

บรรทัด [5] สรุปได้ว่า ทุกๆ สถานะของวัตถุ display จะมีค่า dVol น้อยกว่าหรือเท่ากับ 10 หรือทุกๆ สถานะของระบบการปรับระดับความดังเสียงโทรทัศน์ จุดสีดำที่แสดงระดับเสียงจะมีไม่เกิน 10 จุด

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยนี้ได้แสดงการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน ใช้วิธีการพิสูจน์ทฤษฎีทางคณิตศาสตร์เป็นแนวทางการทวนสอบ ผู้วิจัยได้นำเสนอระบบวัตถุพร้อมทำงานเชิงรูปนัย ซึ่งถูกนิยามเชิงคณิตศาสตร์ และแอกเซียมสำหรับระบบวัตถุพร้อมทำงาน เพื่อนำมาใช้ในการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน สำหรับแอกเซียมสำหรับระบบวัตถุพร้อมทำงานสร้างมาจากแผนภาพแสดงพฤติกรรมของระบบวัตถุพร้อมทำงาน โดยที่ในงานวิจัยนี้ใช้แผนภาพสเตทชาร์ตแบบเพิ่มเติม ซึ่งแผนภาพนี้สามารถแสดงพฤติกรรมของวัตถุพร้อมทำงานได้เป็นอย่างเหมาะสม

ระบบแอกเซียมเมติคสำหรับแบบจำลองการวิเคราะห์เชิงวัตถุ ประกอบด้วย (1) นิยามการเปลี่ยนแปลงสถานะ (2) แอกเซียมของแต่ละสถานะ (3) แอกเซียมของสถานะทั้งหมด (4) แอกเซียมของการติดต่อกันระหว่างวัตถุ แอกเซียมเมติคสำหรับแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงาน ประกอบด้วย (1) แอกเซียมของการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน และ (2) แอกเซียมสำหรับกิจกรรมในอนาคต

ผู้วิจัยได้ทดลองการทวนสอบแบบจำลองการวิเคราะห์สำหรับระบบวัตถุพร้อมทำงานกับระบบ 3 ตัวอย่าง ได้แก่ (1) ระบบเครื่องปรับอากาศ แสดงถึงพฤติกรรมของวัตถุที่มีการส่งเหตุการณ์ระหว่างวัตถุ (2) ระบบสัญญาณไฟจราจร และระบบการปรับระดับความดังเสียงโทรทัศน์ ทั้งสองระบบนี้จะมีจุดเน้นที่พฤติกรรมการทำงานได้เองของวัตถุพร้อมทำงาน ซึ่งได้ผลสรุปคือทุกตัวอย่างระบบได้ผลการวิเคราะห์ระบบที่ถูกต้อง (ผลการวิเคราะห์ระบบ ในที่นี้หมายถึงแผนภาพแสดงพฤติกรรมของวัตถุ) จากทั้ง 3 ตัวอย่างที่ใช้ทดสอบ มีข้อสังเกตดังนี้ (1) การมีและไม่มีแอกเซียมใดๆ เมื่อถึงขั้นตอนการนำข้อมูลจากแผนภาพแสดงพฤติกรรมมาเขียน จะขึ้นอยู่กับแผนภาพแสดงพฤติกรรม ว่ามีเหตุการณ์ที่เกี่ยวข้องกับแอกเซียมหรือไม่ (2) จำนวนของแอกเซียมที่ถูกเขียนออกมาเมื่อทำการพิสูจน์จะมีจำนวนมากหรือน้อย ขึ้นอยู่กับปริมาณของการเปลี่ยนแปลงสถานะของวัตถุ การรับส่งเหตุการณ์ระหว่างวัตถุ และการเปลี่ยนแปลงค่าตัวแปรพร้อมทำงาน

5.2 ข้อเสนอแนะ

1. ปรับปรุงระบบแอกเซียมเมติคให้ยืดหยุ่นมากขึ้น เพื่อให้ระบบแอกเซียมเมติคนั้นเหมาะสมสำหรับการใช้ได้กับแผนภาพอื่นๆ เช่น แผนภาพกิจกรรม (Activity Diagram) แผนภาพลำดับการทำงาน (Sequence Diagram) ซึ่งเป็นแผนภาพแสดงพฤติกรรมเช่นเดียวกับ แผนภาพการเปลี่ยนแปลงสถานะ แผนภาพสเตทชาร์ต และแผนภาพสเตทชาร์ตแบบเพิ่มเติม

2. การตรวจสอบความถูกต้องอีกชนิดหนึ่งซึ่งมีประสิทธิภาพมากในปัจจุบันคือ วิธีการตรวจสอบแบบจำลอง (Model-Checking) เราสามารถที่จะนำมาประยุกต์ใช้กับระบบแอกเซียมเมติกที่มีอยู่ได้

3. การทำให้เป็นการตรวจสอบแบบอัตโนมัติอาจจะใช้วิธีตรรกะอันดับสูง หรือภาษาตรรกะอื่นๆ

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

รายการอ้างอิง

[1] Toshiaki Aoki and Takuya Katayama, "Unification and consistency verification of Object-oriented analysis models", in the proceeding of APSEC'98 Taipei, Taiwan, pp. 296-303.

[2] Tosiaki Aoki , Masaki Hanada and Takuya Katayama, "How to support verification of Object-oriented analysis models in HOL", in proceeding of Sci/SAS'99 Orlado, pp. 525-532.

[3] Takaaki Tateishi, Toshiaki Aoki and Takuya Katayama, "An axiomatic system for verification the Object-oriented analysis model", in proceeding of Sci/SAS'99 Orlando.

[4] Toshimi Minoura and Sungwoon Choi, "Structural active-object system fundamentals", Technical Report 93-40-04, Dept. of Computer Science, Oregon State University, 1993.

[5] James Rumbaugh, Ivar Jacobson and Grady Booch. "The unified modeling language reference manual", Addison-Wesley, 1999.

[6] James Rumbaugh, Ivar Jacobson and Grady Booch. "The unified modeling language user guide", Addison-Wesley, 1999.

[7] Wuttipong Ruanthong and Pornsiri Muenchaisri. "Extension of UML Statechart Diagrams for A Structural Active-Object System", in the proceedings of The 2001 National Computer Science and Engineering Conference, Thailand, Nov 4-7, 2001.

[8] Bertrand Meyer. "Introduction to the theory of programming language", Prentice Hall, 1990.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ประวัติผู้เขียนวิทยานิพนธ์

นายสุวิช ถิระโคตร เกิดวันที่ 23 ตุลาคม 2517 ที่จังหวัดอุบลราชธานี สำเร็จการศึกษาระดับปริญญาตรีวิทยาศาสตรบัณฑิต (เกียรตินิยมอันดับ 2) สาขาสถิติ จากมหาวิทยาลัยมหาสารคาม เมื่อปีการศึกษา 2540 และเข้ารับราชการตำแหน่งอาจารย์ ระดับ 3 สังกัดคณะวิทยาศาสตร์ มหาวิทยาลัยมหาสารคาม เมื่อปี พ.ศ. 2541 จากนั้นเข้าศึกษาต่อระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2542

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย